

**ENHANCING THE MANAGEMENT OF WIRELESS
CLIENTS ON INFRASTRUCTURE BASED WLAN'S:
CASE OF UNDP SOMALIA**

BY:

ANDREW M'MBAIZA KEGODE

MASTERS OF SCIENCE IN DATA COMMUNICATION

KCA UNIVERSITY

NOVEMBER 2013

**ENHANCING THE MANAGEMENT OF WIRELESS
CLIENTS ON INFRASTRUCTURE BASED WLAN'S:
CASE OF UNDP SOMALIA**

BY:

ANDREW M'MBAIZA KEGODE

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF MASTERS OF SCIENCE IN DATA
COMMUNICATION IN THE FACULTY OF COMPUTING AND INFORMATION
MANAGEMENT AT KCA UNIVERSITY**

DECLARATION

I declare that this Research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this Research project contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: Andrew M'mbaiza Kegode

Reg, No. 11/02814

Sign: _____

Date: _____

I do hereby confirm that I have examined the master's Research project of

Andrew M'mbaiza Kegode

AND have certified that all revisions that the Research project panel and examiners recommended have been adequately addressed.

Sign: _____

Date: _____

Dr. Alice Njuguna

ENHANCING THE MANAGEMENT OF WIRELESS CLIENTS ON INFRASTRUCTURE BASED WLAN'S: CASE OF UNDP SOMALIA

ABSTRACT

Network Managements entail managing faults, configurations, accounting, performance and security. This is done to guarantee reliability, availability and confidentiality key issues in computer and network systems. Most of this features can and have always been realized on the wired LAN because of the capability to configure the features on specific physical ports. Wireless LAN's pose the greatest challenges in enforcing these features because they do not have many physical ports like the wired LAN and most clients connect through the same port on an access point. Users are easily managed in systems where user devices are internal to the system e.g. registered authenticated system users. Network administrator's often have issues in managing guest and other mobile users who only connect once in a long time to the network or managing users who come in with new or different devices day in day out and require connecting to the network. Such foreign devices pose great management issues to network administrators because they cannot be accounted for easily yet they consume much of the networked resources. This study is aimed at establishing a solution to manage such mobile guest wireless devices on the corporate wireless LANS so as to realize a similar secure, reliable and well optimized environment with wireless clients on wireless networks in order to realize a well-managed network.

Key words: Local area networks, Network interfaces, Routing, Wireless LAN

TABLE OF CONTENTS

DECLARATION.....	i
ABSTRACT.....	iv
TABLE OF CONTENTS.....	v
ACKNOWLEDGEMENTS.....	vii
LIST OF FIGURES.....	viii
LIST OF TABLES.....	ix
LIST OF ABBREVIATIONS.....	x
DEFINITION OF TERMS.....	xi
1 INTRODUCTION.....	1
1.1 BACKGROUND.....	2
1.1.1 OFFICE WIRELESS LAN ARCHITECTURE.....	4
1.2 PROBLEM STATEMENT.....	6
1.2.1 AIM.....	8
1.2.2 OBJECTIVES OF THE STUDY.....	8
1.3 JUSTIFICATION OF RESEARCH.....	9
2 RELATED LITERATURE.....	10
2.1 State of the Art:.....	10
2.2 State of practices.....	19
2.3 Technological advances.....	19
2.4 Critic of the literature.....	21
3 METHODOLOGY.....	22
3.1 Existing methodologies.....	22
3.2 Evaluation of the current methodologies.....	23
3.3 Proposed Methodology.....	24
4 FIELD STUDIES AND FINDINGS.....	25
4.1 Data types.....	25
4.2 Conceptual Model.....	28
4.3 Characteristics of the proposed solution.....	30
5 IMPLEMENTATION.....	32
5.1 proposed system Requirements.....	32
5.2 Implementation of the system.....	33
5.2.1 Staff WVLAN Configurations.....	36
5.2.2 Guest WVLAN Configurations.....	37

5.2.3 AIRONET 1140 Series access point configuration	39
5.2.4 Gateway Configurations	40
6 RESULTS, CONCLUSION AND RECOMMENDATION	43
6.1 Discussion of results	43
6.2 CONCLUSION.....	49
6.3 Future Research Work	51
6.4 Recommendations.....	52
7 REFERENCES	53

ACKNOWLEDGEMENTS

I give glory to God almighty for seeing me this far. Special thanks to the project coordinators Prof. Ddembe and Ms. Aminah Zawedde, my project Supervisor Dr. Alice Njuguna, for taking me on as a supervisee, and for their patience and tireless effort in guiding throughout the project. Without them this study would have never come to fruition.

To the teaching fraternity at KCAU, particularly to those that I had the privilege of studying under, your contribution to my pursuit for knowledge cannot be understated, thank you.

To my Organization, UNDP Somalia for the faith and confidence in me to deploy the project in the organization.

To my industrial supervisors; Carey Karani- ICT manager, and Paul Demba, John G. Kamotho - LAN/WAN Admins, for their guidance all through the project deployment.

To my family, thank you for your support and believing that this project will see the light of day.

LIST OF FIGURES

Figure1, system architecture

Figure 2: Tagged and untagged Ethernet Frame

Figure 3: Structure of a VLAN Tag.

Figure 4: Sample shot of the DHCP lease.

Figure 5: Systems DHCP Scopes.

Figure 6: Hits on the IDS system.

Figure 7: Conceptual model.

Figure 8: proposed system traffic flow

Figure 9: characteristics of an enhanced managed system.

Figure 10: Proposed System Architecture.

Figure 11: WVLANS configurations

Figure 12: SSID configurations.

Figure13: Settings for the staff SSID.

Figure 14: Settings of how the staff SSID is to be broadcasted

Figure 15: Guest WLAN configuration.

Figure 16: Guest WLAN DHCP configuration

Figure 17: Gateway interfaces

Figure 18: wireless gateway interface settings.

Figure 19: System interfaces Architecture.

Figure 20: Traffic flow out of the network.

Figure 21: Gateway rules.

Figure 22: Number of access points registered by the Wireless LAN controller.

Figure 22: Wireless standards supported by the wireless LAN network.

Figure 24: showing how the SSID's are broadcasted on the client's machine

Figure 25: client machine Configuration settings.

Figure 26: Guest wireless LAN clients.

Figure 27: DHCP output from the organization's server.

LIST OF TABLES

Table 1: IEEE wireless Standards.

Table 2: Comparison of wireless LAN security protocols

Table 3: key WLAN vendor features

Table 4: Location and IP of AP's to be deployed.

LIST OF ABBREVIATIONS

AP – Access Point
SSID- Service Set Identifier
IP – Internet Protocol Address
DHCP- Dynamic Host Control Protocol
LAN- Local Area Network
WLAN – Wireless Local Area Network
VLAN – Virtual Local Area Network
Wi-Fi- Wireless Fidelity
WEP- Wired Equivalent Protocol
WPA- Wi-Fi Protected Access
IEEE- Institute of Electrical and Electronics Engineers
MAC- Media Access Control
LWAP- Lightweight Access Protocol
WLC- Wireless LAN Controller
CRC- Cyclic Redundancy Check
BYOD- Bring Your Own Device.
ACL- Access Control List
RADIUS- Remote Authentication Dial In User Service
IDS- Intrusion Detection System
DNS- Domain Name Service
ASA- Adaptive Security Appliance
NAT- Network Address Translation
WVLAN- Wireless Virtual Local Area Network
ISP- Internet Service Provider
AES- Advanced Encryption Standard
UNDP- United Nations Development Programme
NIC- Network Interface Card
SVI- Switch Virtual Interface

DEFINITION OF TERMS

Network- a group of two or more computer systems linked together –
<http://www.webopedia.com>

Network Management- The process of controlling a network so as to maximize its efficiency and productivity www.dictionaty.com

Wireless Network – Network based on 802.11 standards.

AP (Access point) – Hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN, <http://www.webopedia.com>

DHCP- Dynamic Host Control Protocol- a protocol that assigns IP settings to users to allow them access the network.

Authenticate: A way of association in which a device connects to an Access point for network connection.

SSID- A sequence of characters that uniquely names a wireless local area network,
<http://whatis.techtarget.com>

1 INTRODUCTION

In recent years, wireless networking has become more available, affordable, and easy to use. Many users are adopting wireless technology in great numbers. Vijay (Vijay Chandramouli, 2009) states that the increased demands for mobility and flexibility in our daily life are demands that have led to the development from wired LANs to wireless LANs. Laptop and other WI-FI enabled device users often find free wireless connections in places like coffee shops and airports and can easily connect to it and access the internet or other allowed network resources.

With evolving research into wireless networks, there have been general improvements in wireless network speeds and speeds of up to 100Mbps are likely to be achieved. The move towards achieving near wired LANs speeds has hastened the adoption of wireless network in many organizations of course keeping in mind the flexibility and mobility of users to work from anywhere and sustain their connectivity.

The current market has many wireless enabled gadgets and many organizations are finding the need to incorporate them in their networks in order to increase user productivity, comfort ability and performance. Many organizations have embraced the wireless technology and many use it to allow mobile units access the wired LAN resources as if they were connected to the LAN directly in an infrastructure mode wireless LAN.

Most organizations adopt wireless LAN as an extension of the wired LAN to allow mobile users same access as wired users. Some other organizations have deployed full wireless network where their devices comprises cluster of wireless devices that bridge each other to form a robust wireless network.

The adoption of wireless LAN as an extension of the wired LAN has great impact not only the wireless resources but also the wired LAN resources. Wireless adoption causes many threats to the entire LAN especially in regards to accountability, performance and security. This calls for additional input in order to manage the entire network.

1.1 BACKGROUND

Wireless LAN adoption and use has generally enhanced flexibility and convenience in our working environments (Rathnakar et.al 2009). The adoption has also introduced much work in relation to securing resources given that we live in the security edge and there is need to protect every gadget that connects through the wireless access point and more so protect the organizations resources from unauthorized access and misuse while ensuring that system performance is not compromised. With the increased use of such devices on the wireless LAN, there is need to manage who and what resources can be accessed by different users. In an organization that highly utilizes the use of Wireless LAN, there is greater need to separate what guest and other unauthorized users have access to on the network and what should be accessed by different classes of staff, mostly classified by departments.

In most organizations, guests on the network only need internet access for email services and if necessary a printer, for printing their work. This calls for a way in which guests should only be allowed access to what they require. Managing guests and staff on the wireless network has posed challenges to many organizations, most organizations end up deploying a flat network that allows all users same level of access. Such a network poses many challenges especially in regards to managing the network resources among the different users.

UNDP Somalia is a UN organization that was established to govern the United Nations Development Program's mandate in Somalia. The organization has been operating and discharging its mandate from Nairobi given the volatile state of the Somali country. The organization realizes a huge turnout of guest, mainly delegates, donors and state officers who always come to follow up on issues in regards to dissemination of UNDP Somalia's Mandate.

UNDP Somalia has well over 400 staff members within the compound and has several staff members spread over the Somalia country who often visits the organization in Nairobi to give updates on progress of events in the Somalia country.

Within the organization several Wireless Access points have been deployed to support mobile and transit users and allow them access the internet and office resources wirelessly. The Wireless network was deployed as an extension of the wired LAN to allow mobile users access internet

and other office resources wirelessly, and feel as if they were connected directly to the wired LAN.

The deployed AP's allow mobile users to access the internet and other shared network resources. The AP's pass all the traffic from wireless devices to the wired section of the LAN where the organization's servers have to manage them. Among the services offered to the wireless network by the LAN servers are DHCP lease to clients, access to the internet, and access to the shared resources e.g. printers, and shared server space and access to the office intranet.

The wireless LAN handles many clients than the wired LAN given the large number of wireless devices by staff and many guests that often visit the organization and request for internet access wirelessly.

1.1.1 OFFICE WIRELESS LAN ARCHITECTURE

The office Wireless network architecture is an extension of the wired LAN. Wireless Access Points are deployed on each block and their naming is associated with which block they reside. Each of the AP's has its own SSID to match its location and the organization has a unique service set identifier (SSID) per Wireless Access point assigned depending on location. All the access points (AP's) authenticate users with the same passphrase. Wireless devices connect to the nearest access point with the strongest signal using the same pass phrase. The connected wireless clients are assigned IP settings from the organization's DHCP (Dynamic Host Configuration Protocol server) server and can therefore access any shared resource once they authenticate.

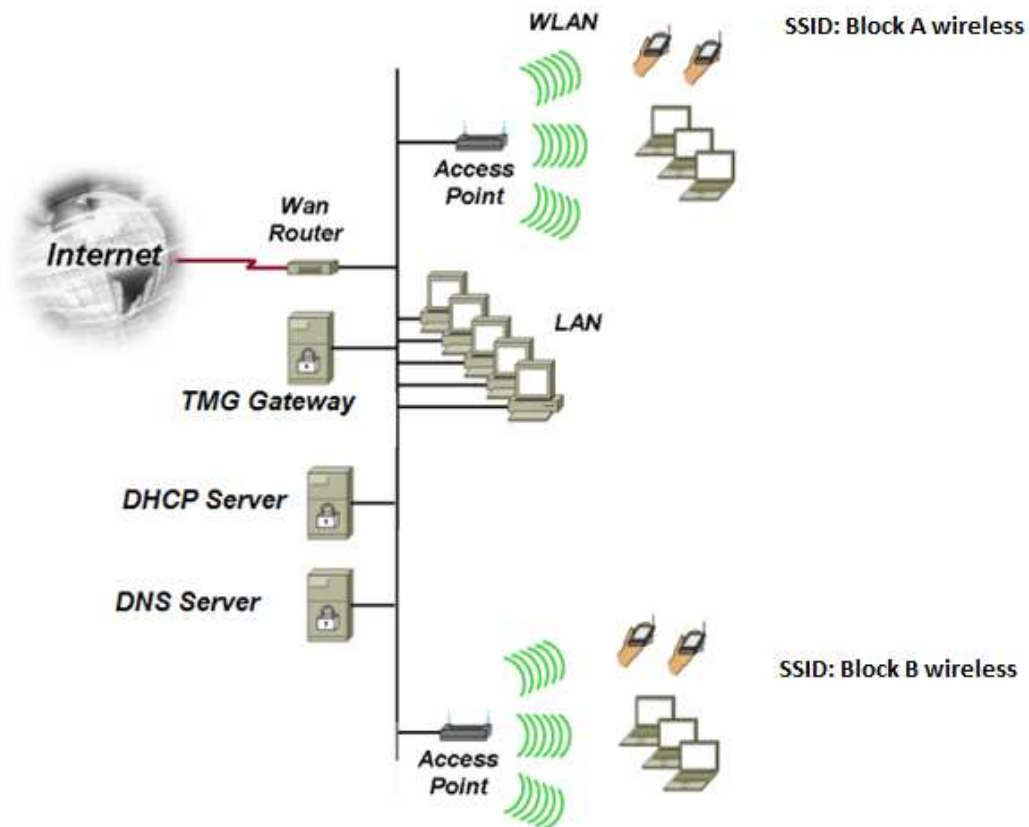


Figure 1: system architecture

The organization runs a domain controller, DHCP server; Print server and File server on the wired network and the servers manage all the users and devices on the network.

1.2 PROBLEM STATEMENT

The wireless Network design was implemented with the aim to support a few of the staff members who were assigned Wi-Fi enabled laptops.

Since then, the organization has grown and seen an increase in number of staff and consequently in number of mobile devices all of which require access to the wireless LAN. Often, the organization hosts visitors and meetings with diplomats and other agency staff. Staff on missions from the field offices too often come to the office and are granted access on the WLAN;, more so, given the policy to allow users bring their own devices that are WIFI enabled such as personal laptops, IPAD'S, Tablets and Mobile phones has in overall led to a large increase in the number of users and devices supported by the wireless Network a situation that was not envisaged in the initial design.

Currently the network is often overwhelmed and the network resources over utilized and misused as a result of increased user devices some of which are official while others non official. There is therefore need to ensure that the network is not overwhelmed with non-mission critical traffic from non-official wireless devices for security reason and to avoid overutilization and misuse of office resources.

If the problem is not well addressed, then it is likely to bring down the entire network thus crippling the organization's operations and hindering its move to achieve its mandate. This study strives to establish a way to provide a wireless network that will address challenges related to the current system.

Based on the architecture in figure 1, the problems that arise in regards to management of the entire network relate to,

- a) Assigning and managing network resources to users (guests and staff)
- b) Allowing guest internet access only while allowing staff access to office resources as if they were directly attached to the wired LAN.
- c) Managing and ensuring that all the access points are always up and running in order to realize office productivity and at the same time allow guest to connect irrespective of their location within the compound.
- d) Allowing users to roam through the network and keep their assigned settings.
- e) Controlling network attacks and viruses directed to the network users from the many guest devices allowed to access the office wireless network.
- f) Securing all devices on the network so that infected devices do not infect other clean or non-protected devices.
- g) Segregating users depending on their devices and allowing them different modes and levels of access to the wireless LAN.

For purposes of this research, problems a, b, c, d and e will be addressed.

1.2.1 AIM

The aim of this study is to assess the current network structure and establish improvements to enhance and hence realize an effective and well optimized wireless network.

1.2.2 OBJECTIVES OF THE STUDY

- To assess the current structure and identify key bottlenecks in the design.
- To identify issues that affect effective implementation of the current wireless LAN Network.
- To propose improvements in the current structure to facilitate effective management of the wireless.
- To design and implement the proposed system.
- To test and validate the proposed system.

1.3 JUSTIFICATION OF RESEARCH

Jonathan Weiss (2002) attributes that Security is a big concern in wireless networking; this is an issue of great concern when it comes to m-commerce and e-commerce applications.

Mobility of users increases the security concerns in a wireless network and especially when you have different classes of users who require different access right or methods.

This study seeks to provide ways to address the security, availability, and performance concern that arise especially when several users have to share the same wireless connection. The issue of concern is how to secure certain resources from access by unauthorized personnel and ensure optimal performance of the system.

The organization has been facing serious issues in regards to managing the connection to the wireless network especially allowing guests to access the internet only and to no other office resources, there was need to have the guest given a separate access method and at the same time have them managed in order to also restrict what they have access to on the office network.

This study aims to address among other issues, Managing the DHCP leases from the DHCP server that currently run into exhaustion, Managing traffic flow on corporate network from different users, enhancing and ensuring constant access to the network by users from all locations within the compound, securing access to and generally preventing misuse of resources by unauthorized personnel.

2 RELATED LITERATURE

2.1 State of the Art:

Wireless LANs are certainly the wave of the future for enterprise networking. Everywhere you look, there is a company deploying a WLAN into their daily operations (Jim Geier, 2003a). Jim believes that if an organization cannot effectively manage its WLAN, benefits quickly diminish and it becomes more of a cost burden than savings.

The wireless networking standards are developed by IEEE; they define a through-the-air interface between a wireless client and an access point or the interface between two or more wireless clients and operate in the unlicensed portion of the *Industrial, Scientific, and Medical* (ISM) frequency spectrum (Masica k 2007). The IEEE standards that govern the use of wireless networks are the 802.11 standards. Since inception, several standards have been developed with the latter being improvements to the predecessors. The IEEE wireless standards are 802.11, 802.11b, 802.11a, and 802.11g, the difference being in the types of data speeds they can support and or the bandwidth in which they operate (Rajul Chokshi and Dr. Chansu, 2001)

The table below shows the standards (Brad Slavin, 2013).

standard	Frequency	Data rates supported
802.11	2.4 GHZ	2Mbits/Second
802.11b	2.4 GHz	11 Mbits/second
802.11a	5 GHZ	54 Mbits/second
802.11g	2.4 GHz	54 Mbits/second
802.11n	2.4/5 GHZ	>100 Mbps

Table 1: IEEE wireless Standards.

The wireless access points authenticate users in order to connect to the wireless network. There are different classes of Access points depending on their capabilities; they include autonomous AP's and light weight Access points. Autonomous AP's can manage themselves while Light weight AP's are centrally managed. Some standalone autonomous AP's can be upgraded to light weight for central management.

The wireless access points authenticate users and encrypt data using different security protocols, they include: WEP- Wired Equivalent Protocol, Wi-Fi Protected Access – WPA, WPA2 each being an enhancement on the later (George C. Ou 2008). Each of the protocol has its unique encryption algorithm with which transmitted data is encrypted.

Each of the protocols has its own characteristics in relation to encryption algorithm, authentication method and data integrity.

The table below shows a summary of the protocols in comparison (Swati S, Shilpi G, 2012).

	WEP	WPA	WPA2
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and keys are generated through four way handshake	Provides robust key management and keys are generated through four way handshake
Hardware Compatibility	Works on existing hardware	Works on existing hardware through	Supported in Wi-Fi devices certified since 2006, Does not

		firmware upgrades on NIC	work with older NIC
Deployment complexity	Easy to setup and configure	Complicated setup required for WPA-enterprise	Complicated setup required for WPA2-enterprise

Table 2: Comparison of wireless LAN security protocols

A wireless LAN can be deployed as an extension of the wired LAN (**Barry Lewis and Peter T. Davis Wiley, 2004**, pg. 33) commonly known as infrastructure based WLAN, or simply a system consisting of wireless clients and wireless access points that bridge each other and hence offer a seamless interconnection of mobile wireless devices known as adhoc WLAN

Wireless clients can obtain their network configurations from a wireless access point configured with the DHCP (Dynamic Host Configuration Protocol) service running as an autonomous AP or can obtain the settings from a network DHCP server configured purposely for that. (**Barry Lewis and Peter T. Davis Wiley, 2004**, pg. 279)

Just like wired LANs, Wireless LAN can be configured so as to support different classes of users and or separate users. This is done in order to optimize performance and enforce security; several methods can be employed to achieve this, some of which include;

a) **Using Separate physical links and systems**, most traffic can be separated by physically separating them, distinct systems are placed on separate switches and or access points, this allows for running two or more separate networks that are physically separated this separation ensures that clients on one network do not communicate directly with other, thus enhancing security, and more so performance as a result of having separate systems run independently thus reducing on traffic congestion, an issue that degrades performance and compromises security.

This method is commonly employed within organizations where special rooms are set aside as hotspots for guest use. Staffs are assigned their own hotspot aside from guest. Much as this method seems to work, the organizations incur much cost in order to support the two connections.

b) Using Enterprise class AP's.

Enterprise class AP's can be used to support many users because they can support multiple SSID's (Service Set Identifier), Each of the SSID's configured on the autonomous AP's can be used to support a particular class of users. The traffic from the users is then routed through the AP trunk to a gateway.

This solution can support several users but since all the traffic flow through the same trunk, the performance of the system is not of much difference as to when only one SSID is used.

c) Using a Wireless LAN Controller (WLC) - a wireless LAN controller is a hardware that can support several lightweight Access point's; a light weight access point is that AP that can pass its control to a central unit for administration. The LAN controller is configured and passes the configuration to the Access point, the access points are then controlled by the LAN controller. WLC controllers eliminate access point congestion problems for mobile users by automatically balancing clients across access points as they connect, (Cisco Systems d).

WLC continually adjust access point loading as users change location and roam though the network. Traditional roles of access points, such as association or authentication of wireless clients, are done by the WLC. Lightweight Access Points (LWAPs) register themselves with a WLC and tunnel all the management and data packets to the WLCs, the configurations are done on the WLC and LWAPs download the entire configuration from WLCs and act as a wireless interface to the clients to enable them access to the network.

According to an evaluation done by Info-Tech (2011) on competitors in the WLAN market, the following were notable performers with the respective attributes.

1. **Aruba**, with leading security, feature-rich, and BYOD-ready solutions from a leading vendor.
2. **Cisco**, a trusted vendor with a strong WLAN solution, a large installed-base, and rapidly evolving wired-wireless unification.
3. **Enterasys**, a compelling wired-wireless unification solution, full featured WLAN, excellent BYOD solution, value-priced.

4. **HP Networking**, with solid WLAN hardware and wired-wireless unification at the lowest cost.
5. **Ruckus**, with outstanding RF features an innovative vendor with innovative solutions and rapidly growing mind-and-market share.

An analysis of some of the desirable key features with some of the leading WLAN vendors in the market can be seen from the table below. (Ziff Davis 2012)

	ARUBA	CISCO	ENTERASYS	HP	RUCKUS
SUPPORT FOR 2.4 AND 5GHZ BAND	YES	YES	YES	YES	YES
LOAD BALANCING	YES	YES	YES	NO.	YES
AUTO POWER AND AUTO CHANNEL	YES	YES	YES	YES	YES
USER IDENTIFICATION by NAME/MAC/IP	YES	YES	YES	YES	YES
PER AP STATISTICS	YES	YES	NO	YES	NO
PER CLIENT STATISTICS	YES	YES	NO	YES	NO
SUPPORT FOR ROAMING	YES	YES	YES	YES	YES
INTERGRATION WITH WIRED NETWORK	NO	YES	YES	YES	-

Table 3: key WLAN vendor features

d) Using a Radius Server- (Remote Authentication Dial In User Service); with a RADIUS server, we can grant individual registered users the allowed access based on authenticated identity instead of the SSID they connect to (Rajul Chokshi and Dr. Chansu Yu.2007), Radius uses a unique username and password to authenticate on the wireless network e.g the Active

directory. The client's username and password are checked against any Active Directory or LDAP server that supports the RADIUS protocol (Meraki white paper, 2009).

User and service authentication and authorization are used to authenticate or deny users certain privileges, users are classified in groups and several rights granted to them, grouping can be done based on Mac addresses and or active directory organizational units. Using a Radius server can allow or deny users access to certain resources.

Since the users' credentials have to be checked against a predefined datasheet, the main drawback to this system is that users have to be registered a scenario that cannot be achieved when you have many guest users.

e) Content-based filtering: upper layer content filters can be used to segregate traffic from various users, this filtering can be done at any of the layers in reference to the OSI –model, traffic is routed in respect to the application in question, http and https traffic is routed to the gateway while ftp traffic is routed to the ftp servers, pop ad IMAP traffic is routed to the mail servers, the main challenge in this system is how to implement it on guest users since they are allowed same access as long as they are using the protocol's in question. This method does not solve our performance issues because traffic from guest and staff travel to the same servers therefore mission critical requests from staff can be starved by those from guest.

f) Using access control lists. ACL's can let you segregate traffic on a network, access control list allow one to either permeate or deny traffic through particular networks, and wireless network can be distinguished using access control list by permeating traffic from certain applications or user to some networks and at the same time deny access to others. ACL's are used to guide traffic through the LAN by defining specific access rights and to which next hop a packet should go, ACL are configured on a router or switch interfaces to either deny or permit traffic.

You configure access lists on a router or switch to filter traffic and provide basic security for any network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router or switch interfaces (Cisco systems c)

Access control List can therefore be applied on traffic from different users in order to have them separated. The access control list is well built by mac addresses from devices. Certain devices are granted access based on their mac addresses while other not. This method cannot effectively address our issue because it's not possible to predetermine the mac address of guest devices to be included in the ACL.

g) Using VLANs. VLANs have successfully been deployed onto the wired LAN, this was achieved by separating users based on switch ports, for wireless clients, it's not possible to apply port based VLANs because users connect via one port to the wireless access point (*Minlan Yu and Jennifer Rexford 2001*).

To create wireless VLANs, enterprise class AP's are deployed. Each SSID can be assigned a particle ID which can be used to implement wireless VLANs, once a user associates with a particular SSID, his/her traffic is tagged with a unique ID that can be mapped to a particular VLAN, such traffic can then be guided through the network using the specific VLAN ID, adopted from the SSID it authenticates with.

VLANs can be deployed in a number of ways, they are;

- Port Based VLAN
- Mac address based VLAN
- Protocol based VLAN
- Policy Based VLAN

Port Based VLAN – different switch ports are placed on the same VLAN and only devices with ports in the same VLAN can communicate to each other directly. Port based VLAN deployment is not possible for wireless clients because, the clients connect through a single port, on the Ap.

Mac address-based VLANs -the MAC address of a workstation is assigned to a VLAN. Each switch or Access point maintains an assignment table of MAC addresses and their corresponding VLAN memberships. The source or destination MAC address determines to which VLAN a packet is passed.

Protocol based VLAN, the delivery of packets depends on protocols, and The VLAN membership of a packet is indicated by a tag that is added to the packet.

Policy Based VLAN- Tagging based on certain policies or user configuration. This May involve classifying network traffic into groups and assigning Quality of service priority bits and VLAN ID to each group E.g. SSID

The figures below show the structure of a normal Ethernet frame and one that has VLAN tag.

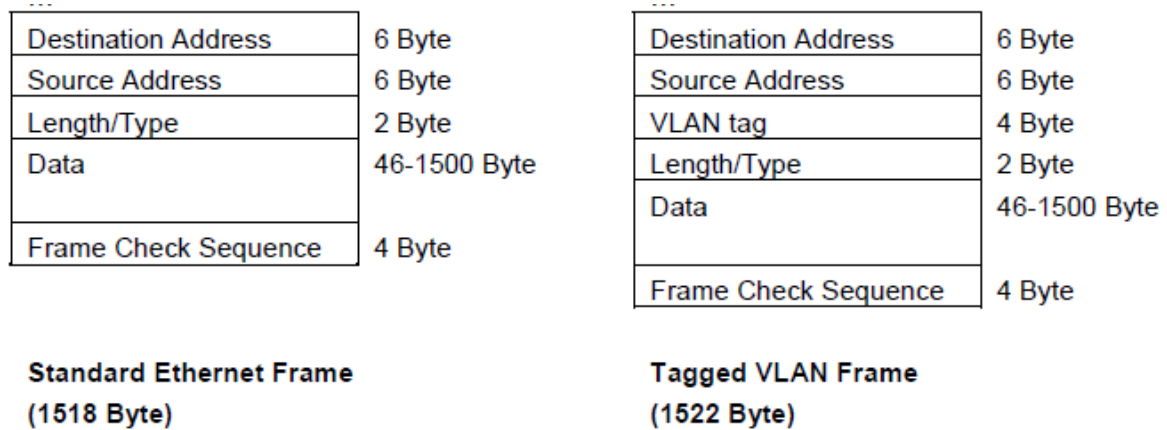


Figure 2: Tagged and untagged Ethernet Frame (SysKonnnect GmbH, 2001):

The VLAN tag provides a basis onto which VLAN traffic can be segregated. The VLAN tag is unique to each VLAN traffic and only packets with same VLAN tag can be routed in the same direction.

A VLAN tag has the following structure (SysKonnnect GmbH, 2001):

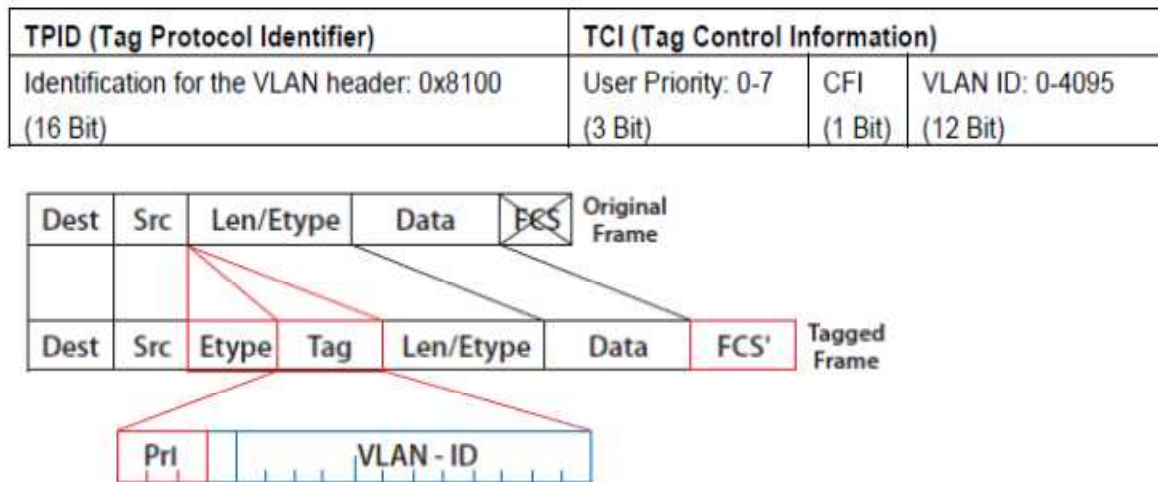


Figure 3: Structure of a VLAN Tag.

VLANs can be identified with any values from 1 to 4094.

The VLAN tag contains information pertaining to priority of the frame and the VLAN ID.

Tagging helps isolate traffic from different VLAN's over a trunk, to implement WVLAN (Wireless Virtual Local Area Network); we require an Access point that supports multiple SSID's. A service set identifier (SSID) is a unique label that distinguishes one WVLAN from another. Wireless devices use the SSID to establish and maintain connectivity. Multiple SSIDs allow users to access different networks through a single access point, each SSID can be associated with a particular VLAN, and the tag is assigned per SSID in order to differentiate traffic from one SSID from the other (*Jim Geier, 2003b*)

A trunk is used to interconnect switches or AP's when VLAN switches and or access points are spread across different zones, a trunk links two or more switches or access points to a switches that have VLANs configured on them, (*George C. Ou,2002*) the trunk carries all the VLANS traffic from one switch to another. Traffic from one device to another is associated with a particular tag that uniquely identifies a particular VLAN (*Rajul Chokshi and Dr. Chansu Yu, 2004*). Network administrators can then map wireless traffic to multiple VLANs and assign them priority. Wireless AP traffic is concentrated through an 802.1q-capable wireless switch or

gateway; the device tags the packets before forwarding them. Through appropriate tagging, the packets move onto roles defined by the tags, whether the role is guest or employee or whatever SSID defined.

2.2 State of practices

Several case studies have been done in this area, most of which have been described in the literature review –state of the art.

They include,

- Physically separating users by device, where we run separate parallel networks with each network supporting a specific class of people.
- Using access control list to route traffic through the network, this allows for directing traffic through the network by permitting or denying its flow to different parts of the network.
- Using a wireless LAN controller to manage Access points and users, the WLAN has the capability to control and pass configurations to all access points and also manage the way users connect to the network.
- Using a radius server to authenticate users, the RADIUS server can be configured to only authenticate authorized users and grant them access to specific network segments or resources.

2.3 Technological advances

Currently, there are various technological advances going on in regards to effective management of the wireless network and LAN resources, they include,

Deploying of central management software's that allow central overall management of the system. There are many software's available in the market both open source and commercial and their use depends on what type of infrastructure you would like to have them run on. Jim, (Jim Geier 2003a) notes that, Wireless network management software will let you get the maximum performance from your WLAN, while making it as secure as possible. For example, management software will constantly monitor every access point in a WLAN, giving instant

feedback so a network administrator can constantly tweak the wireless network, keeping it as fast and secure as possible.

To achieve maximum out of the management tools, they should possess the following features:

(Charlie Schluting, 2009)

- **Centralization.** The tool should allow you to manage the entire network from a central location
- **Multiple Vendor Support.** The software should support access point hardware from a variety of vendors, allowing system design flexibility.
- **Flexibility.** Easy upgradeable software
- **Easy Integration with Existing Network Infrastructure.** The tools should be easily integrated into the existing network.
- **Ease of Use.** The software must have a user friendly operating environment, be easy to navigate, and provide adequate help when needed.
- **Automation.** When configuration changes are needed, the software must be able to automatically implement the changes over large groups of access points. This will eliminate the chance for human error and ensure uniform implementation of the changes.

The systems should be able to automate most of the requirements e.g., load balancing among the available resources, auto powering and auto channel configuring to prevent interfering from adjacent channel.

Development of virtual systems that can easily be integrated into the existing systems to allow seamless working environments and should be able to offer segregation of traffic on the LAN based on certain conditions.

2.4 Critic of the literature.

Despite the breakthrough in segregating wireless traffic, each of the methods cannot work independently and mix of the methods would produce the best result.

As much as the methods can manage traffic, the, ACL, and radius server can only be applied on users the system understands, it will not be possible to manage guest because they are mainly on and off the system, and their credential cannot be predefined into the system.

The methods discussed can only single handedly support organization authorized users in order to group them in classes and allow them different levels of access and or route their traffic differently.

Since guests are external to system and it's not possible to have their credential e.g., mac address and usernames predefined in the system for filtering or into access control list, each of the methods discussed cannot independently address the guest access issues.

3 METHODOLOGY

Networks have been with us and continue to evolve around us as year advance; network problems pose serious challenges to users and network administrators because they have direct impact on the productivity of organizations. To solve network related problems, we need to identify sources of problems then list possible approved solutions to the problem sources; there are different ways to identify problems sources some of which are manual systems or using automated problem detectors. Networks solutions deployed depend with the specific problem in question and not all network related problems are solved in the same way.

3.1 Existing methodologies

METHODS OF SOLVING NETWORK PROBLEMS

The methods used to solve network problems include:

A) Simulation of the system using simulation software's

A **network simulator** is a software or hardware piece that is used to predict the behavior of a network, in the absence of an actual network. A simulator imitates the actual working of a computer network where the computer network is modeled with devices and network traffic, the performance is then analyzed. The simulator can then be customized to fulfill specific analysis needs. Simulators support many protocols that are currently in use today, e.g. UDP, TCP, http and https traffic, and WLAN protocols.

Commonly used simulators include, Cisco packet tracer, OPNET and NetSim

The adoption of simulator methodology is mainly when there need to roll out a large project whose performance cannot really be predicted, the system is simulated prior to roll out to ascertain whether the developed system will work. Simulators can also be used prior to deploying simple and small systems to assess performance. Use of simulators help many organizations' save money and resources that would have been used to deploy projects that would fail to perform or whose performance wouldn't satisfy the owners, with simulators, actual system performance is measured and the deployed system would reflect or have the same characteristics as the simulated one(Robert currier 1999). Network simulators are also used by network designers to test new networking protocols or to change the existing protocols in a controlled and reproducible manner prior to actualization.

B) Deploying the system in real environment.

The second method that can be used to solve similar problems is going straight into action with the option of reverting back in case the expected change is not realized.

In this method, the system is developed in the actual environment and testing done as the system is deployed, if performance is not as per the expectation, the system is constantly tuned to optimal, failure to tune the system to the required expectation results in reverting back to the original system then new changes planned. This method uses a system development model and takes incremental stages.

This method is mainly used for small projects that do not involve large sums of investments, or in situations where the designer has good working knowledge and understands the outcome of the systems hence doesn't require system simulation.

3.2 Evaluation of the current methodologies

Simulation method

Simulations are mainly used in large project and or where the expected results are not well known. Simulations help organizations' save on time and other quantifiable resources that would have been wasted were the project undertaken in real environments and fail to work.

Network designer's use simulation tools to test new protocols and or determine the introduction of new devices or protocols on a network.

The challenges to this method are that, it requires skill and much understanding of simulation software's. The user must be conversant in use of the simulation systems, more so, many of the best simulation tools are commercially available and come at a cost, otherwise, we still have some free open source simulation tools though come with no or little support available only in forums.

Deployment in real environment method

The action method is used in circumstance where the methods have been tested and proven to work. This method is mainly adopted by network experts, who have in-depth knowledge of what the expected outcome should be.

During deployment, the system is deployed in phases and its performance evaluated a failure in performance leads to a re-evaluation of the method and a different approach undertaken.

The challenges to this method is that incase the system fails, then the organization incurs much losses as a result of purchasing items that are not utilized.

For the purposes of this research, the action method will be deployed for same reasons that the system will be developed in parallel to the current system and is expected to not interfere with the current one hence enabling business continuity.

More so, the designer has a better understanding of the system as the development in real environment is undertaken and can design better ways to go around issues that might not be reflected on a simulated system.

3.3 Proposed Methodology

In this research, different types of data will be gathered. The data relates to user response on network performance and network use, network traffic flow, DHCP leases and hits on the intrusion detection system.

To gather data related to user response, interviews of a few users will be conducted to gather users feel on performance of the system, for Network traffic, study the current architecture will be analyzed to establish how data flows through the system. For the DHCP leases, tools that display the DHCP leases will be employed, one such tool is the DHCP server or use of the angry IP scan tool that scans the entire network and returns a table of devices connected to the entire network and their corresponding IP address and Mac addresses.

Data analysis and Isolation

The data gathered will be analyzed for any anomaly and possible sources of such in order to isolate problems

4 FIELD STUDIES AND FINDINGS

4.1 Data types

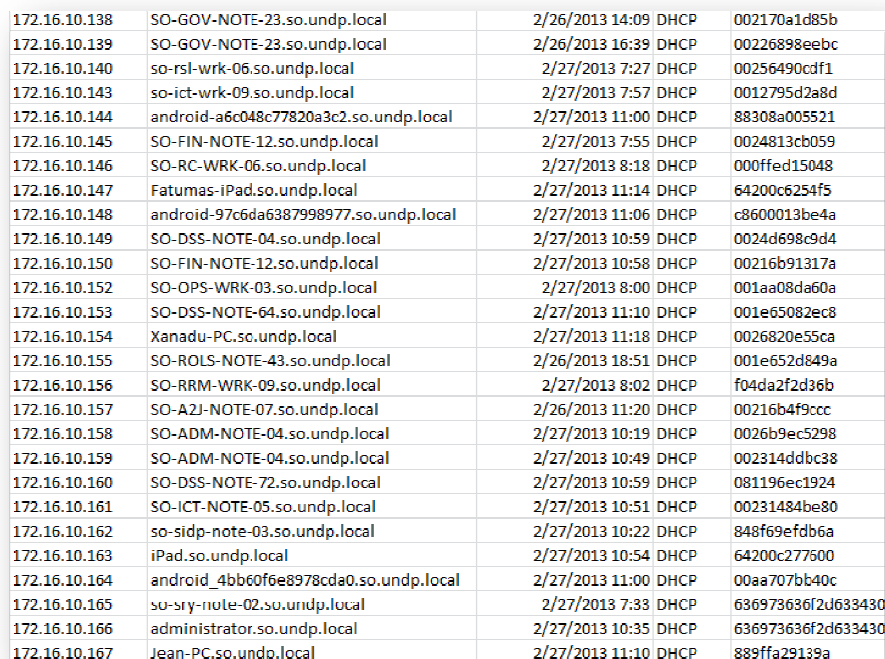
The main distinction of the types of data that flow in the system is data from the authorized staff members regarded as mission critical data and data from guest who visit the organization regarded as non- mission critical.

Field Study Findings.

The research found out that the current system has the following characteristics that need to be addressed.

- The system has no way of segregating guest access to resources as authorized users as seen from the current system architecture in fig 1. All the users have equal access rights once authenticated. The AP's pass all the traffic to the wired section of the LAN and hence allowing all users equal access.

A screen shot from the DHCP server indicated that the system authorizes all the clients with equal access rights to the office network.



172.16.10.138	SO-GOV-NOTE-23.so.undp.local	2/26/2013 14:09	DHCP	002170a1d85b
172.16.10.139	SO-GOV-NOTE-23.so.undp.local	2/26/2013 16:39	DHCP	00226898eebc
172.16.10.140	so-rsl-wrk-06.so.undp.local	2/27/2013 7:27	DHCP	00256490cdf1
172.16.10.143	so-ict-wrk-09.so.undp.local	2/27/2013 7:57	DHCP	0012795d2a8d
172.16.10.144	android-a6c048c77820a3c2.so.undp.local	2/27/2013 11:00	DHCP	88308a005521
172.16.10.145	SO-FIN-NOTE-12.so.undp.local	2/27/2013 7:55	DHCP	0024813cb059
172.16.10.146	SO-RC-WRK-06.so.undp.local	2/27/2013 8:18	DHCP	000ffed15048
172.16.10.147	Fatumas-iPad.so.undp.local	2/27/2013 11:14	DHCP	64200c6254f5
172.16.10.148	android-97c6da6387998977.so.undp.local	2/27/2013 11:06	DHCP	c8600013be4a
172.16.10.149	SO-DSS-NOTE-04.so.undp.local	2/27/2013 10:59	DHCP	0024d698c9d4
172.16.10.150	SO-FIN-NOTE-12.so.undp.local	2/27/2013 10:58	DHCP	00216b91317a
172.16.10.152	SO-OPS-WRK-03.so.undp.local	2/27/2013 8:00	DHCP	001aa08da60a
172.16.10.153	SO-DSS-NOTE-64.so.undp.local	2/27/2013 11:10	DHCP	001e65082ec8
172.16.10.154	Xanadu-PC.sc.undp.local	2/27/2013 11:18	DHCP	0026820e55ca
172.16.10.155	SO-ROLS-NOTE-43.so.undp.local	2/26/2013 18:51	DHCP	001e652d849a
172.16.10.156	SO-RRM-WRK-09.so.undp.local	2/27/2013 8:02	DHCP	f04da2f2d36b
172.16.10.157	SO-A2J-NOTE-07.so.undp.local	2/26/2013 11:20	DHCP	00216b4f9ccc
172.16.10.158	SO-ADM-NOTE-04.so.undp.local	2/27/2013 10:19	DHCP	0026b9ec5298
172.16.10.159	SO-ADM-NOTE-04.so.undp.local	2/27/2013 10:49	DHCP	002314ddbcb38
172.16.10.160	SO-DSS-NOTE-72.so.undp.local	2/27/2013 10:59	DHCP	081196ec1924
172.16.10.161	SO-ICT-NOTE-05.so.undp.local	2/27/2013 10:51	DHCP	00231484be80
172.16.10.162	so-sidp-note-03.so.undp.local	2/27/2013 10:22	DHCP	848f69efdb6a
172.16.10.163	iPad.so.undp.local	2/27/2013 10:54	DHCP	64200c277500
172.16.10.164	android_4bb60f6e8978cda0.so.undp.local	2/27/2013 11:00	DHCP	00aa707bb40c
172.16.10.165	so-sry-note-02.so.undp.local	2/27/2013 7:33	DHCP	636973636f2d633430
172.16.10.166	administrator.so.undp.local	2/27/2013 10:35	DHCP	636973636f2d633430
172.16.10.167	Jean-PC.so.undp.local	2/27/2013 11:10	DHCP	889ffa29139a

Figure 4: Sample shot of the DHCP lease.

- The systems constantly run out of DHCP leases and hence the system administrator has a standby DHCP scope that is activated when such issues arise in order to service more clients. This happens when we have a large influx of guests to the origination.

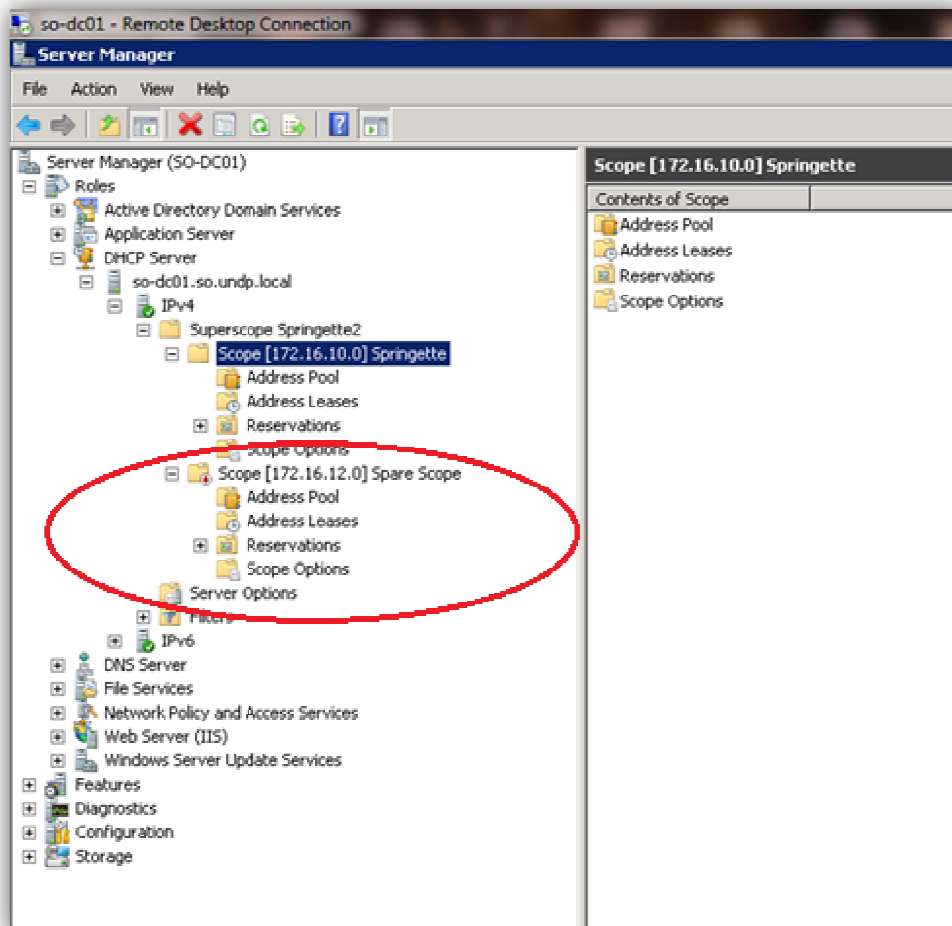


Figure 5: Systems DHCP Scopes.

- Once authenticated, guests have the same rights as staff and can use the network as though they were guest, hence not easily accounted for.

- The performance of the LAN systems is greatly degraded when we have a large inflow of guest and hence reduction in productivity from staff due to bandwidth constraints as a results of guest traffic.
- When there are more visitors in the organization, the IDS records many hits.

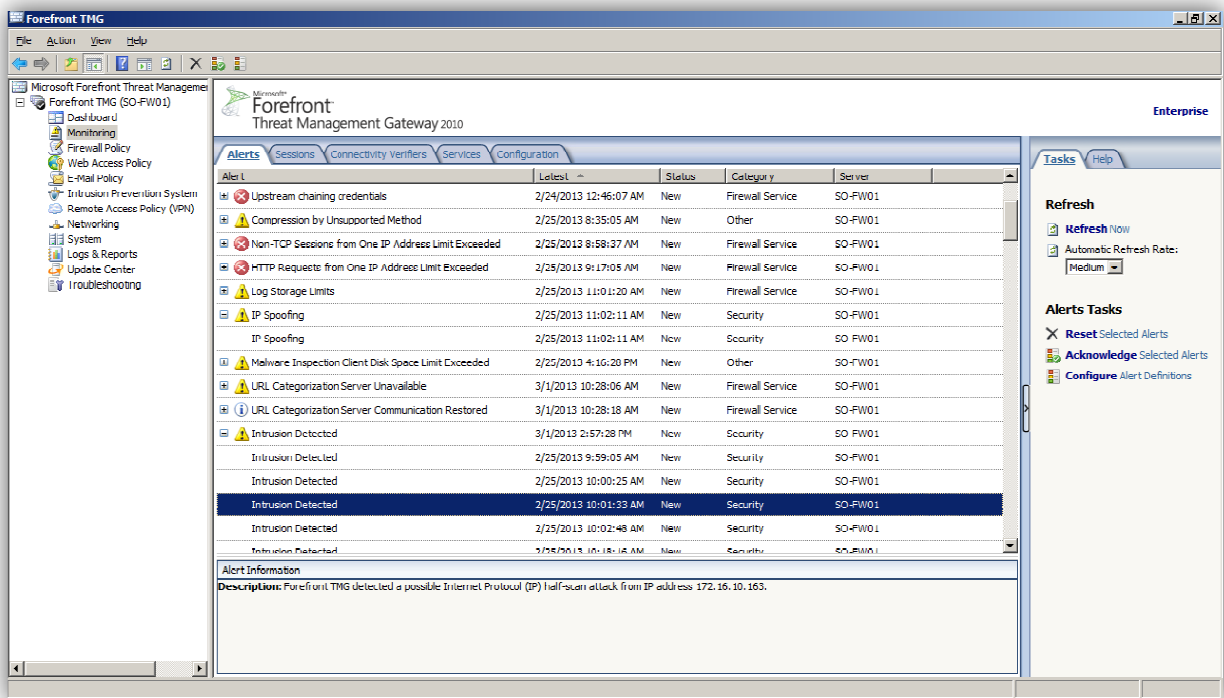


Figure 6: Hits on the IDS system.

- The current system architecture has many faults introduced in by allowing guest unrestricted access to the network and this would lead to accountability, performance and security concerns.
- An interview with the Network admin revealed that the current system authenticates everyone and all have equal rights of access, sophisticated guest can connect to any network resource for use or surveillance, hence the need for this research.

4.2 Conceptual Model.

The proposal will adopt a model as outlined in the architecture below.

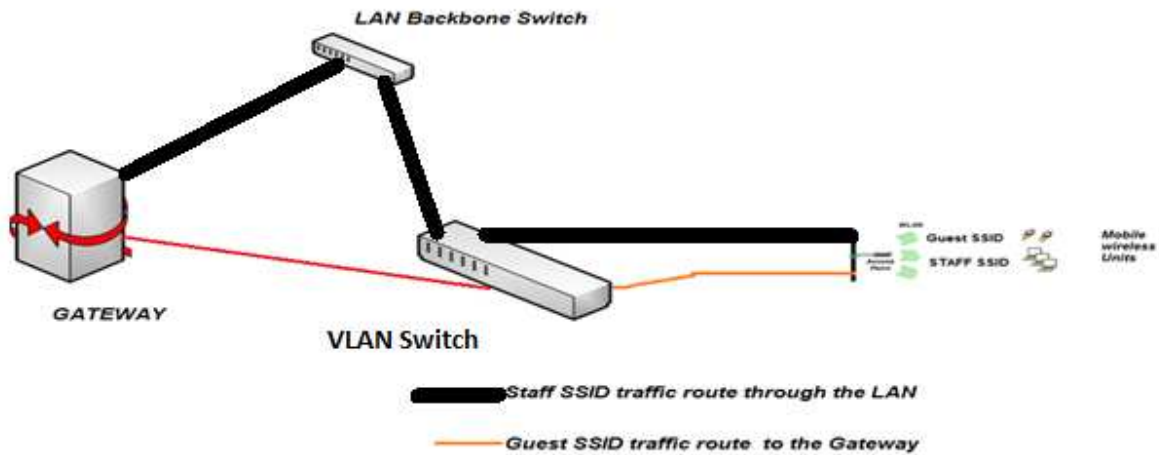


Figure 7: Conceptual model.

From the model, it can be depicted that traffic from different users takes different route out through the gateway.

Based on the information relating to the system architecture in place and the problem statement, the design for the proposed system is to take the form below,

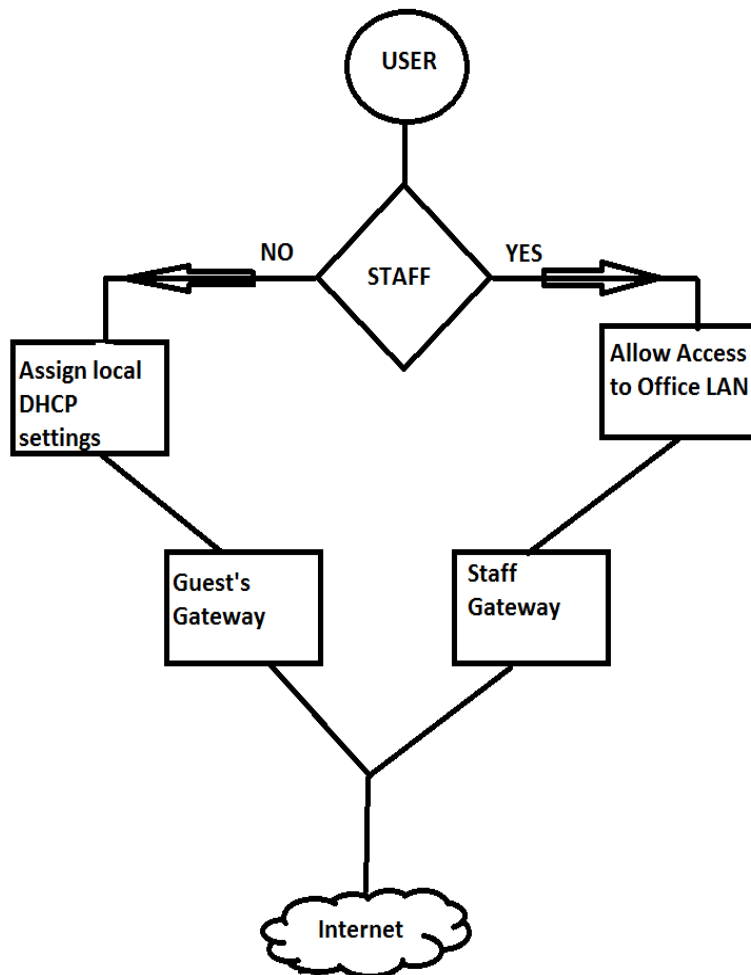


Figure 8: proposed system traffic flow

The figure 2 above illustrates how the traffic from guests and staff should flow in the system with the aim to achieve our specific objectives of having a well-managed system.

From the design, it is expected that the wireless access points picks traffic from two distinct categories of users, the guests and office staff. The traffic from office staff should be passed

onto the office LAN to enable staff access the network as if they were directly connected to the wired LAN. The guest's traffic should be guided out of the network through the gateway in a way that it does not pass onto the LAN.

4.3 Characteristics of the proposed solution.

This research aims to provide and formulate a way to manage access to enterprise wireless network for guests and staff and at the same time manage the network resources among users.

The solution should have a way of segregating guests and staff traffic and guide it differently through the LAN. For a well-managed network, then the resources in question below should be tuned to optimal they are:

- Network traffic flow
- DHCP leases,
- Virus and attacks control.
- Access to other network devices e.g. Printers.
- Ensure 100% uptime availability of the network to users.

The projects main goal is to ensure that the resources in question are put into proper use and are well utilized within the organization.

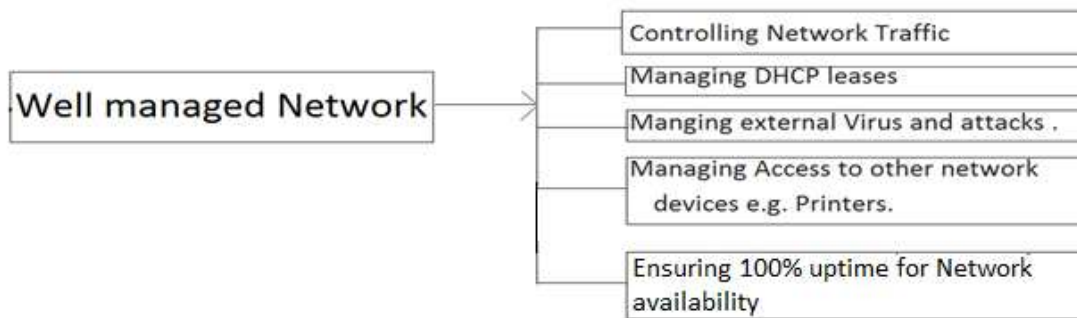


Figure 9: characteristics of an enhanced managed system.

The goal is to have a network that supports guest users access only to the internet from the office or certain common resources and at the same time allow only authorized staff members access resources only allowed to them.

To achieve the concept depicted in the model the architecture of the proposed system will take the form below

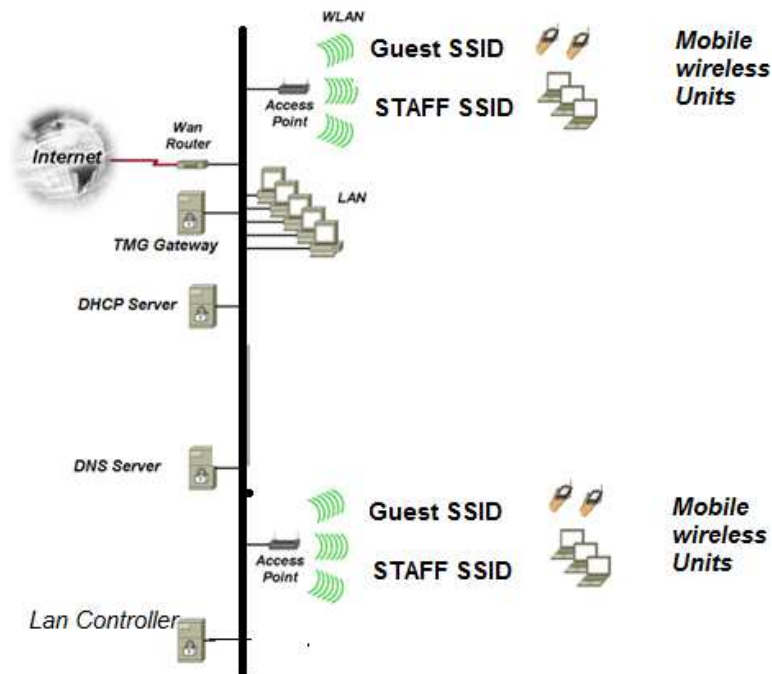


Figure 10: Proposed System Architecture.

The above architecture will be adopted because it has little impact on the current architecture and hence implementation will be easy with the current architecture in place as a fall back plan.

In the architecture, staff and guest have access to the wireless network via the available access points. The access points are light weight in nature configured to pass only two Service Set Identifiers, the guest SSID and the Staff SSID.

The access points have a LAN controller that passes over all the configurations to them so that it's done synchronously. Once a configuration is done on the LAN controller, it is then pushed to the controllers who effect the changes.

The Access points broadcast 2 SSID's one for the staff and the other for the Guest. The user's associate with one of the SSID's in order to connect to the network and since the WLC manages the AP's then roaming in the network can e achieved.

5 IMPLEMENTATION

Since the designers have an understanding of what is expected of the system and the methods involved are well documented and proved to work in many circumstances, and given that the system will have no or less impact on the current system, the proposed system will be developed in a real environment with the current system in place as a fall back plan or fail over.

5.1 proposed system Requirements

To effectively implement the proposed system, the following was required.

- Wireless LAN Controller.
- Light Weight Access Points
- 1 Network interface on the gateway for the guest wireless network.

To implement the system, the following were used.

- Cisco 5508 Series Wireless Controller
- Cisco Aironet 1140 Series Access Point.

Besides the reasons highlighted in the current state of the art for WLAN controllers and the need to have the proposed system integrate well with the wired LAN, the reasons for adopting this were,

- They are highly scalable and fit into our requirements
- For standardization purposes i.e. all the network equipment's are Cisco.
- The WLC has capability to create several traffic and have it routed as per the directions.
- It was a requirement from HQ that we use CISCO.

The Cisco Aironet 1140 Series Access Point was also picked for its capability to be upgraded to light weight and they both would easily fit into our proposed model.

5.2 Implementation of the system.

To implement the proposed system, the Cisco 5508 Series Wireless Controller was configured for two SSID's, The AP's were upgraded to light weight and an extra NIC card Installed and configured on the gateway to route out guest traffic.

CISCO 5508 SERIES WIRELESS CONTROLLER CONFIGURATION

The interfaces for wireless users are first created in the WLC so as to manage the wireless users. In this case, two interfaces are created, one to handle guest and the other to handle internal users and at the same time serve as an administrative interface so that network administrators can log into the WLC from the staff interface.

The interface created should match those on the Switched network/Wired LAN in order to pass wireless traffic smoothly to the wired LAN.

The interfaces on the switched network to be added to the WLC are;

Guest interface

IP Address: 192.168.80.2

Subnet mask: 255.255.255.0

Gateway: 192.168.80.1

Staff Interface

IP Address: 172.16.10.75

Subnet Mask: 255.255.254.0

Gateway: 172.16.10.2

Note that the staff Interface corresponds to the IP address of the WLC, this is to enable it sit directly on the staff network so that its traffic is passed directly on the internal network.

To add the new sub-interfaces to the WLC, log into the WLAN controller web page and navigate to **Controller>Interface**. In the Interfaces page, click on the **New** button, input the Interface

name of the sub-interface (guests and Management) and the VLAN ID (80 for guests and 0 for management) of the interface and click on the Apply button. In the new interface page, input the IP address of the interface in the same network as the SVI on the core switch, input the subnet mask, put the default gateway, input DHCP server IP addresses and click on Apply. The new interfaces are successfully created.

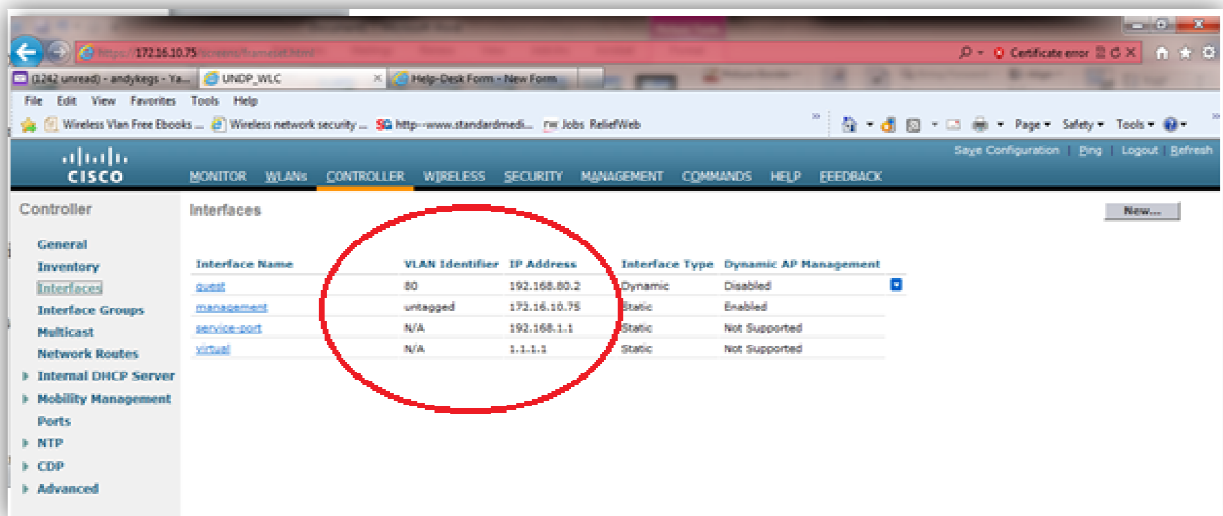


Figure 11: WVLANS configurations.

The two SSID's that were created are the guest known as UNDP-GUEST and the staff SSID broadcasted as UNDP_SOM.

This SSID's are to be passed onto the light weight access points by the Wireless LAN controller. The wireless SSIDs are centrally created on the controller and downloaded to the lightweight Aps when they are associated to the controller. To add a wireless SSID, Navigate to **WLANs** menu on the controller, On the WLANs page, select **Create New** on the menu drop down on the top right hand corner of the page and click on the **Go** button. On the New WLAN page, input the name and profile name of the new wireless SSID's (UNDP-GUEST and UNDP) and click on the **Apply** button. On the General tab of the new SSID, select the **enable** button and select the interface you want to associate the SSID to on the **Interface** drop down.

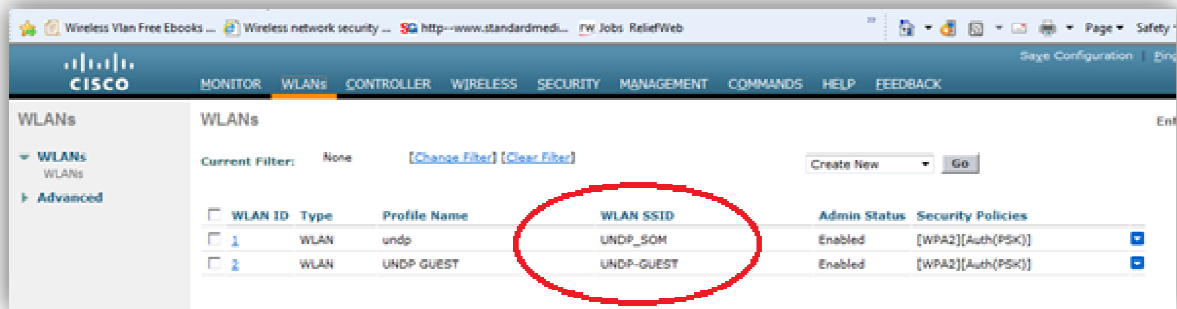


Figure 12: SSID configurations.

Since we intend to use a pre-shared secured wireless SSID, Select the security Tab then on the **Layer 2** tab select WPA+WPA2 option, select the **WPA2 Policy** and **AES WPA2 Encryption** options, click on the PSK authentication key management option and input the pre-shared key. On the **Advanced** options tab **DHCP Addr. Assignment** checkbox for Guest and leave it unchecked for the staff SSID, leave the NAC State dropdown on the default none for both.

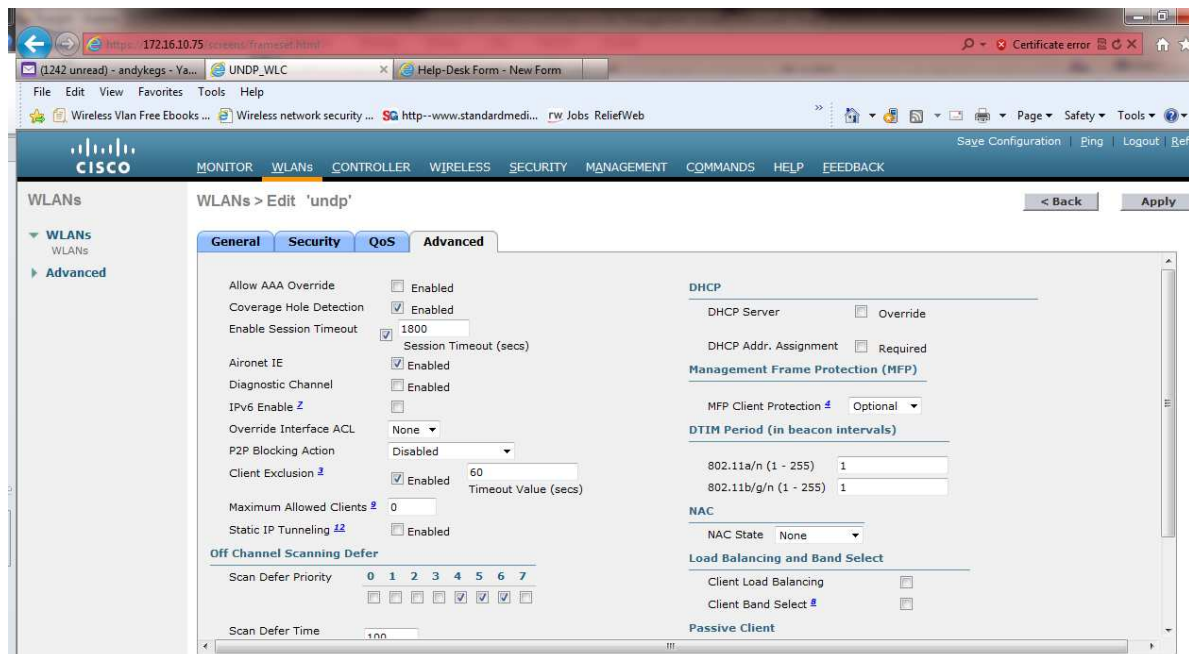


Figure 13: Staff SSID Security configurations.

Note that, Each of the SSID's is associated with a particular VLAN. The guest VLAN is on VLAN 80. The staff traffic is left on the untagged VLAN 0 so that it traffic can move easily through the LAN.

5.2.1 Staff WVLAN Configurations

Since the Staff traffic from the wireless access point is expected to flow to the LAN, the configurations take the form below.

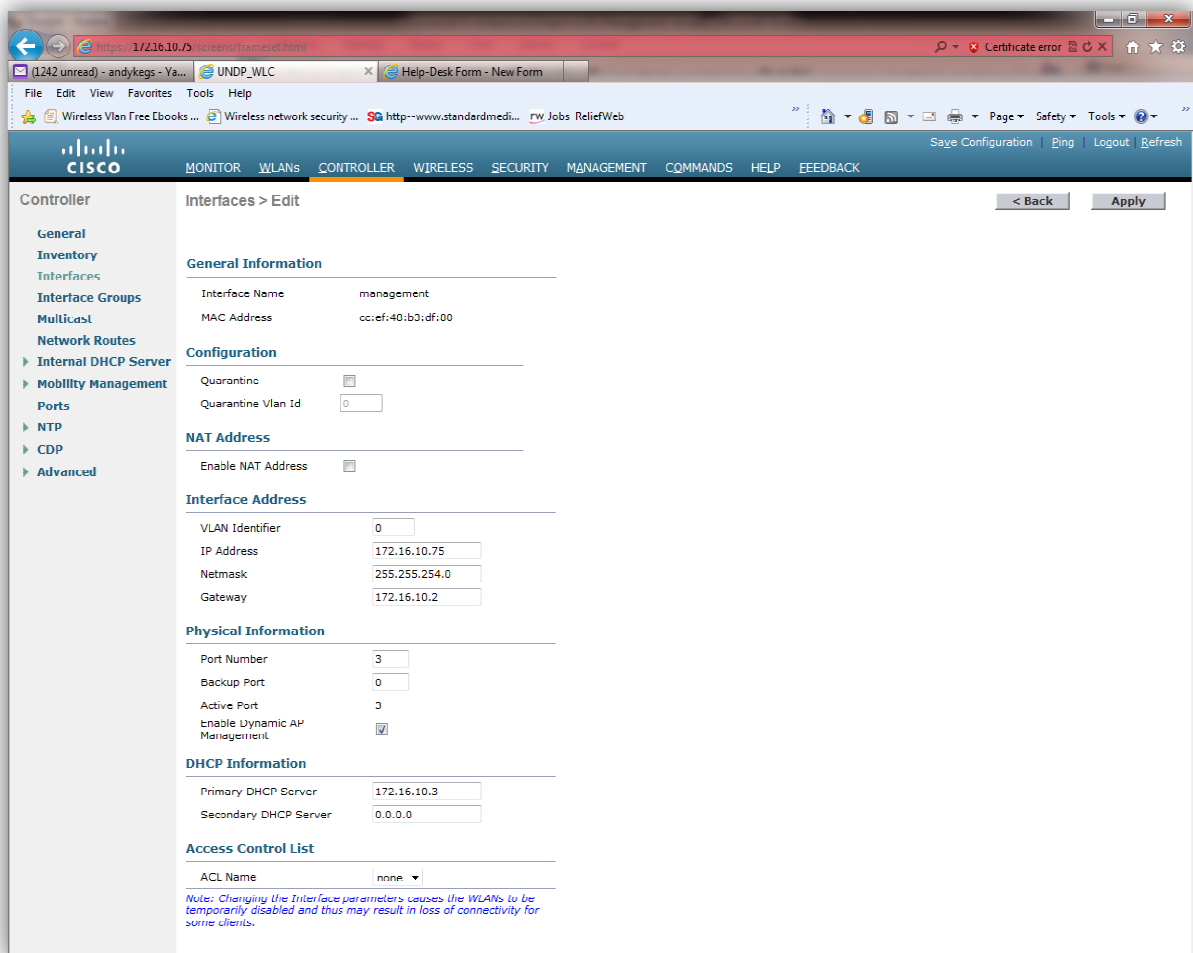


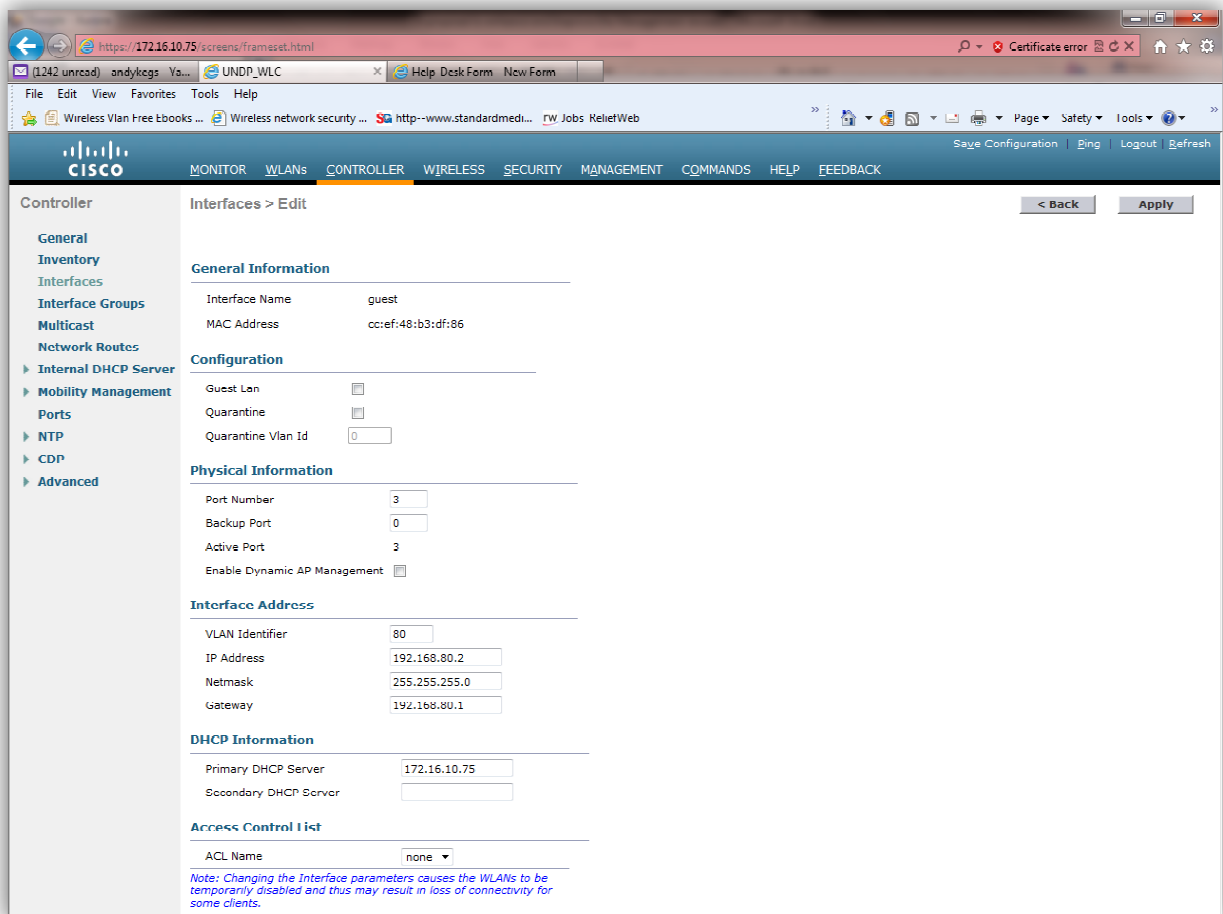
Figure14: Settings for the staff SSID.

From the configuration in the figure 13 above, we note that,

- The staff traffic is untagged hence flows through the system untagged.
- The DHCP settings are obtained from the office DHCP server who's IP is 172.16.10.3 located on the wired section of the LAN.
- The gate way for the staff VLAN is the office gateway whose IP is 172.16.10.2.

5.2.2 Guest WVLAN Configurations

For the guest Network, the configurations take the form.



The screenshot shows the Cisco Controller configuration page for a Guest WLAN interface. The page is titled "Interfaces > Edit" and includes a navigation menu on the left with options like General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main configuration area is divided into several sections:

- General Information:** Interface Name: guest, MAC Address: cc:ef:48:b3:df:86
- Configuration:** Guest Lan: , Quarantine: , Quarantine Vlan Id: 0
- Physical Information:** Port Number: 3, Backup Port: 0, Active Port: 3, Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: 80, IP Address: 192.168.80.2, Netmask: 255.255.255.0, Gateway: 192.168.80.1
- DHCP Information:** Primary DHCP Server: 172.16.10.75, Secondary DHCP Server:
- Access Control List:** ACL Name: none

A note at the bottom states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

Figure 15: Guest WVLAN configuration.

From the configurations, it is noted that the VLAN is tagged to VLAN ID 80, the guest VLAN with a class C IP address of 192.168.80.2 so that they are on a different network from the staff network.

The default gateway is 192.168.80.1, which is the new interface on the gateway meant specifically for this purpose.

From the configurations, DHCP is enabled with the WLC (172.16.10.75) as the primary DHCP server. The guest WVLAN DHCP configuration takes the form below.

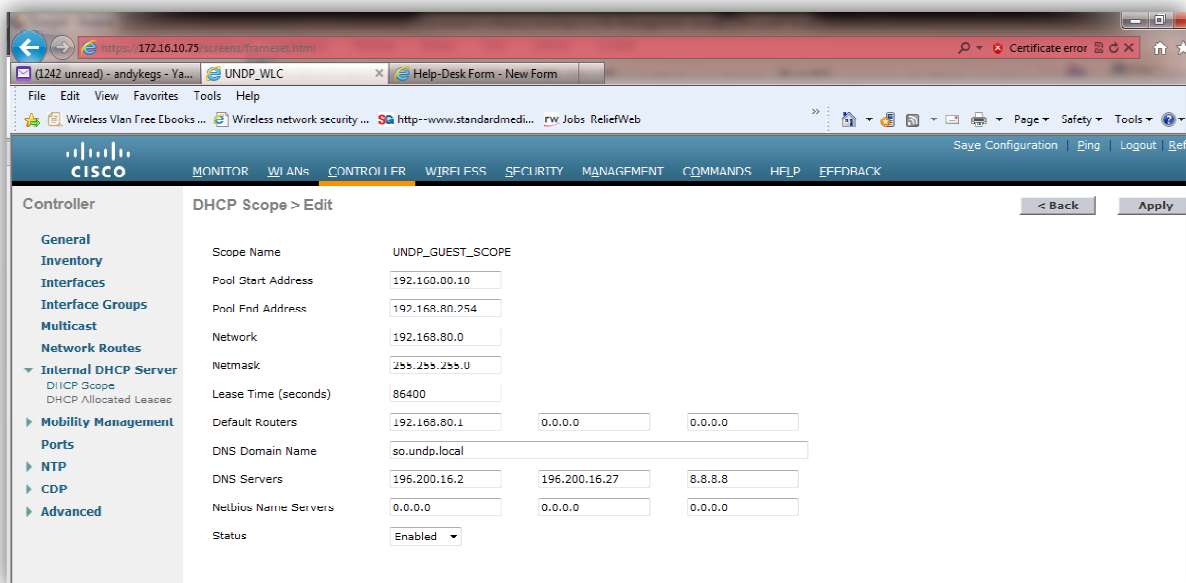


Figure 16: Guest WVLAN DHCP configuration

From the configurations, it is noted that

The WVLAN is on class C network 192.168.80.0; its default gateway is 192.168.80.1 an interface on the organization's gateway.

The DNS servers are set to the ISP providers DNS server so that the clients do not resolve with the internal DNS servers.

The LAN controller passes over the DHCP settings onto the Guest wireless LAN clients.

The guest Network is assigned a class C network because it does not have many clients.

5.2.3 AIRONET 1140 Series access point configuration

The AP's come with Autonomous status by default so as to enable them manage the wireless connection on their own.

They are first configured with the LAN IP addresses in order for them to be able to communicate on the LAN,

Table below shows a list for the AP's deployed.

AP NAME	LOCATION	IP ADDRESS.
Block A	Rols Floor	172.16.10.61
Block B1	UNDSS Floor	172.16.10.62
Block B2	RSL Floor	172.16.10.63
Block C(Management Floor)	Management Floor	172.16.10.64
Block C (Training Room)	Training Room	172.16.10.65
Block E	RC Floor	172.16.10.66
Block F	Helen Clark Conference Room	172.16.10.67
Block G	Rols Prefab	172.16.10.68
Block H	Sioc Prefab	172.16.10.69

Table 4: Location and IP of AP's to be deployed.

To be able to use them for our system, the AP's had to be upgraded to light weight so that they could be managed by the WLAN controller.

Once the Access points have been upgraded, and rebooted, they are able to find the WLAN controller on the network and pick up further settings from it.

The settings configured on the LAN controller above are passed onto the Access Points after they have been upgraded to light weight and associate with the WLC.

5.2.4 Gateway Configurations

To enable the guest traffic to flow out of the system, the gateway was configured with an extra interface card to handle guests' traffic

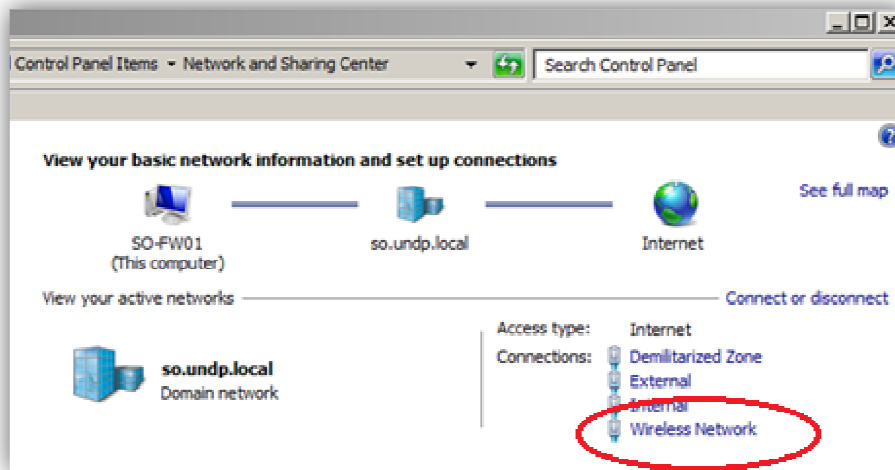


Figure 17: Gateway interfaces.

The Interface settings are:

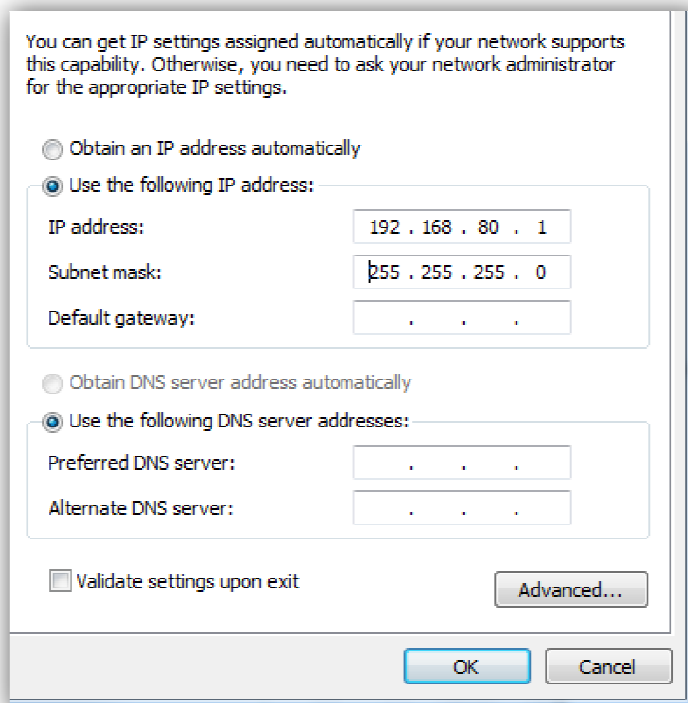


Figure 18: wireless gateway interface settings.

The interface is put on the same VLAN as the guest VLAN on the back bone switch so that they are members of the same VLAN.

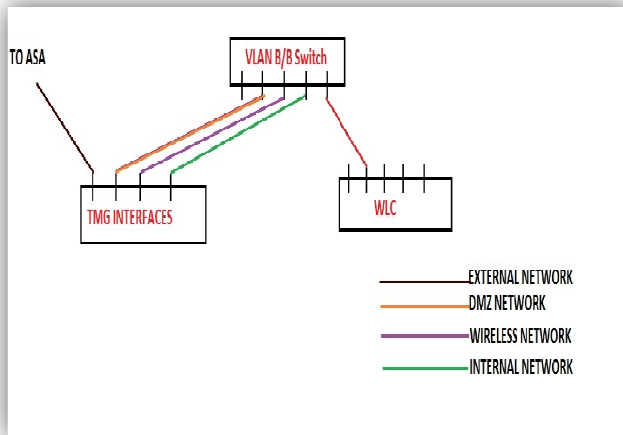


Figure 19: System interfaces Architecture.

In order to guide traffic out the system, all traffic from the guest network was routed to the organization's ASA, whose IP is configured on the external interface of the threat management gateway.

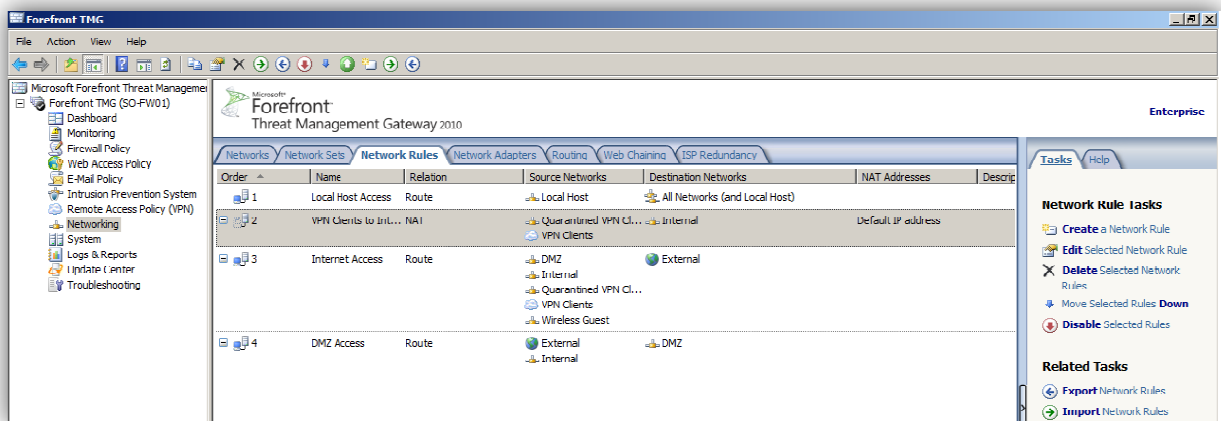


Figure 20: Traffic flow out of the network.

Several rules were described to enable guest on the guest network to access the internet and not to the internal network, a key requirement for the successful deployment of the project

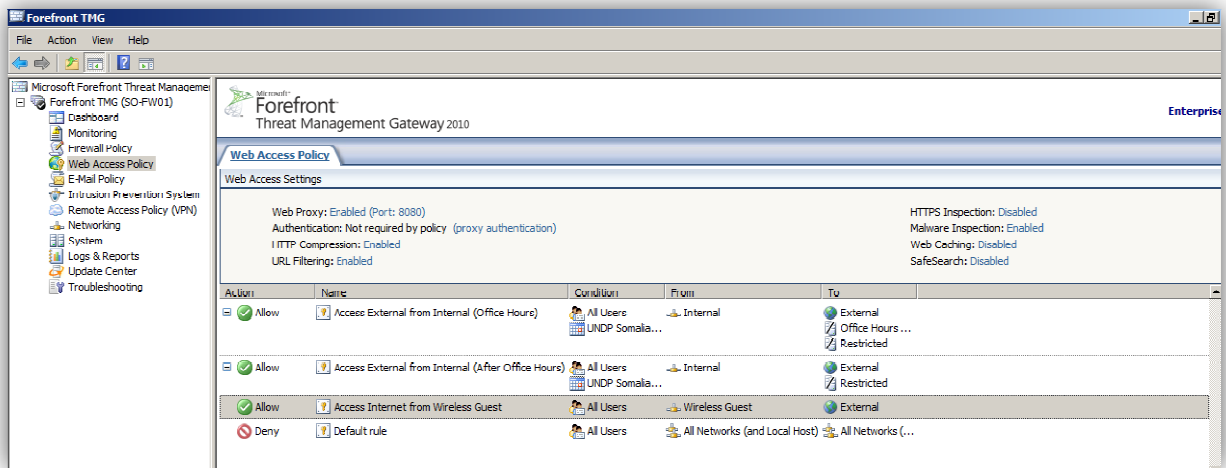
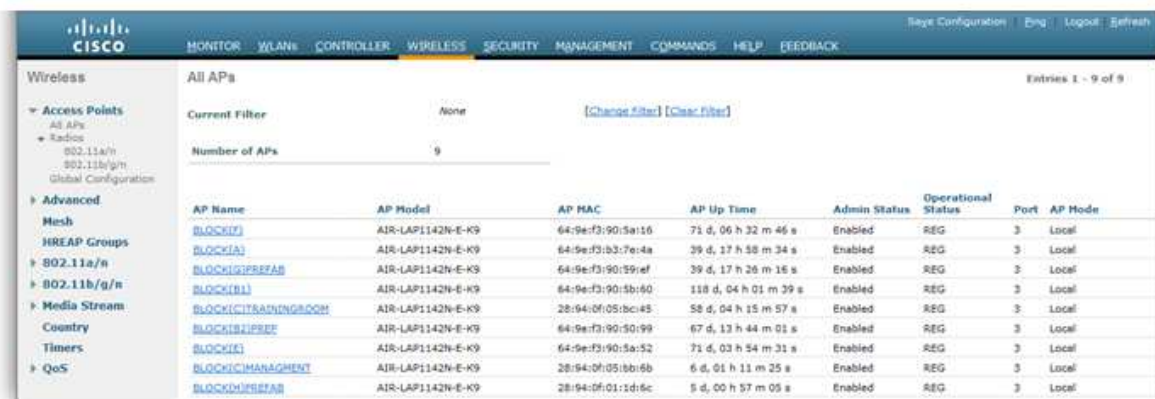


Figure 21: Gateway rules.

6 RESULTS, CONCLUSION AND RECOMMENDATION

6.1 Discussion of results

After deployment all the access points were registered by the LAN controller and the configured settings passed onto them by the controller. For this case, 9 AP's were deployed and the access points were registered as shown below.



The screenshot shows the Cisco Wireless LAN Controller interface. The 'All APs' section displays a table with 9 entries. The table columns are: AP Name, AP Model, AP MAC, AP Up Time, Admin Status, Operational Status, Port, and AP Mode. All APs are listed as 'Enabled' and 'REG' (Registered).

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
BLOCK17	AIR-LAP1142N-E-K9	64:9e:f3:90:5a:16	71 d, 06 h 32 m 46 s	Enabled	REG	3	Local
BLOCK1A	AIR-LAP1142N-E-K9	64:9e:f3:b3:7e:4a	39 d, 17 h 58 m 34 s	Enabled	REG	3	Local
BLOCK1GPREFA8	AIR-LAP1142N-E-K9	64:9e:f3:90:59:ef	39 d, 17 h 26 m 16 s	Enabled	REG	3	Local
BLOCK1B1	AIR-LAP1142N-E-K9	64:9e:f3:90:5b:60	118 d, 04 h 01 m 39 s	Enabled	REG	3	Local
BLOCK1CTRADINGROOM	AIR-LAP1142N-E-K9	28:94:0f:05:b0:e5	58 d, 04 h 15 m 57 s	Enabled	REG	3	Local
BLOCK1J2PREP	AIR-LAP1142N-E-K9	64:9e:f3:90:50:99	67 d, 13 h 44 m 01 s	Enabled	REG	3	Local
BLOCK1E1	AIR-LAP1142N-E-K9	64:9e:f3:90:5a:52	71 d, 03 h 54 m 31 s	Enabled	REG	3	Local
BLOCK1CMANAGEMENT	AIR-LAP1142N-E-K9	28:94:0f:05:bb:6b	6 d, 01 h 11 m 25 s	Enabled	REG	3	Local
BLOCK1URSTAF	AIR-LAP1142N-E-K9	28:94:0f:01:1d:6c	5 d, 00 h 57 m 05 s	Enabled	REG	3	Local

Figure 22: Number of access points registered by the Wireless LAN controller.

From the figure, it can be shown that, once the AP's have been registered, they can be managed from the controller, as seen, all the Aps are up, and in case any goes down, it can easily be detected from the controller. The Access points are not likely to go down unless there is a cut in the patch cable connecting it to the distribution switches or if the patch cable is disconnected from the access point. In case any access point goes down, its status would easily be detected on the LAN controller and the system administrator can easily go check. In this case, the access point can easily be monitored for uptime in order to ensure 99.999% uptime availability. This is to increase office productivity since connectivity is on all through and more so, allow users to work comfortably from all the regions within the organization.

Wireless devices support different 802.11 standards as explained in the literature review state of the art section, some being upgrades from the other, this is because of the different encryption algorithms supported by the different protocols. The Access points are configured to accept the standards are a, b and g with which most devices range. In this case, most user gadgets have been accommodated and hence irrespective of what device one has, a connection can be established and access granted.

AP Name	Infrastructure Validation	Radio	Operational Status	Infrastructure Protection Capability	Infrastructure Validation Capability
BLOCK(F)	Disabled	b/g	Up	Full	Full
BLOCK(F)	Disabled	a	Up	Full	Full
BLOCK(A)	Disabled	b/g	Up	Full	Full
BLOCK(A)	Disabled	a	Up	Full	Full
BLOCK(G)PREFAB	Disabled	b/g	Up	Full	Full
BLOCK(G)PREFAB	Disabled	a	Up	Full	Full
BLOCK(B1)	Disabled	b/g	Up	Full	Full
BLOCK(B1)	Disabled	a	Up	Full	Full
BLOCK(C)TRAININGROOM	Disabled	b/g	Up	Full	Full
BLOCK(C)TRAININGROOM	Disabled	a	Up	Full	Full
BLOCK(B2)PREFAB	Disabled	b/g	Up	Full	Full
BLOCK(B2)PREFAB	Disabled	a	Up	Full	Full
BLOCK(E)	Disabled	b/g	Up	Full	Full
BLOCK(E)	Disabled	a	Up	Full	Full
BLOCK(C)MANAGEMENT	Disabled	b/g	Up	Full	Full
BLOCK(C)MANAGEMENT	Disabled	a	Up	Full	Full
BLOCK(H)PREFAB	Disabled	b/g	Up	Full	Full
BLOCK(H)PREFAB	Disabled	a	Up	Full	Full

Figure 23: Wireless standards supported by the wireless LAN network.

The WLAN controller is configured with two SSID's which are passed onto the Access points for broadcast, once a client switches on the wireless device for wireless access within the organization, the two SSID's are broadcasted.

The SSID's broadcasted are UNDP_SOM and UNDP-GUEST just as had been configured on the Wireless LAN controller.

The broadcasted SSID's appears as show below on the client's machine



Figure 24: showing how the SSID's are broadcasted on the client's machine

For internal organization's staff, they select the UNDP_SOM broadcasted SSID and enter the pass phrase which was configured on the LAN controller.

For guests and non-staff members, they select the UNDP-GUEST SSID broadcasted and enter the pass phrase/key. The guest wireless network key is pinned on the notice board and on the boards in all the conference areas and hot spots in the office.

Once authenticated, the users can roam around with their machines in the office and still sustain the connection.

The Access point's radius has been set to only broadcast in and within the office compound. Outside the compound there is no signal and so visitors outside the organization cannot pick the signal.

The configurations of the SSID's have been configured with WPA+WPA2 because of its advanced security features as discussed in the literature review section. Users can choose to connect automatically when the network is in range. Since all the AP's broadcast the same SSID's, then roaming users are always connected irrespective of the location because the hand

over from one AP to another is seamless as it does not need manual reconnection, this is in order to ensure that users can work from any location and need not turn off their active connection or programs as they move within the organization.

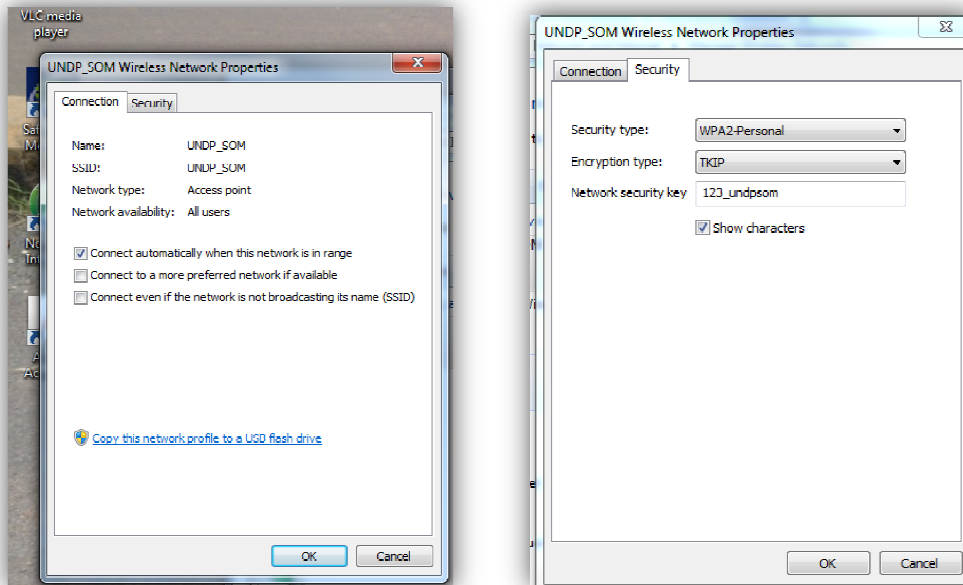


Figure 25: client machine Configuration settings.

The guest network is configured to pick its network settings from the LAN controller. All guest connected to the UNDP-Guest network are assigned DHCP settings by the LAN controller as elaborated in section 5.2.2 for the guest network configuration. The figure below shows some of the clients that are connected to the guest network. The guests are leased IP address by the WLAN controller to enable them access the network.

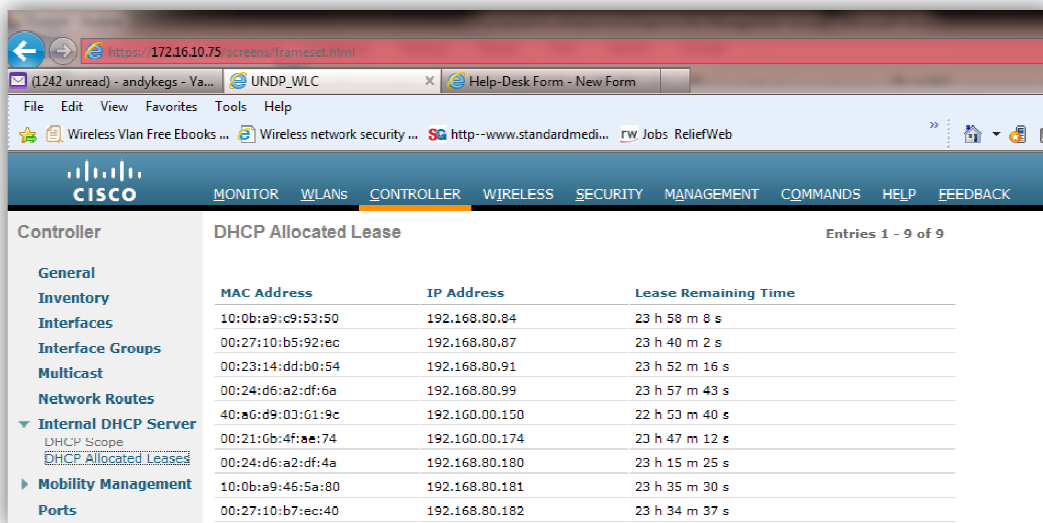


Figure 26: Guest wireless LAN clients.

Since guests come in and leave anytime, the leases are only for a 24hr session, meaning after 24hrs, the IP leases are withdrawn and if the guest device is still on the network, new settings are re-leased to the user. This is done in order to avoid committing an IP for long to a client who does not exist, the guest network can only support up to 245 clients as configured in the configuration page for the guest's DHCP scope i.e. IP 192.168.80.10 to 192.168.80.254. If this is not done, then we are likely to run out of IP address as a result of non-existing devices holding IP's that can be assigned to other devices.

From the results, the administrator can easily tell how many guest clients are on the network at any given time by logging into the WLAN controller, a situation that is not possible with autonomous AP where the administrator has to log into each AP in order to know how many clients are connected through it. The network administrator can also tell how long a device has been connected to the network by checking on the lease remaining time.

All official wireless devices are associated with the staff SSID broadcasted as UNDP_Som. From the settings on the configuration for the staff SSID in section 5.2.1, the connected devices obtain their IP settings from the organization's DHCP server configured at IP 172.16.10.4. This ensures that the devices have access to the organization's resources from wherever they are connected. The staff DHCP server is connected to the wired network and issues DHCP settings

to both wired and wireless devices. Unlike the previous settings where the DHCP server issued IP setting to all devices, including guest devices, only wired office machines and mobile wireless devices connected to the staff SSID as assigned DHCP settings, this ensures that only the authorized internal devices have access to the office network and hence authorized to utilize office network resources, like shared printers, shared work spaces and server resources.

With this separation, the number of clients serviced by the organization's DHCP server has significantly reduced and hence the server does not constantly run out DHCP leases as before. This in essence ensures that the DHCP server and other office servers, e.g. the domain controller can effectively manage the users on the office network and the system administrator can easily monitor and confirm that the organization's resources are utilized by only authorized users.

The figure below shows an extracted sample of results from the organization's DHCP server for the leases.

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access
172.16.10.160	SO-OPS-NOTE-03.so.undp.local	7/25/2013 9:21:33 AM	DHCP	0026b9f36f47		Full Access
172.16.10.161	SO-OPS-NOTE-03.so.undp.local	7/25/2013 12:52:52 PM	DHCP	002710b82ac8		Full Access
172.16.10.162	SO-RC-NOTE-11.so.undp.local	7/25/2013 9:43:11 AM	DHCP	e0db55df0d5f		Full Access
172.16.10.163	SO-RC-NOTE-11.so.undp.local	7/25/2013 12:44:23 PM	DHCP	6067209a9f90		Full Access
172.16.10.164	SO-ICT-WRK-02.so.undp.local	7/25/2013 7:37:47 AM	DHCP	001aa08e3689		Full Access
172.16.10.165	SO-ICT-NOTE-05.so.undp.local	7/25/2013 1:04:35 PM	DHCP	00231484be80		Full Access
172.16.10.166	SO-PRO-NOTE-01.so.undp.local	7/25/2013 12:26:14 PM	DHCP	00231484c364		Full Access
172.16.10.167	SO-ADM-NOTE-04.so.undp.local	7/25/2013 1:22:38 PM	DHCP	002314ddbc38		Full Access
172.16.10.168	so-grol-note-04.so.undp.local	7/25/2013 1:10:33 PM	DHCP	843a4b0740e0		Full Access
172.16.10.169	so-ict-wrk-09.so.undp.local	7/25/2013 8:34:48 AM	DHCP	0012795d2a8d		Full Access
172.16.10.170	SO-GOV-NOTE-26.so.undp.local	7/25/2013 1:10:48 PM	DHCP	002314ddb054		Full Access
172.16.10.171	SO-RMU-NOTE-03.so.undp.local	7/25/2013 1:11:59 PM	DHCP	60672076663c		Full Access
172.16.10.172	so-pmst-note-01.so.undp.local	7/25/2013 9:30:55 AM	DHCP	848f69efd3e		Full Access
172.16.10.173	so-pmst-note-01.so.undp.local	7/25/2013 1:18:33 PM	DHCP	08119661bb88		Full Access
172.16.10.174	SO-DSS-NOTE-04.so.undp.local	7/25/2013 1:19:57 PM	DHCP	0024d698c9d4		Full Access
172.16.10.175	SO-DSS-NOTE-21.so.undp.local	7/25/2013 12:32:12 PM	DHCP	0026c6c38fb8		Full Access
172.16.10.176	so-prep-note-78.so.undp.local	7/25/2013 12:41:47 PM	DHCP	100ba9cd00c4		Full Access
172.16.10.177	so-unaid-wrk-07.so.undp.local	7/25/2013 8:39:44 AM	DHCP	0014223f5fe1		Full Access
172.16.10.178	SO-REG-WRK-01.so.undp.local	7/25/2013 9:11:42 AM	DHCP	001aa08da20c		Full Access
172.16.10.180	so-rols-note-16.so.undp.local	7/25/2013 12:58:50 PM	DHCP	100ba9c94008		Full Access
172.16.10.181	SO-FIN-NOTE-99.so.undp.local	7/25/2013 8:57:59 AM	DHCP	d4bed92170cf		Full Access

Figure 27: DHCP output from the organization's server.

From the results, only official machines are assigned settings, this is done in order to only allow the office devices access to the office LAN.

Since all the office devices have anti-virus software that is automatically updated by the anti-virus server, all the organization's machines are well secured and monitored by the anti-virus server. The anti-virus server downloads new virus definitions and passes them over to the clients; the machines are always up to date with the latest virus definitions. There has been a significant reduction on the hits on the intrusion detection system as a result of virus activity. This is a result of some machines for users on long missions with limited access to the internet for anti-virus update. Once the machines get connected to the office network, they are updated and scanned for virus automatically by the anti-virus server. Unlike in the previous system where the IDS recorded much hits as a result of guests' unprotected devices on the network, which constantly infected the office machines.

6.2 CONCLUSION

Through the research, the following were notable,

- The prior network was assessed and the key bottleneck identified as having to do with allowing guest to access the network hence misuse of the office resources.
- Several factors were identified as sources of problems, mostly attributed to poor design that is not scalable and hence leading to poor management.
- Improvements suggested were to have guests have their own access way in order to manage what they have access to on the network.
- The implemented design is seen to work well and helped address most of the challenges experienced with the initial system.
- The enhance system can now accommodate growing performance needs, availability and scalability demands.

From the results it can be concluded, the adoption of the new systems has generally enhanced the management of the network. Key notable features are,

- The system can be centrally managed hence changes to the system are automatically updated in the system.
- Guest and staff traffic have been completely isolated hence ensuring that network resources are not misused.
- Overall network system health has greatly improved with the isolation of guest infested devices from the staff network.

In overall, the network performance has greatly improved and hence productivity and ease of work by staff. More so, the system administrator has control of the system and can easily account for most of the network features

6.3 Future Research Work

As future work, the network can further be configured to isolate devices depending on the access modes so that hand held devices can be managed separate from guest laptops.

The network can be configured in a way to enable guest devices on the network that have virus infections be scanned for virus and those devices that are not protected be installed with a free anti-virus software from a central guest server this will prevent the affected guest devices from infecting non protected devices.

6.4 Recommendations

The following are notable recommendations to the organization.

More VLANS should be implemented so as to map users by departments and in overall improve network efficiency by managing traffic.

Strict wireless access policies should be enforced so that staff are not be allowed to have their personal wireless gadgets to the staff WVLAN.

To other researchers, this research project can be further enhanced in order to help better manage the unseen guest prior to his or her connection onto the network.

7 REFERENCES

Thomas Timmermann 2012, *How to Choose the Right network Monitoring Solution White Paper*
http://cdn.paessler.com/common/files/pdf/whitepaper/selection-criteria_en.pdf ,
28th January 2013.

Meraki 2009, *wireless LAN security version 1.0, White paper*
http://www.meraki.com/lib/pdf/meraki_whitepaper_network_security.pdf , 2nd February 2013.

Jim Geier 2003a, *WLAN Management Considerations*
<http://www.wi-fiplanet.com/tutorials/article.php/2177931/WLAN-Management-Considerations.htm> 2nd February 2013

US-CERT 2006, *Using Wireless Technology Securely, Updated 2008*
http://www.us-cert.gov/reading_room/Wireless-Security.pdf , 28th January 2013

Barry Lewis and Peter T. Davis 2004, *Wireless Networks for Dummies*; Wiley Publishing
Inc.111 River Street Hoboken, NJ 07030-5774
http://www.datateknikk.no/ebooks_dummies/Wireless_Networks%20for_Dummies.pdf ,
26th January 2013

Rajul Chokshi and Dr. Chansu Yu 2007, *Study on VLAN in Wireless Networks*, Department of
Electrical and Computer Engineering Cleveland State University Cleveland, Ohio 44115
<http://academic.csuohio.edu/yuc/papers/VLAN.pdf> , 26th January 2013

George C. Ou 2002, *Enterprise Level Wireless LAN Security*,
<http://www.lanarchitect.net/Articles/Wireless> , 24th January 2013

Cisco systems a, Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, *Configuring VLANs*, Chapter 14 OL-21881-03, http://www.cisco.com/en/US/docs/wireless/access_point/12.4.25d.JA/Configuration/guide/scg12.4.25d.JA-chap14-vlan.pdf, 2nd February 2013

SysKonnct GmbH 2001, *Virtual Networks- white paper* <http://staff.pccu.edu.tw/~lchou/reference/network/vlan.pdf> , 26th January 2013

Jim Geier2003b, *Implementing Multiple SSIDs* <http://www.wi-fiplanet.com/tutorials/article.php/2196451>, 29th January 2013

Cisco Systems b, Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, *Configuring Network Security with ACLs*, <http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/19ew/configuration/guide/secure.pdf> ,26th January 2013

Charlie Schluting 2009, *Understanding Your WLAN Management Options* <http://www.enterprisenetworkingplanet.com/netsysm/article.php/3855716/Understanding-Your-WLAN-Management-Options.htm>, 27th January 2013

Cisco systems c, *Chapter 3 Using Access Control Lists (ACLs)* http://www.hp.com/rnd/support/manuals/pdf/release_06628_07110/Bk2_Ch3_ACL.pdf, 18th Jan 2013.

Cisco systems d, *UNDERSTANDING THE LIGHTWEIGHT ACCESS POINT PROTOCOL (LWAPP)*, Cisco systems white paper. http://www.intermec.com/public-files/white-papers/en/CiscoLWAPP_wp_web.pdf, 18th January 2013

ROBERT CURRIER 1999, *Network World Test Alliance Network World*, 05/24/99- <http://www.networkworld.com/reviews/0524rev.html> ,18th January 2013

Brad Slavin 2013, *WI-Fi Security – The Rise and fall of WPS* Posted on January 18, 2013

<http://www.netstumbler.com/2013/01/18/wi-fi-security-the-rise-and-fall-of-wps> , 28th January 2013

Rathnakar et.al 2009, Wireless LAN Security- challenges and solutions, International Journal of Computer and Electrical Engineering, Vol. 1, No. 3, August 2009 1793-8163

<http://www.ijcee.org/papers/039.pdf> , 25th March 2013

Jonathan Weiss- SANS Institute 2002, WIRELESS NETWORKS: Security Problems and Solutions

<http://www.sans.org/reading-room/whitepapers/wireless/wireless-networks-security-problems-solutions-172> , 25th March 2013

Lisa Phifer, 2011- Buyer's Guide to Enterprise WLAN Controllers

<http://www.enterprisenetworkingplanet.com>, 28th January 2013

Info-Tech Research Group 2011, Vendor Landscape: Wireless LAN

<http://www.enterasys.com/company/literature/info-tech-wlan-vendor-landscape.pdf>

06th March 2013.

Swati Sukhija, Shilpi Gupta 2012, Wireless Network Security Protocols A Comparative Study: International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

www.ijetae.com 24th February 2013

Ziff Davis 2012, *Enterprise WLAN comparison Guide*.

https://s3.amazonaws.com/formcomposer/assets/asset/production/items/1269/zd-cg-entp-wlan-xirrus-product-info_112612.pdf

24th February 2013