SEGMENTING NETWORKS FOR BETTER SECURITY, MANAGEABILITY AND SCALABILITY:
THE CASE OF PENTECOST UNIVERSITY COLLEGE

Paul Danquah

Abstract

Fundamental to the Network Administrator's consideration of risk on a network are issues of security namely; confidentiality, integrity and availability of information assets. The ability to effectively and efficiently manage the network and make room for growth without degradation in network performance are equally considerable concerns.

The segmentation of a significantly large Local Area Network with a possible annual growth rate of over 10% is undoubtedly the surest way to effectively manage the network, ensure security of information assets and make it scalable.

This paper seeks to assess the Pentecost University College(PUC) campus network at Sowutuom to determine how optimally segmented it is and the most practical option of using Virtual LANs to optimize the segmentation for effective and efficient security, management and scalability.

Based on the information gathered and analysis carried out on the network, a proposal is advanced to enhance the segmentation of the campus network with an eye towards the future growth.

1. Introduction

The use of networks to share information resources has become part and parcel of the corporate agenda of modern universities.

The continual increase in number of students and staff in PUC has lead to the increase in dependants on systems. The extension of university campus networks for usage by students and staff leads to a possible exposure of classified information such as the confidential, secret, and possibly top secret information about the university.

There is also the danger of exposing sensitive but unclassified information such as Technical Information, Budget Information, Financial/Payroll Information, Contract information to mention a few.

The staff population averages 130 while the annual student population averages 1700; there are about 170 user workstations on the PUC Local Area Network with 5 servers.

The exposure of information is possible once there is no segmentation of the PUC network. Possible vulnerabilities include students accessing staff computersfrom across the unsegmented network. Segmenting means that available bandwidth is used more efficiently because there is less traffic both within and between segments of a network.(Sportack, p.156)

Manageability of the network is always a challenge when there is no segmentation regardless of software available to monitor and maintain computer systems. These management software can be divided into hardware monitoring and software monitoring solutions. Solutions that monitor the computer hardware, like temperature and power variations, are hardware monitoring systems whereas software that manages software driven services are referred to as software monitoring

systems. Emphasis on manageability however has to do more with using manageable switches.

The challenge of scalability refers to how well a hardware or software system can adapt to increased demand. A scalable network system would be one that could start with just a few nodes but can easily expand to thousands of nodes. Scalability is an extremely important feature because it implies investment can be made in a system with confidence without outgrowing it.

The desire, however, to stay ahead of the competition while minimizing cost by leveraging technology means the assessment of risk in terms of vulnerabilities and threats to PUC's information assets is driven by pressure to achieve results.

It is uncertain whether the risk of exposing information assets, the challenge of managing a non segmented network effectively and the readiness for scaling the PUC network has drawn management attention.

There is the temptation to wait till disaster strikes before necessary precautions are put in place confirming the good old saying that "necessity is the mother of inventions".

This paper in turn suggests the creation of Virtual Local Area Networks (VLANs) to solve the three major issues to be addressed namely; security, manageability and scalability.

2. CURRENT SITUATION

PUC's current Local Area Network is non-segmented which is not ideal. There are fourteen 24-port non manageable Ethernet switches on the entire PUC campus with the total number of users (workstations) on the PUC Local Area Network being 170 with 5 servers at the moment.

There are four Wireless Access Points located at various blocks in the school spanning a 50 meter radius respectively.
The servers are namely Internet Proxy running Squid on Ubuntu Linux platform, DHCP on Ms Windows 2003 Server, McAfee Antivirus running on Windows 2003 Server, FACT for Accounts and Integrated School Management System(ISMS).

The current network setup has all systems resident on a single broadcast domain in a hierarchical star-bus topology using the Ethernet (CSMA/CD) technology as the access method on the network.
Physically computers within the same building use Unshielded Twisted Pair Cat5 cables for connectivity while in between blocks is predominantly Fibre Optic cabling.

The identified critical assets are servers:- DHCP running on Microsoft Windows 2003, Ubuntu Proxy server on Linux and used Internet access, The following applications systems were also identified:- Academic Records administered with the ISMS(Integrated School Management System), FACT accounting software used by the accounts department and the McAfee Antivirus software. There are no tools for bandwidth monitoring and Networking Devices like routers and switches.

The current setup and method of access raises the following possible issues that are worth considering with regards to the need for segmentation of PUC network.

2.1 Security

As students, staff and laboratory computers reside on a single broadcast domain, all PUC staff computers are exposed for exploitation if there are any known vulnerabilities. This situation makes it possible for especially individuals' computers (laptops) used from the locations where the IT department has limited administrative control to be used when intended to scan/sniff the PUC network for any vulnerabilities and possible exploitation.

Computers under the IT department's jurisdiction being laboratory computers, lecture hall computers and office computers are restricted from having the access privileges to scan or sniff the entire PUC network for such vulnerabilities.
It is also important to mention that causing a Denial of Service attack on the network is quite easy to

achieve given the single broadcast domain setup currently in operation.

2.2 Manageability

With the present network infrastructure, there are fourteen of 24-port non manageable switches with 4 Wireless Access Points distributing three various ranges of IP addresses different from the cabled network.

The use of Ethernet switches campus wide implies that each machine plugged onto the network resides in a unique collision domain. The existence of a single broadcast domain without manageable switches makes it almost impossible to determine the exact location of equipment/switches on the network.

The non-availability of manageable switches on the network makes the change management of switches a challenge. This in turn poses further difficulty to troubleshooting of situations where individual workstations flood the network.

2.3 Scalability

Considering the need for expansion of the network to meet future needs, it is imperative that this expansion is done in an orderly manner to ensure the continual availability of services that are required over the network.

Change and growth in any environment can introduce loopholes, overlaps, missing objects and oversights that can lead to new vulnerabilities.

Currently, systems are added to the network as and when needed with general expansions also carried out in a similar manner without the necessary thorough documentation and planning as required.

3. OBJECTIVES OF THE STUDY

The objectives of this study is to determine and clearly outline the measures that need to be taken to ensure the PUC network and IT infrastructure are effectively managed, secure and setup to make room for growth and expansion.
This in effect ensures namely;

3.1. The understanding of performance trends and expectations for the systems from network through applications.

3.2. Better troubleshooting by quickly identifying probes, diagnosis and fixing before end user notices thereby increasing reliability and availability. This enables users accomplish work more effectively and maximize productivity.

3.3. To ensure that security of the system is not compromised by ensuring confidentiality and integrity of information with an efficient and effective audit and accounting system.

3.4. Enough room is made for future growth with continual improvement in services and reduction of bottlenecks, effective tuning and optimization of systems to improve Quality of service and balance workloads.

3.5. To provide a cost effective phased approach to implementing the solution.

4. LITERATURE SURVEY

Typically, network traffic is concentrated between certain specific groups of users or workgroups. While traffic is heavier within workgroups, there is less traffic between workgroups.

If all the workgroups are put on the same network then the available bandwidth is reduced due to the total traffic.

Therefore, it is a common practice to segment LANs so that traffic within a workgroup is contained within its segment and only traffic bound for other segments/workgroups is broadcast beyond the workgroup's segment.

A Switch may be used to isolate a group of computers on the network which share the same printers or files. The heavy traffic directed to those network resources remains within that segment - making traffic on the rest of the network lighter.

As indicated in Intel's white paper on Using Segmentation to Increase Network Performance (December 2004), Performance is also increased because computers are not wasting time processing unnecessary net traffic and network stability is increased because when faults occur they are limited to segments and do not affect the entire network Switches make intelligent decisions, based upon the MAC address of the source and destination, about whether or not to pass along a signal to the next segment.

Ideally, network growth is well planned and orchestrated in advance to meet the additional burdens of business growth. Too often, though, network expansion is reactive rather than proactive. Business growth just is not that predictable. This is especially true for rapid growth in small start-ups, for consolidating branch offices into a regional office, or even in the acquisition-fueled growth of a multinational corporation size is no antidote for growth pains. While information technology (IT) managers try to plan for network growth, rapid or unexpected growth can stretch IT budgets and staff to the limit. Then the overriding objective becomes, "Let us just get something up and running right now." This, in turn, may result in missing the full potential for realizing greater network performance and scalability, leaving the IT staff to face major performance enhancements in the future. Fortunately, IT managers can mitigate the burdens of rapid growth by using network segmentation. Segmentation is a quick and cost-effective method for multiplying network bandwidth, depending on the number of segments used.

Additionally, performance gained through segmentation can be further augmented by various other upgrades, including upgrading servers from Fast Ethernet (100 Mbps) to Gigabit Ethernet (GbE), replacing dumb hubs with smart switches, and adding switched redundant links for higher network reliability.

The basic function of segmentation is to split traffic loads, thus alleviating bottlenecks. This is, in essence, comparable to changing a two-lane highway into a four-lane highway. More traffic flows quicker. Add another segment more lanes and even more traffic can flow quickly.

In addition to enhancing throughput, segmentation offers network administrators other advantages, such as high security and reliability. These can be gained by careful definition of segments and judicious selection of the implementing hardware.

Juniper Networks, Inc's white paper in 2006 on Network segmentation describes VLANs as used in widely distributed computing environments, and carrier (managed services) environments as a means to identify and then segment traffic at a very granular level.

Virtual Local Area Networks

Cisco's Network Security Principles and Practices 2003 describes VLANs as a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. Reconfiguration of the network can be done through software rather than by physically unplugging and moving devices or wires. (p.105)

Cisco Inc's paper on VLANs further explains that VLANs can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate bridge group for each VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management.

None of the switches within the defined group will

bridge any frames, not even broadcast frames, between two VLANs. Several key issues need to be considered when designing and building switched LAN inter-networks.

LAN Segmentation
Security
Broadcast Control
Performance
Network Management
Communication Between VLANs

LAN Segmentation

VLAN technology enables logical networks to overlay the physical switched infrastructure such that any collection of ports on the LAN can be combined into an autonomous user group or community of interest. The technology logically segments the network into separate Layer 2 broadcast domains whereby packets are switched between ports designated to be within the same VLAN. By containing traffic originating on a particular LAN only to other LANs in the same VLAN, switched virtual networks avoid wasting bandwidth, a drawback inherent to traditional bridged and switched networks in which packets are often forwarded to LANs with no need for them. Implementation of VLANs also improves scalability, particularly in LAN environments that support broadcast- or multicast-intensive protocols and applications that flood packets throughout the network.

Security

Segmentation also improves security by isolating groups. High-security users can be grouped into a VLAN, possible on the same physical segment, and no users outside that VLAN can communicate with them.

Broadcast Control

Switches essentially isolate collision domains for attached hosts and only forward appropriate traffic out to particular ports, VLANs also provide complete isolation between VLANs. A VLAN is a bridging domain and all broadcast and multicast traffic is contained within it.

Performance

When users are logically grouped, it enables the respective groups to make intensive use of a networked system assigned to a VLAN that contains just that specific group and its servers. That group's work will not affect other users.
The VLAN configuration improves general network performance by not slowing down other users sharing the network.

Network Management

The grouping of users into various logical groups facilitates easier network management. With the advent of manageable switches, it is not necessary to pull cables to move a user from one physical network to another. The various additions, moves, and changes are achieved by configuring ports into the appropriate VLAN using manageable network switches.

Communication Between VLANs

Communication between VLANs is accomplished through routing, and the traditional security and filtering functions of the router can be used. Cisco IOS software provides network services such as security filtering, quality of service (QoS), and accounting on a per VLAN basis. As switched networks evolve to distributed VLANs,

Centralized versus Decentralized Information Systems

Patrick Wall's paper on "Centralized versus Decentralized Information Systems in Organizations", coherently and vigorously discusses the two schools of thought as enumerated below.

Centralization of Information Systems refers to the allocation of all IT resources to one particular business unit that provides IT services to the whole firm (Gordon & Gordon, 2000). This typically would leverage on convenience in control and cost saving.

Decentralization of Information Systems on the other hand gives individual business units autonomy over their own IT resources without any major considerations over other units unless it is essential to the overall organization policy (Gordon & Gordon, 2000). Decentralization typically tends to be more flexible with control given to individual business units.


PENTECOST
UNIVERSITY COLLEGE
1st
CONGREGATION
COMING SOON AT THE JAMES MCKEOWN AUDITORIUM

Advantages and Disadvantages of Centralized Information Systems (Kroenke & Hatch, 1994) outlines the advantages of Centralized systems as they provide centralized control using established technology and vendors, thus it involves less technical risks, duplication of effort, resources and expertise thereby saving cost and time.

On the other hand, the information systems professionals who install and operate such systems are also expensive. Due to one central system carrying out all the requested tasks, this system is obviously going to be much slower than a decentralized arrangement where each business unit has its own autonomous system for local tasks. Lastly, there is the danger of total shutdown of operations upon the failure of the centralized system.

Advantages and Disadvantages of Decentralized Information Systems: Customization for local processing is possible hence there is increased autonomy (Hodgkinson, 1996), thereby leading to better organizational flexibility and responsiveness. Startup costs are relatively low (Kroenke & Hatch, 1994). Another key advantage is that reliability is increased greatly because multiple computer systems are involved; if one computer system fails other part of it will still be able to function.

Decentralized Information Systems on the other hand leads to a duplication of resources, effort and expertise, which wastes time and causes cost to increase. Due to the lack of a centralized administration and control of decentralized systems, conflicting ideas and clashes in policy arise leading to delays and inefficiency. (Kroenke & Hatch, 1994).

5. METHODOLOGY

The main approach is to observe the current PUC setup taking into account the underlying topology, technology, components and services that run on the PUC network.

With knowledge of this, there could then be a qualitative analysis of information gathered with consideration of the effective and efficient setup of manageable, secure and scalable systems.

The analysis would involve the identification of limitations of the current setup and subsequently the proposal of solutions to the current limitations. Ultimately, there would be a proposal for accommodating future growth while ensuring continual improvement in services and reduction of bottlenecks, effective tuning and optimization of systems to improve quality of service and balance workloads.

It needs to be mentioned that given the processes and procedures binding PUC as an institution, it is relatively more feasible approaching the problem with a phased solution.

6. DATA COMPILED FOR STUDY (PUC Network Description)

6.1 Distribution of Workstations and Servers on Block basis

The Administration Block has two computer labs of 68 and 44 computers respectively with a total of 21 additional staff computers. There are two servers within the block namely the DHCP and Antivirus Servers. The Administration Annex has 20 Workstations with the Auditorium and Lecture blocks having 8 and 11 Workstations.

6.2 Switches and Access Points

The switches, access points and switch cabinets are distributed on the campus as depicted in diagram 6.5; Nine switches located in the Administration block, one in the Auditorium, two in the Lectures block and two in the Administration Annex. The four Linksys Wireless Access points are distributed as follows; one is located in the Administration block, two in the Lecture block and one in the Administration Annex.

6.3 Cabling, Technology and Addressing

All systems are resident on a single broadcast domain in a hierarchical star bus topology. Using the Ethernet(CSMA/CD) technology as the access method on the network, computers connect to each other within same blocks using Unshielded Twisted Pair Category5 cables for connectivity, while in

between blocks Fibre Optic cabling is predominantly used . The Wireless network operates WiFi network to which both students and staff connect within the 2.4GHz frequency range.

The IP address range is 100.1.1.0/16 being issued out to all machines on the cabled network while the various access points issue different IP ranges namely; 192.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24

6.4 Servers

The major hardware and software servers identified are Ubuntu Proxy server on Linux and used Internet access, DHCP running on Microsoft Windows 2003, Academic Records server administered with the ISMS(Integrated School Management System), FACT accounting software used by the accounts department and the McAfee Antivirus software. There are no server tools for monitoring of Networking resources.

However, considering the cost involved in changing PUC's current non-segmented network into an optimally segmented one, it will be most prudent to go about the process in phases.

The segmentation will be done by making use of the same physical media to create independent logical networks within a physical network. Several VLANs can co-exist within such a network.

This would increase the number of broadcast domain but aid in network administration by separating logical segments of the Local Area Network; in the case of PUC the segments would be separate for students, staff (various departments) and residents. This is achieved by the configuration of VLANs through software rather than hardware however, this can only be achieved by the use of manageable switches which support the implementation of VLANs.

Given the layout of PUC's campus network as described in section 6 and shown in the attached PUC layout diagram and also the fact that the network has no single manageable switch, It is imperative that manageable switches are acquired to initiate the entire segmentation process.

In this regard, it is recommended that the project starts with the purchase of seven of 24-port manageable switches with fibre/UTP modules.

The segmentation would have unique VLANs for all computer laboratory computers, academic registry, accounts department and all other staff respectively. This configuration is based on the identified information asset of the institution.

The Wireless network can be segmented via the use of MAC addresses of staff computers to automatically distinguish lecturers from students upon connection to the wireless network. This implies the Access Points would need to have the capability to identify MAC addresses and subsequently associate it with the appropriate VLAN on the cabled network.

7.1 Phase One

The first phase will involve the installation of manageable switches at the following locations and a spare switch will be kept for emergencies.

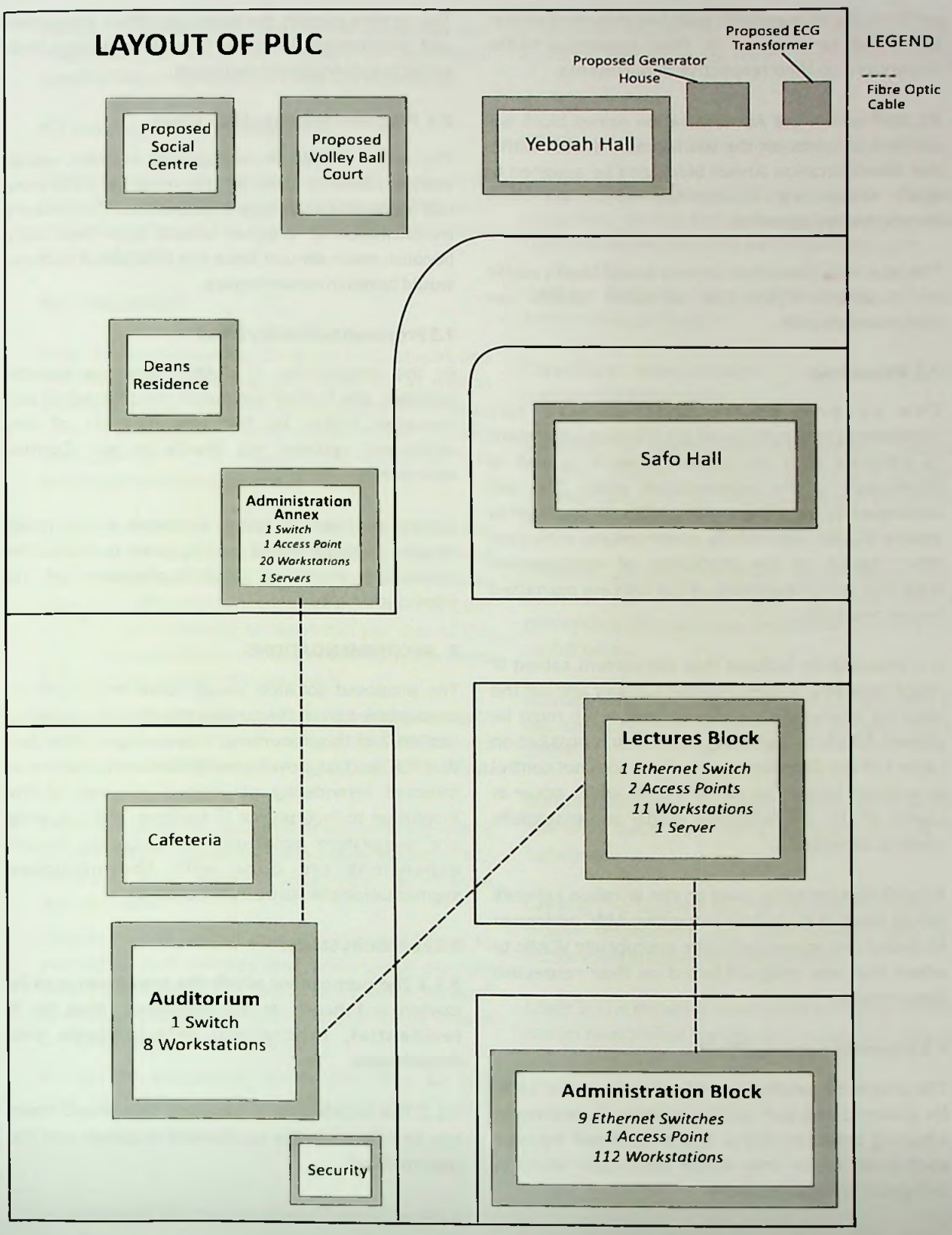
- Administration Annex
- Auditorium
- Administration
- Lectures Block

All the computer lab computers will be connected to non manageable switches and then crossed-over to a single port on the manageable port within the Administration block and assigned a unique VLAN eg-VLAN2.

All staff within the Administration block will connect to other ports on the manageable switch within the Administration block and be assigned to their respective VLANs dependent on their respective departments.

All staff within the Lectures block will connect to ports on the manageable switch within the Lectures block and be assigned to their respective VLANs dependent on their respective departments.

All staff within the Auditorium block will connect to


LAYOUT OF PUC
Proposed ECG Transformer
Proposed Generator House
LEGEND
Fibre Optic Cable
Proposed Social Centre
Proposed Volley Ball Court
Yeboah Hall
Deans Residence
Safo Hall
Administration Annex
1 Switch
1 Access Point
20 Workstations
1 Servers
Lectures Block
1 Ethernet Switch
2 Access Points
11 Workstations
1 Server
Cafeteria
Auditorium
1 Switch
8 Workstations
Administration Block
9 Ethernet Switches
1 Access Point
112 Workstations
Security

ports on the manageable switch within the Lectures block and be assigned to their respective VLANs dependent on their respective departments.

All staff within the Administration Annex block will connect to ports on the manageable switch within the Administration Annex block and be assigned to their respective VLANs dependent on their respective departments.

The Internet connection servers would ideally reside on a unique VLAN that all other VLANs can communicate with.

7.2 Phase Two

The second phase will involve the installation/configuration of the Wireless equipment to integrate with the cabled network as well as conforming to the segmentation policy. This will subsequently be refined with a VTP configuration to ensure VLANs successfully communicate with each other based on the resolution of management regarding which segments of the LAN are permitted to communicate.

It is essential to indicate that the current cabled IP range issued by the DHCP server is public and not the ideal for a private LAN; this current setup must be altered. Much as logical segmentation is possible on Layer 3 of the OSI reference model it does not control broadcasts hence the use of VLANs which occur at Layer2 of the OSI reference model and essentially controls broadcasts.

All staff laptops to be used on the Wireless network would need to have their respective MAC addresses recorded and appended to the appropriate VLANs to which they are assigned based on their respective departments.

7.3 Proposed Security Effect

The proposed solution would separate virtual LANs for students and staff with respective departments; ensuring their respective traffic does not traverse each other hence they would technically reside in different broadcast domains.

This in turn curtails the exposure office computers and information stored on them from having their possible vulnerabilities exploited.

7.4 Proposed Manageability Effect

The use of VLANs on manageable switches would enable administrators of the network determine traffic patterns and usage trends better. The network troubleshooting process would also invariably become much simpler since the location of systems would be much easier to track.

7.5 Proposed Scalability Effect

By the introduction of VLANs using manageable switches, any further expansion can be tracked and managed better by the identification of any additional systems via Media Access Control addresses.

Control over various added segments is also made simpler as there would be the need to factor the expansion purpose in the planning of its interconnectivity.

8. RECOMMENDATIONS

The proposed solution would solve the problems encountered given the current situation described in section 2 of this document. However given the fact that PUC is a fast growing institution with a culture of frequent remodeling of various sections of the institution to incorporate IT facilities, the following are suggestive solutions to ensuring future expansions are done with the proposed segmentation plan to be incorporated.

8.1 Feasibility Study:

8.1.1 The purpose for which the expansion is to be carried out needs to be identified, thus be it residential, laboratory, office usage and department.

8.1.2 The location for expansion, this would assist one to determine the equipment required and the cost involved.

8.2 Analysis and Design of Network Extension:

Based on the identified purpose of extension and magnitude, it would be possible to determine which VLANs (segments) to place the extension.

8.3 Building and Implementation:

With all the above measures provided, there could then be installation, configuration, testing and implementation of the expansion's integration into PUC's network.

9. CONCLUSION

With the ever increasing size of the PUC network and the challenge of keeping systems secure as well as making it possible for users to have access to network services at all times, there is no doubt that effective management of the network and the traffic that traverses it is the way forward.

The segmentation via VLANs would increase the number of **broadcast domains** but reduce the size of each **broadcast domain.** This in turn reduces network traffic and increases network security both of which are currently hampered in the case of the single large broadcast domain as well as make room for expansion to meet future needs.

It would also enhance control over multiple traffic types and ease the management difficulties encountered on the network by the creation of sub networks.

The most pertinent issue that needs to be addressed is the expertise to manage the segmentation of the network with careful attention to change management.

Change in any secure environment could lead to oversights and overlaps that bring about possibly new vulnerabilities and complexities hence the need to manage change to ensure changes do not lead to compromised or reduced security.

Change of equipment would no more be just plug_and_play, but one would need to thoroughly understand the current infrastructural layout and the impact of the changes made to the existing systems.

GLOSSARY

VLANs :Virtual Local Area Networks

Broadcast Domains: A local network where broadcasts on the network can be seen/received. Typical domains would be an Ethernet network.

Collision Domain: A group of machines contending for the same bandwidth.

Classified Information: Trade secrets and confidential information

Sensitive but Unclassified Information : Technical secrets, Budget, Information, Financial/Payroll Information, Contract Information and Information for Office Use only.

Ethernet switches: Ethernet Switch automatically divides the network into multiple domains contending for respective bandwidth on the various switch ports.

Manageable Switches: Configurable switches that can be monitored via monitoring software such as SNMP.

MAC Addresses: A hardware address that uniquely identifies each node of a network in IEEE 802 networks.

Layer 2: The Datalink layer of the ISO's OSI reference model responsible for flow control and error notification in network transmissions.

Layer 3: The Network layer of the ISO's OSI reference model responsible logical addressing, path selection and connectivity.

REFERENCES

Centralized versus Decentralized Information Systems in Organizations, http://emhain.wit.ie/~pwall/CvD.htm, Retrieved April, 26, 2009

Cisco IOS Switching Services Configuration Guide, Retrieved May 8, 2007 from http://www.cisco.com/en/US/products/hw/routers/ps221/products_configuration_guide

Dorothy E Denning, *Information Warfare and Security,* Addison Wesley, 1999

Gordon, J. & Gordon, S. (2000). *Structuring the Interaction between IT and Business Units: Prototypes for Service Delivery,* Information Systems Management, Winter 2000, Vol. 17, No. 1, Auerback Publications, 2000 Corporate Blvd., NW Boca Raton, FL, USA.

Tipton H. F. and Micki Krause, *Information Security Management Handbook,* Boca Raton, CRC Press LLC,

Hodgkinson, S. (1996). *"The role of the Corporate IT Function in the Federal IT Organization",* in "Information Management: The Organizational Dimension" by Earl, M., 247-269, Oxford University Press, Great Clarendon Street, Oxford, New York, USA

Intel® Advanced Network Services, Retrieved March 15, 2009 from www.intel.com/network/connectivity/resources/doc_library/white_papers/30514101.pdf

ISO/IEC 17799 Part I *Code of Practice for Information Security Management*, First Edition 2000-2001.

Juniper Networks, Retrieved May 9, 2007 from www.juniper.net/products/integrated/network_segmentation.pdf

Kroenke, D. & Hatch, R. (1994). *Management Information Systems,* McGraw-Hill, Watsonville, CA, USA 2003.

Retrieved March 9, 2009 from www.dell.com/downloads/global/power/ps4q04-20040154-Intel.pdf

Retrieved April 27, 2007 from www.hermit.cc/teach/ho/lan/segment.htm

13. S Bosworth and M.E. Kabay, *Computer Security Handbook 4e*, Wiley & Sons, 2002

Stuart McClure, et al *Hacking Exposed, network security secrets & solutions 4e,* McGraw-Hill / Osborne

ABOUT THE AUTHOR

Paul Danquah is a Lecturer with the Faculty of IT, Pentecost University College. He has a background of MSc Information Security from Anglia Ruskin University (UK), BSc HONs in Computing from the University of Greenwich (UK), Graduate Diploma in MIS and the professional certifications MCSE and CCNP.