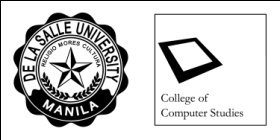
****De La Salle University

College of Computer Studies

AY 2018-2019

### LBYADM3 Case Study

**Objectives:**

This case study is formulated as a supplement to classroom instruction in order for students to demonstrate the following:

* The ability to analyze a set of given requirements; and
* Knowledge of a variety of concepts and best practices, as well as technical know-how in designing a network that fits the requirements.

**Background:**

The Computer Technology Department manages 4 instructional laboratories (G403, G405, G407 and G408) used for student classes and research projects that deal with the fields of electronics, automation, networking, and information security. These labs host computers and equipment that support the learning and hands-on work in these areas for students. The sections below describe the current laboratory structure and operations and the specific requirements needed for

***Key People***

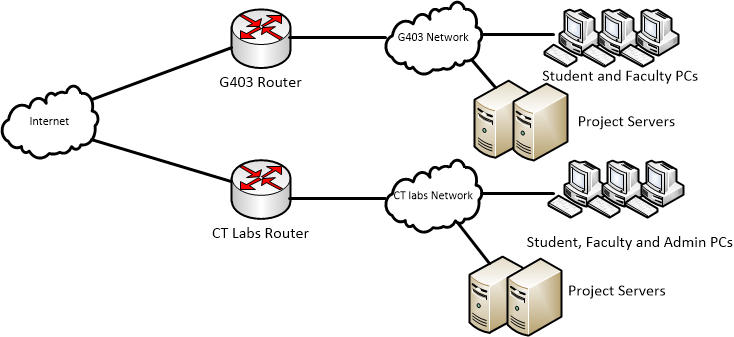
The users of the laboratories include:

1. Administrators – These include the CT laboratory coordinator who manages the overall operations of all 3 laboratories, the Center for Networking and Information Security (CNIS) lab administrator who specifically manages the operations of G403, and the lab technicians who are responsible for laboratory maintenance. Administrators generally are in charge of providing the equipment and software needed for classes, enforcing lab policies, and monitoring laboratory usage.
2. Faculty – These include primarily CT faculty members who regularly hold classes and lead research projects in the laboratories. Faculty members from other departments may also use the laboratories on a case to case basis with the approval of CT lab coordinator depending on the nature of the work they intend to do in the laboratories.

1. Students – These include BSCS-CSE, BSCS-NE and BSIT students who take classes held in these laboratories and who do their research and project work inside the laboratories. These also include occasional guests who temporarily use the laboratories for an activity or seminar.

***Laboratory Structure and Facilities***

The laboratories currently connect to 2 separate networks, both of which provide Internet connectivity to users through NAT at the network edge. G405, G407 and G408 are connected together, while G403 belongs to its own network. Both laboratory networks were designed with a flat network topology wherein administrators, faculty and students including any personal devices brought in by users all belong to the same subnet. The figure below illustrates the topology of the laboratory networks.



1. G407 – The G407 laboratory is used for electronics and control system classes. The laboratory has 8 PCs for student use during their experiments and a faculty PC.
2. G408 – The G408 laboratory is used only for research. Faculty and students who need a workspace for their projects such as their thesis are commonly assigned spaces in this laboratory. The laboratory provides Internet access, but does not have any permanent computers. Users who are assigned to this lab normally bring in their own equipment (e.g. PCs, servers, laptops, etc) or borrow them from the laboratories with the permission of the CT lab coordinator depending on the nature of their respective projects.
3. G405 **–**  The G405 laboratory is used for all types of classes including electronics, networking and security. The laboratory has 13 PCs for student use during their experiments and a faculty PC.
4. G403 – The G403 laboratory (a.k.a CNIS) is used for networking and security classes. The laboratory has 22 PCs for student use during their experiments and a faculty PC. Some servers used by student research projects (e.g. thesis / capstone) can be temporarily hosted here with the permission of the CNIS lab administrator
5. Technicians’ Area – The technician’s area is a separate room which serves as the work area of laboratory administrators and technicians. There are 3 PCs in this room that are wired to the same physical network as G408, G405 and G407.

**Project Specifications:**

You are tasked to define security policy suitable for an instructional laboratory in relation to Internet and general network use, as well as implement the network security controls that support the policy. The following lab structure, operational changes and assumptions will need to be considered:

* The laboratory network should now unify all 4 laboratories including the technician’s work area such that they connect to a single network infrastructure. Assume that physical rewiring of the network is possible. The following are the external IP addresses available to the network:
  + External addresses : 172.16.4.20x and 172.16.4.21x/24 (x=group num) webserver or external WAN
  + Gateway : 172.16.4.1
  + DNS : 172.16.4.4
* Students and faculty will need Internet connectivity to web (HTTP/s), email and instant messaging. Email services are hosted by Gmail; and users are expected to connect using both browsers and email clients such as Outlook or Mozilla Thunderbird. Instant messaging on the other hand, primarily uses Viber only. Lab administrators need access to all services due to the occasional task of testing access to new services when required by classes.
* Website access needs to be controlled especially during class hours to ensure that the finite bandwidth available to the laboratories is properly managed. In general, sites that are not related to the work expected to be performed in the laboratories by the user groups need to be restricted. Furthermore, sites that may aid in criminal activity or have potential to disrupt lab operations should be restricted for all groups. Separate web access policies may be defined for different user groups depending on the nature of their work.
* A web server hosting the CT research project website will now be added to the laboratory network. The web server runs both HTTP and HTTP/S services and is expected to be accessible at any time to both lab network users and the public Internet.
* Individual servers that are set up for research projects of faculty and students will all be physically located inside G408. They can be accessible from anywhere inside the lab network, and also from the Internet if the groups wish to do so outside DLSU after regular working hours. Research servers that will be setup for external access cannot be allocated their own public IP addresses and hence will have to rely on a private connection if they are to be accessed from outside the lab / school.
* Any additional facilities needed by students or faculty (e.g. equipment / software / network access) for their work are coursed through lab administrators. Acquisition and installation of these are performed by lab admin to ensure that they do not have adverse impact to lab operations.

**Submission Requirements:**

This case project will be performed in groups of 4 students each. Each group must provide documentation of the security policy and network design, and demonstrate a proof of concept of the network with the security mechanisms that support the security policy. The following outlines the details of each requirement and corresponding deadline:

|  |  |  |
| --- | --- | --- |
| **Deliverable** | **Specifics** | **Due Date** |
| Draft Formal Security Policy | Complete sections, with policies focusing on Internet access and network usage. Submit document through upload or link via Canvas.  Note: Security policy may be updated as the case study progresses | Completed |
| Draft Documentation | Includes network topology and outline of security-related configurations on infrastructure devices. Documentation should be detailed enough to replicate the configuration. Submit document through upload or link via Canvas.  Section 1: Logical Network topology  Section 2: Firewall and NAT rules / config documentation  Section 3: AAA config documentation  Section 4: Remote Access config documentation  Section 5: Web filtering rules / config documentation  Note: This is 1 document only, with 5 sections. Previous sections may be updated as the case study progresses. | March 25, 2019  March 25, 2019  April 15, 2019  (part of final doc) |
| Partial Proof of Concept | Demo of working setup with partial security controls. Hosts may be demoed using a combination of actual devices and VMs. The PoC should include the following as a minimum: complete network segments, firewall filtering, web server external access. | March 25, 2019 |
| Final Formal Security Policy | Complete sections with updates if applicable | April 15, 2019 |
| Final Documentation | Complete from sections 1-5 with updates to relevant sections if applicable | April 15, 2019 |
| Complete Proof of Concept | Demo of working setup with complete security controls. Hosts may be demoed using a combination of actual devices and VMs. The network setup need not include all devices, but a representative device of each user group / subnet will need to be included in the demo. | April 15, 2019 |

**Rubric for Assessment:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Wt** | **Exemplary - 7 pts** | **Satisfactory – 5 pts** | **Developing – 3 pts** | **Beginning - 1 pt** |
| Detailed Security Policy | 1 | Security policy is well-written, easy to comprehend, and is complete with all necessary sections. Has negligible technical or grammatical issues. | Security policy is complete with the necessary sections, but contains minor technical or grammatical issues | Security policy lacks minor sections and /or needs improvement is terms of technical writing and proper grammar | Security policy lacks several major sections and is generally badly written |
| Well-planned Network Topology | 1 | Network design is well planned with the proper set of infrastructure devices and complete network segments that allow reasonable protection of assets and users, and easy segregation and identification among users | Network design is well planned with the proper set of infrastructure devices and complete network segments that allow reasonable protection of assets and users and segregation among users. | Network follows basic rules of hand for segmentation. The correct infrastructure devices are used; however some design issues may allow easy compromise of certain assets. | Network design does not have well-planned segments and is limited to flat network design |
| Network Access | 2 | Network access control mechanisms such as firewalls are fully working. The necessary access control measures are implemented with a well-planned balance between control and accessibility | Network access control mechanisms such as firewalls are fully working. The necessary access control measures are implemented; however, there are some issues with ease of access | Network access control mechanisms such as firewalls are working but have a major control or some minor control errors | Network access control mechanisms such as firewalls are not working (e.g. no access control or prevents functionality of major operational requirements) |
| Remote Access | 1 | External access is provided and is adequately protected | External access with some minor security issues | External access is implemented but has some functionality issues | No form of external access is provided or mechanisms implemented are not working |
| Presentation | 1 | The group can present the informal security policy, can explain the security implementation in the network  The group can answer questions and explain why certain implementation were favored over another | The group can present the informal security policy, can explain the security implementation in the network  The group can answer questions but has difficulty explaining why certain implementation were favored | The group can present the informal security policy, can explain the security implementation in the network  The group is not able to answer questions | The group is not able to present the informal security policy, explain the network topology design, and explain the security implementation in the network |
| Work Contribution  (to be evaluated by peers) | 1 | Member has contributed a fair share to the project and has commendable work ethic | Member has contributed a fair share to the project and has satisfactory work ethic | Member has contributed less than other members of the group or has some issues in work ethic | Member has minimal contribution to the project and is generally difficult to work with |