SUMMATIVE ASSESSMENT

[FINAL PROJECT - 40% of the overall grade]

Submission due: May 5th, 2021 at 12:00 PM.

Final Project Brief

Computer Networks have emerged as the communication of 2 or more devices through different media, aimed at sharing resources. From personal devices networks such as phones connected via Bluetooth to exchange music files; to sharing a local printer in a small office; to metropolitan areas such as province hospitals that share patients data and finally to global networks such as social media and banking systems for the ease of money transfer across continents in a matter of milliseconds.

Services such as the world wide web, known to most today as the Internet, play an important role in the sharing of information in today's age, facilitating the rapid of information consumption through online newspapers, online learning platforms, telemedicine and so much more. Hadn't been for the ability of resources sharing of computers, today we would be living in a completely different world.

The Goal of This Exercise

The goal of this exercise is to instill in learners the skills needed for planning, designing, implementing, configuring, and securing a network that facilitates the sharing of information and resources at different levels of an organization and the wider Internet.

Organization Description and Network Requirements

Silverback is an organization that specializes in wildlife conservation headquartered in Kigali and has offices in Kenya and Mauritius. Silverback has just launched its office at the Kigali Heights building and you have been tasked to design and implement its network, having in mind that it will need a reliable connection with its offices in Kenya and Mauritius but also have access to the Internet to facilitate their work with other partners. The following details have been shared with you and they should guide you in designing and implementing this particular network:

1. **Part 1**
    a. Silverback at KH will have 3 teams (Marketing, Finance, and IT) with 10 employees located on 2 different floors. On floor 1, there will be 4 employees; 1 IT officer, 1 finance officer, and 2 marketing officers, while on floor 2 there will be 6 employees; 1 IT officer, 1 finance officer, and 4 marketing officers.
    b. Each team will have access to its own file server that other teams should not have access to and a shared printer among the teams. These shared resources will be located on floor 2.
    c. Marketing officers on both floors of the office prefer to connect to the network wirelessly, while the IT and finance teams prefer

ethernet - IEEE 802.3 connections because of security concerns and connection reliability.

d. After assessing the needs of the network users, you are required to come up with an IP addressing scheme that the network should adopt. Choosing which class of IP address to use, and the network segmentation using subnets.
e. Silverback's office is expected to grow really fast and hence it is recommended that you pay attention to how different resources such as servers and hosts on the network will get their addresses (static IP addresses vs dynamic IP addresses).
f. The file server is also playing the role of a web server that all teams should have access to since it hosts an intranet web page that the organization uses for newsletter and to communicate company-wide priorities.
g. On the same file server also runs a DNS server that facilitates reaching the intranet website using its domain name intranet.silverback
h. Using the same server, the users should also able to send emails to each other.
i. It has been recommended that you connect floors 1 and 2 on 2 separate routers using the OSPF interior gateway protocol. Since the number of users on both floors is expected to grow pretty fast, it is also recommended that users on each floor be connected to a switch.
j. The Kenya office has needs that are similar to those of floor 1 of the Kigali Heights office while Mauritius has a local network similar to the floor 2 network. Refer to point **a.** for respective network needs.
k. Silverback offices in Kenya and Mauritius are both connected to each other and to the router on floor 2 of the Kigali Heights office using an exterior gateway protocol (BGP).

l. Part 1 Deliverables:

i. A Lucidchart network design for Silverback's offices which should contain at least 20 end devices, 4 switches, 4 servers,

1 printer, and 4 routers. Notes that provide a small description/role of each device on the network should be included.

ii. A packet tracer file (lastname_firstname-networks_final_project.pkt) that contains adequately configured networks as described above.

iii. The following services and protocols should be observed in your network design and implementation:
    1. IEEE 802.3
    2. IEEE 802.11
    3. IPv4 Addressing
    4. HTTP
    5. HTTPS
    6. DNS
    7. SMTP
    8. DHCP
    9. VTP (VLAN Trunking Protocol)
    10. OSPF
    11. BGP

2. **Part 2**
    a. Silverback has also identified the need to have an online presence that will improve its online reach to donors and to achieve the same you recommend them to use a cloud service, namely AWS. The following are the requirements you identify needed to successfully implement this goal:
        i. 2 Ubuntu Server instances on AWS, with one being public-facing and accessible via the Internet, and the back-end instance that will only be accessed privately via the public-facing server.
            1. An elastic public IP address should be configured for the public-facing instance to avoid changes in address records every time the instance is rebooted.
            2. On the public-facing instance, a web server should be installed to serve web pages to users as requested.

3. Through AWS's VPC you make sure only SSH and HTTPS inbound traffic to the public-facing server is allowed and as a precaution, you also take advantage of the Ubuntu Server built-in firewall to filter traffic coming in and out of the server.
4. On the backend server (which is not publicly accessible) you install Mysql that will host the database and other backend services.
5. Since you will need access to the Mysql database directly without needing to log in to AWS, you decide to deploy a VPN service (OpenVPN) you can use to gain access to the backend server.

b. Part 2 Deliverables:

i. The elastic public IP address of the public-facing instance
ii. Private IP addresses of the private and public-facing instances
iii. Install and configure UFW on the public-facing server
iv. HTTPS web server with an SSL/TLS certificate with the webpage reading "***Welcome to ALU Rwanda Networks Course***"
v. Mysql installation on the private instance
vi. Create an OpenVPN user: **networks** and password: **Rw&a@ALU2021**

3. Part 3

a. One of the finance team colleagues reaches out to you about a problem they are facing about being unable to access the publicly available web server that you just hosted on AWS, in order to troubleshoot where the problem might be, you decide to open Wireshark and capture only (using filters) HTTPS traffic to and from the Ubuntu server address. From the analysis, you notice that everything looks okay. You then decide to run an Nmap scan to determine if HTTPS traffic from (1.1.1.0/24 network which is your colleague is using) is being filtered by the server, which turns out to be the case. You then go ahead and make the

changes on the Ubuntu Server's firewall to allow traffic from the client.

b. **Part 3 Deliverables:**
    i. An HTTPS filtered packet capture (lastname_https_capture.pcap) of traffic between your local machine and the remote server(public-facing Ubuntu Server instance).
    ii. On the remote server, apply a rule to deny traffic destined for HTTPS on the remote server coming from 1.1.1.0/24
    iii. Save a file (remote_server_https.txt) of an Nmap scan of the remote server that confirms traffic filtering of the HTTPS requests from 1.1.1.0/24

Submission criteria

A PDF file name (eg: Ruti_Dauphin-Networks_Final_Project) that contains the following and formatted as follows should be submitted on Canvas:

1. Part 1
    a. A link to the lucidchart design of the implemented network.
    b. A link to the packet tracer file of the implemented network.
2. Part 2
    a. The public IP address of the public-facing instance.
    b. The private address of the public-facing instance.
    c. The private IP address of the private instance.
    d. OpenVPN username and password
3. Part 3
    a. A link to the Wireshark packet capture file.
    b. A link to the Nmap scan file of the public-facing server.