Assignment 2 – FIT9137 S1 2020

Submission instructions

Deadline: Friday, 12 June 2020 (11:55pm)

- **Submission format:** One PDF for the report. You can use any freely available PDF converter or lab computer to make a PDF file from an editable one. In addition, you need to submit the .imn file generated by the CORE network simulator.
- **Submission platform:** Moodle.
- **Files to submit:** You need to submit one file with your student ID as part of the name: StudentID_LastName_Assign2.pdf. You also need to submit your network simulator file for task 2.
- **Late submissions:**
  - Via special consideration request
  - Or, without special consideration request, you lose 10% of your mark per day that you submit late. Submissions will not be accepted more than 3 days late.

Plagiarism and Academic Integrity

It is an academic requirement that your submitted work be original. Zero marks will be awarded **for the whole submission** if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. – The University Plagiarism Policy applies to all assessments.

Marks

- This assignment is worth **12% of the total unit marks.**
- This assignment is marked out of **45 nominal marks.**

Network Design and bug fixing

Download your personalised CORE Simulator network from Moodle, by entering your student ID. Make sure the student ID matches the one in the simulator.

The configuration shows a (fictitious) company network. The company purchased a block of IP addresses (a class B network) and has subdivided it into an intranet server network, a client network, and several backbone networks.

The network configuration has a number of errors. Your task is to find and fix those errors, to implement new functionality, and to extend the network with a new subnet.

Submission: You need to submit your modified network configuration (the .imn file) through Moodle, and describe your fixes and changes along with screenshots (configuration, terminal, Wireshark capture etc.) in a report.

Tasks:

a) Set up static routing tables in all four routers such that the three networks containing computers (the clients, the www server, and the intranet server) can reach each other. Take into account the link speeds between the routers, to find routes that deliver good speed and latency (**you are not allowed to change the link speeds**). In the report, describe the reasons for the particular routes you chose.

   (10 marks)

b) Find **three errors** in the network configuration. All errors are in either the configuration of the IP addresses and masks and/or the static routing tables. For each error, describe **what** the problem is, **how** you found it, the **fix** you applied, and how you can **test** that the fix works.
   After fixing the errors, you should be able to execute the command lynx www.fit9137 successfully.

   (6 marks)

c) The network currently has no gateway to the Internet. We want to make router **R3** the gateway router. Add default routes to all other routers such that any packet whose destination is outside of the company network is routed via **R3**.

   (5 marks)

d) Add a **new subnet with 4 clients** that are connected to the existing network using a new router. The subnet is allocated the network address 192.168.200.0/24.
The new router should be named **External**. It connects to the gateway router **R3** and should be configured with a default route to **R3**. To get full marks, the clients need to be configured with DHCP, i.e., the new **External** router must be running a DHCP server. You can use router R1 and the clients in its subnet as an example of how to set up DHCP.

(12 marks)

e) The server with the label **www** acts as the company's public web server, and the server with the label **ssh** as the remote-login (secure shell) server. The company decided to update its security policy and implement a **Demilitarised Zone (DMZ)**. Your task is to implement a firewall on router **R3** such that:
   a. Any packets for the specific servers in the DMZ are accepted (HTTP packets for **www**, SSH packets for **ssh**, and DNS packets for **dnsserver**), as well as any ICMP packets for devices in the DMZ.
   b. Any packets from inside the company network are accepted.
   c. Any packets relating to connections that were established from inside the company network are accepted.
   d. Any SSH packets from the **ssh** server into the company network are accepted.
   e. Any other packets are blocked.

   Document the design of the DMZ, including the firewall rules you used, in your written report. Document **four test cases** that verify different aspects of your DMZ firewall. A test case would consist of a command executed on a particular device, e.g. a ping, lynx or ssh command, that shows the desired behaviour. Use the new subnet added in d) to test the behaviour for devices that are outside the company network.

   (12 marks)

Hints for testing: There are a number of things you can test. Try out whether the *ping* and *traceroute* commands work as expected between different pairs of devices. Remember that both commands require routing to work in both directions: Let's assume you ping from node A to to B, then the ping packet needs to be routed from A to B, but the response needs to be routed back from B to A in order for the ping command to display the result!

You can use the *lynx* command line web browser to test whether you can access the web server. The network contains a DNS server, so if a client is configured correctly, the command *lynx www.fit9137* should succeed.