FIT9137

Semester 2 2025

Assessment 3 Specification

Submission Guidelines:

- **Deadline**: Semester-2 Week-14 Tuesday 2025 [4th Nov 2025 11:55 PM]
- You need to submit
  - **(i) A network configuration file** (a CORE file, FirstName_STUDENT_ID.imn): containing the required changes to complete the assignment tasks.
  - **(ii) A report file** (PDF, FirstName_STUDENT_ID.pdf): containing descriptions of your work (max 2000 words).
- Both the files must be submitted via Moodle under a single submission link. Do not compress these two files into one and submit a compressed file. Such submissions may receive a mark of zero.
- A handwritten document is **not** acceptable and will **not** be marked even if converted and submitted electronically.
- Your assessment MUST show a status of "**Submitted for grading"** and you will receive an email confirmation for your submission. Assessment files left in **DRAFT** mode are **not** accepted and will **not** be marked. Make sure to finalise your submission by the deadline.
- It is the student's responsibility to make sure that the submitted files can be opened on a standard computer (without requiring specialised software), and that all contents such as images and texts shown are understandable/readable (in English). After uploading the files as **draft** (before **finalising** the submission), **we recommend you download your submitted files and check that they open and run properly. If the files are not readable, openable, or corrupted, then you may receive a mark of zero**. Once you finalise your submission, you will not be able to revise it.
- Written texts in your PDF must be submitted as actual texts, and **not** an image of a text. Accordingly, screenshots of typed texts as images are **not** accepted (of course, this rule excludes the screenshots you take to show the computer's display).
- This assessment will be submitted through Turnitin. For the CORE configuration file, you may see a warning/error message returned by Turnitin after you upload your files. That is completely fine and **you can simply ignore the Turnitin warning/error message for the IMN file**.

- All special consideration/extension requests must be submitted via https://www.monash.edu/students/admin/assessments/cant-complete

Marks: This Assessment is marked out of **100** marks, and it is worth **45**% of your UNIT total marks. You must submit both the CORE configuration file and the PDF report. If you submit only one of the files, you will receive a mark of zero.

Feedback: Your Tutor will provide you with marks and feedback (if your submitted PDF file and the CORE *.imn file are readable and markable)

Brief Description

Assessment will include the materials covered within Weeks 6-12. In particular, the Assessment will consist of questions related to network and transport layers, structures and functions of local area, backbone and wide area networks, and network security. The format of the student submission will be a written report and a network configuration.

Learning Outcomes covered

This Assessment covers material from Weeks 6-12. This is an **individual** Assessment. By completing this Assessment, you will understand the learning outcomes 3 to 6.

- Examine networks using the underlying fundamental theories, models and protocols for data transmission.
- Analyse and formulate the functions and architectures of (wireless) local area networks, wide area networks and the Internet.
- Identify cybersecurity threats and ethical considerations on the Internet.
- Apply and implement cybersecurity enabling techniques and countermeasures such as virtual private networks (VPN).

Academic Integrity

This is an **individual** Assessment and group work is prohibited. For this Assessment, students will use the core network emulator to complete a series of tasks on an individual core configuration file that is generated for every student. It is an academic integrity requirement that your submitted work be original. Penalties will be applied to the whole submission if there is any evidence of copying, collaboration, pasting from websites, or copying from textbooks. When asked to use the Internet, books, or other academic resources to answer a question, it does not mean to copy the text verbatim from the source. You must write the answers in your own words such that your understanding of the answer is evident. You must always cite your references within the text and list them at the end of the report. Academic integrity policies apply to all assessments. You can refer to this link below for more information:
https://www.monash.edu/student-academic-success/learnhq/maintain-academic-integrity

Penalties

Late submissions will result in a 5% deduction of the total marks per calendar day (up to 7 days). For example, if you get 80/100 marks originally and submit 2 days late, then you would get a 10-mark penalty (5 marks/day) and your final marks would be 70/100. Note that the total number of late submission days is calculated by rounding up, e.g., if a submission is strictly more than 5 days (5 days

+ 1 hour and at most 6 days) late, then a 6-day penalty would be applied. Submissions **more** than 7 calendar days late will receive a mark of zero (0) and no assessment feedback will be provided.

(i) Assessment 3 : Network Configuration and Security

Introduction

For this assessment you will use the **core network emulator** to complete a series of tasks on a core configuration file (*.imn file) that is generated for you. To download your individualised core configuration file, open the FIT9137 Moodle page, then navigate to the Assessments section and follow the provided instructions for Assessment 3 to download the **".imn"** file for you to use. **You must use your individualised IMN file (tied to your Monash student ID) for this assessment; otherwise using any other IMN file will result in a zero mark.**

The following information explains the assessment tasks and the details of the network that you will find in your configuration file. You are required to complete tasks A, B, and C that will require you to make changes to your configuration file. You also need to submit supporting documentation that outlines the fixes and changes that you have made to your configuration file (may include screenshots) to complete each task. You must write this report to explain

- the changes you make,
- the configurations you add to achieve the goals of each task,
- your reasons for each change/configuration, and
- the tests you perform to check the task is accomplished.

It's important to note that your submitted core file will be marked by running the configuration and testing that the tasks are completed. The report will serve as a reference to be checked during marking. However, if a test fails when running your submitted core file, you will receive no mark for that failed test (i.e., part of a task) regardless of your explanations in the report. If tasks are similar (i.e. repeated tasks on multiple routers or nodes), you only need to explain your reasons once, and then just report the changes you make to individual services on each node.

Network Structure

The provided network is composed of two organisations labelled **Talos** and **Delos**, a router named **Internet** playing the role of the Internet, and a global DNS server named **clio**. The internal subnets of **talos** are labelled **Internal**, and the public servers of the **talos** network are placed in a separate subnet named **DMZ**. The Internet facing router of the Talos organisation, **R3**, is also its network firewall. The Delos network is divided into two subnets: **(i)** a subnet for the organisation clients and private servers and **(ii)** a subnet for its public servers. The public servers of **Delos** are named **apollo**, **artemis**, and **demeter** providing web, domain name, and mail services respectively.

DNS Setup

You do not need to make any changes to DNS servers; this section only explains the DNS setup. The core file is configured to resolve the domain names between the two organisations, `talos.edu` and `delos.edu`. This is achieved through a global DNS server named `clio`. The server only resolves the names for the two domains in the configuration (`talos.edu` and `delos.edu`) by sending the request to the corresponding nameserver for each domain and sending back the response to the requesting client. Each DNS server in aforementioned networks must have access to UDP port 53 of the server `clio` as the organisation DNS servers resolve the names on behalf of their respective clients.

Important Notes about the CORE Emulator

(a) If you make changes to a core configuration file and then close the CORE window without saving the changes into your imn file, you will **not** be warned, and **the changes will be lost**. Hence, if you wish to keep the changes you have made, you must save these changes into your imn file **before** closing the CORE window. **Please note: changes are to be saved for static routing, DHCP configuration & Firewall configurations.**

(b) Any changes you make to the nodes when the emulation is running will be lost when you stop the emulation. You can test the changes you want to make when the emulation is running and once you have the correct commands, then add them through the GUI in the proper service. For example, to add static routes to a router that persist and will be stored with the configuration file, you need to add `ip route add` commands to the `StaticRoute` service of that router.

(c) Make sure to keep a backup of your CORE file somewhere outside of the VM in case you encounter issues with your VM, and you need to replace the VM. This will make sure that you would not lose the work you have done. It is your responsibility to back up your work.

(d) In the provided configuration file, you must **NOT** alter the overall network structure or topology, including device and node names or IP addresses allocations, nor can you add or remove nodes. Additionally, you are **NOT** allowed to modify link speeds or link delays, and implementing any extra network services such as dynamic routing, VLAN, VPN, or NAT is **prohibited**. If you do not obey these rules, your submitted work will be deemed invalid and will receive a zero mark.

(e) It is recommended to use **tcpdump** if you wish to capture traffic and to observe whether the packets reach their intended destination when trying to accomplish the tasks. To use `tcpdump`, you can right click on a node and move the mouse to select tcpdump in the provided list and then select the intended interface. You can also run tcpdump from the command line using the command `tcpdump -l - i eth0` to print the summary of the captured packets from the eth0 interface in the terminal. To write the captured packets to a file, use the command with `w` option followed by a filename. For instance, running the command `tcpdump -w /home/muni/R3_eth3.pcap - i eth3` on the node `R3` will capture the

traffic on its **eth3** interface and store the frames in a file named **R3_eth3.pcap** under **/home/muni** directory. You can then stop the capture with `Control+C` and use Wireshark to analyse the captured packets.

(ii) Assessment Tasks

Task A: Routing [18+18+9 = 45 Marks]

The routing tables of the routers in the provided network are **NOT** configured. The correct configuration of this task allows **any host from any network to reach any other host** in the entire network. You must satisfy the following requirements while completing this task:

1. All hosts inside the **talos.edu** network must be reachable from any other host within this network through an *optimal path* (the route achieving the highest bandwidth). All routers must be configured solely with static routing tables; dynamic routing is **NOT** allowed. You need to add static routes to routers **R1**, **R2**, **R3**, and **R4** to accomplish this goal. [18 Marks]
2. You must explain your reasons for choosing an optimal path in the report. Static routing decisions should consider the information (such as the number of hops, the delays, the link speeds) provided in the configuration file. The transmission delays are dependent on the link speeds that are provided. The notation ***us*** for links represents the propagation delay in ***microseconds***. You can assume that the processing and queuing delays at the routers are negligible. We expect you to use the information given and decide the best route. Show some calculations or numeric data in support of your decisions about the optimal path. [18 Marks]
3. The default route for all the routers in the **talos.edu** network must be set in a way that makes router **R3** the default gateway. The default route for the R3 and minerva routers must be set in a way that makes the **Internet router** as the default gateway of **R3** and **minerva** (the only router of delos.edu network). You will lose marks if you create routing loops. [9 Marks]

Task B: DHCP Server [8 + 2 = 10 Marks]

The clients of **delos** are configured with static IP addresses. Your task is to:

1. Configure DHCP server on the node **minerva** to assign dynamic IP addresses and other required settings to the client machines in the client's subnet.
2. You can make use of the DHCP server configuration on **R1** as a reference to follow.
3. Enable DHCP client service on clients of **delos**.

Note: The node **leto** is a private local server in the client's subnet and must have a static IP address as assigned for the given configuration.

Task C: Firewall [45 Marks]

The node `R3` is the firewall for `talos` network. Configure the Firewall service on this node denying all other traffic **EXCEPT** the following mentioned in rules 1 to 7 satisfying the requirements as mentioned below:

1. Allow traffic from anywhere (outside of Talos) to DMZ for the provided service by each server. This must be limited to only the public service(s) that a server provides: `dns` only DNS, `web` only HTTP, `mail` only SMTP. [9 Marks]
2. Allow servers in DMZ to initiate a communication if it is required by the service the server provides and it is allowed only for that service (stateful inspection: DMZ to External). [6 Marks]
3. Allow internal hosts to access all services provided by servers in the DMZ (stateful inspection: Internal to DMZ). This includes all services that DMZ servers provide. Please note that all servers in DMZ run SSH service which you can use to test your rules for the internal subnets. You can be more permissive here (use of address ranges and all IP traffic in your rules). [6 Marks]
4. Allow internal hosts to reach other internal hosts (if the internal traffic passes through R3). All traffic is allowed if it is internal to internal communication. [3 Marks]
5. Allow internal nodes to access external servers, however packets from external to internal are only allowed if they are responses to communications that were initiated from inside (stateful inspection: Internal to External). Use utmost caution in allowing services to access. [9 Marks]
6. Allow only the nodes in clients subnet of `talos` to ssh to node `R3` (any host connected to the `R1.eth0` subnet). [4 Marks]
7. Permit node R3 to send ICMP echo request messages to internal talos nodes and all DMZ servers, and receive ICMP echo replies from those nodes and servers. Also, permit internal talos.edu network nodes and all DMZ servers to send ICMP echo request messages to node R3 and receive ICMP echo reply from the node R3. [8 Marks]
8. As mentioned earlier, all other traffic must be dropped. If this requirement is not satisfied, you will receive a zero mark for the firewall task regardless of any other correct rule you add, as it may expose the entire network. You will lose partial marks if your rules are too permissive allowing more traffic than specified to reach the destination for each requirement.

Important Notes for Task C:

(a) You only receive marks if the test for each requirement succeeds. No partial marks will be given (i) if your rules are too permissive allowing more traffic than specified for each requirement or (ii) if only part of a rule is correct. When two rules are required for the incoming and outgoing traffic, no partial marks will be given if one of the rules is correct.

(b) For stateful inspection, the traffic is allowed if it is initiated from the more trusted side of the firewall to the less trusted side. The traffic in the opposite direction, from the less trusted interface to the more trusted interface, is only allowed if the packets are the responses to an initiated communication from the more trusted side. The trust level in the requirements is indicated as **Higher to Lower** for each

stateful inspection, meaning the connection initiation is allowed from the higher level to the lower level and only the responses for the initiated connections are allowed from the lower level to the higher level.

(c) If you have reachability issues in Task A, i.e. a host is not reachable from another host, you may lose marks in firewall tests as well when the traffic must be allowed. You will not lose any marks for firewall rules if a host is reachable but through a sub-optimal path and the firewall rules are correct.

(d) **After completing your network and security configurations, you must submit the CORE file with Firewall service enabled on the node `R3`.**

(iii) Useful Notes

(a) This Assessment will allow you to practically demonstrate your understanding and application of the concepts learned in the unit. To successfully complete the requirements of the Assessment, you must be able to practically demonstrate the required functionality working by including the required configurations into the provided configuration file, but also justify your understanding by supporting the defined configurations with a brief description pertaining to how and why they work. This justification needs to be included as part of your report and can be supplemented with the required configurations command-text (or screenshot) of which are included in the configuration file for each of the outlined tasks and sub-tasks. (You may include references where applicable or necessary.)

(b) **Accessing SSH Server:** There may be situations where you need to test SSH access for a server or a router. And, when you run the SSH command you get prompted for a password. By being prompted for a password it means the SSH service is accessible on that server or router. You can SSH using the user account “muni” i.e. ssh muni@<destination> where <destination> is the IP Address of the server or router that you are testing for SSH access. Also, type “muni” when prompted to enter a password.

(c) **Nodes, Clients, Hosts & Servers:** Nodes refers to any point or interface with an IP address (typically in a router or a server or a client). Hosts mean servers and clients only. Servers are high-end devices represented by the server icons and clients are ordinary computers.

(d) **Example tools to use (not an exhaustive list):** ping, traceroute, iperf (client and server), lynx, ssh.

(e) **Reference Notes:** Please acknowledge any reference appropriately and the use of any AI tools (refer to the Assessment link on Moodle to access information from Learn HQ).