



<b>Programme:</b>	MSc Cyber Security Technology
<b>Module Code:</b>	LD7082
<b>Module Title:</b>	Computer Networks & Security
<b>Distributed on:</b>	<b>June 02, 2025</b>
<b>Submission Time and Date:</b>	To be submitted by 15:59 GMT on <b>August 28th, 2025</b>
<b>Word Limit:</b>	4000
<b>Weighting</b>	This coursework accounts for [100]% of the total mark for this module
<b>Submission of Assessment</b>	<p><b>Electronic Management of Assessment (EMA):</b> Please note if your assignment is submitted electronically, it will be submitted online via Turnitin by the given deadline. You will find a Turnitin link on the module's eLP site.</p> <p><b>It is your responsibility to ensure that your assignment arrives before the submission deadline stated above. See the University policy on <a href="#">late submission of work</a>.</b></p> <p><b>Please note that assignments are subject to anonymous marking.</b></p>

### Instructions on Assessment:

This assignment constitutes **100%** towards the final mark for this module. Any queries relating to this assignment should be discussed with the module tutor. This is an **INDIVIDUAL** piece of work contributing to the module assessment. Deliverables should be assembled into a single report document, which includes (critical appraisal, research, and snapshot evidence of tasks carried out and justification of technologies used). Submission will be in the form of an **MS Word report (4000 words)**.

### **Case Study:**

*Network security attacks can result in financial cost and compromised availability. If a small business is targeted with security attack, it could create a lack of trust among employees and customers, forcing them to switch to a more prominent brand name they think can provide better security. A recent survey showed that 37% of small businesses in UK have lost customers and 17% have lost revenue due to downtime, proving that security should be now a number one agenda for small businesses.*

*DFS (Digital Finance Services) is a well-established small finance service provider, which offers online finance solutions and services to its clients. DFS has the following four departments within its main headquarter Human resource (HR), Information Systems (IS), Customer Centric (CC) and Marketing (MK). So far DFS was using third party services to maintain its IT services.*

*However, as the business is expanding rapidly. The senior management has decided to own their own network infrastructure including Local Area Network (LAN), Wide Area Network (WAN) and an external Server-Side location connected via appropriate WAN technology with prioritizing secure communication between HR department and external site. The server-side site will host DNS, WEB and EMAIL servers.*

*Due to security requirements, it has been decided that all four departments will be on a separate network segment within the same local area network. Other than IT all departments have five users, whereas IT has only two users. Furthermore, IT users must have accessibility to ping all users in the LAN. None of the server is located within the local area network but will be hosted from external site accessible via WAN connection. To strengthen the security it is suggested that IPSec Tunnel has to be created between the HR and the external site via WAN connection. Also Access Control List (ACL) can be used for further security control.*

*You have been hired as network security engineer to design the network for DFS according to the requirements set by the senior management. You will consult appropriate robust network design model to meet the design requirements. You will also implement Access Control Lists and Virtual Private Network to enable secure communication considering security and network performance factors paramount to safeguard Confidentiality, Integrity and Availability of data and communication.*



### **Section 1: Research – 30%**

*(suggested word limit for this section is 1200 words)*

For network design, there is no one "good network design," and there is certainly no "one size fits all." A good network design is based on many concepts, some of which are summarized by key general principles: Critically appraise network design principles to achieve performance, scalability and security at different layers of the Open Systems Interconnection (OSI) model.

### **Section 2: Design – 20%**

*(suggested word limit for this section is 800 words)*

For a given scenario, students are required to **design, configure** and **troubleshoot** network using virtual equipment and **simulate** topologies, connections, protocols and implement configuration using the appropriate simulator application. Design and configuration evidence should be included in the report as a walkthrough snippets.

**Note:** The following marking criteria will apply and must be included to meet all the practical implementation requirements in this section:

- Hierarchical Network Design Model (LAN) (3 Marks)
- Subnetting (Design IP Addressing and Allocation) (3 Marks)
- VLAN Configuration, VLAN Trunking 802.1Q, Inter-VLAN Routing (4 Marks)
- DHCP Server, DNS Server, Web Server, Email Server (3 Marks)
- Dynamic Routing Protocol Configuration using OSPF (WAN) (4 Marks)
- IPSec tunnelling to enhance the security (3 Marks)

### **Section 3: Evaluation – 20%**

*(suggested word limit for this section is 800 words)*

Critically evaluate your design implementation effectiveness in terms of **access control, user privileges**, and effective use of **IPSec VPN**, hardening the devices, security features of hardware devices such as switches and routers.

**Note:** The following marking criteria will apply and must be included to meet all the practical implementation requirements in this section:

- User Privileges (Encrypted Passwords Configuration for Console, User, Privilege Exec Mode) (3 Marks)
- 2 Variations of Extended Access Control List (ACL) (7 Marks)
- IPSec VPN Configuration (10 Marks)

### **Section 4: Ethical Considerations – 30%**

*(suggested word limit for this section is 1200 words)*

Computer security designers should act in a professional manner and show due diligence to comply with legal obligations particularly related to CIA. Critically discuss what social and ethical considerations to be addressed to protect the proposed network design from any cyber threats.

Note: You may use the Code of Conduct of the British Computer Society (available at <http://www.bcs.org>), or to read General Data Protection Regulation contains (GDPR) guide available on gov.uk

## **Mapping to Programme Goals and Objectives**

*This assignment will assess the following learning outcomes:*

1. *Demonstrate a comprehensive understanding and critical evaluation of essential network design principles and security implementation at all OSI layers.*
2. *Design, implement, test and document a small LAN involving the use of routers and switches.*
3. *Critically analyse the main goals and concepts of network security and apply techniques to support message integrity, confidentiality, authentication and network access.*
4. *Critically appraise social, ethical and accessibility considerations in network and security design solution.*

## **Module Specific Assessment Criteria and Rubric**



Criteria	0-39% Standard Not Met 1	40-49% Standard Not Met 2	50-59% Meets Standard 1	60-69% Meets Standard 2	70-79% Exceeds Standard 1	80-89% Exceeds Standard 2	90-100% Exceeds Standard 3
<b>Section 1: Research – 30%</b>	The performance in this criterion does not meet the required standards. Significant improvements are needed to demonstrate an understanding of the topic.	The performance in this criterion is below the expected standard. There are fundamental gaps in understanding or execution.	The performance in this criterion meets the minimum standard. Basic understanding is demonstrated, but there is room for improvement in depth or execution.	The performance in this criterion meets the standard. The understanding is clear and demonstrates a satisfactory level of depth or execution.	The performance in this criterion exceeds the standard. The understanding is strong, and the execution shows a good level of depth or complexity.	The student's performance in this criterion exceeds the standard. The understanding is comprehensive, and the execution demonstrates a high level of depth or complexity.	The student's performance in this criterion far exceeds the standard. The understanding is exceptional, and the execution showcases an outstanding level of depth, insight, and complexity.
<b>Section 2: Design – 20%</b>	The performance in this criterion does not meet the required standards. Significant improvements are needed to demonstrate an understanding of the topic.	The performance in this criterion is below the expected standard. There are fundamental gaps in understanding or execution.	The performance in this criterion meets the minimum standard. Basic understanding is demonstrated, but there is room for improvement in depth or execution.	The performance in this criterion meets the standard. The understanding is clear and demonstrates a satisfactory level of depth or execution.	The performance in this criterion exceeds the standard. The understanding is strong, and the execution shows a good level of depth or complexity.	The student's performance in this criterion exceeds the standard. The understanding is comprehensive, and the execution demonstrates a high level of depth or complexity.	The student's performance in this criterion far exceeds the standard. The understanding is exceptional, and the execution showcases an outstanding level of depth, insight, and complexity.
<b>Section 3: Evaluation – 20%</b>	The performance in this criterion does not meet the required standards. Significant improvements are needed to demonstrate an understanding of the topic.	The performance in this criterion is below the expected standard. There are fundamental gaps in understanding or execution.	The performance in this criterion meets the minimum standard. Basic understanding is demonstrated, but there is room for improvement in depth or execution.	The performance in this criterion meets the standard. The understanding is clear and demonstrates a satisfactory level of depth or execution.	The performance in this criterion exceeds the standard. The understanding is strong, and the execution shows a good level of depth or complexity.	The student's performance in this criterion exceeds the standard. The understanding is comprehensive, and the execution demonstrates a high level of depth or complexity.	The student's performance in this criterion far exceeds the standard. The understanding is exceptional, and the execution showcases an outstanding level of depth, insight, and complexity.
<b>Section 4: Ethical Considerations – 30%</b>	The performance in this criterion does not meet the required standards. Significant improvements are needed to demonstrate an understanding of the topic.	The performance in this criterion is below the expected standard. There are fundamental gaps in understanding or execution.	The performance in this criterion meets the minimum standard. Basic understanding is demonstrated, but there is room for improvement in depth or execution.	The performance in this criterion meets the standard. The understanding is clear and demonstrates a satisfactory level of depth or execution.	The performance in this criterion exceeds the standard. The understanding is strong, and the execution shows a good level of depth or complexity.	The student's performance in this criterion exceeds the standard. The understanding is comprehensive, and the execution demonstrates a high level of depth or complexity.	The student's performance in this criterion far exceeds the standard. The understanding is exceptional, and the execution showcases an outstanding level of depth, insight, and complexity.

## ASSESSMENT REGULATIONS

You are advised to read the guidance for students regarding assessment policies. They are available online [here](#).

### Academic Misconduct

The Assessment Regulations for Taught Awards (ARTA) contain the ***Regulations and procedures applying to cheating, plagiarism, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct.***

The full policy is available [here](#)

You are reminded that plagiarism, collusion, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct, as referred to in the Academic Misconduct procedure of the assessment regulations, are taken very seriously. Assignments in which evidence of plagiarism or other forms of academic misconduct is found may receive a mark of zero.

### Late submission of work



Where coursework is submitted without approval, after the published hand-in deadline, the following penalties will apply. For coursework submitted up to 1 working day (24 hours) after the published hand-in deadline without approval, **10% of the total marks available for the assessment** (i.e. 100%) **shall be deducted** from the assessment mark.

*For clarity: a late piece of work that would have scored 65%, 55% or 45% had it been handed in on time will be awarded 55%, 45% or 35% respectively as 10% of the total available marks will have been deducted.*

The Penalty does not apply to Pass/Fail Modules, i.e. there will be no penalty for late submission if assessments on Pass/Fail are submitted up to 1 working day (24 hours) after the published hand-in deadline.

Coursework submitted **more than 1 day (24 hours)** after the published hand-in deadline without approval will be marked as zero but will be eligible for referral. The reassessment should where appropriate, and as determined by the Module Leader, be the same method (e.g. essay) but maybe with a different task (e.g. different essay title) or with the same task (e.g. the same essay title) as indicated in the Module handbook. In modules where there is more than one assessment component, Students are not required to complete all assessment components if an overall Pass Mark (40% UG, 50% PGT) has been achieved.

The only permitted exception will be in cases where the University is prevented from doing so by a PSRB requirement. In the case of PSRB requirements, a variation order will be required from the regulations.

In modules, where there is more than one assessment component and an overall pass mark has not been achieved, Students will be eligible for a referral\* in the individual failed module and/or not attempted component(s) of assessment.

These provisions apply to all assessments, including those assessed on a Pass/Fail basis.

The full policy can be found [here](#)

### **Word limits**

The word count is to be declared on the front page of your assignment and the assignment cover sheet. The word count does not include appendices, glossary, footnotes, tables and references.

Please note, in text citations [e.g. (Smith, 2011)] and direct secondary quotations [e.g. "*dib-dab nonsense analysis*" (Smith, 2011 p.123)] are INCLUDED in the word count.

If this word count is falsified, students are reminded that under ARTA this will be regarded as academic misconduct.

For those assessments where students are required to keep to the word limit, it is proposed that they should be informed that the marker will stop reading at the point when they judge that the word limit exceeds the recommended word count by more than 10%. The marker will indicate the point at which they stop reading on the text.

***Students must retain an electronic copy of this assignment (including ALL appendices) and it must be made available within 24 hours of them requesting it be submitted.***

The full Word Limit Policy is available [here](#)