



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS
UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN
SECURITY AND FORENICS
4th YEAR 1st SEMESTER 2024/2025 ACADEMIC YEAR
MAIN CAMPUS

COURSE CODE: ICB

COURSE TITLE: NETWORK MANAGEMENT AND SECURITY

EXAM VENUE: LAB 14

STREAM:

DATE: 7/1/25

EXAM SESSION: 9-11.00 AM

TIME: 2.00 HOURS

INSTRUCTIONS:

- 1. Answer Question 1 (Compulsory) and ANY other two questions**
- 2. Candidates are advised not to write on the question paper**
- 3. Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE [30 MARKS]

- a) You're the IT manager at Acme Corporation, a large company occupying five floors of an office building. Several employees from different departments have reported poor Wi-Fi connectivity, especially in conference rooms and break areas. Outline five specific troubleshooting steps you would take to diagnose and improve the Access Point coverage across the office space. **(5 marks)**
- b) As the network administrator at TechSolutions Inc., a growing software development company with 200 employees, you need to implement network traffic monitoring. The CEO has asked for a way to ensure bandwidth is being used efficiently and to detect any potential security threats. Propose two distinct methods you would use to monitor network traffic, explaining how each would work in your company's environment. **(4 marks)**
- c) You're the lead network engineer at StartupX, a fast-growing e-commerce platform. The CEO reports that over the past week, the website load times have increased dramatically, causing customer complaints and potential loss of sales. Describe your step-by-step approach to diagnose the cause of the slowdown and outline potential solutions you would implement to resolve this issue quickly. **(6 marks)**
- d) You're presenting a network upgrade proposal to JOOUST, a University with headquarters in Bondo and campuses in Kisumu, Siaya, Nambale and Nairobi. The project manager, who has a background in logistics but limited technical knowledge, asks you to explain "network convergence" and why it's important for their multi-branch business. How would you explain this concept in simple, relatable terms? **(2 marks)**
- e) Your IT consulting firm has been hired by a regional bank that recently acquired a small local credit union. Upon initial assessment, you discover the credit union's network was poorly designed and potentially insecure. Identify and explain three specific security threats this network might face, and briefly describe how each could impact the bank's operations or data security. **(6 marks)**
- f) You're a sales engineer for NetOptimize Corp, a network optimization service provider. You're meeting with the CIO of a mid-sized manufacturing company that has been experiencing network performance issues. Present three compelling, business-focused reasons why they should invest in your network optimization services. Be sure to relate each reason to potential improvements in their operations or bottom line. **(3 marks)**
- g) You're the network architect for City General Hospital, a busy urban medical center. The hospital director has approved implementation of Quality of Service (QoS) on the network but wants to understand its benefits. Explain the two primary purposes of QoS in this healthcare context, providing specific examples of how it would improve hospital operations and patient care. **(4 marks)**

QUESTION TWO [20 MARKS]

- a) You're a cybersecurity consultant hired by a major financial institution to assess their network vulnerabilities. During your presentation to the board, you need to explain the risks associated with switch traffic interception. Describe five specific methods that a potential attacker could use to view switch traffic in the bank's network, detailing how each method works and its potential impact on the organization's data security. For each method, suggest a practical countermeasure the bank could implement. **(10 marks)**
- b) As part of a red team exercise for a multinational corporation, you've been tasked with simulating a network attack to test the company's defenses. The company has a complex network infrastructure spanning multiple office locations and includes both on-premises and cloud-based services. Outline a detailed, step-by-step approach you would take to conduct this simulated attack, explaining your rationale for each step and the potential vulnerabilities you're exploiting. **(10 marks)**

QUESTION THREE [20 MARKS]

- a) You're the network architect for a rapidly growing tech startup that's expanding its operations across multiple departments and physical locations. The CEO has asked you to implement subnetting to improve network security and efficiency. In a brief report to the executive team, explain at least 5 specific advantages of subnetting in this context, providing examples of how each advantage would benefit the company's growing network infrastructure. **(5marks)**
- b) As an IT consultant, you've been hired by a traditional manufacturing company looking to modernize its operations through network convergence. The company currently maintains separate networks for data, voice, and video communications. Prepare a presentation for the board of directors outlining at least six key advantages of implementing a converged network, explaining how each advantage would specifically benefit the company's operations and bottom line. **(6marks)**
- c) You're the cybersecurity lead for a large call center that's considering transitioning from traditional phone lines to a VoIP system. Your manager has asked you to assess the potential risks of this move. Identify and explain at least 5 specific vulnerabilities associated with converged networks, particularly in relation to VoIP implementation in a call center environment. For each vulnerability, briefly describe how it could be exploited and its potential impact on the call center's operations. **(5 marks)**
- d) As part of a training session for new IT hires at a medium-sized e-commerce company, you need to explain how Network Address Translation (NAT) works. Using a diagram, illustrate the NAT process in the context of the company's network setup **(4 marks)**

QUESTION FOUR [20 MARKS]

- a) Identify and describe two specific scenarios in which media interference could negatively impact data transmission over a cabled network. Provide examples to illustrate these effects. **(4 marks)**

- b) As a network manager, outline three practical measures you would implement to enhance the security of a wireless network in a corporate environment. Discuss the potential impact of each measure. **(6marks)**

- c) Analyze the various tunneling protocols utilized by VPNs in real-world applications. Compare their features and effectiveness in securing data transmission. **(10 marks)**

QUESTION FIVE [20 MARKS]

- a) Imagine you are a cybersecurity expert tasked with assessing network vulnerabilities. Describe five specific steps you would take to identify and exploit weaknesses in a network scenario, including the tools or methods you would use at each stage. **(10 marks)**

- b) Evaluate the various tunneling protocols used by VPNs in real-life applications. Discuss how these protocols function, their strengths and weaknesses, and how they contribute to overall network security. Use examples to support your evaluation. **(10 marks)**