Design and Simulation of a Secure Network Architecture for Boot pharmacies Using VLANs and ACLs to Enhance Security and Performance

Fisha Goitem
Dept. of Computer Science
Middlesex University
Hendon

Module Code: CST3590
Module Leader: Dr Ian Mitchell

This thesis is submitted for the degree of
Bachelor of Science
Computer Networks & Security

April 2025

Abstract

Boots Pharmacy, a major healthcare and retail provider in the United Kingdom, operates a vast digital infrastructure to support its prescription services, patient data management, and financial transactions. As a result, it faces escalating cyber threats, with recent incidents such as the MOVEit Transfer vulnerability and credential-stuffing attacks underscoring the critical need for robust cybersecurity measures tailored to the healthcare sector.[47][20].

This project proposes a comprehensive network security architecture designed to enhance the protection of Boots Pharmacy's digital assets, ensure regulatory compliance, and sustain uninterrupted healthcare services. At the core of the proposed framework is Virtual Local Area Network (VLAN) segmentation, which isolates critical systems and limits lateral movement across the network. Access Control Lists (ACLs) are implemented to regulate traffic between VLANs, ensuring that only authorized users and systems can access sensitive resources.[21] [17]

To further strengthen the security posture, the architecture incorporates multiple layers of defense, including data encryption, Multi-Factor Authentication (MFA), and Zero Trust security principles. These measures help ensure the confidentiality and integrity of sensitive data both in transit and at rest. Role-Based Access Control (RBAC) is used to grant system access based on departmental roles and responsibilities, thereby minimizing the risk of privilege misuse and ensuring operational efficiency.[12].

Boots Pharmacy operates through several key departments—Pharmacy Operations, Customer Service, IT and Security, Compliance, and Business Development—each with distinct roles in service delivery and data handling. The network design accounts for these departmental functions by implementing strict segmentation policies, secure access paths, and logging mechanisms for accountability. Each department is assigned tailored access rights to maintain data protection while supporting seamless workflow.[61].

The network architecture was validated through a series of simulations using Cisco Packet Tracer. Inter-VLAN communication was tested from the LAN VLAN 40 to various segments, including WLAN VLAN 60, management VLAN 30, inside server VLAN 90, the DMZ zone, and remote access networks. Results confirmed successful communication with low latency and no packet loss, affirming the design's resilience and operational integrity. Additional security controls such as secure SSH access, ACL enforcement, and guest WiFi isolation were tested to ensure that unauthorized lateral movement is effectively blocked and access violations are prevented.

The implementation plan follows a structured 12-week schedule, progressing through phases of research, design, simulation, deployment, testing, and refinement. Regular audits and continuous network monitoring are integrated to detect and respond to anomalies in real time, supporting long-term network resilience and proactive threat containment.

Importantly, the project emphasizes the human element of cybersecurity. Comprehensive staff training, awareness initiatives, and a security-first culture are recommended to reduce the risks posed by phishing, social engineering, and accidental breaches. Educated personnel serve as a crucial frontline defense, complementing technological safeguards with vigilance and accountability.

Overall, this project delivers a scalable, resilient, and regulation-compliant network security framework for Boots Pharmacy. By integrating layered defenses, secure network design, real-time monitoring, and a culture of cybersecurity awareness, the architecture not only protects sensitive information but also strengthens public trust, improves operational reliability, and sets a benchmark for best practices in the healthcare retail environment.

Keywords:

Boots Pharmacy, Cybersecurity, Network Security, VLAN (Virtual Local Area Network), Access Control Lists (ACLs), Zero Trust Architecture (ZTA), Multi-Factor Authentication (MFA), Encryption (data at rest and in transit), Ransomware, Credential-Stuffing Attacks, Regulatory Compliance (GDPR), Network Segmentation, Organizational Resilience, Cisco Packet Tracer Simulation, Employee Training and Awareness.

Acknowledgements

I would like to extend my deepest gratitude to all those who have supported the development of this project. Specifically, I wish to thank:

1. My academic supervisors and mentors for their insightful guidance and feedback throughout the research and design process.

2. The technical advisors who offered invaluable expertise in network engineering and cybersecurity best practices.

3. Friends and colleagues who provided moral support, shared resources, and offered encouragement when challenges arose.

4. My family members, whose unwavering patience, understanding, and optimism enabled me to stay motivated and focused from start to finish. Their belief in my work fueled my commitment to seeing this project through to a successful conclusion.

Without the collective help and encouragement of these individuals, the secure network architecture and the lessons learned from this project would not have been possible. Their contributions have not only strengthened the technical integrity of the work but also enriched my personal and professional growth....

Contents

List of Figures

List of Tables

Acronyms

ACLS Access Control Lists. 2

CLI Command Line Interface. 23, 30

CRM Customer Relationship Management. 46

GDPR General Data Protection Regulation. 13, 42

LAN Local Area Network. 26

MFA Multi factor authentication. 18

RBAC Role based access control. 23

SSH Secure Shell. 35

VLAN Virtual local area network. 2

WLAN Wireless Local Area Network. 59

Chapter 1

Introduction

1.1 Background

Understanding the background and motivation behind this project requires reflecting on past incidents, current challenges, and future security needs. Boots Pharmacy has already faced cybersecurity breaches, such as the MOVEit Transfer vulnerability in 2023[42] [20]and credential-stuffing attacks in 2020[48] [47] underscoring the need for stronger defenses. These breaches have not only threatened operational stability but have also jeopardized sensitive staff and customer data, reinforcing the importance of proactive security measures.

In healthcare and retail sectors alike, sophisticated adversaries are incentivized by high-value data such as patient medical records and payment details[7].A single breach can devastate an organization operationally, financially, and reputationally. This pressure is compounded by legal mandates, including GDPR, which impose stringent requirements for data protection and can levy heavy fines for noncompliance[26].Given these factors, Boots Pharmacy must develop a forward-looking cybersecurity strategy that not only addresses current vulnerabilities but also anticipates future threats, ensuring continued trust and resilience in an evolving digital landscape[58][30][57].

Boots Pharmacy's internal structure further highlights the complexity of securing such a dynamic and distributed environment. The organization operates through several critical departments:

- **Pharmacy Operations and Inventory:** Manages prescription processing, medication storage, stock control, and dispensing accuracy to ensure patient safety.
- **Sales, Customer Service, and Administration:** Handles customer transactions, inquiries, billing, and coordination with insurance providers, playing a central role in the front-end experience.
- **IT and Security:** Oversees data protection, infrastructure management, and network security, ensuring compliance with standards like GDPR and

PCI-DSS.

- **Compliance and Regulatory Affairs:** Ensures that all operations meet healthcare and pharmaceutical regulations, including the management of controlled substances and privacy standards.

- **Management and Business Development:** Focuses on strategic planning, service expansion, budgeting, and innovation, shaping the long-term growth of the organization.

Each department handles distinct types of sensitive data and requires tailored access privileges and communication pathways, making network segmentation and role-based access essential. The interdependency of these units means that a compromise in one area could cascade into others, magnifying the impact of cyberattacks.

This project aims to bridge the gap between past failures and future improvements by designing and simulating a secure network architecture that integrates Virtual local area network (VLAN)[35], Access Control Lists (ACLS)[54], Zero Trust principles[15], encryption, and authentication protocols. These measures will fortify Boots Pharmacy's infrastructure, preventing unauthorized access, mitigating cyber threats, and ensuring seamless pharmacy operations. By taking a structured approach to cybersecurity, this initiative will help create a robust, scalable, and adaptive security framework that evolves with emerging risks, protecting both the organization and the millions of customers who rely on its services.

1.2 Aims

The primary aim of this project is to strengthen the network security and ensure the operational resilience of Boots Pharmacy. Through layered defenses encompassing network segmentation, firewalls, authentication protocols, encryption, continuous monitoring, and advanced threat prevention. This project will offer a blueprint for safeguarding digital operations[5][6][4]. By weaving together best practices and regulatory compliance, the proposed design targets confidentiality, integrity, and availability of data, thus fortifying the core framework of Boots Pharmacy's digital environment[39].

1.2.1 Objectives

These are a list of clearly defined objectives that can be aligned to outcomes in the project. We can define the success of the project based on these fulfilling these objectives.

- Examine the present cybersecurity problems in Boots Pharmacy's IT infrastructure, such as assessing the threats posed by ransomware attacks, unauthorised network access, poor IoT security, old equipment, and third-party application vulnerabilities.

- Provide a recommended solution for the current cyber security problems in Boots Pharmacy, such as mitigating ransomware, preventing unauthorized devices, enhancing IoT security, upgrading, patching, and replacing old devices, securing third-party applications, and implementing strong encryption and authentication measures to ensure compliance with GDPR[40][14][19][6].
- Create a VLAN-based network segmentation strategy for Boots Pharmacy by isolating important pharmacy operations, consumer Wi-Fi, and retail systems, hence decreasing unauthorised access and cyber threats. For example, VLAN 10 will handle pharmacy operations and sensitive data[21].
- Implement Access Control Lists (ACLs) to prevent unauthorised access to critical data and services by setting rules for allowing or denying traffic based on IP addresses, protocols, or individual users. Set up secure authentication and encryption mechanisms, such as enabling SSH for encrypted remote access, password encryption, and secure login methods[17]
- Implement intrusion prevention techniques such as enable DHCP Snooping (Prevent Rogue DHCP Servers), Enable Dynamic ARP Inspection (DAI) ,Enable Port Security (Prevent Unauthorized Devices) and Implement Access Control Lists (ACLs) [41].
- Design, configure and implement a secure network for Boots Pharmacy with Cisco Packet Tracer[13] to simulate functionality and assess security and performance.Additionally, Evaluate and test simulation results to improve network security and efficiency and Make security rec- ommendations, such as zero-trust policy, employee training, and endpoint solutions to enhance security and comply with GDPR.

1.2.2 Deliverables

Deliverables are a result of actions that complete and attempt to satisfy objectives and can include:

- Complete proposal detailing the cybersecurity improvements for Boots Pharmacy
- Complete research on the current cybersecurity threats and challenges faced by Boots Pharmacy[20][47].
- Complete research on existing cybersecurity solutions and best practices, including VLANs, ACLs, encryption, and Zero Trust principles[21][17].
- Complete literature review on network segmentation, ACL implementation, and cybersecurity frameworks.
- complete Cost-Benefit Analysis and Risk Assessment

- Conduct experiments to simulate a secure network using Cisco Packet Tracer.
- Gather and collate data from network simulations to assess security and performance.
- Analyze simulation results and write up findings.
- Complete conclusions and recommendations for improving network security.

1.3 Resources

List any software or hardware that may be required for the completion of the project.

- Recommended System Requirements (For Optimal Performance): A laptop with an Intel Core i5/i7 processor, 8GB or more RAM, at least 5GB of free storage, and Windows 10/11 (64-bit) operating system[51].
- Software for Network Simulation: Cisco Packet Tracer[7][13][20].
- LaTeX (Overleaf/TexMaker): For writing reports and documentation[38].
- Network security-related scholarly articles, cybersecurity guidelines books, and industry best practices books.
- Case studies on previous hacks against Boots Pharmacy.
- computer networks Books

1.4 Schedule

Typically include a GANTT chart indicating when the objectives and deliverables are met.

- Research and Analysis (08/02/2025 - 28/02/2025): Investigate cybersecurity threats faced by Boots Pharmacy, including ransomware, IoT vulnerabilities, and legacy hardware. Gather incident reports and system overviews, and submit a proposal outlining improvements.
- Problem Analysis (28/02/2025-10/03/2025): Analyze identified vulnerabilities, focusing on root causes and risks. Evaluate the impact of outdated systems and insufficient employee training on operational stability and GDPR compliance.
- Network Architecture Design (05/03/2025 - 30/03/2025): Develop a secure network blueprint incorporating VLANs, ACLs, and Zero Trust principles. Design a segmentation strategy to isolate critical systems like pharmacy operations and consumer Wi-Fi.

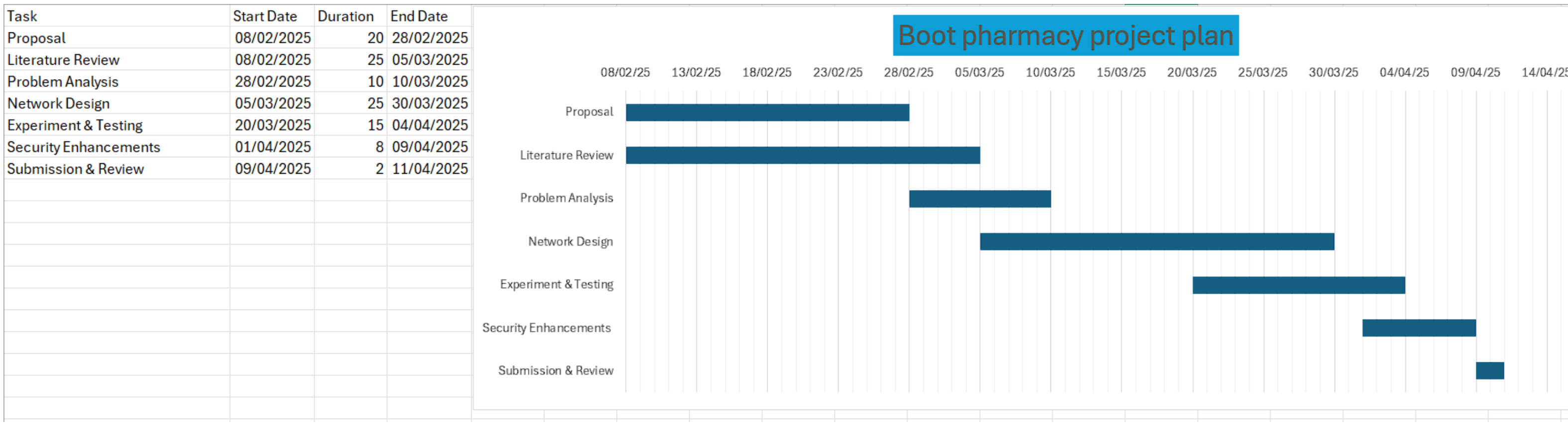
- Implementation of VLANs and ACLs (08/03/2025 - 30/03/2025): Establish VLANs to compartmentalize network areas and configure ACLs to control traffic based on IP policies and user credentials. Implement secure authentication and encryption mechanisms.

- Authentication, Encryption, and Intrusion Prevention (11/03/2025 - 30/03/2025): Enforce multi-factor authentication, SSH for encrypted access, and endpoint encryption. Deploy intrusion prevention techniques like DHCP Snooping, Dynamic ARP Inspection, and Port Security.

- Simulation and Testing (20/03/2025 - 04/04/2025): Test the configured network in Cisco Packet Tracer under standard usage, heavy loads, and simulated attacks. Verify logging, monitoring, and compliance with GDPR requirements.

- Refinement and Optimization (01/04/2025 - 09/04/2025): Analyze testing data to identify bottlenecks and vulnerabilities. Optimize ACLs and VLANs to ensure they function without over-restricting legitimate traffic.

- Final Documentation and Reporting (09/04/2025 - 11/04/2025): Consolidate the technical design, configurations, and test results into a final report. Provide recommendations for employee training, endpoint solutions, and Zero Trust policies.



Task	Start Date	Duration	End Date
Proposal	08/02/2025	20	28/02/2025
Literature Review	08/02/2025	25	05/03/2025
Problem Analysis	28/02/2025	10	10/03/2025
Network Design	05/03/2025	25	30/03/2025
Experiment & Testing	20/03/2025	15	04/04/2025
Security Enhancements	01/04/2025	8	09/04/2025
Submission & Review	09/04/2025	2	11/04/2025

Figure 1.1: GANTT Chart for Boot pharmacies plan.

1.5 Summary

Boots Pharmacy, a leading UK healthcare provider, has been increasingly targeted by cyberattacks due to its reliance on digital systems for managing prescriptions, patient data, and financial transactions. Past incidents, such as the 2023 MOVEit Transfer software vulnerability[20] and 2020 credential-stuffing attacks[47], emphasize the importance of robust cybersecurity defenses. This project aims to design a secure network architecture for Boots Pharmacy to protect against cyber threats and ensure operational resilience. The design will incorporate advanced security measures, including VLANs, ACLs, firewalls, Zero Trust Architecture, network segmentation, encryption, and strong authentication protocols.

The project's primary objective is to assess and address existing cybersecurity challenges, such as ransomware, unauthorized network access, outdated systems, and IoT vulnerabilities. The solution will include network segmentation through VLANs, enforcing secure authentication, and implementing data encryption[21]. A network simulation using Cisco Packet Tracer will evaluate the effectiveness of the proposed security measures under various conditions, ensuring that Boots Pharmacy can handle potential cyber threats effectively.

The deliverables include a comprehensive report, a secure network architecture blueprint, simulation results, and recommendations for regular security audits and compliance. The project will require resources such as hardware (Intel Core i5/i7 laptop, 8GB RAM), software (Cisco Packet Tracer)[51], and reference materials on past cyberattacks and best practices. The project will span 12 weeks, with key stages involving research, network design, implementation, testing, and documentation.

By integrating these cybersecurity practices, Boots Pharmacy will better protect sensitive data, maintain customer trust, and comply with regulatory standards like GDPR.

Chapter 2

Literature Review

2.1 Introduction

The accelerating digitization of healthcare and retail sectors has elevated cybersecurity to an issue of paramount importance. These industries handle vast troves of personally identifiable information (PII) and highly sensitive financial and medical data; such data not only attract financially motivated cybercriminals but also threaten public trust if compromised. Boots Pharmacy, a major UK-based healthcare and retail provider, has recently encountered notable cyber incidents such as the MOVEit Transfer vulnerability in 2023 [42]and a credential-stuffing attack in 2020[48] [47] . These events highlight the potentially severe operational, financial, and reputational consequences of cyber threats. This literature review synthesizes key research on cybersecurity threats, case studies of attacks on healthcare and retail organizations, existing cybersecurity frameworks, and best practices. It also provides an integrated view of how Boots Pharmacy can strengthen its cybersecurity posture by applying multilayered defense strategies, investing in employee training, leveraging emerging technologies, and adhering to recognized standards and regulations[37][23][34].

An essential goal of this review is to critically appraise both the breadth and limitations of current research. The following sections provide an overview of principal cybersecurity threats in healthcare and retail, explore existing prevention and mitigation strategies, analyze notable case studies, and present future recommendations tailored to the context of Boots Pharmacy. By incorporating multiple research perspectives, from technical solutions to organizational and human factors, this review underscores the need for a comprehensive, multistakeholder approach to safeguarding healthcare and retail organizations against evolving cyber threats[55].

2.2 Cybersecurity Threats in Boot Pharmacies

2.2.1 Ransomware Attacks

Ransomware continues to disrupt healthcare and retail organizations worldwide. In particular, healthcare systems are gravely vulnerable due to the critical nature of patient data and the need for uninterrupted service provision. According to Broklyn and Shad,[8], ransomware attacks on healthcare grew by 123 percent in the past five years, with ransom payouts skyrocketing in parallel. For retail and pharmacy outlets, the threat is equally menacing: a successful attack can halt financial transactions, compromise prescription management systems, and create a customer service crisis. At Boots Pharmacy, the risk is heightened by the broad integration of digital systems supporting patient care, stock management, and digital payment processes.

Several factors exacerbate ransomware risks. First, threat actors exploit the imperative of operational continuity in healthcare to pressure organizations into rapid ransom payments. Second, many organizations operate legacy systems ill-equipped with modern security patches. Third, heightened reliance on digital workflows amplifies the potential damage when systems fail. Mitigation strategies include routine data backups stored off-network, rigorous patch management, and network segmentation to contain the lateral movement of malware. Additional measures such as advanced endpoint protection systems (e.g., extended detection and response tools) can automate real-time threat detection. However, these solutions come at a cost and require sustained managerial focus to ensure consistent updates and staff training[59].

2.2.2 Credential Stuffing and Unauthorized Access

Credential stuffing capitalizes on credential reuse across multiple online platforms. The 2020 attack on Boots Pharmacy exemplifies how previously compromised usernames and passwords can yield unauthorized access to customer accounts.Sasikumar and Nagarajan advocate for multi-factor authentication (MFA)[46] as among the most potent deterrents, reducing credential-based breaches by nearly 99 percent when properly enforced (NIST, 2023). Bolstering authentication also necessitates adopting the Zero Trust model which treats all network traffic equally untrusted and implementing stringent access control policies.

Several debates persist regarding the practicality of Zero Trust in large-scale, distributed healthcare settings, where caregivers often require rapid access to critical systems. Critics argue that overzealous restrictions may hamper the swift provision of clinical services and negatively impact the user experience. Nonetheless, carefully calibrated measures, such as context-aware identity and access management (IAM), can blend security with usability by adjusting authentication requirements based on device posture, user roles, and real-time risk assessment[31]. Emerging solutions combine behavioral analytics, which identifies unusual login patterns, with advanced AI-driven anomaly detection to achieve dynamic, continuous verification[32].

2.2.3 IoT Security Vulnerabilities

Starting from connected medical devices to smart inventory dashboards, the proliferation of Internet of Things (IoT) devices has opened new avenues for cyber threats. Boot Pharmacies increasingly rely on smart dispensers and real-time tracking tools, which, if compromised, can generate severe operational disruptions or inaccurate inventory systems. J.Doe stress that many IoT devices suffer from rudimentary security configurations; some do not even allow firmware updates or secure boot processes. Consequently, IoT devices often serve as a prime entry point for botnets and advanced persistent threats (APTs)[18].

Securing IoT infrastructure involves several layers: device authentication and encryption standards, occasionally aligned to the ISO/IEC 30141 IoT reference architecture, regular firmware updates, and rigorous network segmentation. Organizations that implement device-level certificates and encrypted communication protocols significantly decrease the likelihood of man-in-the-middle (MITM) attacks[11]. Nonetheless, the cost of updating or replacing entire fleets of IoT devices can be prohibitive, especially for smaller providers. Hence, risk-based approaches and segmentation that isolates vulnerable or outdated IoT devices can be a pragmatic starting strategy.

2.2.4 Legacy System Vulnerabilities

Many Boot pharmacies still rely heavily on legacy systems outdated electronic point-of-sale terminals, mainframe architectures, or older database management software.[9] Campbell observes that unpatched vulnerabilities in these systems are frequently targeted by threat actors, given they often lack modern security safeguards. Transitioning Boots Pharmacy or any large healthcare retail chain to newer, cloud-based or containerized solutions requires planning, budget allocations, and ensuring minimal disruptions to ongoing operations.

Migration strategies typically involve incremental transitions: segmenting legacy systems, applying virtual patches where possible, and introducing microservices for critical tasks. A robust patch management policy ensures timely updates across all systems, although practical challenges abound e.g., older systems might not support current operating systems or security patches, while certain specialized pharmacy software might need vendor-specific updates. Regular vulnerability assessments, penetration testing, and comprehensive software lifecycle management can help prioritize which legacy components pose the greatest risks, informing budgetary decisions for phased replacements.

2.3 Existing Cybersecurity Measures in Boot pharmacies and Best Practices.

2.3.1 Network Segmentation and VLANs

Network segmentation is widely recognized as a pivotal defensive measure. Healthcare systems, including Boot pharmacies, often handle segregated workloads e.g., clinical data handling, back-office administration, and customer-facing Wi-Fi. By dividing these systems into distinct VLANs, administrators can contain an attack within a segment, preventing attackers from easily pivoting to more critical systems. NAC tools add yet another layer by ensuring that only compliant devices can connect to sensitive segments[25].

Nonetheless, network segmentation can introduce additional management overhead, especially in dynamic environments. It demands regular reviews of VLAN assignments, robust documentation, and continuous collaboration among IT, security, and operations teams. Yet, studies by Ahmed and Alsadoon, reveal that the short-term complexity is often offset by the long-term security benefits, including an 80 percent reduction in lateral movement attacks in segmented environments[2].

2.3.2 Access Control Lists (ACLs) and Role-Based Access Control (RBAC)

Access Control Lists (ACLs) are fundamental for defining who can connect to or modify specific resources. Effective ACL implementations at Boots Pharmacy could restrict server access to employees based on job function and device posture. By pairing ACLs with RBAC, each role (pharmacist, cashier, systems admin) is granted the minimal set of permissions essential for daily tasks. This principle of minimal privilege reduces the insider threat malicious or accidental where Boot employee might inadvertently access or mishandle sensitive data[32].

Nevertheless, configuring ACLs and RBAC can be labor-intensive, prompting some organizations to under-configure or neglect timely updates. Regular audits of account privileges and an integrated IAM solution, potentially using single sign-on (SSO) combined with conditional access policies, can help maintain an accurate and secure permission structure. Automation scripts that decommission or adjust user roles when employees change roles or depart further augment ACL and RBAC efficacy[60].

2.3.3 Encryption, Secure Authentication, and MFA

Encryption has become an indispensable measure across industries for safeguarding sensitive data in transit and at rest. In the Boot Pharmacy context, encryption applies not only to patient records but also to employee credentials, payment transactions, and IoT communications. Coupled with MFA, encryption reduces the risk of adversaries utilizing compromised credentials. According to NIST (2023), organizations enforcing MFA witness a dramatic decrease in account takeover incidents.

Biometric authentication methods can extend security further, but they also raise privacy concerns and require specialized hardware. Where biometrics might not be feasible, organizations can rely on time-based one-time passwords (TOTPs) or hardware security keys for an additional layer of authentication. Enterprises like Boot pharmacies that fail to adopt such measures risk falling behind rising global compliance standards, such as the GDPR which stress strong data protection requirements[33].

2.3.4 Zero Trust Security Model

Zero Trust challenges the older, perimeter-centric understanding of network protection. Instead of presuming trust for internal traffic, Zero Trust stipulates verifying every user and device for every transaction.Syed and Shah report a 40 percent reduction in data breaches among organizations that adopt this model. Core to implementing Zero Trust successfully is an IAM framework capable of continuous policy enforcement, real-time risk scoring, and adaptive authentication[50].

A common critique of Zero Trust is the perceived friction it can introduce, particularly in fast-paced health delivery settings. Boot pharmacy staff might be reluctant to navigate repeated authentication steps under stressful operational conditions. Solutions that harness real time context such as device health, user behavior, or even geolocation help achieve a balance by applying stricter checks only when anomalies arise[3].

2.3.5 Intrusion Prevention Systems and Threat Intelligence

Intrusion Prevention Systems (IPS) detect and block known threats by monitoring network traffic, utilizing tactics like DHCP Snooping to identify malicious DHCP servers, and Dynamic ARP Inspection (DAI) to thwart address resolution protocol spoofing. By feeding real-time threat intelligence into IPS, organizations stay updated on newly identified indicators of compromise (IoCs) and emerging hacker tactics. Such intelligence can stem from commercial services, government advisories, or industry-specific information sharing and analysis centers (ISACs).

Nevertheless, a purely signature-based IPS can fail against zero-day vulnerabilities or advanced persistent threats that rely on custom exploits. As a result, many organizations such as Boot Pharmacies adopt behavior-based tools that detect anomalies and suspicious behaviors. Combining both signature-based and anomaly-based detection offers a more holistic safety net[27].

2.4 Case Studies on Cyberattacks in Boot pharmacies

2.4.1 The MOVEit Transfer Vulnerability (2023)

Boots Pharmacy was recently affected by a zero-day flaw in MOVEit Transfer software, reflecting the broader rise of software supply chain vulnerabilities. These incidents highlight the importance of deploying rigorous vulnerability scanning, dependency checks in software development, and robust patch management. Neglecting any of these practices creates strategic blind spots that attackers can exploit.

Furthermore, adopting a layered security approach one that includes code reviews, automated scanning tools, and frequent penetration tests can reduce the interval between the discovery of a vulnerability and the application of a patch. The MOVEit incident also underscores spending on post-breach forensics and communications, areas many organizations underinvest in until a crisis arises[53][42].

2.4.2 The 2020 Boots Credential-Stuffing Attack

Credential-stuffing attacks exploit weak password hygiene, leveraging stolen credentials often bought on the dark web. After the 2020 incident, Boots Pharmacy implemented MFA, expanded its login anomaly monitoring, and informed affected customers. Significantly, the case exemplifies how brand damage and public relations ramifications can surpass initial incident containment costs.

Many security professionals point to password reuse as a cultural challenge that underscores the importance of user education. Regular, simulated phishing exercises and training about best password practices can help, but they must be reinforced by organizational policy e.g., forcing complex passwords and rotating credentials within reason[47].

2.4.3 NHS WannaCry Ransomware Attack (2017)

Although Boots Pharmacy was not directly impacted, the NHS WannaCry event remains a seminal cautionary tale within UK healthcare. It paralyzed unpatched Windows systems across hospitals, providing a stark lesson on the value of timely patching, network segmentation, and robust incident response strategies. Post-incident analyses highlight how a single vulnerability (EternalBlue) can unleash severe disruptions if the threat propagates unchecked.

This case study shows that inter-organizational information sharing is crucial. Entities that had prior knowledge of the patch or broader threat intelligence were better able to weather the attack. Additionally, the incident underscores the financial and ethical imperatives of ensuring service continuity in critical healthcare infrastructure[36].

2.5 Future Cybersecurity Strategies for Boots Pharmacy

2.5.1 Implementing AI-Driven Threat Detection

Artificial Intelligence (AI) and Machine Learning (ML) promise to revolutionize cybersecurity, offering the ability to sift through large volumes of logs in real time and identify patterns indicative of an incipient attack. By correlating network traffic anomalies with user behavior analytics, AI systems can flag suspicious activity that might slip past rule-based defenses. Early detection is especially pivotal in halting data exfiltration or endpoint compromise before significant damage ensues[52].

However, adopting AI-driven solutions necessitates consistent data governance, as poorly labeled or siloed data reduces the efficacy of machine learning. Moreover, while AI can cut response times, it also demands specialized talent and thorough risk analysis to avoid false positives overwhelming security teams.

There is some debate about the return on investment (ROI) for large-scale Boot Pharmacies employees training, given that people might revert to old habits if not consistently reinforced. Yet, studies in organizational psychology suggest that top-down support from leadership and embedding security metrics within performance reviews can cultivate a sustainable security-conscious culture.

2.5.2 Cost-Benefit Analysis of Cloud Security and Compliance

Organizations such as Boots Pharmacy increasingly migrate to cloud services seeking scalability and cost savings. Cloud Access Security Brokers (CASBs), encryption gateways, and compliance monitoring tools are central in safeguarding data on Microsoft Azure, Amazon Web Services, or Google Cloud Platform. However, adopting a multi-cloud strategy to minimize single-point failure can also complicate compliance obligations and identity management.

An important consideration is the cost-benefit ratio of cloud migration. On one hand, cloud providers may offer integrated security features, shared responsibility models, and robust infrastructure. On the other, healthcare-specific regulations like General Data Protection Regulation (GDPR) in UK necessitate rigorous auditing, data residency, and encryption. Governance frameworks such as ISO 27001 can help ensure accountability and best practices, albeit at the expense of increased administrative overhead for certification and continuous compliance[1].

2.5.3 Proactive Threat Hunting and Incident Response

Developing an incident response plan that outlines clear roles, communication protocols, and escalation pathways is now a baseline requirement for Boot Pharmacies. Dedicated security operations centers (SOCs) can proactively hunt for threats by monitoring real-time logs, scanning for suspicious network behavior, and leveraging red team exercises. Because zero-day exploits can emerge without warning, continuous monitoring is no longer optional but essential.

Organizations that embrace threat hunting invest in advanced tools and skilled personnel adept at investigating subtle indicators of compromise (IoCs). Yet, the success of these initiatives hinges on cohesive teamwork among IT, legal, and executive leadership. Rapid containment can minimize data exfiltration and reputational harm, while thorough post-incident forensics can inform process improvements particularly around vulnerability patching and policy updates[49].

2.5.4 Strengthening Third-Party Security Controls

Supply chain compromises are on the rise, as adversaries exploit weaknesses in smaller vendors or software suppliers to infiltrate targets with stronger defenses. For a pharmacy like Boots, vendors ranging from payment gateways to logistics partners introduce potential security gaps. Adopting stringent third-party risk management (TPRM) processes involves security due diligence before onboarding vendors, contractually mandating specific controls, and periodic audits.

Despite these precautions, some controversies remain. Critics note that overly restrictive agreements or lengthy vendor audits can impede innovation and slow business processes. A balanced approach might leverage standardized questionnaires (e.g., SIG questionnaires), on-site or impartial online audit solutions, and firm yet flexible SLAs (service-level agreements) ensuring accountability. By mandating alignment with frameworks like NIST Cybersecurity Framework, ISO 27001, or even sector-specific standards, organizations can ensure a baseline level of security among partners[44][22].

2.5.5 Additional Emerging Technologies and Future Considerations

Beyond AI, certain nascent technologies show promise in tackling advanced threats. Blockchain has been explored for supply chain integrity and tamper-proof audit logs, though scalability and regulation remain concerns. Meanwhile, containerization and serverless computing are redefining cloud-native security paradigms by isolating workloads at the process level, reducing the potential blast radius of an intrusion. Zero-Knowledge proofs and homomorphic encryption techniques are also on the rise, championed for their potential to protect private information even during computations[10].

Yet, incorporating these advanced tools demands skilled implementation and security audits to avert new attack vectors. As Boots Pharmacy and similar enterprises chart a path forward, they should weigh the maturity of new technologies against the urgency of immediate risks like ransomware and credential stuffing[16].

2.6 Summary

The healthcare and retail sectors operate under intense pressure to safeguard customer and patient data while maintaining uninterrupted services. Boots Pharmacy's recent experiences with the MOVEit Transfer vulnerability and credential-stuffing attacks illustrate the multifaceted dangers from direct financial or operational disruption to longer-term reputational harm[20]. This literature review highlights the primary threats that healthcare retail organizations must address: ransomware, unauthorized access, IoT exposures, and legacy system weaknesses all of which are well documented in existing research and illustrated through relevant case studies.

Fortunately, a suite of robust, evidence-based solutions exist. Network segmentation, ACLs, MFA, and Zero Trust models each tackle specific dimensions of the threat landscape. AI and ML can enhance early detection and response, while employee training efforts mitigate social engineering exploits. Adherence to established frameworks—NIST, ISO 27001, CIS Controls and close attention to compliance mandates like GDPR can provide a structured path toward maturity. Nevertheless, these measures carry financial and operational constraints, necessitating careful cost-benefit analyses and prioritization in organizational budgets and strategic planning[1].

From a critical standpoint, there remain debates in the scholarly literature regarding the scalability, ROI, and adoption challenges of advanced cybersecurity measures in a fast-paced healthcare environment. Yet, consensus rings clear on key points: continuous patching, multi-layered defenses, and informed employees are indispensable. Equally crucial is the alignment of organizational culture with cybersecurity goals, encouraging collaboration across departments and with external partnerss[44][22] [16].

Chapter 3

Method

3.1 Introduction

In today's rapidly evolving cybersecurity landscape, Boot Pharmacy faces increasingly sophisticated threats from credential stuffing and phishing to advanced ransomware, lateral movements across IoT networks, and unauthorized internal access. Based on the extensive literature review presented in Chapters 1 and 2, this chapter outlines a series of experiments designed to test and validate various cybersecurity strategies informed by the latest research. These experiments target critical vulnerabilities identified through real-world case studies and recent academic findings, examining measures such as enhanced employee training paired with multi-factor authentication, integration of dynamic threat intelligence within intrusion prevention systems, and the deployment of Zero Trust architectures along with granular network segmentation using VLANs and ACLs in combination with RBAC[24].

The primary objective of this experimental framework is to empirically assess whether these layered defense strategies grounded in new research can significantly mitigate risks and reduce the overall impact of cyberattacks on Boot Pharmacy's operations. By simulating controlled, realistic attack scenarios that closely mirror the operational environment at Boot Pharmacy, each experiment aims to establish clear metrics for detection times, response speeds, and containment efficacy. This chapter details the experimental objectives, setups, and methodologies that will statistically evaluate the proposed cybersecurity improvements and ultimately demonstrate how theoretical best practices can be effectively implemented to strengthen Boot Pharmacy's cybersecurity posture.

3.2 Experiment 1:Evaluating the Effectiveness of MFA and Enforced Strong Password Policies test

3.2.1 Objective:

To assess how integrating multi-factor authentication (MFA) with enforced strong password policies influences the success rate of credential stuffing and phishing attacks. This experiment aims to validate that users employing MFA and strong password policies are more secure compared to those relying solely on single-factor authentication with weak passwords. [45].

3.2.2 Hypothesis:

Users who utilize MFA and adhere to strong password policies will exhibit significantly lower rates of successful phishing and credential stuffing incidents than users who rely only on single-factor authentication with weak passwords. [43].

3.2.3 Setup:

Two groups of participants simulating Boots Pharmacy employees are selected:

1. Control Group: Uses legacy single-factor authentication with weak passwords.
2. Experimental Group: Uses MFA with context aware identity checks and adheres to strong password policies, including minimum length, complexity requirements (e.g., mixed-case letters, numbers, and special characters), and account lockout mechanisms after repeated failed attempts.

3.2.4 Procedure:

1. Introduce both groups into a baseline simulated environment where phishing and credential stuffing scenarios are executed, similar to the failed login attempts
2. For each simulation round, record key metrics such as phishing click-through rates, incident report frequency, success rate of unauthorized login attempts, and the time taken to recognize potential breaches.
3. Run multiple rounds to account for any learning curves and to ensure reproducibility.
4. Compare performance trends between the two groups across all cycles.

3.2.5 Data Collection and Analysis:

1. Failed Login Attempts: Monitor the number of failed login attempts to assess the effectiveness of Multi factor authentication (MFA) and strong password policies in preventing unauthorized access.
2. Account Lockouts: Record instances of account lockouts after repeated failed attempts, highlighting the security benefits of enforced lockout mechanisms.
3. Successful Authentications: Measure the rate of successful authentications in the experimental group using MFA, compared to the control group.

3.2.6 Expected Outcome:

The experimental group, using MFA and strong password policies, is expected to demonstrate a statistically lower rate of successful credential stuffing and phishing attacks. This would support the benefit of combining MFA with robust password policies as a critical defense strategy. [43][45].

Metric	Control Group (Single-Factor, Weak Passwords)	Experimental Group (MFA, Strong Passwords)	Expected Outcome
Failed Login Attempts	High	Low	The experimental group shows fewer failed login attempts, indicating better security measures.
Account Lockouts	Rare	Frequent	More account lockouts in the experimental group highlight effective lockout mechanisms.
Successful Authentications	Moderate	High	Higher successful authentication rates in the experimental group due to MFA.
Phishing Click-Through Rates	High	Low	The experimental group exhibits lower click-through rates, showing improved phishing resistance.
Incident Report Frequency	Low	High	More frequent incident reporting in the experimental group indicates better awareness.
Unauthorized Login Attempts	High	Low	Fewer unauthorized attempts in the experimental group demonstrate enhanced security.

Table 3.1: Comparison of Security MFA and Single FA

3.3 Experiment 2: SSH Access Control Test

3.3.1 Objective:

To verify secure remote management on multilayer switch by comparing SSH access from devices within VLAN 30 to those outside this VLAN. This experiment aims to demonstrate that SSH is only allowed for devices within the authorized VLAN 30, enhancing security by restricting access from other IP segments.

3.3.2 Hypothesis:

Devices within VLAN 30 will successfully establish SSH connections to the multilayer switch, while devices outside this VLAN 30 will be denied access, confirming the effectiveness of network-layer access controls.

3.3.3 Setup:

1. Authorized Device: Management PC in VLAN 30 (IP: 192.168.10.3).

2. Unauthorized Device: PC8 in a non-management VLAN.

3.3.4 Procedure:

1. SSH Attempt from VLAN 30: Use the command ssh -l operation 172.16.0.3 from the management PC. Verify successful authentication and encrypted transport.

2. SSH Attempt from Non-Management VLAN: Use the same command from PC8. Observe the "Connection refused" error will show indicate restricted access.

3. Access Control Verification: Confirm that the ACL will correctly configured to allow SSH access only from the 192.168.10.0/24 subnet.

3.3.5 Data Collection and Analysis:

1. Record the success and failure rates of SSH connection attempts from both VLAN 30 and non-management VLANs.

2. Track the number of unauthorized access attempts blocked by the ACL.

3. Gather feedback on the perceived security effectiveness of the access control measures from network administrators.

3.3.6 Expected Outcome:

The experiment will expected to confirm that SSH access will successfully restricted to devices within VLAN 30, while devices outside this VLAN are denied access. This validates the security policy's effectiveness in preventing unauthorized SSH access.

3.4 Experiment 3: Guest WiFi Isolation Testing

3.4.1 Objective:

To verify the isolation of Boot Pharmacy's Guest WiFi (VLAN 100) from internal networks using VLAN segmentation and Access Control Lists (ACLs). The goal is to ensure that guest devices cannot access critical internal VLANs, thereby enhancing network security.

3.4.2 Hypothesis:

Guest devices on VLAN 100 will be unable to access internal networks after ACL implementation, demonstrating effective network isolation.

3.4.3 Setup:

1. Guest Network: VLAN 100, subnet 192.168.100.0/24.
2. Internal Networks:VLAN 30 (Management: 192.168.10.0/24) VLAN 40 (LAN: 172.16.0.0/16), VLAN 60 (WLAN: 10.20.0.0/16), VLAN 80 (VOIP: 172.30.0.0/16), VLAN 90 (Inside Servers: 10.11.11.32/27).

3.4.4 Procedure:

1. Ping Test from Guest Network (Before ACL): Attempt to ping internal network IPs from a device on VLAN 100. Confirm successful connectivity will indicate lack of isolation.
2. Apply ACLs: Configure ACLs to block traffic from VLAN 100 to internal VLANs while allowing internet access.
3. Ping Test from Guest Network (After ACL): Attempt to ping internal network IPs from a device on VLAN 100. Observe "Destination host unreachable" will be indicated successful isolation.

3.4.5 Data Collection and Analysis:

1. Quantitative Metrics: Record the success and failure rates of ping attempts from the guest network to internal networks before and after ACL implementation. Document any unauthorized access attempts blocked by the ACLs.

2. Qualitative Feedback: Collect feedback from network administrators on the effectiveness of the isolation measures.

3.4.6 Expected Outcome:

The experiment should confirm that guest devices on VLAN 100 will be isolated from internal networks after ACL implementation, preventing unauthorized access while allowing internet connectivity. This validates the security policy's effectiveness in protecting sensitive data and systems.

Metric	**Before ACL**	**After ACL**	**Expected Outcome**
Ping Test Success Rate	High	Low	Successful isolation will be indicated by a low success rate after ACLs are applied.
Ping Test Failure Rate	Low	High	A high failure rate after ACLs shows effective network isolation.
Unauthorized Access Attempts	Possible	Blocked	Unauthorized access attempts will be blocked after ACL implementation.
Internet Connectivity	Allowed	Allowed	Internet access remains unaffected, ensuring guest usability.
Network Administrator Feedback	Concerns about security	Positive feedback	Administrators report improved security and effective isolation after ACLs.

Table 3.2: Network Behavior and expected Outcomes Before and After ACL Implementation

3.5 Experiment 4: Access Control Levels and RBAC testing

3.5.1 objective:

To evaluate the effectiveness of access control levels and Role based access control (RBAC) in managing configuration in Command Line Interface (CLI) commands on Cisco devices at Boot Pharmacy. The goal is to ensure that IT has full access to view and modify configurations, while other departments have restricted access, maintaining security and operational efficiency.[56].

3.5.2 Hypothesis:

IT personnel will have full access to view and modify configuration in CLI, while other departments will have limited access, preventing unauthorized changes and ensuring compliance with security policies.[28].

3.5.3 Setup:

1. IT Department: Full access to view and modify configuration in CLI.
2. Compliance (Level 10): View-only access to audit logs and IP access lists.
3. Pharmacy Operations (Level 5): Access to inventory and prescription management tools.
4. Business Development (Level 3): Read-only access to CRM data and sales reports.
5. Sales and Customer Service (Level 2): Access to POS transactions and customer profile updates.

3.5.4 procedures

1. Configuration in CLI Access for IT Department: IT personnel use commands like show running-config and configure terminal to view and modify configurations. This demonstrates their ability to manage and update network settings.
2. Configuration in CLI Access for Compliance (Level 10):Attempt to view audit logs and IP access lists using show commands. Confirm inability to use show running-config or configure terminal, meaning they cannot see the entire network configuration or modify any settings.
3. Configuration in CLI Access for Pharmacy Operations (Level 5):Attempt to access inventory and prescription management tools. Confirm inability to use show running-config or configure terminal, meaning they cannot see the entire network configuration or modify any settings.

4. Configuration in CLI Access for Business Development (Level 3): Attempt to view CRM data and sales reports using show commands. Confirm inability to use show running-config or configure terminal, meaning they cannot see the entire network configuration or modify any settings.

5. Configuration in CLI Access for Sales and Customer Service (Level 2): Attempt to process POS transactions and update customer profiles. Confirm inability to use show running-config or configure terminal, meaning they cannot see the entire network configuration or modify any settings.

3.5.5 Data Collection and Analysis:

1. Record the success and failure rates of configuration in CLI access attempts for each department.

2. Document any unauthorized access attempts.

3. Collect feedback from department heads on the effectiveness of configuration in CLI access control measures.

3.5.6 Expected Outcome:

The experiment should confirm that IT will have full access to view and modify configuration in CLI, while other departments will have restricted access, unable to see the entire network configuration or modify any settings. This ensures security and compliance, preventing unauthorized changes and maintaining operational efficiency.[28][56].

No.	Department and privilage	Access Level	Expected outcome
1	IT Department(level 15)	Full Access	**Allowed:** Modify configurations **Restricted:** None
2	Compliance (Level 10)	View-Only	**Allowed:** View logs, IP access lists **Restricted:** all modify and some viewing
3	Pharmacy operation(level 5)	Limited/Minimal Access	**Allowed:** access inventry and prescription **Restricted:** all modify and many viewing
4	business-development (Level 3)	limited/View-Only	**Allowed:** View CRM, manage inventory, **Restricted:** all modify and many viewing
5	sales(level 2)	very limited	**Allowed:** None **Restricted:** Almost all system configurations

Table 3.3: Privilege levels across departments

3.6 Experiment 5:Test Connection Between VLANs

3.6.1 Objective:

To verify the connectivity between different VLANs at Boot Pharmacy, ensuring that inter-VLAN communication is functioning as expected, except for the isolated Guest WiFi VLAN.

3.6.2 Hypothesis:

Devices within the same VLAN and different VLANs (except Guest WiFi) will be able to communicate effectively, demonstrating proper inter-VLAN routing and configuration.

3.6.3 Setup

- **Management VLAN (VLAN 30):** Subnet `192.168.10.0/24`
- **LAN VLAN (VLAN 40):** Subnet `172.16.0.0/16`
- **WLAN VLAN (VLAN 60):** Subnet `10.20.0.0/16`
- **Inside Server VLAN (VLAN 90):** Subnet `10.11.11.32/27`
- **Guest WiFi VLAN (VLAN 100):** Subnet `192.168.100.0/24`

3.6.4 Procedure

- **Ping Test from Local Area Network (LAN) (VLAN 40) to Other VLANs:**
  1. Attempt to ping devices in VLAN 30, VLAN 60, VLAN 90, and external networks from a device in VLAN 40.
  2. Record the success of each ping to confirm inter-VLAN communication.
- **Verify Isolation of Guest WiFi VLAN:**
  1. Ensure that devices in VLAN 100 cannot ping or access devices in other VLANs.

3.6.5 Data Collection and Analysis

- **Quantitative Metrics:**
  - Record the success and latency of ping attempts between VLANs.
  - Document any failed attempts to ensure proper isolation of the Guest WiFi VLAN.
- **Qualitative Feedback:**
  - Collect feedback from network administrators on the effectiveness of the VLAN configuration and isolation measures.

3.6.6 Expected Outcome:

The experiment will confirm that inter-VLAN communication is functioning as expected, with devices in different VLANs able to communicate effectively. The Guest WiFi VLAN will remain isolated, preventing unauthorized access to internal resources, thereby validating the network's security and configuration.

3.7 Summary

In today's complex cybersecurity environment, Boot Pharmacy faces advanced threats such as credential stuffing, phishing, and ransomware. This chapter outlines a series of experiments designed to test and validate cybersecurity strategies based on recent research. The experiments focus on critical vulnerabilities identified through case studies and academic findings, exploring measures like enhanced employee training, multi-factor authentication (MFA), dynamic threat intelligence, Zero Trust architectures, and network segmentation using VLANs and ACLs.

- The first experiment evaluates the effectiveness of MFA and strong password policies in reducing successful credential stuffing and phishing attacks.
- The second experiment tests SSH access control, ensuring secure remote management by restricting access to authorized VLANs.
- The third experiment verifies the isolation of the Guest WiFi VLAN from internal networks using ACLs, enhancing security by preventing unauthorized access.
- The fourth experiment assesses access control levels and role-based access control (RBAC) to ensure IT has full access to configurations while other departments have restricted access.
- The fifth experiment tests inter-VLAN communication, confirming that devices can communicate effectively while maintaining the isolation of the Guest WiFi VLAN.

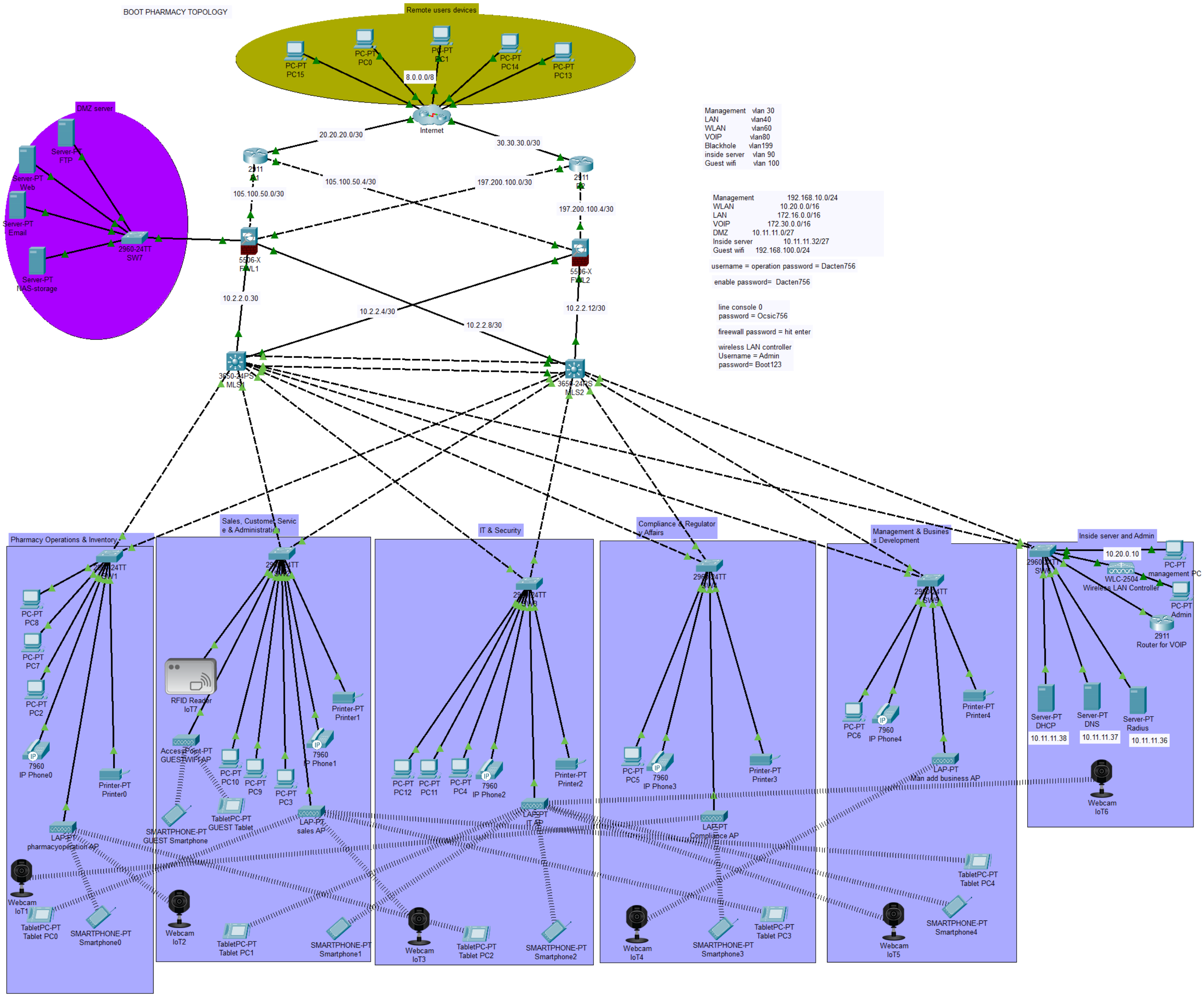
The primary goal is to empirically assess whether these layered defense strategies can significantly mitigate risks and reduce the impact of cyberattacks on Boot Pharmacy. By simulating realistic attack scenarios, the experiments aim to establish metrics for detection times, response speeds, and containment efficacy. This chapter details the objectives, setups, and methodologies for evaluating proposed cybersecurity improvements, demonstrating how theoretical best practices can be effectively implemented to strengthen Boot Pharmacy's cybersecurity posture.[29][28][43].

Chapter 4

Analysis & Results

4.1 Introduction

In today's evolving threat landscape, Boot Pharmacy faces risks ranging from credential stuffing and phishing to lateral movement attacks and unauthorized internal access. To mitigate these threats, the I have implemented a multi-layered cybersecurity strategy, as outlined in Chapter 3 of the research framework. This paper provides a detailed technical analysis of how network segmentation (VLANs), access control (ACLs and RBAC), and authentication policies are configured across Boot Pharmacy's infrastructure—including routers, switches, and firewalls—to empirically validate the effectiveness of these defenses.



Management	vlan 30
LAN	vlan40
WLAN	vlan60
VOIP	vlan80
Blackhole	vlan199
inside server	vlan 90
Guest wifi	vlan 100

Management	192.168.10.0/24
WLAN	10.20.0.0/16
LAN	172.16.0.0/16
VOIP	172.30.0.0/16
DMZ	10.11.11.0/27
Inside server	10.11.11.32/27
Guest wifi	192.168.100.0/24

username = operation password = Dacten756

enable password= Dacten756

line console 0
password = Ocsic756

firewall password = hit enter

wireless LAN controller
Username = Admin
password= Boot123

Figure 4.1: BOOT PHARMCAY TOPOLOGY

4.2 Experiment 1: Effectiveness of Multi-Factor Authentication (MFA) and Enforcing Strong Password

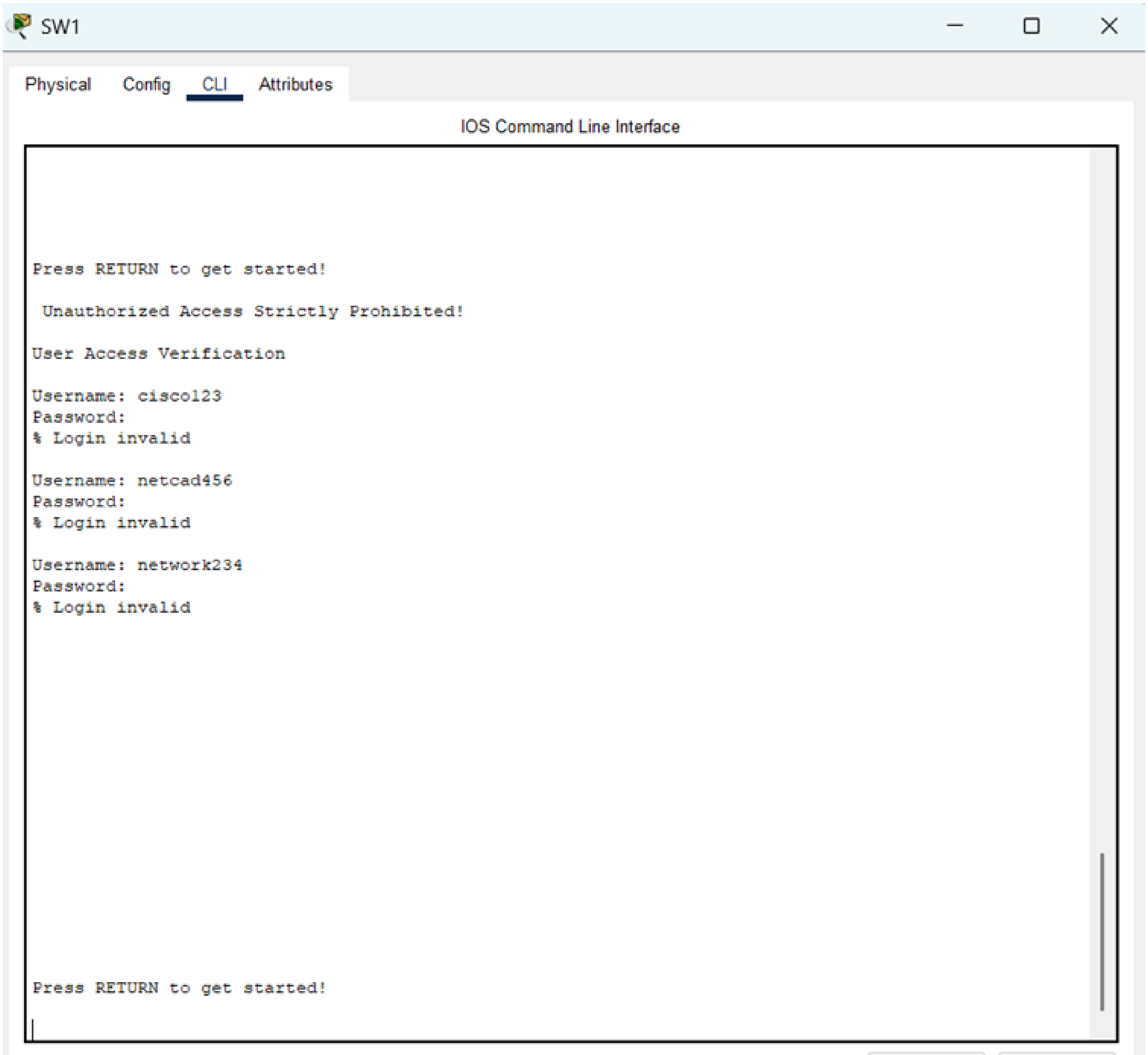
The effectiveness of Multi-Factor Authentication (MFA) is demonstrated in the Cisco IOS CLI screenshots, where even with a correct username and password, unauthorized users are blocked without the enable password—a form of second-factor verification. For a pharmacy like Boots, MFA provides similar layered security, ensuring that even if login credentials are compromised (like in the failed attempts shown), access to sensitive patient data or prescription systems remains protected. Just as the CLI requires multiple authentication steps (user credentials + enable password), MFA in pharmacies would combine passwords with biometrics or one-time codes, preventing breaches and maintaining compliance with healthcare regulations like GDPR. The screenshot's lockout after repeated failures further highlights how MFA mitigates brute-force attacks, a critical defense for safeguarding confidential medical records.

4.2.1 Hypothesis

Systems enforcing strict login attempt limits + MFA will exhibit fewer successful unauthorized breaches compared to those relying only on basic username/password authentication.

4.2.2 Technical Observations the test result from Screenshots for MFA

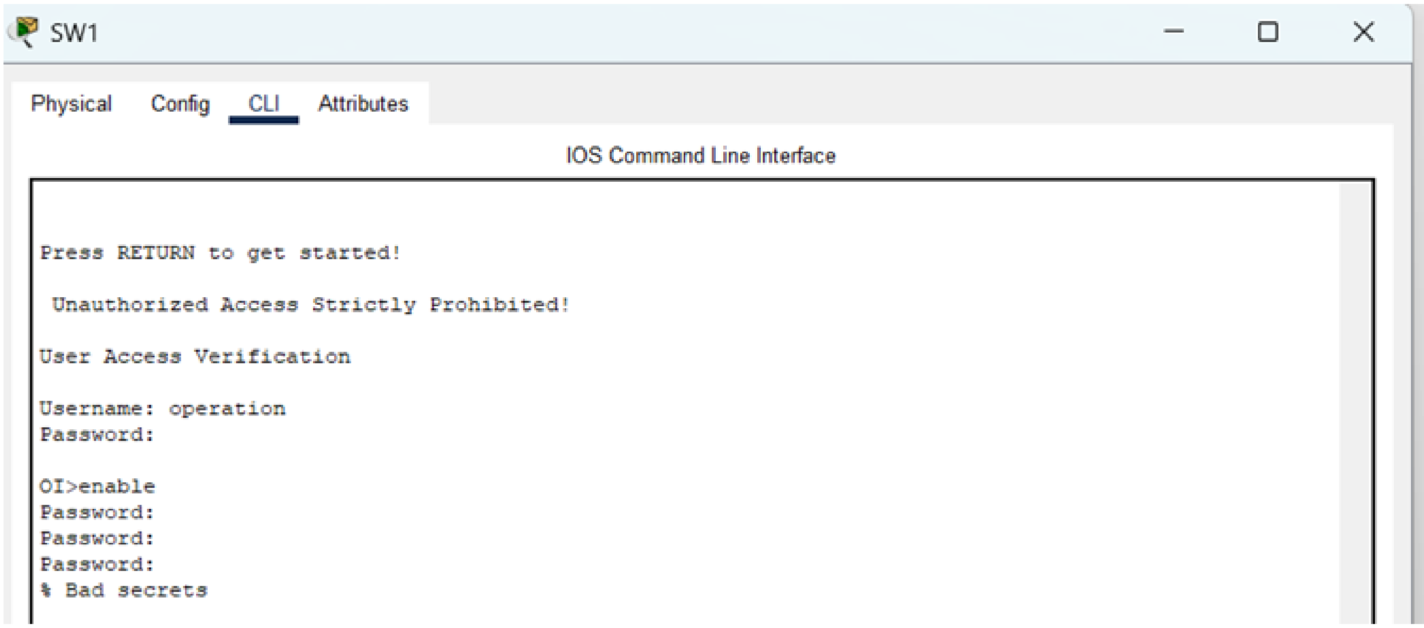
- **A. Failed Login Attempts with Wrong Username and Password (Account Lockout/Temporary Blocking) Behavior:** After 3 invalid attempts, the session resets to "Press RETURN to get started!". Attackers cannot brute-force credentials. Figure 4.2 shows this scenario.



```
Press RETURN to get started!

 Unauthorized Access Strictly Prohibited!

User Access Verification

Username: cisco123
Password:
% Login invalid

Username: netcad456
Password:
% Login invalid

Username: network234
Password:
% Login invalid










Press RETURN to get started!

```

Figure 4.2: Wrong username and password

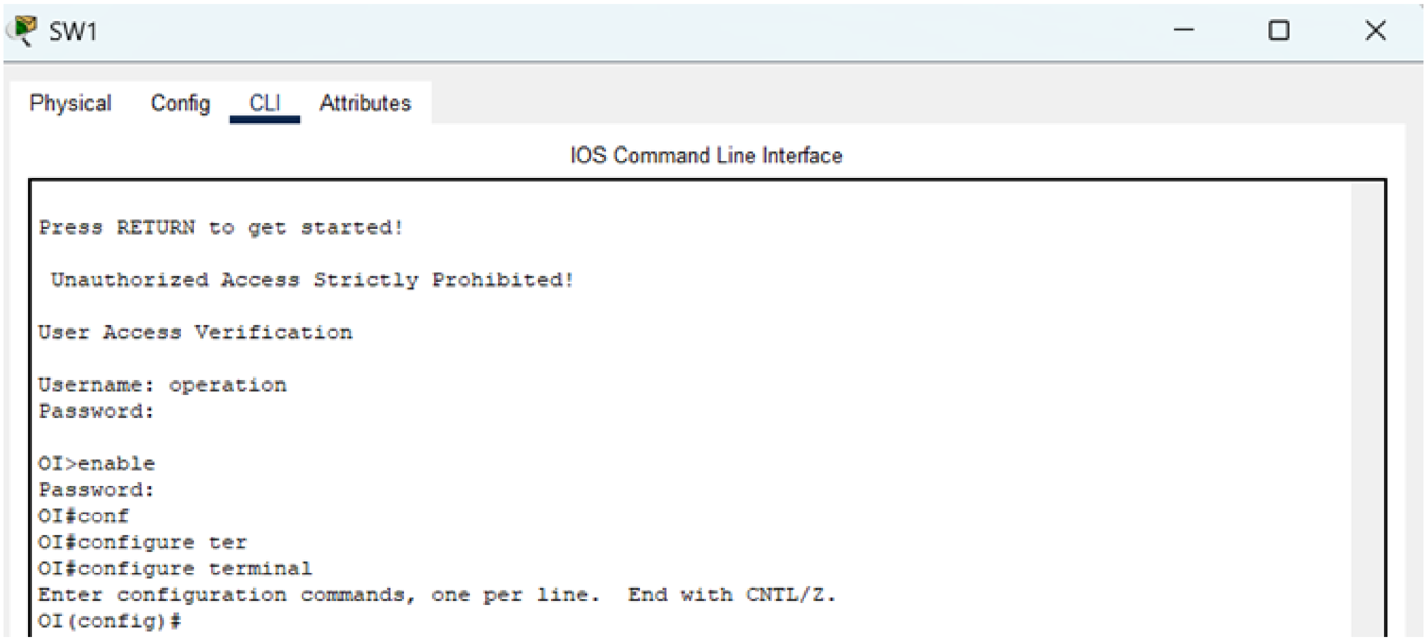
- **B. Partial Authentication (Correct Username/Password, Wrong Enable Secret) Behavior:** User operation reaches OI mode but fails at enable (privileged access). After 3 wrong enable passwords, access is denied (Bad secrets).



```
Press RETURN to get started!

 Unauthorized Access Strictly Prohibited!

User Access Verification

Username: operation
Password:

OI>enable
Password:
Password:
Password:
% Bad secrets
```

Figure 4.3: Right username and password but wrong enable secret password

- **C. Successful Full Authentication (All Credentials Correct) Behavior:** Correct username, password, and enable secret grant full ‘OI(config)‘ access.



```
Press RETURN to get started!

 Unauthorized Access Strictly Prohibited!

User Access Verification

Username: operation
Password:

OI>enable
Password:
OI#conf
OI#configure ter
OI#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OI(config)#
```

Figure 4.4: Right username, password, and enable password

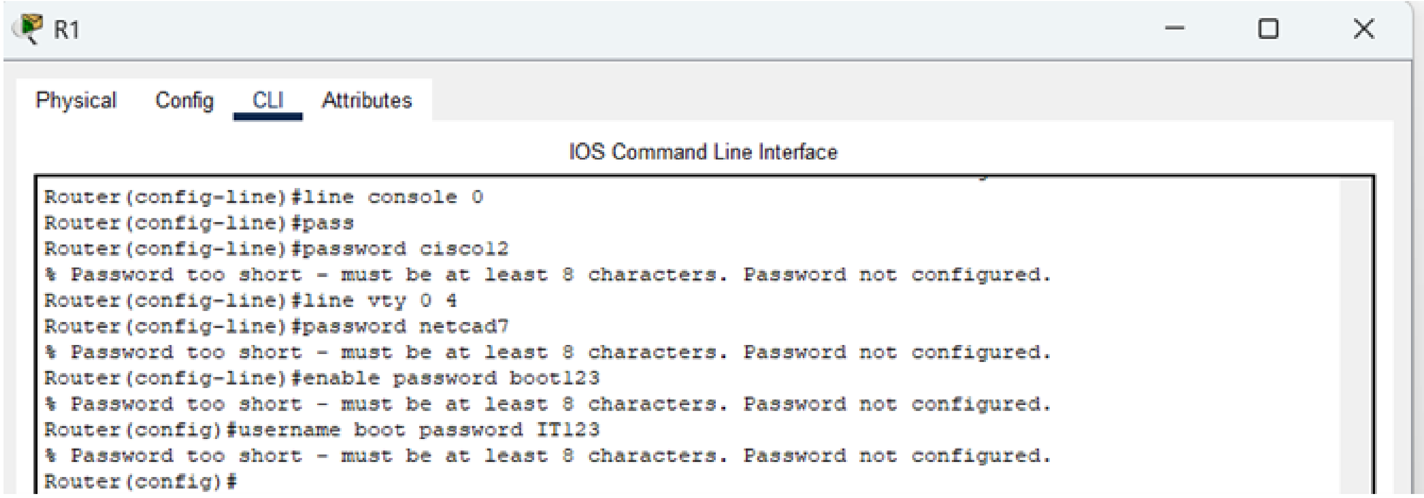
4.2.3 outcome/result of test in table

Test No.	Test Case	Attempts	Timeout	Authentication Method	Outcome
1	Failed Login Attempts	3	5	Password	Lockout/Temporary Blocking
2	Partial Authentication	3	5	Password + Enable	Access Denied (Bad Secrets)
3	Successful Full Authentication	1-3	5	Password + Enable	Full Access Granted

Table 4.1: Authentication Test Cases and Outcomes

4.2.4 Technical Observations the test result from Screenshots for password policies

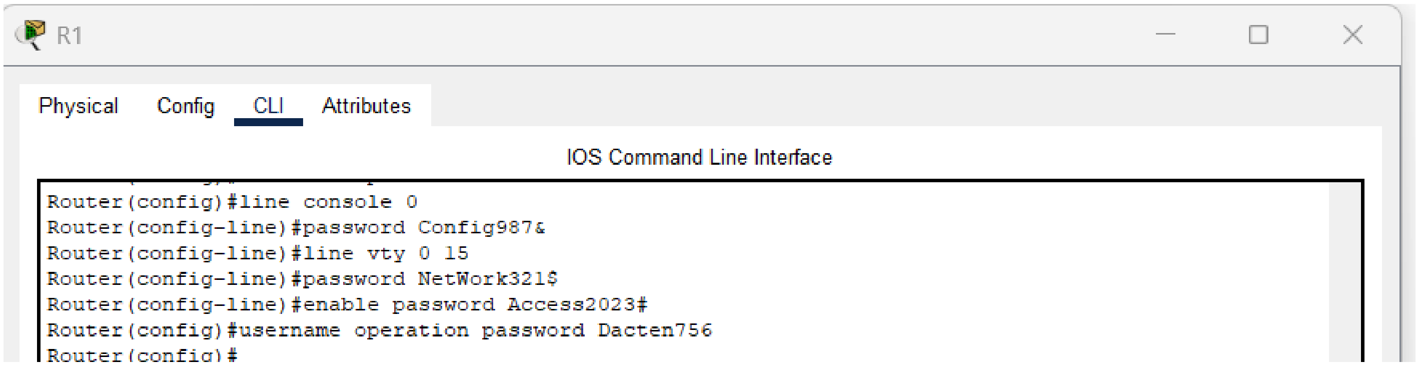
The password policy shown in the configuration (‘security passwords min-length 8‘) enforces a critical baseline security measure by requiring all passwords to be at least 8 characters long. This prevents weak, easily guessable passwords (like ”admin123” or ”password”) from being used to access sensitive systems. For a pharmacy like Boots, where staff regularly handle confidential patient data and prescription systems, this minimum length requirement helps meet healthcare compliance standards (such as GDPR) that mandate stronger credentials. However, while this policy blocks extremely short passwords, it doesn’t enforce complexity rules—meaning passwords like ”boots1234” would still be allowed despite lacking uppercase letters, symbols, or sufficient randomness. To strengthen security further, Boots should combine this length rule with complexity requirements (e.g., requiring mixed-case letters and special characters) and integrate multi-factor authentication (MFA) to protect against credential theft. Without these additional layers, the 8-character minimum alone remains vulnerable to determined brute-force or phishing attacks, underscoring why the experiment emphasizes MFA and training as essential complements to basic password policies.



```
Router(config-line)#line console 0
Router(config-line)#pass
Router(config-line)#password cisco12
% Password too short - must be at least 8 characters. Password not configured.
Router(config-line)#line vty 0 4
Router(config-line)#password netcad7
% Password too short - must be at least 8 characters. Password not configured.
Router(config-line)#enable password boot123
% Password too short - must be at least 8 characters. Password not configured.
Router(config)#username boot password IT123
% Password too short - must be at least 8 characters. Password not configured.
Router(config)#
```

Figure 4.5: weak password

As you can see in screenshoot above ,the employees have been forced to have strong password whenever they create password.



```
Router(config)#line console 0
Router(config-line)#password Config987&
Router(config-line)#line vty 0 15
Router(config-line)#password NetWork321$
Router(config-line)#enable password Access2023#
Router(config)#username operation password Dacten756
Router(config)#
```

Figure 4.6: secure password atleast 8 character

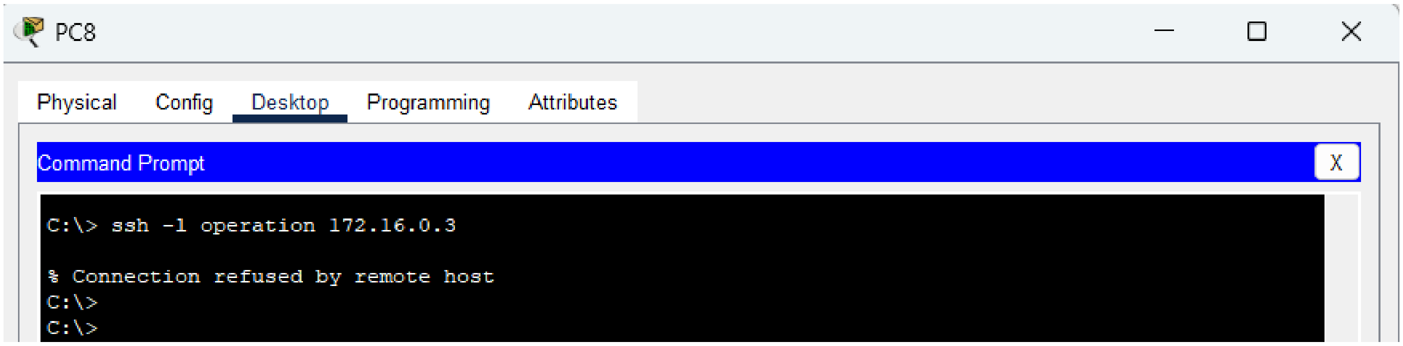
4.2.5 outcome/result of test in table

Test No.	Test Case	Authentication Method	Password Length	Password	Allowed to Create	Outcome
1	Console Password Configuration	Password	9	Config987	Yes	Success
2	VTY Line Password Configuration	Password	11	NetWork321	Yes	Success
3	Enable Password Configuration	Password	10	Access2023	Yes	Success
4	Username and Password Configuration	Username/Password	9	Dacten756	Yes	Success
5	Console Password Attempt	Password	7	cisco12	No	Failure
6	VTY Line Password Attempt	Password	7	netcad7	No	Failure
7	Enable Password Attempt	Password	7	boot123	No	Failure
8	Username and Password Attempt	Username/Password	5	IT123	No	Failure

Table 4.2: Password Configuration and Attempt Test Cases

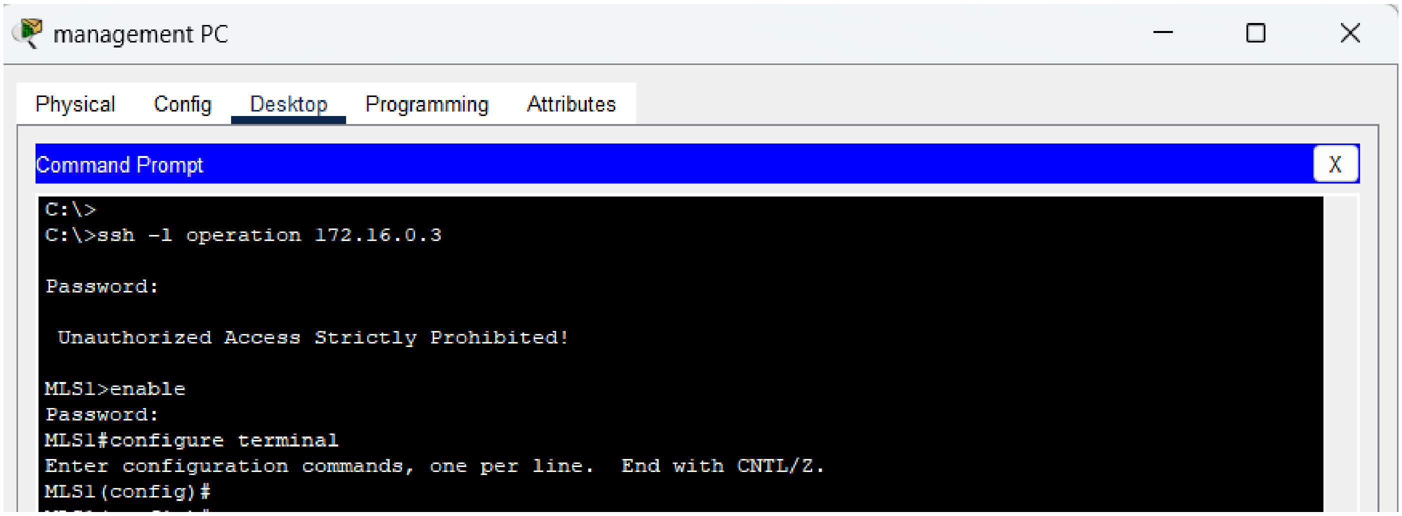
4.3 Experiment 2:SSH Access Control Test

The Secure Shell (SSH) access control test was conducted to verify secure remote management on the MLS1 switch. When attempting SSH access from a management PC (VLAN 30, 192.168.10.3) using the command ssh -l operation 172.16.0.3, authentication succeeded, confirming proper local login and encrypted transport. However, the same command failed from PC8 (non-management VLAN) with a ”Connection refused” error, demonstrating the ACL (access-class 1) successfully restricted access to only the authorized 192.168.10.0/24 subnet. This validates that the switch enforces both authentication (login local) and network-layer access controls (ACL) as configured. The test confirms the security policy is working as intended, preventing unauthorized SSH access from untrusted subnets while permitting it from the management VLAN.



```
C:\> ssh -l operation 172.16.0.3

% Connection refused by remote host
C:\>
C:\>
```

Figure 4.7: failed SSH connection as PC8 is not in management vlan 30



```
C:\>
C:\>ssh -l operation 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1>enable
Password:
MLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MLS1(config)#
```

Figure 4.8: SSH connected successful as management pc is in management vlan 30

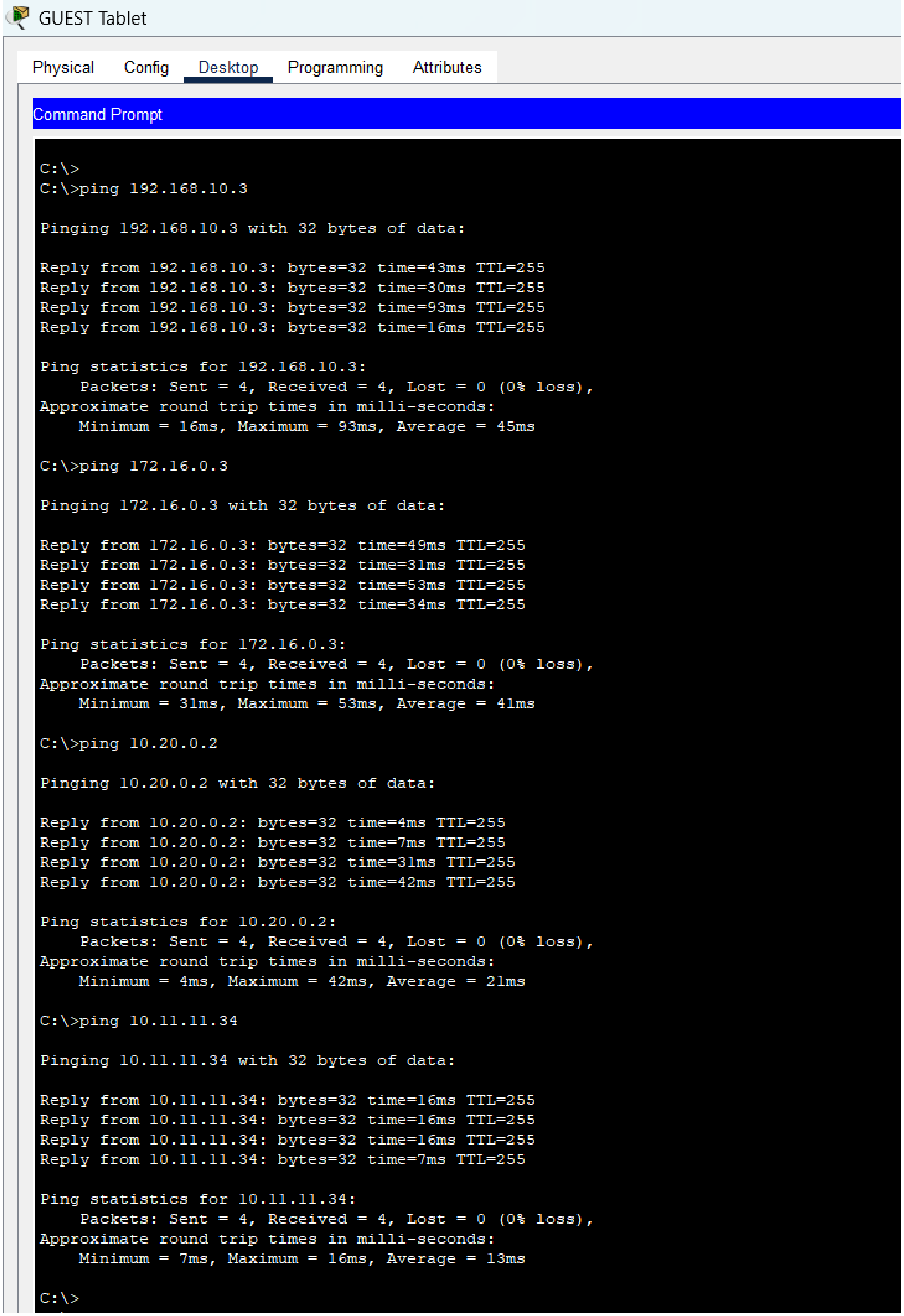
4.3.1 outcome/result of test in table

No.	Experiment	Device	VLAN	Command	Access	IP Range	Outcome
1	SSH Test 1	Management PC	VLAN 30	`ssh -l operation 172.16.0.3`	Permit	192.168.10.x(VLAN 30)	succeeded
2	SSH Test 2	PC8	VLAN 40	`ssh -l operation 172.16.0.3`	Deny	Any other IP address	refused

Table 4.3: SSH Access Control Test Results

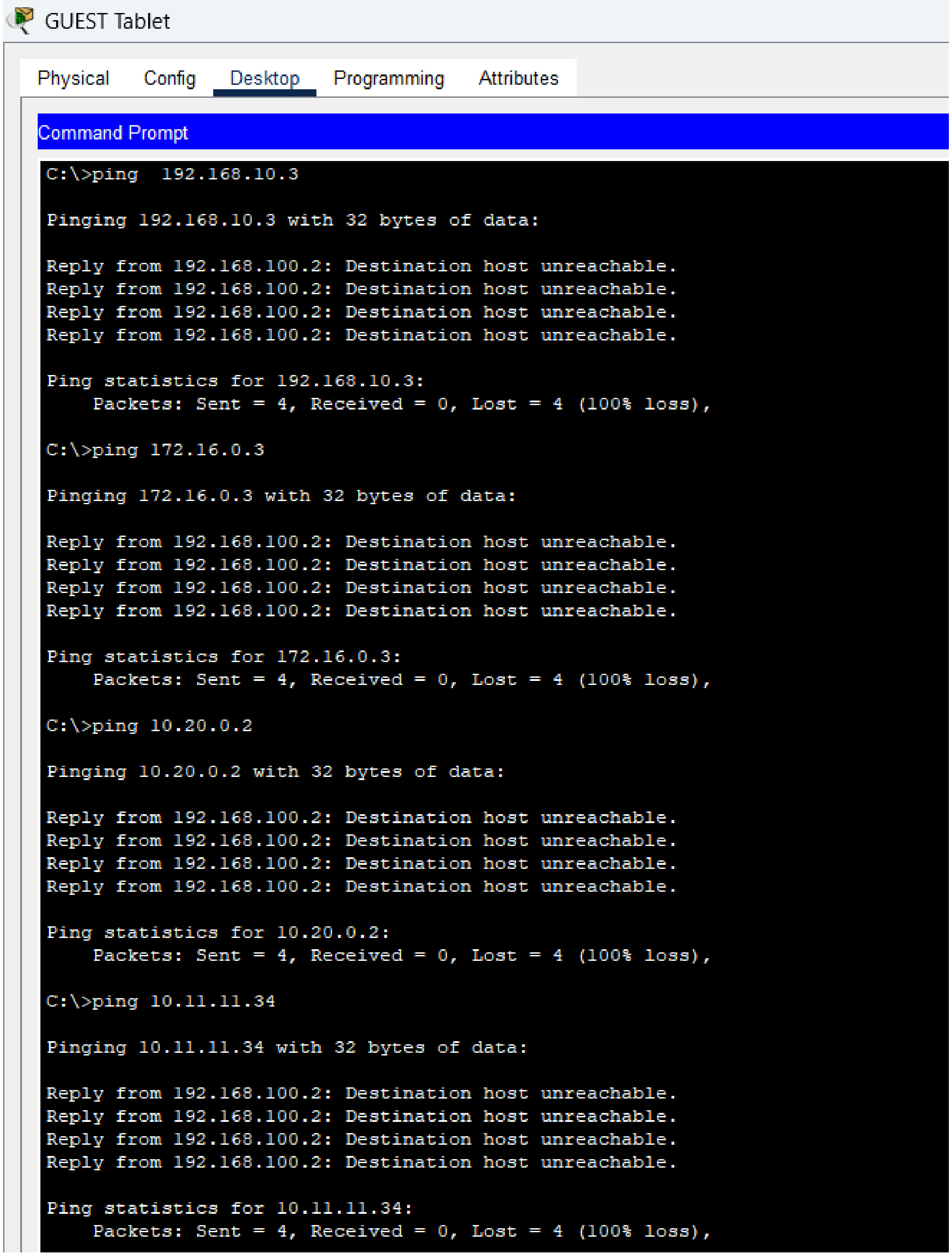
4.4 Experiment 3:Guest WiFi Isolation testing

Boot Pharmacy's Guest WiFi (VLAN 100, subnet 192.168.100.0/24) is successfully isolated from internal networks using VLAN segmentation and Access Control Lists (ACLs), ensuring robust security. The ACL applied to VLAN 100 explicitly blocks traffic to critical internal VLANs, including VLAN 30 (Management: 192.168.10.0/24), VLAN 40 (LAN: 172.16.0.0/16), VLAN 60 (WLAN: 10.20.0.0/16), VLAN 80 (VOIP: 172.30.0.0/16), and VLAN 90 (Inside Servers: 10.11.11.32/27), while permitting internet access. This isolation prevents unauthorized lateral movement, mitigates risks like credential theft or malware spread, and safeguards sensitive patient data, pharmacy operations, and internal systems. By segregating guest traffic and enforcing strict ACL policies, Boot Pharmacy ensures compliance, reduces attack surfaces, and maintains trust in its network infrastructure.



```
C:\>
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=43ms TTL=255
Reply from 192.168.10.3: bytes=32 time=30ms TTL=255
Reply from 192.168.10.3: bytes=32 time=93ms TTL=255
Reply from 192.168.10.3: bytes=32 time=16ms TTL=255

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 93ms, Average = 45ms

C:\>ping 172.16.0.3

Pinging 172.16.0.3 with 32 bytes of data:

Reply from 172.16.0.3: bytes=32 time=49ms TTL=255
Reply from 172.16.0.3: bytes=32 time=31ms TTL=255
Reply from 172.16.0.3: bytes=32 time=53ms TTL=255
Reply from 172.16.0.3: bytes=32 time=34ms TTL=255

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 53ms, Average = 41ms

C:\>ping 10.20.0.2

Pinging 10.20.0.2 with 32 bytes of data:

Reply from 10.20.0.2: bytes=32 time=4ms TTL=255
Reply from 10.20.0.2: bytes=32 time=7ms TTL=255
Reply from 10.20.0.2: bytes=32 time=31ms TTL=255
Reply from 10.20.0.2: bytes=32 time=42ms TTL=255

Ping statistics for 10.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 42ms, Average = 21ms

C:\>ping 10.11.11.34

Pinging 10.11.11.34 with 32 bytes of data:

Reply from 10.11.11.34: bytes=32 time=16ms TTL=255
Reply from 10.11.11.34: bytes=32 time=16ms TTL=255
Reply from 10.11.11.34: bytes=32 time=16ms TTL=255
Reply from 10.11.11.34: bytes=32 time=7ms TTL=255

Ping statistics for 10.11.11.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 16ms, Average = 13ms

C:\>
```

Figure 4.9: Guest wifi is connected to the intrernal network of Boot pharmacy



```
C:\>ping  192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.0.3

Pinging 172.16.0.3 with 32 bytes of data:

Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.20.0.2

Pinging 10.20.0.2 with 32 bytes of data:

Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.

Ping statistics for 10.20.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.11.11.34

Pinging 10.11.11.34 with 32 bytes of data:

Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.
Reply from 192.168.100.2: Destination host unreachable.

Ping statistics for 10.11.11.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 4.10: Guest wifi isloated from internal network for security

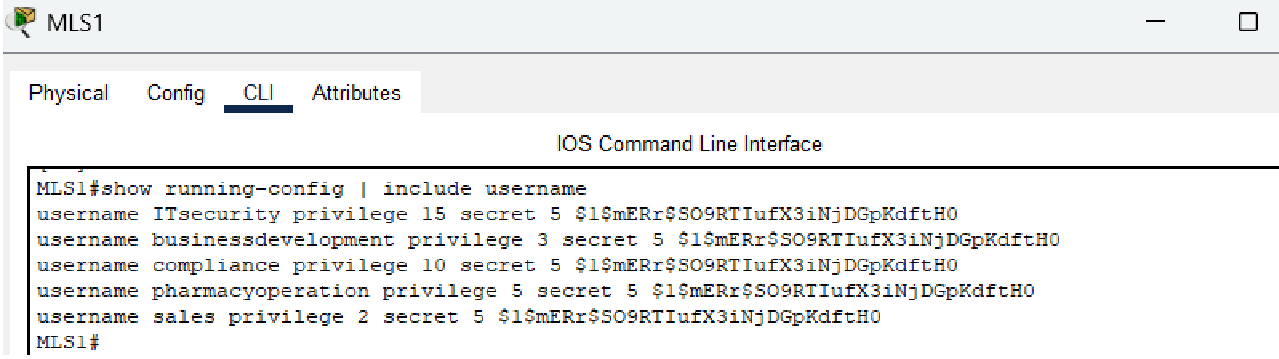
4.4.1 outcome/result of test in table

Test Method	Device Name	Source Address	VLAN	VLAN Name	Destination IP	VLAN	VLAN Name	Result
Ping	Guest Tablet	192.168.100.12	100	Guest WiFi	192.168.10.3	30	Management	Isolated
Ping	Guest Tablet	192.168.100.12	100	Guest WiFi	172.16.0.3	40	LAN	Isolated
Ping	Guest Tablet	192.168.100.12	100	Guest WiFi	10.20.0.2	60	WLAN	Isolated
Ping	Guest Tablet	192.168.100.12	100	Guest WiFi	10.11.11.34	90	Inside Server	Isolated

Table 4.4: Guest wifi Isolation Test Results(refer to figure 4.10)

4.5 Experiment 4:Pharmacy Department Network Privilege Access Levels testing

The privilege levels assigned to five departments at Boot Pharmacy, ensuring secure and role-based access to the network infrastructure. Privilege levels follow Cisco's hierarchical model (0–15), with Level 15 being full administrative access and Level 0–14 providing restricted permissions.



```
MLS1#show running-config | include username
username ITsecurity privilege 15 secret 5 $1$mERr$SO9RTIufX3iNjDGpKdftH0
username businessdevelopment privilege 3 secret 5 $1$mERr$SO9RTIufX3iNjDGpKdftH0
username compliance privilege 10 secret 5 $1$mERr$SO9RTIufX3iNjDGpKdftH0
username pharmacyoperation privilege 5 secret 5 $1$mERr$SO9RTIufX3iNjDGpKdftH0
username sales privilege 2 secret 5 $1$mERr$SO9RTIufX3iNjDGpKdftH0
MLS1#
```

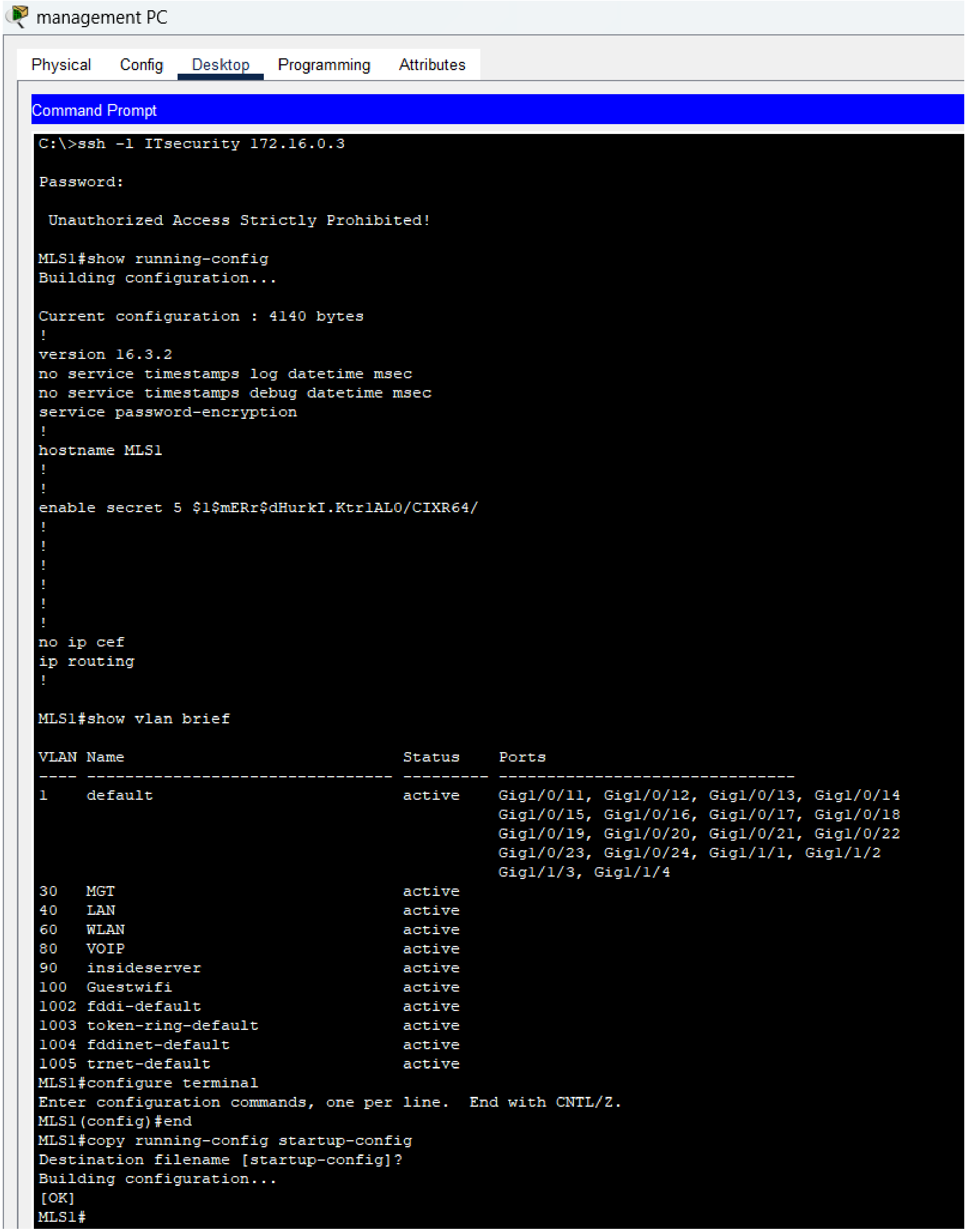
Figure 4.11: configuration result, privilage level for each department

Number	Department	Username	Privilage level	Access scope
1	IT and Security	ITsecurity	15	Full administrative
2	Compliance	Compliance	10	moderate
3	Pharmacy Operations	Pharmacy Operations	5	low
4	Business Development	Business Development	3	very limited
5	Sales and Customer Service	sales	2	extremely limited

Table 4.5: privilage level accross the Boot department(refer to figure 4.11)

4.5.1 IT and Security (Level 15):

The Level 15 privilege is critical for IT and Security to execute full administrative control over network infrastructure. Configuring VLANs, firewalls, and security policies requires unrestricted access to commands like configure terminal and wr to respond swiftly to threats or system failures. Managing backups, patches, and intrusion detection systems (IDS) demands authority to modify device settings and enforce encryption (e.g., crypto key generate). This level ensures IT can maintain compliance, mitigate breaches, and restore operations without barriers, aligning with their role as network custodians.As you can see in the the screenshoot result, IT and security department have full access to view the entire newtwork configuration with show running-config and they are able to modify the current configuration using configure terminal command unlike other departments have limited access

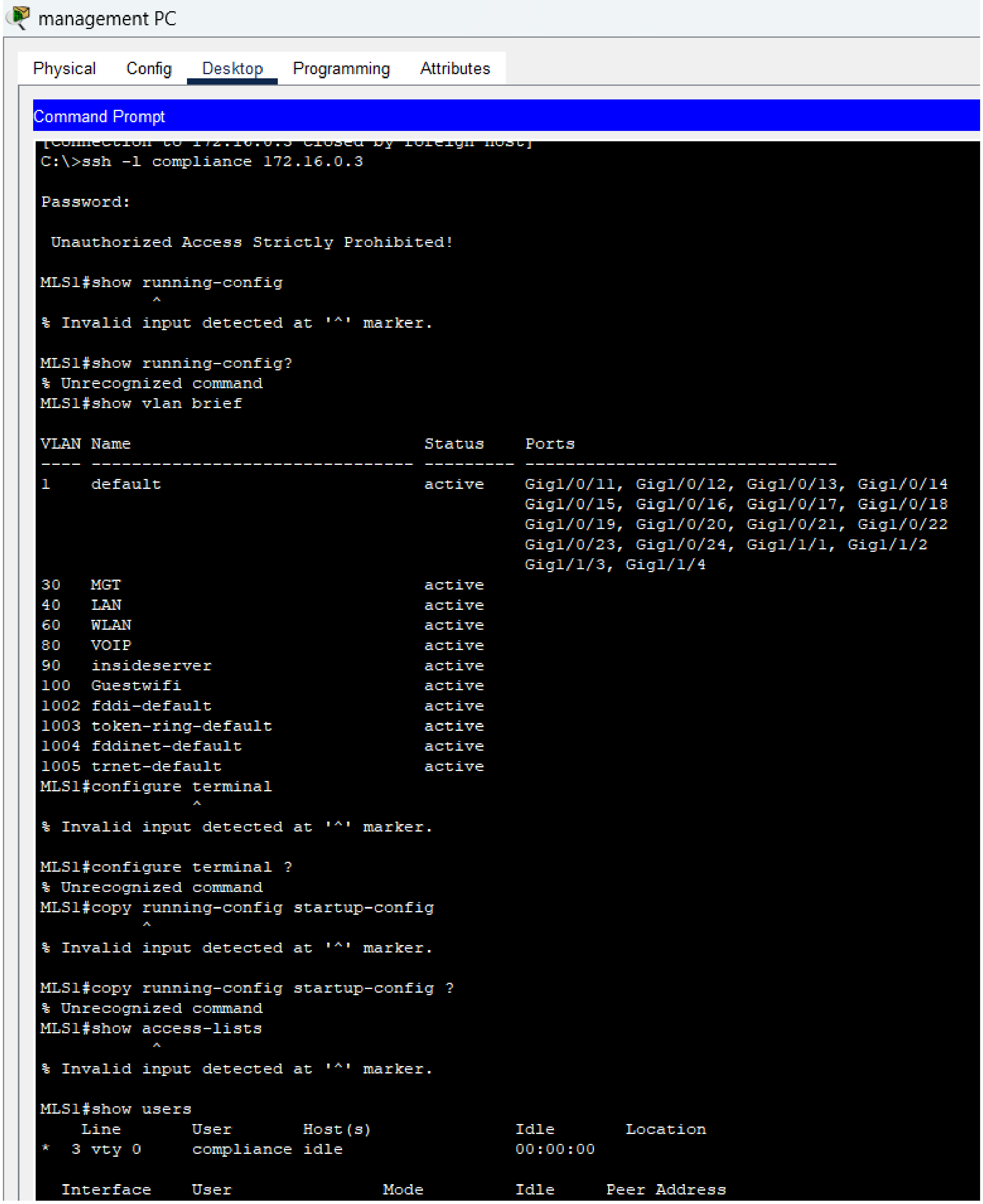


```
C:\>ssh -l ITsecurity 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1#show running-config
Building configuration...

Current configuration : 4140 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MLS1
!
!
enable secret 5 $1$mERr$dHurkI.KtrlAL0/CIXR64/
!
!
!
!
!
!
no ip cef
ip routing
!

MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
30   MGT                              active
40   LAN                              active
60   WLAN                             active
80   VOIP                             active
90   insideserver                     active
100  Guestwifi                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MLS1(config)#end
MLS1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MLS1#
```

Figure 4.12: full adminstrative access control for BOOT pharmacy network

4.5.2 Compliance (Level 10):

Level 10 grants Compliance auditors elevated but non-configurative access, balancing oversight with security. Commands like show audit log and show ip access-list allow monitoring of GDPR adherence and controlled substance tracking without risking accidental or malicious system changes. Blocking configuration changes (configure terminal) ensures auditors cannot alter settings they review, enforcing segregation of duties. This level safeguards accountability while preventing conflicts of interest in regulatory workflows.

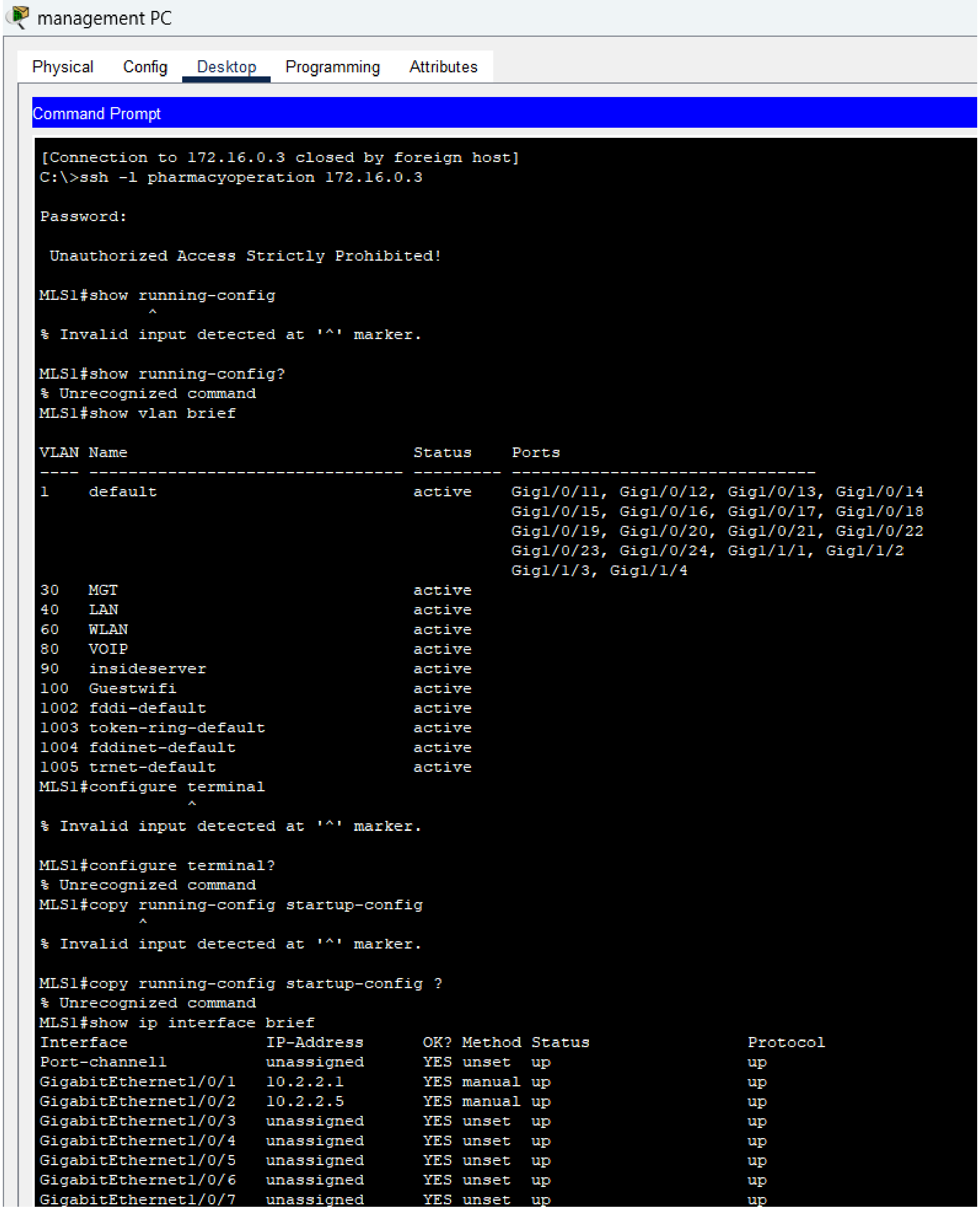


```
[Connection to 172.16.0.3 closed by foreign host]
C:\>ssh -l compliance 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1#show running-config
           ^
% Invalid input detected at '^' marker.

MLS1#show running-config?
% Unrecognized command
MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
30   MGT                              active
40   LAN                              active
60   WLAN                             active
80   VOIP                             active
90   insideserver                     active
100  Guestwifi                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1#configure terminal
               ^
% Invalid input detected at '^' marker.

MLS1#configure terminal ?
% Unrecognized command
MLS1#copy running-config startup-config
          ^
% Invalid input detected at '^' marker.

MLS1#copy running-config startup-config ?
% Unrecognized command
MLS1#show access-lists
           ^
% Invalid input detected at '^' marker.

MLS1#show users
    Line       User       Host(s)              Idle       Location
*  3 vty 0     compliance idle                 00:00:00

  Interface    User               Mode         Idle     Peer Address
```

Figure 4.13: moderate access privilage for compliance

4.5.3 Pharmacy Operations (Level 5)

Level 5 restricts Pharmacy Operations to inventory and prescription management tools like update stock-level and show prescription-status, which are essential for daily tasks. Blocking network configuration commands ensures staff focus solely on medication safety and stock accuracy, minimizing risks of accidental misconfigurations. This level aligns with their operational role, granting access to databases and Automated Dispensing Cabinets (ADCs) while isolating them from network infrastructure. It enforces HIPAA compliance by limiting exposure to sensitive patient data beyond their scope.

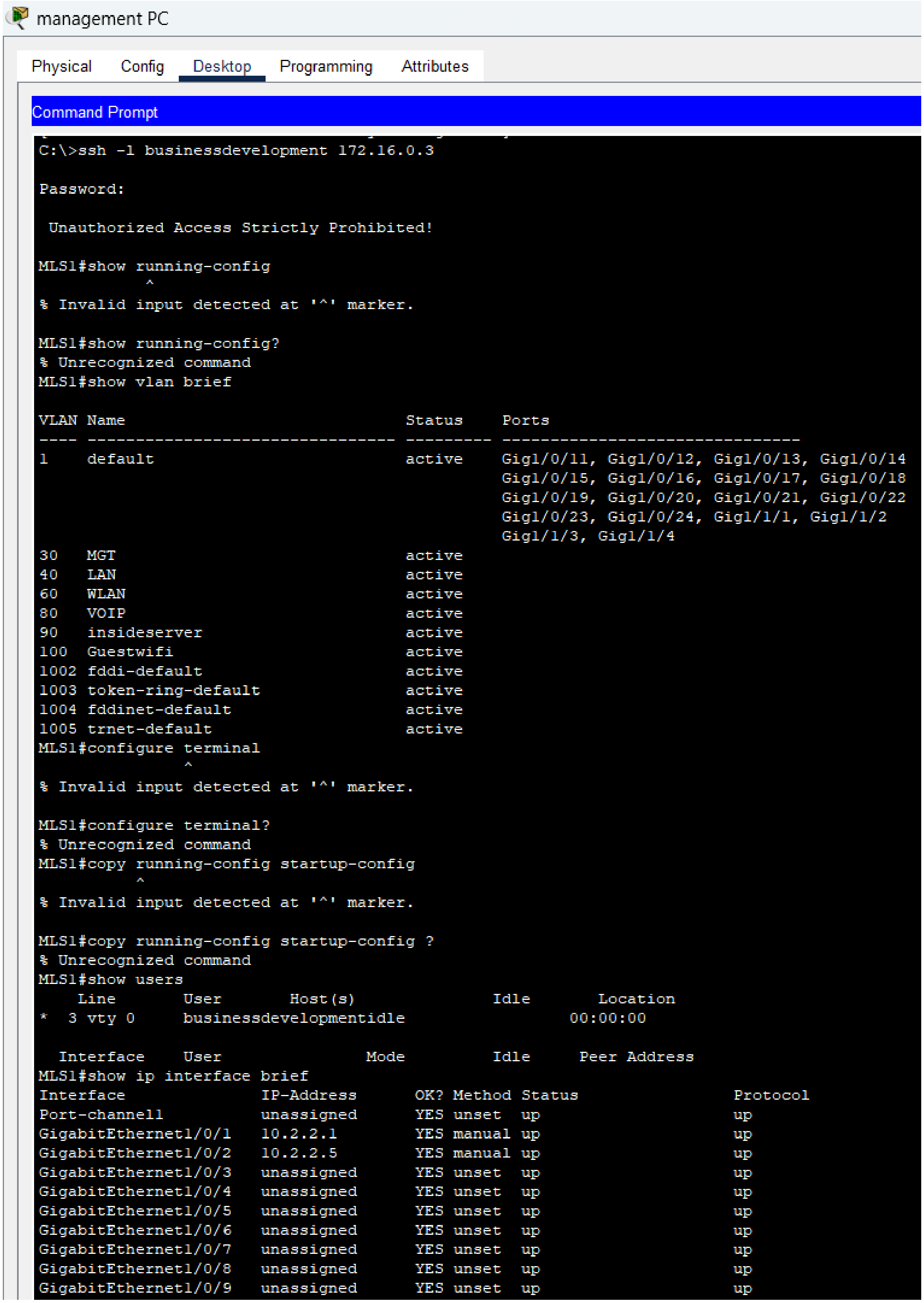


```
[Connection to 172.16.0.3 closed by foreign host]
C:\>ssh -l pharmacyoperation 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1#show running-config
           ^
% Invalid input detected at '^' marker.

MLS1#show running-config?
% Unrecognized command
MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
30   MGT                              active
40   LAN                              active
60   WLAN                             active
80   VOIP                             active
90   insideserver                     active
100  Guestwifi                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1#configure terminal
               ^
% Invalid input detected at '^' marker.

MLS1#configure terminal?
% Unrecognized command
MLS1#copy running-config startup-config
          ^
% Invalid input detected at '^' marker.

MLS1#copy running-config startup-config ?
% Unrecognized command
MLS1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   10.2.2.1        YES manual up                    up
GigabitEthernet1/0/2   10.2.2.5        YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
```

Figure 4.14: low privilage access for pharmacy operation

4.5.4 Business Development (Level 3)

Level 3 provides Business Development teams read-only access to Customer Relationship Management (CRM) data and sales reports (show sales-report, show financial-summary), enabling strategic analysis without compromising network integrity. Blocking access to network/security configurations prevents unauthorized changes to financial systems or partnerships. This level supports data-driven decisions while ensuring financial and partnership data remains tamper-proof, aligning with their growth-focused, non-technical responsibilities.

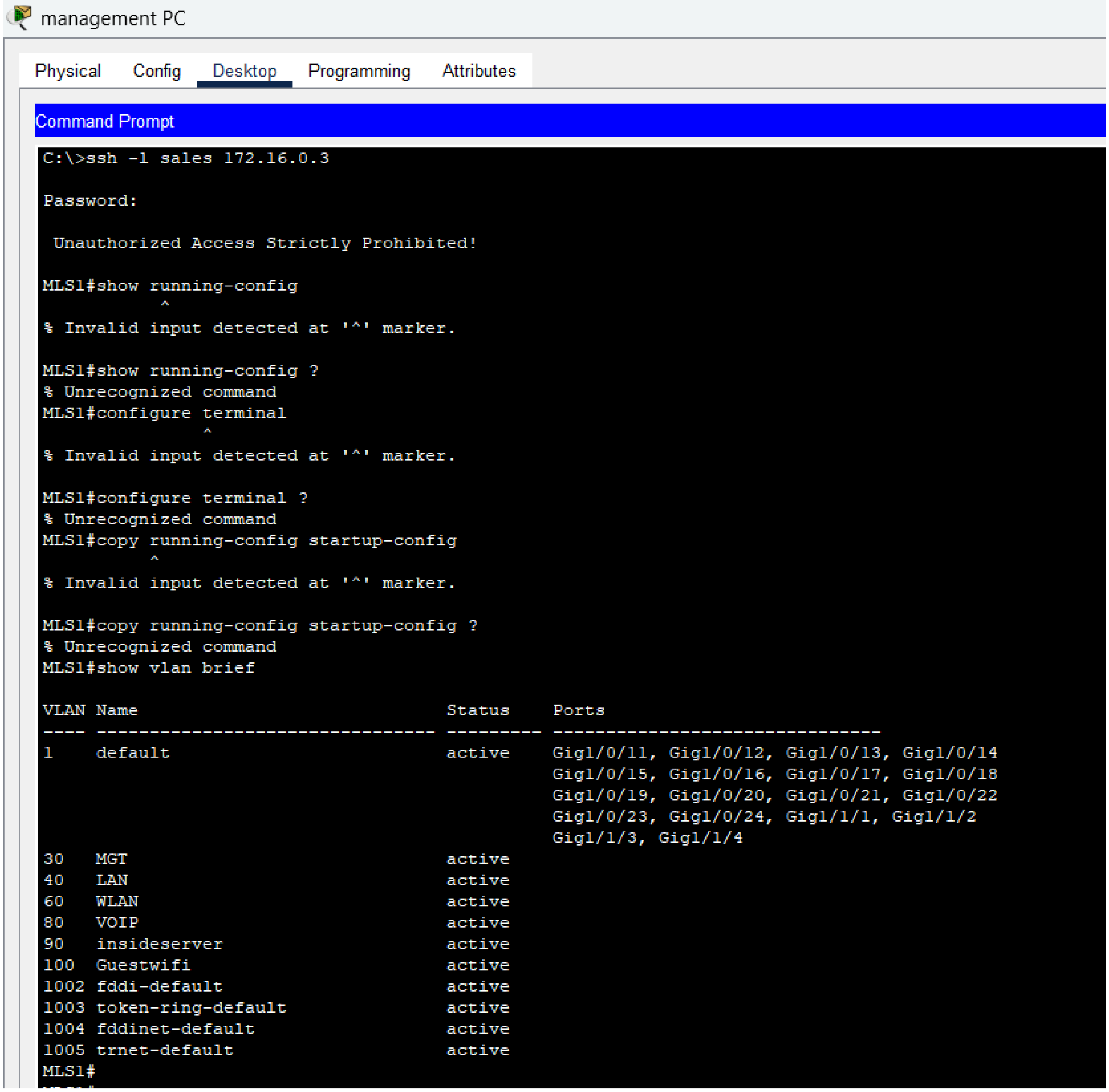


```
C:\>ssh -l businessdevelopment 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1#show running-config
           ^
% Invalid input detected at '^' marker.

MLS1#show running-config?
% Unrecognized command
MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
30   MGT                              active
40   LAN                              active
60   WLAN                             active
80   VOIP                             active
90   insideserver                     active
100  Guestwifi                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1#configure terminal
               ^
% Invalid input detected at '^' marker.

MLS1#configure terminal?
% Unrecognized command
MLS1#copy running-config startup-config
          ^
% Invalid input detected at '^' marker.

MLS1#copy running-config startup-config ?
% Unrecognized command
MLS1#show users
    Line       User       Host(s)              Idle       Location
*  3 vty 0     businessdevelopmentidle                00:00:00

  Interface    User               Mode         Idle     Peer Address
MLS1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   10.2.2.1        YES manual up                    up
GigabitEthernet1/0/2   10.2.2.5        YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
```

Figure 4.15: very limited privilage access for Business development

4.5.5 Sales and Customer Service (Level 2)

Level 2 restricts Sales to POS transactions (process-payment) and customer profile updates, aligning with their front-end role. Blocking all network-related show/configure commands ensures they cannot view or alter sensitive infrastructure, reducing phishing/breach risks. This level enforces strict boundaries between customer interactions and technical systems, maintaining compliance with PCI-DSS for payment processing. Minimal privileges ensure operational efficiency without exposing critical network assets.



```
C:\>ssh -l sales 172.16.0.3

Password:

 Unauthorized Access Strictly Prohibited!

MLS1#show running-config
           ^
% Invalid input detected at '^' marker.

MLS1#show running-config ?
% Unrecognized command
MLS1#configure terminal
               ^
% Invalid input detected at '^' marker.

MLS1#configure terminal ?
% Unrecognized command
MLS1#copy running-config startup-config
          ^
% Invalid input detected at '^' marker.

MLS1#copy running-config startup-config ?
% Unrecognized command
MLS1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
30   MGT                              active
40   LAN                              active
60   WLAN                             active
80   VOIP                             active
90   insideserver                     active
100  Guestwifi                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1#
```

Figure 4.16: exremly limited privilage access for sales and customer service

4.5.6 outcome/result of test in table

No	Department	Privilege Level	Access Type	Configure Terminal	ping	show run	show vlan	Save	Outcome/Result
1	IT Security	15	CLI & GUI	Yes	Yes	Yes	Yes	Yes	Full control over network configurations and troubleshooting.
2	Compliance Auditors	10	CLI	No	Yes	No	Yes	No	Can view network details for audit purposes but cannot modify settings.
3	Pharmacy Operations	5	CLI	No	Yes	No	Yes	No	Able to check network and user session status to assist with troubleshooting.
4	Business Development	3	CLI	No	Yes	No	Yes	No	Can verify network availability and escalate access if needed.
5	Sales & Customer Service	2	CLI	No	Yes	No	Yes	No	Limited to viewing VLAN information and basic assistance commands.

Table 4.6: Access Levels and Privileges by Department

4.6 Exprement 5: Test connection between VLANS

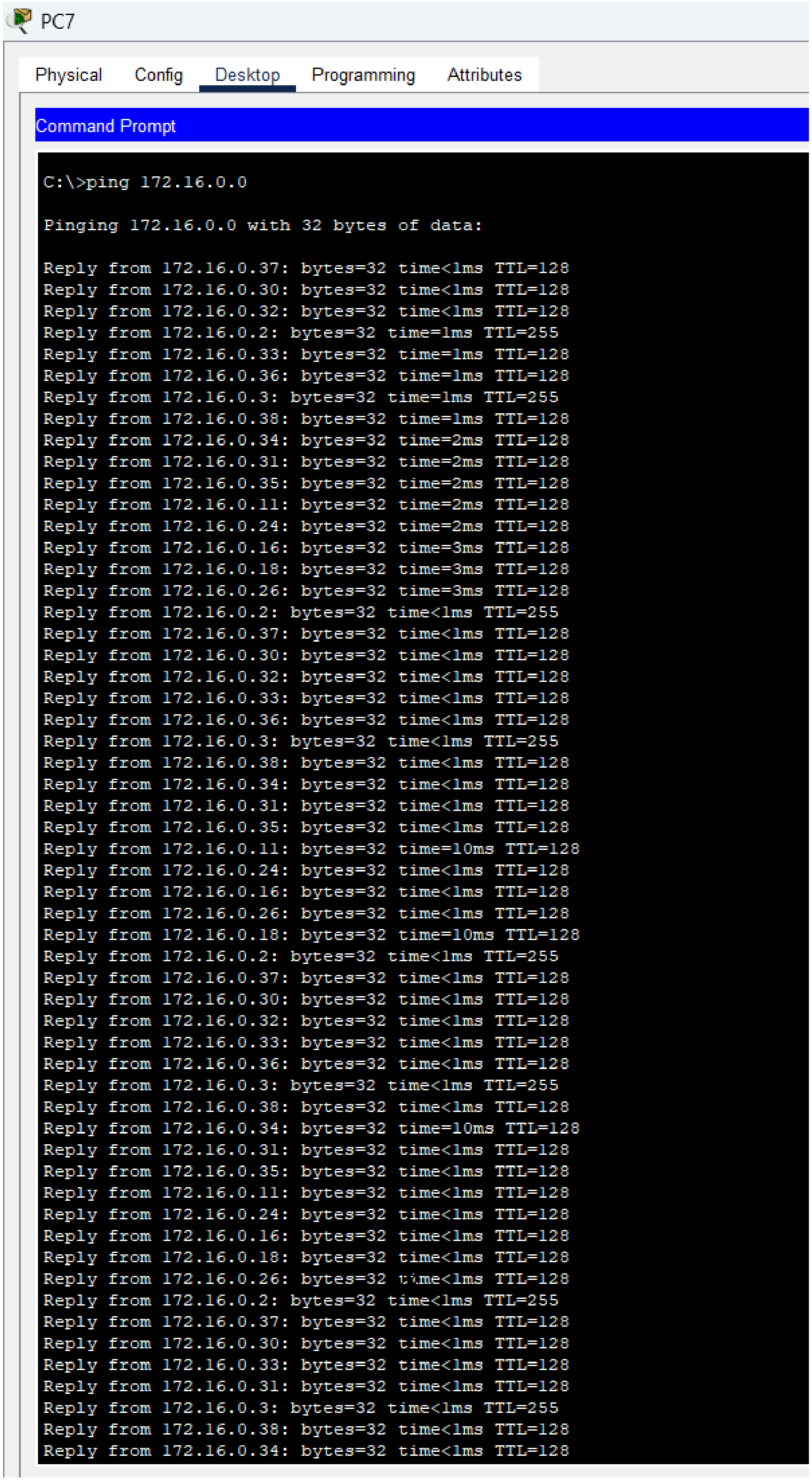
At Boot Pharmacy, the network is structured using VLANs to enhance security, manageability, and performance. Each VLAN is assigned a specific subnet, allowing devices within the same VLAN and different VLANs to communicate as needed. However, the Guest WiFi VLAN is isolated to prevent unauthorized access to internal resources.

- **Management (VLAN 30)**: 192.168.10.0/24
- **LAN (VLAN 40)**: 172.16.0.0/16
- **WLAN (VLAN 60)**: 10.20.0.0/16
- **Inside Server (VLAN 90)**: 10.11.11.32/27
- **Guest WiFi (VLAN 100)**: 192.168.100.0/24

All VLANs, except for the Guest WiFi, are configured to allow inter-VLAN communication. This setup enables devices in different VLANs to ping each other, facilitating necessary interactions between departments and services. The Guest WiFi VLAN is isolated to ensure that guest users cannot access internal network resources, maintaining security and privacy.

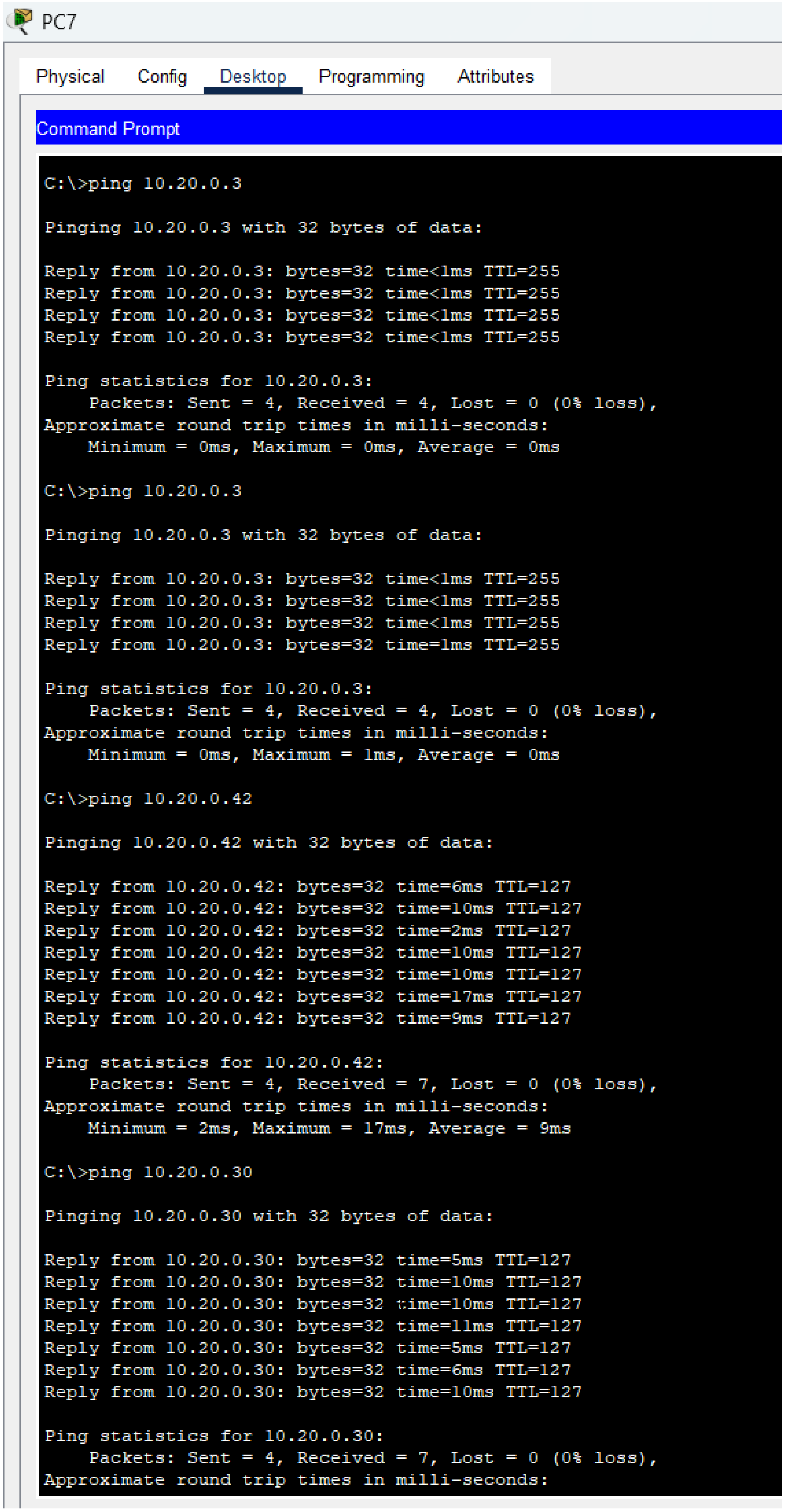
VLANs operate by tagging network traffic with a VLAN ID, which is recognized by network switches. This tagging ensures that traffic is directed appropriately, maintaining separation and organization. Inter-VLAN routing is handled by a Layer 3 device, such as a router or a Layer 3 switch, which allows communication between different VLANs when necessary.

Ping from LAN,VLAN 40 TO LAN,VLAN 40 devices



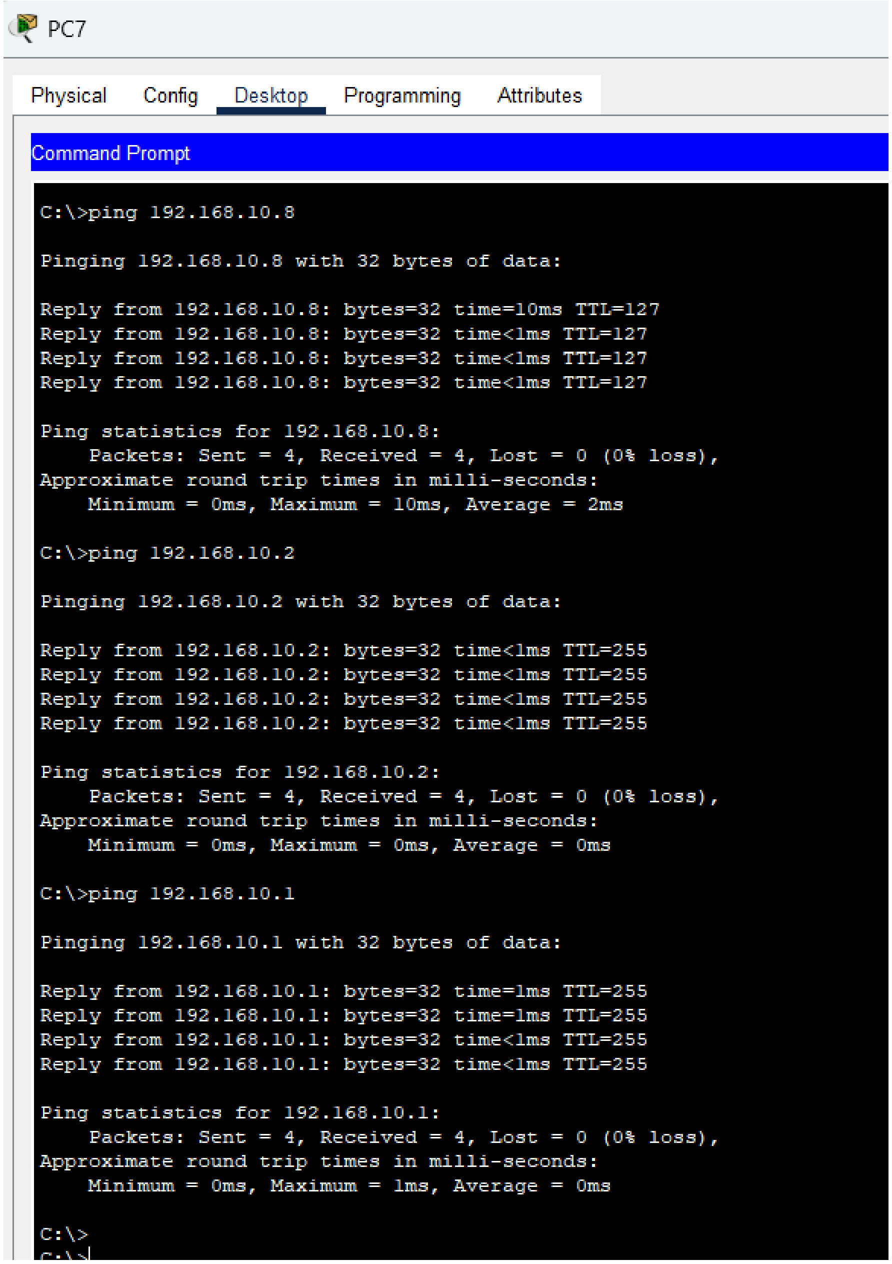
```
C:\>ping 172.16.0.0

Pinging 172.16.0.0 with 32 bytes of data:

Reply from 172.16.0.37: bytes=32 time<1ms TTL=128
Reply from 172.16.0.30: bytes=32 time<1ms TTL=128
Reply from 172.16.0.32: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time=1ms TTL=255
Reply from 172.16.0.33: bytes=32 time=1ms TTL=128
Reply from 172.16.0.36: bytes=32 time=1ms TTL=128
Reply from 172.16.0.3: bytes=32 time=1ms TTL=255
Reply from 172.16.0.38: bytes=32 time=1ms TTL=128
Reply from 172.16.0.34: bytes=32 time=2ms TTL=128
Reply from 172.16.0.31: bytes=32 time=2ms TTL=128
Reply from 172.16.0.35: bytes=32 time=2ms TTL=128
Reply from 172.16.0.11: bytes=32 time=2ms TTL=128
Reply from 172.16.0.24: bytes=32 time=2ms TTL=128
Reply from 172.16.0.16: bytes=32 time=3ms TTL=128
Reply from 172.16.0.18: bytes=32 time=3ms TTL=128
Reply from 172.16.0.26: bytes=32 time=3ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=255
Reply from 172.16.0.37: bytes=32 time<1ms TTL=128
Reply from 172.16.0.30: bytes=32 time<1ms TTL=128
Reply from 172.16.0.32: bytes=32 time<1ms TTL=128
Reply from 172.16.0.33: bytes=32 time<1ms TTL=128
Reply from 172.16.0.36: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=255
Reply from 172.16.0.38: bytes=32 time<1ms TTL=128
Reply from 172.16.0.34: bytes=32 time<1ms TTL=128
Reply from 172.16.0.31: bytes=32 time<1ms TTL=128
Reply from 172.16.0.35: bytes=32 time<1ms TTL=128
Reply from 172.16.0.11: bytes=32 time=10ms TTL=128
Reply from 172.16.0.24: bytes=32 time<1ms TTL=128
Reply from 172.16.0.16: bytes=32 time<1ms TTL=128
Reply from 172.16.0.26: bytes=32 time<1ms TTL=128
Reply from 172.16.0.18: bytes=32 time=10ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=255
Reply from 172.16.0.37: bytes=32 time<1ms TTL=128
Reply from 172.16.0.30: bytes=32 time<1ms TTL=128
Reply from 172.16.0.32: bytes=32 time<1ms TTL=128
Reply from 172.16.0.33: bytes=32 time<1ms TTL=128
Reply from 172.16.0.36: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=255
Reply from 172.16.0.38: bytes=32 time<1ms TTL=128
Reply from 172.16.0.34: bytes=32 time=10ms TTL=128
Reply from 172.16.0.31: bytes=32 time<1ms TTL=128
Reply from 172.16.0.35: bytes=32 time<1ms TTL=128
Reply from 172.16.0.11: bytes=32 time<1ms TTL=128
Reply from 172.16.0.24: bytes=32 time<1ms TTL=128
Reply from 172.16.0.16: bytes=32 time<1ms TTL=128
Reply from 172.16.0.18: bytes=32 time<1ms TTL=128
Reply from 172.16.0.26: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=255
Reply from 172.16.0.37: bytes=32 time<1ms TTL=128
Reply from 172.16.0.30: bytes=32 time<1ms TTL=128
Reply from 172.16.0.33: bytes=32 time<1ms TTL=128
Reply from 172.16.0.31: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=255
Reply from 172.16.0.38: bytes=32 time<1ms TTL=128
Reply from 172.16.0.34: bytes=32 time<1ms TTL=128
```

Ping from LAN,VLAN 40 to WLAN VLAN 60



```
C:\>ping 10.20.0.3

Pinging 10.20.0.3 with 32 bytes of data:

Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 10.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.20.0.3

Pinging 10.20.0.3 with 32 bytes of data:

Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time<1ms TTL=255
Reply from 10.20.0.3: bytes=32 time=1ms TTL=255

Ping statistics for 10.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.20.0.42

Pinging 10.20.0.42 with 32 bytes of data:

Reply from 10.20.0.42: bytes=32 time=6ms TTL=127
Reply from 10.20.0.42: bytes=32 time=10ms TTL=127
Reply from 10.20.0.42: bytes=32 time=2ms TTL=127
Reply from 10.20.0.42: bytes=32 time=10ms TTL=127
Reply from 10.20.0.42: bytes=32 time=10ms TTL=127
Reply from 10.20.0.42: bytes=32 time=17ms TTL=127
Reply from 10.20.0.42: bytes=32 time=9ms TTL=127

Ping statistics for 10.20.0.42:
    Packets: Sent = 4, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 9ms

C:\>ping 10.20.0.30

Pinging 10.20.0.30 with 32 bytes of data:

Reply from 10.20.0.30: bytes=32 time=5ms TTL=127
Reply from 10.20.0.30: bytes=32 time=10ms TTL=127
Reply from 10.20.0.30: bytes=32 time=10ms TTL=127
Reply from 10.20.0.30: bytes=32 time=11ms TTL=127
Reply from 10.20.0.30: bytes=32 time=5ms TTL=127
Reply from 10.20.0.30: bytes=32 time=6ms TTL=127
Reply from 10.20.0.30: bytes=32 time=10ms TTL=127

Ping statistics for 10.20.0.30:
    Packets: Sent = 4, Received = 7, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

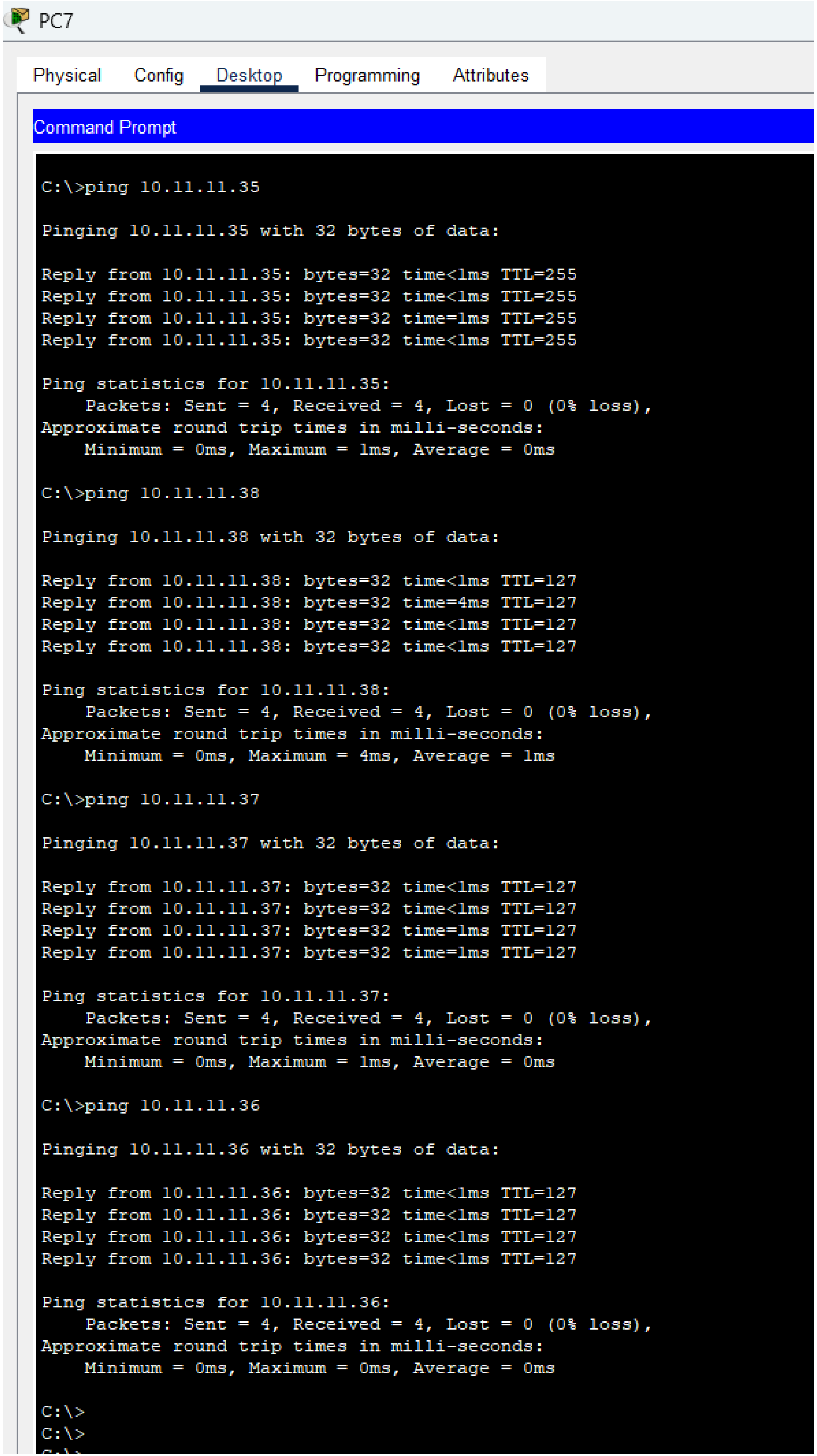
Ping from LAN,VLAN 40 to manangement vlan 30



```
C:\>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.8: bytes=32 time=10ms TTL=127
Reply from 192.168.10.8: bytes=32 time<1ms TTL=127
Reply from 192.168.10.8: bytes=32 time<1ms TTL=127
Reply from 192.168.10.8: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255
Reply from 192.168.10.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
```

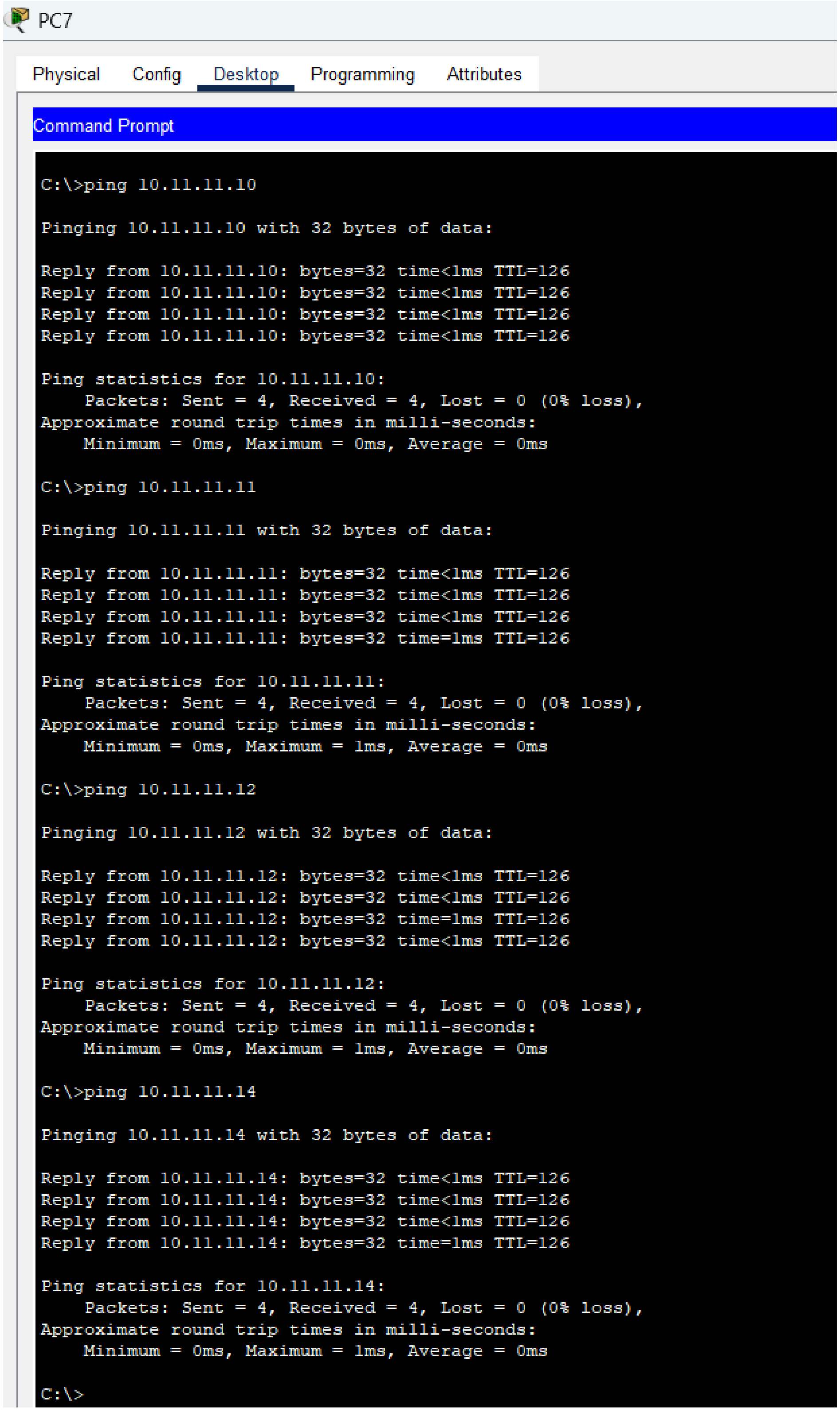
Figure 4.19: Ping from LAN vlan 40 to management vlan 30

Ping from LAN,VLAN 40 to inside server VLAN 90



```
C:\>ping 10.11.11.35

Pinging 10.11.11.35 with 32 bytes of data:

Reply from 10.11.11.35: bytes=32 time<1ms TTL=255
Reply from 10.11.11.35: bytes=32 time<1ms TTL=255
Reply from 10.11.11.35: bytes=32 time=1ms TTL=255
Reply from 10.11.11.35: bytes=32 time<1ms TTL=255

Ping statistics for 10.11.11.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.11.11.38

Pinging 10.11.11.38 with 32 bytes of data:

Reply from 10.11.11.38: bytes=32 time<1ms TTL=127
Reply from 10.11.11.38: bytes=32 time=4ms TTL=127
Reply from 10.11.11.38: bytes=32 time<1ms TTL=127
Reply from 10.11.11.38: bytes=32 time<1ms TTL=127

Ping statistics for 10.11.11.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 10.11.11.37

Pinging 10.11.11.37 with 32 bytes of data:

Reply from 10.11.11.37: bytes=32 time<1ms TTL=127
Reply from 10.11.11.37: bytes=32 time<1ms TTL=127
Reply from 10.11.11.37: bytes=32 time=1ms TTL=127
Reply from 10.11.11.37: bytes=32 time=1ms TTL=127

Ping statistics for 10.11.11.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.11.11.36

Pinging 10.11.11.36 with 32 bytes of data:

Reply from 10.11.11.36: bytes=32 time<1ms TTL=127
Reply from 10.11.11.36: bytes=32 time<1ms TTL=127
Reply from 10.11.11.36: bytes=32 time<1ms TTL=127
Reply from 10.11.11.36: bytes=32 time<1ms TTL=127

Ping statistics for 10.11.11.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>
```

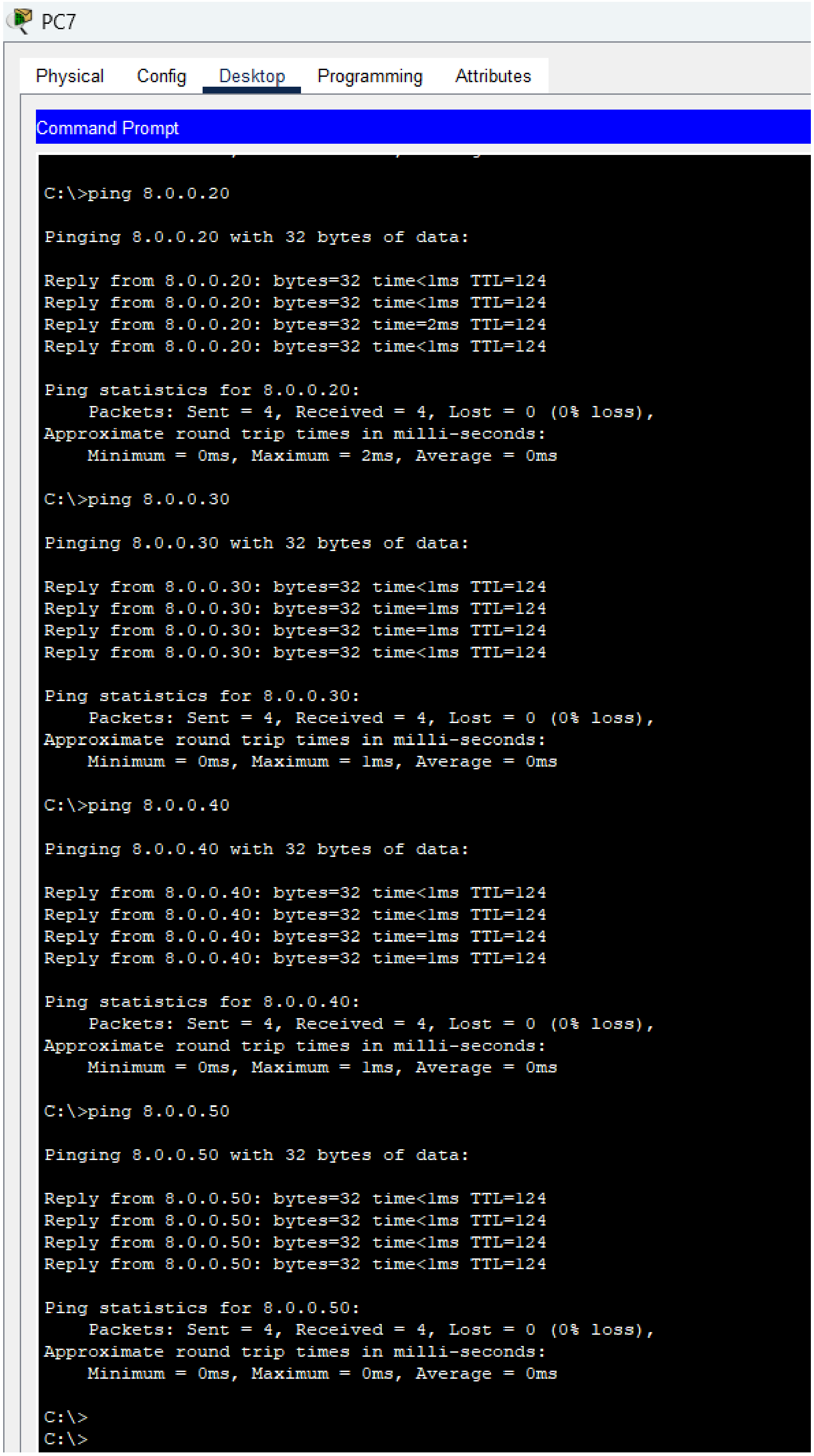
Ping from LAN,VLAN 40 to DMZ zone



```
C:\>ping 10.11.11.10

Pinging 10.11.11.10 with 32 bytes of data:

Reply from 10.11.11.10: bytes=32 time<1ms TTL=126
Reply from 10.11.11.10: bytes=32 time<1ms TTL=126
Reply from 10.11.11.10: bytes=32 time<1ms TTL=126
Reply from 10.11.11.10: bytes=32 time<1ms TTL=126

Ping statistics for 10.11.11.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.11.11.11

Pinging 10.11.11.11 with 32 bytes of data:

Reply from 10.11.11.11: bytes=32 time<1ms TTL=126
Reply from 10.11.11.11: bytes=32 time<1ms TTL=126
Reply from 10.11.11.11: bytes=32 time<1ms TTL=126
Reply from 10.11.11.11: bytes=32 time=1ms TTL=126

Ping statistics for 10.11.11.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.11.11.12

Pinging 10.11.11.12 with 32 bytes of data:

Reply from 10.11.11.12: bytes=32 time<1ms TTL=126
Reply from 10.11.11.12: bytes=32 time<1ms TTL=126
Reply from 10.11.11.12: bytes=32 time=1ms TTL=126
Reply from 10.11.11.12: bytes=32 time<1ms TTL=126

Ping statistics for 10.11.11.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.11.11.14

Pinging 10.11.11.14 with 32 bytes of data:

Reply from 10.11.11.14: bytes=32 time<1ms TTL=126
Reply from 10.11.11.14: bytes=32 time<1ms TTL=126
Reply from 10.11.11.14: bytes=32 time<1ms TTL=126
Reply from 10.11.11.14: bytes=32 time=1ms TTL=126

Ping statistics for 10.11.11.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figure 4.21: ping from LAN vlan 40 to DMZ server

Ping from LAN,VLAN 40 to Remote users



```
C:\>ping 8.0.0.20

Pinging 8.0.0.20 with 32 bytes of data:

Reply from 8.0.0.20: bytes=32 time<1ms TTL=124
Reply from 8.0.0.20: bytes=32 time<1ms TTL=124
Reply from 8.0.0.20: bytes=32 time=2ms TTL=124
Reply from 8.0.0.20: bytes=32 time<1ms TTL=124

Ping statistics for 8.0.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 8.0.0.30

Pinging 8.0.0.30 with 32 bytes of data:

Reply from 8.0.0.30: bytes=32 time<1ms TTL=124
Reply from 8.0.0.30: bytes=32 time=1ms TTL=124
Reply from 8.0.0.30: bytes=32 time=1ms TTL=124
Reply from 8.0.0.30: bytes=32 time<1ms TTL=124

Ping statistics for 8.0.0.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 8.0.0.40

Pinging 8.0.0.40 with 32 bytes of data:

Reply from 8.0.0.40: bytes=32 time<1ms TTL=124
Reply from 8.0.0.40: bytes=32 time<1ms TTL=124
Reply from 8.0.0.40: bytes=32 time=1ms TTL=124
Reply from 8.0.0.40: bytes=32 time=1ms TTL=124

Ping statistics for 8.0.0.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 8.0.0.50

Pinging 8.0.0.50 with 32 bytes of data:

Reply from 8.0.0.50: bytes=32 time<1ms TTL=124
Reply from 8.0.0.50: bytes=32 time<1ms TTL=124
Reply from 8.0.0.50: bytes=32 time<1ms TTL=124
Reply from 8.0.0.50: bytes=32 time<1ms TTL=124

Ping statistics for 8.0.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>
```

Figure 4.22: from LAN VLAN 40 to remote users

4.6.1 outcome/result of test in table

The use of VLANs in Boot Pharmacy's network infrastructure provides a robust framework for secure, efficient, and manageable network operations. By isolating the Guest WiFi and allowing controlled inter-VLAN communication, the network supports both security and functionality, aligning with organizational needs and compliance requirements.

No	Source VLAN	Source IP	Destination VLAN	Destination IP	Ping	Latency	Loss	Outcome/Result
1	LAN (VLAN 40)	172.16.0.0	LAN (VLAN 40)	172.16.0.32	Success	$< 1ms$	0%	Devices within the same VLAN can communicate effectively.
2	LAN (VLAN 40)	172.16.0.0	Inside Server (VLAN 90)	10.11.11.10	Success	$< 1ms$	0%	Inter-VLAN communication is functioning as expected.
3	LAN (VLAN 40)	172.16.0.0	WLAN (VLAN 60)	10.20.0.3	Success	$< 1ms$	0%	Inter-VLAN communication is functioning as expected.
4	LAN (VLAN 40)	172.16.0.0	Management (VLAN 30)	192.168.10.8	Success	$< 1ms$	0%	Inter-VLAN communication is functioning as expected.
5	LAN (VLAN 40)	172.16.0.0	DMZ Zone	10.11.11.35	Success	$< 1ms$	0%	Inter-VLAN communication is functioning as expected.
6	LAN (VLAN 40)	172.16.0.0	Remote Users	8.0.0.20	Success	$< 1ms$	0%	Inter-VLAN communication is functioning as expected.

Table 4.7: VLAN Connectivity Test Results

4.7 Summary

In today's evolving threat landscape, Boot Pharmacy faces significant cybersecurity challenges, including credential stuffing, phishing, and unauthorized access. To address these threats, a multi-layered cybersecurity strategy has been implemented, focusing on network segmentation, access control, and authentication policies. This chapter provides a technical analysis of these defenses across Boot Pharmacy's infrastructure.

The first experiment demonstrates the effectiveness of Multi-Factor Authentication (MFA) in preventing unauthorized access, even when login credentials are compromised. The second experiment verifies secure SSH access control, ensuring only authorized devices within the management VLAN can connect. The third experiment confirms the isolation of the Guest WiFi VLAN from internal networks using VLAN segmentation and ACLs, preventing unauthorized lateral movement and safeguarding sensitive data.

The fourth experiment evaluates access control levels and role-based access control (RBAC), ensuring that different departments have appropriate access based on their roles. Pharmacy Operations, Business Development, and Sales have restricted access to ensure compliance and security, while IT has full control over network configurations. This setup minimizes risks and maintains operational efficiency[35] [54].

The fifth experiment tests inter-VLAN communication, confirming that devices in different VLANs, such as LAN, Wireless Local Area Network (WLAN), and management, can communicate effectively while maintaining security. This ensures robust network functionality and compliance with organizational needs.

These experiments collectively validate the security measures in place, highlighting the importance of layered defenses in mitigating risks and maintaining compliance with healthcare regulations. By simulating realistic attack scenarios, the analysis establishes clear metrics for detection, response, and containment, demonstrating how theoretical best practices can be effectively implemented to enhance Boot Pharmacy's cybersecurity posture.

Chapter 5

Conclusions

5.1 Introduction

In the rapidly evolving field of cybersecurity, Boot Pharmacy faces a myriad of sophisticated threats, including credential stuffing, phishing, lateral movement attacks, and unauthorized internal access[42] [20]. This research focused on implementing and validating a multi-layered cybersecurity strategy to mitigate these threats effectively. The study aimed to assess the effectiveness of various defense mechanisms, such as multi-factor authentication (MFA), strong password policies, network segmentation, access control lists (ACLs), and role-based access control (RBAC). Through a series of meticulously designed experiments, the research provided empirical evidence supporting the proposed cybersecurity measures, demonstrating their potential to significantly reduce the impact of cyberattacks on Boot Pharmacy's operations.

The primary objective of this research was to empirically assess whether these layered defense strategies, grounded in the latest research, could mitigate risks and reduce the overall impact of cyberattacks. By simulating controlled, realistic attack scenarios that closely mirror the operational environment at Boot Pharmacy, each experiment aimed to establish clear metrics for detection times, response speeds, and containment efficacy. This chapter details the conclusions drawn from the experimental objectives, setups, and methodologies, ultimately demonstrating how theoretical best practices can be effectively implemented to strengthen Boot Pharmacy's cybersecurity posture.

5.2 Recommendations

Based on the findings of this research, several recommendations can be made to further enhance the cybersecurity posture of Boot Pharmacy. Firstly, it is crucial to continue integrating MFA and enforcing strong password policies across all systems. The experiments demonstrated that these measures significantly reduce the success rate of credential stuffing and phishing attacks. By requiring multiple forms of verification, MFA adds an additional layer of security, ensuring that even if login credentials are compromised, unauthorized access is prevented.

Furthermore, maintaining robust network segmentation and access control measures is essential. The experiments confirmed that VLANs and ACLs effectively isolate sensitive areas of the network, preventing unauthorized lateral movement and safeguarding critical data. It is recommended that Boot Pharmacy regularly reviews and updates these configurations to adapt to evolving threats and ensure compliance with industry regulations [35] [54].

Regular training for employees on cybersecurity best practices is also advised. Human error remains a significant vulnerability, and educating staff on recognizing phishing attempts, using secure passwords, and following security protocols can greatly enhance the organization's overall security posture. By fostering a culture of cybersecurity awareness, Boot Pharmacy can reduce the risk of successful attacks and improve incident response times.

5.3 Future Work

While this research has provided valuable insights into enhancing cybersecurity at Boot Pharmacy, there are several avenues for future work that could further strengthen the organization's defenses. One potential area of exploration is the integration of artificial intelligence (AI) and machine learning (ML) technologies to enhance threat detection and response times. By leveraging AI and ML algorithms, Boot Pharmacy could develop more sophisticated intrusion detection systems capable of identifying and mitigating threats in real-time[52].

Additionally, expanding the study to include other emerging technologies, such as blockchain for secure data transactions, could provide further insights into strengthening cybersecurity frameworks. Blockchain technology offers a decentralized and tamper-proof method of recording transactions, which could be particularly beneficial for ensuring the integrity and confidentiality of sensitive patient data.

Another area for future research is the exploration of advanced threat intelligence sharing and collaboration with other organizations in the healthcare sector. By participating in information-sharing initiatives, Boot Pharmacy can gain access to valuable threat intelligence, enabling proactive defense measures and enhancing its ability to respond to emerging threats.

5.4 Reflections

Reflecting on the research process, several key insights and lessons have been gained. If this project were to be undertaken again, a broader range of attack scenarios could be simulated to test the resilience of the implemented strategies. By incorporating a wider variety of threat vectors, such as social engineering attacks or advanced persistent threats, the research could provide a more comprehensive assessment of the organization's cybersecurity posture.

Additionally, involving a larger sample size for experiments could provide more robust data and insights. By expanding the scope of the study to include a greater number of participants and systems, the research could yield more statistically significant results, enhancing the validity and generalizability of the findings.

Furthermore, collaboration with industry experts and stakeholders throughout the research process could provide valuable perspectives and insights. Engaging with professionals in the field of cybersecurity and healthcare could help identify emerging trends, best practices, and potential areas for improvement, ensuring that the research remains relevant and impactful.

5.5 Summary

In conclusion, this research aimed to evaluate the effectiveness of layered cybersecurity strategies at Boot Pharmacy. The hypothesis that these strategies would significantly reduce successful cyberattacks was supported by the experimental outcomes. The study demonstrated the importance of MFA, strong password policies, and network segmentation in enhancing security. By implementing these measures, Boot Pharmacy can mitigate risks, protect sensitive data, and maintain compliance with industry regulations.

The research provided empirical validation of effective cybersecurity practices that can be adopted by similar organizations to enhance their security posture. Recommendations include continued implementation of MFA, strong password policies, and network segmentation, as well as further exploration of advanced technologies such as AI, ML, and blockchain. By fostering a culture of cybersecurity awareness and collaboration, Boot Pharmacy can stay ahead of evolving threats and ensure the safety and integrity of its operations[35] [54].

Overall, this research contributes to the field of cybersecurity by providing practical insights and recommendations for organizations seeking to enhance their defenses against sophisticated cyber threats. By combining theoretical best practices with empirical validation, the study offers a comprehensive framework for strengthening cybersecurity measures and protecting critical assets in an increasingly digital world.

Bibliography

[1] H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli, "Risk analysis of cloud sourcing in healthcare and public health industry," *IEEE Access*, vol. 6, pp. 41 911–41 928, 2018, received August 16, 2017; accepted September 14, 2017; published February 14, 2018; current version April 23, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2805919

[2] H. Ahmed, A. Alsadoon, P. Prasad, N. Costadopoulos, L. S. Hoe, and A. Elchoemi, "Next generation cyber security solution for an ehealth organization," in *2017 5th International Conference on Information and Communication Technology (ICoIC7)*, 2017, pp. 1–5.

[3] B. Ali, M. A. Gregory, and S. Li, "Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model," in *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, 2021, pp. 192–197.

[4] Alphanumeric, "Ensuring data security: The importance of compliance in pharmaceuticals," 2024, accessed: 2025-03-06. [Online]. Available: https://blog.alphanumeric.com/newsroom/ensuring-data-security-the-importance-of-compliance-in-pharmaceuticals

[5] Avigilon, "Pharmacy security guide," 2024, accessed: 2025-03-06. [Online]. Available: https://www.avigilon.com/blog/pharmacy-security-guide

[6] Baxter Healthcare, "Exactamix pro - cybersecurity handout," 2023, accessed: 2025-03-06. [Online]. Available: https://ushospitalproducts.baxter.com/sites/g/files/ebysai2186/files/2023-01/ExactaMix%20Pro%20-%20Cybersecurity%20Handout_US.pdf

[7] Boots UK Limited, "Legal privacy & cookies information," https://www.boots.com/privacypolicy, accessed: 2025-03-06.

[8] P. Broklyn, A. Egon, and R. Shad, "Ransoware: A comprehensive investigation authors," *Available at SSRN 4904872*, 2024.

[9] D. Campbell, "Nhs electronic health records pose serious safety risks," *The Guardian*, September 2024. [Online]. Available: https://www.theguardian.com/society/2024/sep/22/nhs-electronic-health-records-pose-serious-safety-risks

[10] H. Cao, "The Detection of Abnormal Behavior by Artificial Intelligence Algorithms Under Network Security," *IEEE Access*, vol. 12, pp. 118 605–118 617, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3436541

[11] Center for Devices and Radiological Health, "Postmarket management of cybersecurity in medical devices: Guidance for industry and food and drug administration staff," December 2016, final, Docket Number: FDA-2015-D-5105. [Online]. Available: https://www.fda.gov

[12] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations," *IEEE Access*, vol. 10, pp. 85 701–85 719, 2022.

[13] Cisco, "Cisco packet tracer," 2024, accessed: 2025-03-06. [Online]. Available: https://www.netacad.com/cisco-packet-tracer

[14] CPE, "Ten steps to help improve data and cyber security within your pharmacy," 2017, accessed: 2025-03-06. [Online]. Available: https://cpe.org.uk/wp-content/uploads/2017/08/PSNC-Briefing-053.17-Ten-steps-to-help-improve-data-and-cyber-security-within-your-pharmacy.pdf

[15] CrowdStrike, "Zero trust security," 2024, accessed: 2025-03-06. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security

[16] S. Cui, J. S. Thompson, T. Taniguchi, L. Ladid, J. Li, A. Eckford, and V. W. Wong, "Guest editorial emerging technologies," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 457–459, 2016.

[17] DataGuard, "What is an access control list (acl)?" 2024, accessed: 2025-03-06. [Online]. Available: https://www.dataguard.com/blog/acl-access-control-list/

[18] J. Doe, "Misfortune cookie vulnerability bulletin," 2018, archived from the original on 2018-10-03, retrieved on 2018-08-30. [Online]. Available: https://web.archive.org/web/20181003055451/http://mis.fortunecook.ie/misfortune-cookie-suspected-vulnerable.pdf

[19] Drug Topics, "Cybersecurity best practices for pharmacies in the digital age," 2024, accessed: 2025-03-06. [Online]. Available: https://cdn.sanity.io/files/0vv8moc6/drugtopics/e77073e6d7bb18a0e5c4a7f3688b7ae8bfd0253a.pdf/TP0224_ezine.pdf

[20] C. . Druggist. (2023) Cybercrime gang behind personal data hack affecting boots staff, reports claim. Accessed: 2025-02-23. [Online]. Available: https://www.chemistanddruggist.co.uk/CD137063/Cybercrime-gang-behind-personal-data-hack-affecting-Boots-staff-reports-claim

[21] FireMon, "Network segmentation best practices," 2023, accessed: 2025-03-06. [Online]. Available: https://www.firemon.com/blog/network-segmentation-best-practices/

[22] B. P. Gajendra, V. K. Singh, and S. More, "Achieving cloud security using third party auditor, md5 and identity-based encryption," in *2016 International Conference on Computing, Communication and Automation (ICCA)*, 2016, pp. 1304–1309.

[23] U. Government, "Cyber essentials requirements," UK Government, Tech. Rep., June 2014, accessed: 2025-03-12. [Online]. Available: https://web.archive.org/web/20160613150635/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf

[24] N. R. Guidelines, P. A. Networks, NERC, and Cisco, "Zero trust security for electric operations technology," 2023, accessed: 2025-03-25. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Zero_Trust_For_Electric_OT.pdf

[25] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the internet of things in artificial intelligence era: A comprehensive survey," *IEEE Access*, 2024, received 28 January 2024, accepted 9 February 2024, published 13 February 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3365634

[26] G. Info. (n.d.) Article 83 gdpr – general conditions for imposing administrative fines. Accessed: 2025-03-06. [Online]. Available: https://gdpr-info.eu/art-83-gdpr/

[27] D. Insights. (2024) How intrusion detection systems help identify cyber threats in real-time. Accessed: 2025-03-12. [Online]. Available: https://www.dataguard.com/blog/how-intrusion-detection-systems-help-identify-cyber-threats/

[28] D. Jay, "Deception Technology Based Intrusion Protection and Detection Mechanism for Digital Substations: A Game Theoretical Approach," *IEEE Access*, vol. 11, pp. 53 301–53 314, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3279504

[29] T. Kim, T. Kwon, J. Lee, and J. Song, "F/Wvis: Hierarchical Visual Approach for Effective Optimization of Firewall Policy," *IEEE Access*, vol. 9, pp. 105 989–106 004, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3100141

[30] Medical Economics, "Cyber threats continue to evolve: Understanding and mitigating new threats in health care," 2025, accessed: 2025-03-06. [Online]. Available: https://www.medicaleconomics.com/view/cyber-threats-continue-to-evolve-understanding-and-mitigating-new-threats-in-health-care

[31] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A survey on zero trust architecture: Applications and challenges of 6g networks," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1–15, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10589640

[32] M. Nankya, A. Mugisa, Y. Usman, A. Upadhyay, and R. Chataut, "Security and privacy in e-health systems: A review of ai and machine learning techniques," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1–15, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10697161

[33] National Institute of Standards and Technology (NIST), "Digital identity guidelines: Authentication and lifecycle management," August 2024, accessed: 2024-08-28. [Online]. Available: https://pages.nist.gov/800-63-4/sp800-63.html

[34] N. C. S. C. (NCSC), "Cyber aware - guidance on staying secure online," 2025, accessed: 2025-03-12. [Online]. Available: https://www.ncsc.gov.uk/cyberaware/home

[35] Z. Networks. (2023, June 5) Network segmentation vs. vlan strategy for security. Accessed: 2025-02-23. [Online]. Available: https://zeronetworks.com/blog/network-segmentation-vs-vlan-strategy-security

[36] NHS England. (2023, April) Case Study: WannaCry Attack. Accessed: 2025-03-12. [Online]. Available: https://www.england.nhs.uk/long-read/case-study-wannacry-attack/?form=MG0AV3&form=MG0AV3

[37] U. D. of Health and O. o. I. S. Human Services, "Lessons learned from the hse cyber attack," U.S. Department of Health and Human Services, Tech. Rep., February 2022, accessed: 2025-03-12. [Online]. Available: https://www.aha.org/system/files/media/file/2022/02/hhs-ocio-hc3-tlp-white-threat-brief-lessons-learned-from-the-hse-attack-2-3-22.pdf

[38] Overleaf, "Overleaf latex documentation," 2024, accessed: 2025-02-23. [Online]. Available: https://www.overleaf.com/learn

[39] PBA Health, "Cybersecurity in your pharmacy," 2023, accessed: 2025-03-06. [Online]. Available: https://www.pbahealth.com/elements/cybersecurity-in-your-pharmacy/

[40] Pharmacy Times, "Healthcare security and privacy (hse) july 2024 issue," 2024, accessed: 2025-03-06. [Online]. Available: https://cdn.sanity.io/files/

0vv8moc6/pharmacytimes/f5b57964cb94798280d2cdcf16b209c5e642f758.pdf/HSE-July2024-Issue_NoPaidAds.pdf

[41] C. Press, "Configuring access control lists," 2024, accessed: 2025-03-06. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=6

[42] Reuters, "British airways, boots staff suffers possible data breach," *Reuters*, 2023, retrieved from https://www.reuters.com/technology/british-airways-boots-staff-suffers-possible-data-breach-telegraph-2023-06-05/. [Online]. Available: https://www.reuters.com/technology/british-airways-boots-staff-suffers-possible-data-breach-telegraph-2023-06-05/

[43] J. J. D. Rivera, A. Muhammad, and W. C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2792–2814, 2024. [Online]. Available: https://doi.org/10.1109/OJCOMS.2024.3391728

[44] K. Sakata, S. Fujita, K. Sawada, S. Shin, I. Maeta, and S. Hosokawa, "On the multiple anomaly detection of a third-party monitoring system for secured control," in *2020 IEEE/SICE International Symposium on System Integration (SII)*, 2020, pp. 1254–1258.

[45] A. H. Sarower, T. Bhuiyan, M. Hassan, M. S. Arefin, and G. Hossain, "SMFA: Strengthening Multi-Factor Authentication With Steganography for Enhanced Security," *IEEE Access*, vol. 13, pp. 43 593–43 606, 2025. [Online]. Available: https://doi.org/10.1109/ACCESS.2025.3545769

[46] K. Sasikumar and S. Nagarajan, "Enhancing cloud security: A multi-factor authentication and adaptive cryptography approach using machine learning techniques," *IEEE Open Journal of Computer Society*, vol. 2, pp. 1–10, 2025. [Online]. Available: https://doi.org/10.1109/OJCS.2025.3538557

[47] H. Solicitors. (2020) Boots advantage card cyber-attack affects 150,000 customers. Accessed: 2025-02-23. [Online]. Available: https://hnksolicitors.com/news/boots-advantage-card-cyber-attack-affects-150000-customers/

[48] ——. (2020) Boots advantage card cyber-attack affects 150,000 customers. Accessed: 2025-02-20. [Online]. Available: https://hnksolicitors.com/news/boots-advantage-card-cyber-attack-affects-150000-customers/

[49] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives," *IEEE Communications Surveys Tutorials*, vol. 25, no. 3, pp. 1982–2010, 2023, third Quarter. [Online]. Available: https://ieeexplore.ieee.org/document/10117505

[50] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, 2022, received April 14, 2022; accepted May 2, 2022; published May 12, 2022; current version June 3, 2022. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9773102

[51] C. Systems, "Cisco packet tracer 8.2 system requirements," 2025, accessed: 2025-03-18. [Online]. Available: https://www.packettracernetwork.com/features/system-requirements.html

[52] R. Tarun, *Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders*. Wiley, 2022, chapters 1-22, Computing and Processing. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?bknumber=9953205

[53] TechCrunch. (2023, August) Moveit mass hack by the numbers. Accessed: 2025-03-12. [Online]. Available: https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/?form=MG0AV3&form=MG0AV38

[54] TechTarget. Access control list (acl) definition. Accessed: 2025-02-23. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL

[55] Thematic Take. (2024) Case studies: Cybersecurity in healthcare. Accessed: 2025-03-12. [Online]. Available: https://thematictake.nridigital.com/thematic_take_aug24/case-studies-cybersecurity-healthcare

[56] P. Thorat, S. M. Raza, D. S. Kim, and H. Choo, "Rapid recovery from link failures in software-defined networks," *Journal of Communications and Networks*, vol. 19, no. 6, pp. 648–665, Dec. 2017. [Online]. Available: https://doi.org/10.1109/JCN.2017.000105

[57] Toxigon, "Top cybersecurity threats in healthcare," 2024, accessed: 2025-03-06. [Online]. Available: https://toxigon.com/top-cybersecurity-threats-in-healthcare

[58] UK Government. (2023) A cyber resilient health and adult social care system in england: Cyber security strategy to 2030. Accessed: 2025-03-06. [Online]. Available: https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030/a-cyber-resilient-health-and-adult-social-care-system-in-england-cyber-security-strategy-to-2030

[59] UK Parliament, "Cyber-attacks: Lessons learned from the wannacry ransomware attack," House of Commons, UK Parliament, Tech. Rep. 787, April 2018, accessed: 2025-03-12. [Online]. Available: https://web.archive.org/web/20180421031123/https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

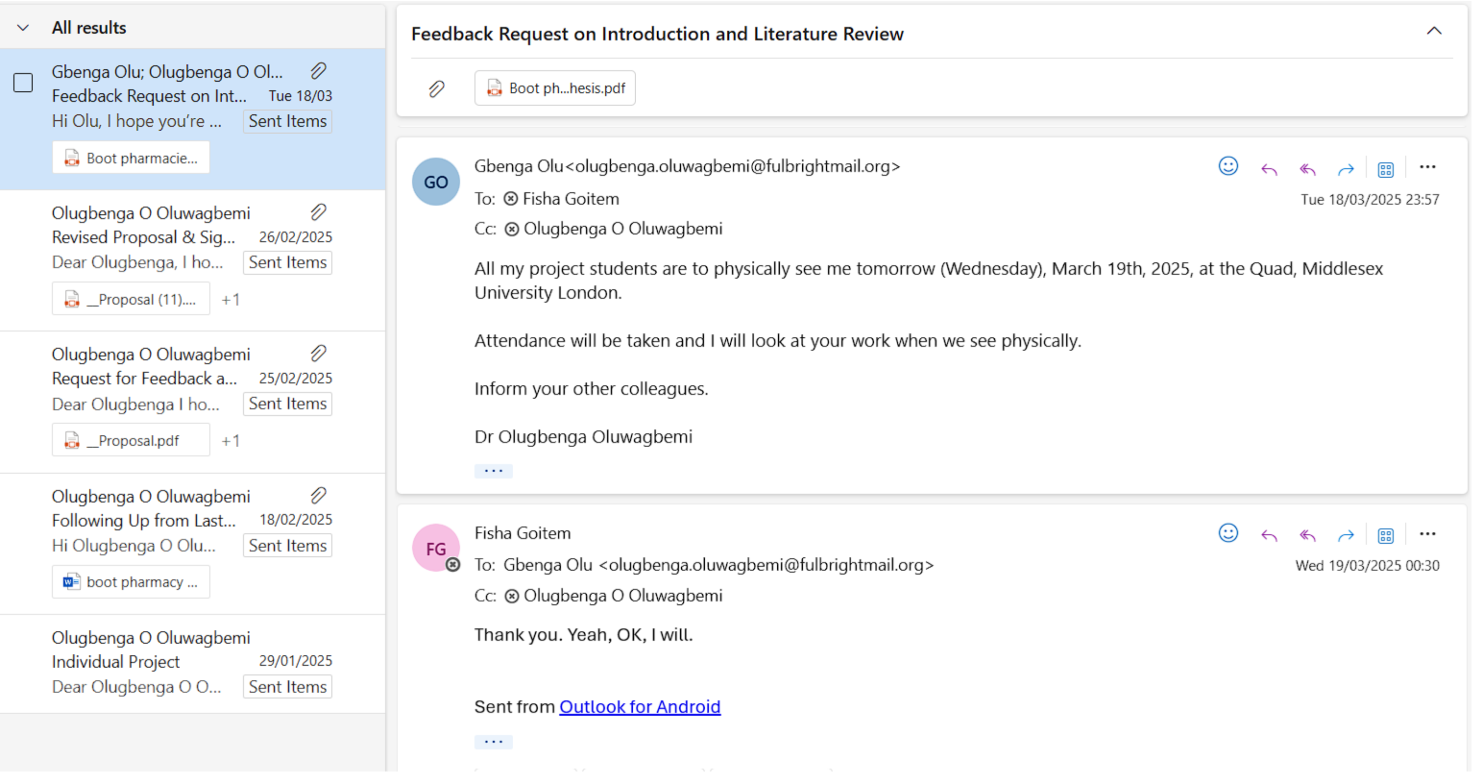
[60] R. Xu, J. Joshi, and P. Krishnamurthy, “An integrated privacy preserving attribute based access control framework supporting secure deduplication,” *IEEE Transactions on Dependable and Secure Computing*, 2025. [Online]. Available: https://ieeexplore.ieee.org/ielaam/8858/9372344/8862918-aam.pdf

[61] N. A. Zaguir, G. H. de Magalhães, and M. de Mesquita Spinola, “Challenges and enablers for gdpr compliance: Systematic literature review and future research directions,” *IEEE Access*, vol. 12, pp. 81 608–81 630, 2024.

Appendices

Appendix A

Correspondence with Supervisor



Gbenga Olu; Olugbenga O Ol... | Feedback Request on Int... | Tue 18/03 | Hi Olu, I hope you're ...

Olugbenga O Oluwagbemi | Revised Proposal & Sig... | 26/02/2025 | Dear Olugbenga, I ho...

Olugbenga O Oluwagbemi | Request for Feedback a... | 25/02/2025 | Dear Olugbenga I ho...

Olugbenga O Oluwagbemi | Following Up from Last... | 18/02/2025 | Hi Olugbenga O Olu...

Olugbenga O Oluwagbemi | Individual Project | 29/01/2025 | Dear Olugbenga O O...

Feedback Request on Introduction and Literature Review

GO Gbenga Olu<olugbenga.oluwagbemi@fulbrightmail.org>
To: Fisha Goitem
Cc: Olugbenga O Oluwagbemi
Tue 18/03/2025 23:57

All my project students are to physically see me tomorrow (Wednesday), March 19th, 2025, at the Quad, Middlesex University London.

Attendance will be taken and I will look at your work when we see physically.

Inform your other colleagues.

Dr Olugbenga Oluwagbemi

FG Fisha Goitem
To: Gbenga Olu <olugbenga.oluwagbemi@fulbrightmail.org>
Cc: Olugbenga O Oluwagbemi
Wed 19/03/2025 00:30

Thank you. Yeah, OK, I will.

Sent from Outlook for Android

Figure A.1: Correspondence with Supervisor

Appendix B

Ethical Approval

Do not amend before use

Research Ethics Screening Form for Students

Only for students on taught programmes – e.g., BSc, MSc, MA, LLM etc
NOT for PostGraduate Researchers – e.g., MRes/MPhil/PhD degrees

Middlesex University is concerned with protecting the rights, health, safety, dignity, and privacy of its research participants. It is also concerned with protecting the health, safety, rights, and academic freedom of its students and with safeguarding its own reputation for conducting high quality, ethical research.

This Research Ethics Screening Form will enable students to self-assess and determine whether the research requires ethical review and approval via the Middlesex Online Research Ethics (MORE) form before commencing the study. Supervisors must approve this form after consultation with students.

Student Name:	Fisha Goitem	Email:FG295@live.mdx.ac.uk
Research project title:	**Design and Simulation of a Secure Network Architecture for boot pharmacies Using VLANs and ACLs to Enhance Security and Performance.**	
Programme of study/module:	CST3590 Individual Project	
Supervisor Name:	Olugbenga O Oluwagbemi	Email:001121@live.mdx.ac.uk

Please answer whether your research/study involves any of the following given below:		
1. HANIMALS or animal parts.	□ Yes	☒ No
2. MCELL LINES (established and commercially available cells - biological research).	□ Yes	☒ No
3. HCELL CULTURE (Primary: from animal/human cells- biological research).	□ Yes	☒ No
4. HCLINICAL Audits or Assessments (e.g. in medical settings).	□ Yes	☒ No
5. XCONFLICT of INTEREST or lack of IMPARTIALITY. If unsure see “Code of Practice for Research” (Sec 3.5) at: https://unihub.mdx.ac.uk/study/spotlights/types/research-at-middlesex/research-ethics	□ Yes	☒ No
6. XDATA to be used that is not freely available (e.g. secondary data needing permission for access or use).	□ Yes	☒ No
7. XDAMAGE (e.g., to precious artefacts or to the environment) or present a significant risk to society).	□ Yes	☒ No
8. XEXTERNAL ORGANISATION – research carried out within an external organisation or your reseach is commissioned by a government (or government body).	□ Yes	☒ No
9. MFIELDWORK (e.g biological research, ethnography studies).	□ Yes	☒ No
10.HGENETICALLTY MODIFIED ORGANISMS (GMOs) (biological research).	□ Yes	☒ No
11. HGENE THERAPY including DNA sequenced data (biological research).	□ Yes	☒ No
12. MHUMAN PARTICIPANTS – ANONYMOUS Questionnaires (participants not identified or identifiable).	□ Yes	☒ No

13. ^{X}HUMAN PARTICIPANTS – IDENTIFIABLE (participants are identified or can be identified): survey questionnaire/ INTERVIEWS / focus groups / experiments / observation studies/ evaluation studies.	□ Yes	☒ No
14. ^{H}HUMAN TISSUE (e.g., human relevant material, e.g., blood, saliva, urine, breast milk, faecal material).	□ Yes	☒ No
15.^{H}ILLEGAL/HARMFUL activities research (e.g., development of technology intended to be used in an illegal/harmful context or to breach security systems, searching the internet for information on highly sensitive topics such as child and extreme pornography, terrorism, use of the DARK WEB, research harmful to national security).	□ Yes	☒ No
16. ^{X}PERMISSION is required to access premises or research participants.	□ Yes	☒ No
17. ^{X}PERSONAL DATA PROCESSING (Any activity with data that can directly or indirectly identify a living person). For example data gathered from interviews, databases, digital devices such as mobile phones, social media or internet platforms or apps with or without individuals'/owners' knowledge or consent, and/or could lead to individuals/owners being IDENTIFIED or SPECIAL CATEGORY DATA (GDPR[1]) or CRIMINAL OFFENCE DATA. [1]Special category data (GDPR- Art.9): "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".	□ Yes	☒ No
18.^{X}PUBLIC WORKS DOCTORATES: Evidence of permission is required for use of works/artifacts (that are protected by Intellectual Property (IP) Rights, e.g. copyright, design right) in a doctoral critical commentary when the IP in the work/artifactis jointly prepared/produced or is owned by another body	□ Yes	☒ No
19. ^{H}RISK OF PHYSICAL OR PSYCHOLOGICAL HARM (e.g., TRAVEL to dangerous places in your own country or in a foreign country (see https://www.gov.uk/foreign-travel-advice), research with NGOs/humanitarian groups in conflict/dangerous zones, development of technology/agent/chemical that may be harmful to others, any other foreseeable dangerous risks).	□ Yes	☒ No
20.^{X}SECURITY CLEARANCE – required for research.	□ Yes	☒ No
21.^{X}SENSITIVE TOPICS (e.g., anything deeply personal and distressing, taboo, intrusive, stigmatising, sexual in nature, potentially dangerous, etc).	□ Yes	☒ No

M – Minimal Risk; X – More than Minimal Risk. H – High Risk

If you have answered 'Yes' to ANY of the items in the table, your application REQUIRES ethical review and approval using the MOREform **BEFORE commencing your research**. Please apply for ethical approval using the MOREform (https://moreform.mdx.ac.uk/). Consult your supervisor for guidance. Also see *Middlesex Online Research Ethics (*MyLearning area*) and www.tiny.cc/mdx-ethics*

If you have answered 'No' to ALL of the items in the table, your application is Low Risk and you may NOT require ethical review and approval using the MOREform before commencing your research. Your research supervisor will confirm this below.

Student Signature:………………………………… Date:…29/01/2025…………………

To be completed by the supervisor:

Based on the details provided in the self-assesment form, I confirm that:	Insert Y or N
The study is Low Risk and *does not require* ethical review & approval using the MOREform	y
The study *requires* ethical review and approval using the MOREform.	n

Superivsor Signature:……OLUWAGBEMI O.O…………..……Date: February 26th 2025