TESCO GETGO SMART STORE NETWORK DESIGN AND IMPLEMENTATION

Krish Patel

Table of Contents

1.0 Abstract

This project focuses on designing and implementing a secure, scalable, and high-performance network infrastructure for a Tesco GetGo smart store, a retail concept that leverages Internet of Things (IoT) devices and artificial intelligence (AI) to deliver a seamless, checkout-free shopping experience (Tesco PLC, 2020). The network will be adaptable for widespread use across future locations. The key objective was to address the limitations of Tesco's existing network to support these advanced technologies.

Adopting an Agile (Scrum-based) methodology, the design incorporates Virtual LANs (VLANs) for network segmentation, ACL's for vigorous threat protection, a Virtual Private Network (VPN) solution integrated with Multi-Factor Authentication (MFA) for secure remote access, and an Intrusion Detection and Prevention System (IDPS) for enhanced security.

A working prototype was developed using Cisco Packet Tracer, demonstrating the functionality and effectiveness of the design (Cisco, 2020). Challenges, such as configuring ACL's, setting up the VPN, and addressing inter-VLAN routing issues, were overcome through iterative testing, configuration adjustments, and reference to Cisco documentation.

In addition, I created a Gantt chart (Appendix B), which I adhered to throughout the project. This chart helped me manage my time effectively, track progress, and develop problem-solving strategies. By overcoming challenges such as learning new topics, I built upon my time management skills, ensuring that the project remained on track while maintaining high standards.

Ultimately, the project contributed to the success of Tesco's GetGo expansion by requiring a shift away from traditional thinking and toward a more collaborative, experimental approach. These new ways of approaching work reveal new solutions which, in turn, can improve customer experience (Accenture, 2023) and efficiency.

2.0 Introduction

2.1 Project Aims and Problem Statement

The project's core aim was to design and implement a secure, scalable, and high-performance network infrastructure specifically for Tesco's GetGo smart stores. These stores, representing a significant advancement in retail technology, leverage IoT devices, AI, and computer vision to offer customers a checkout-free shopping experience. IoT in retail significantly enhances the customer experience through personalised marketing and layout optimisation (Velos IoT, 2025). As Anderson mentions, the innovative model, while beneficial, presents extensive demands on the network (Anderson, 2020).

Tesco's existing network, while sufficient for traditional retail operations, could face critical challenges in the context of GetGo:

- **Heightened Security Risks:** The extensive use of IoT devices (cameras, sensors, smart shelves) significantly expanded the network's attack surface, requiring a comprehensive security strategy to prevent data breaches, protect customer privacy, and ensure operational integrity. The potential consequences of insufficient security can include financial losses, reputational damage, and legal liabilities, particularly concerning data protection regulations.
- **Demanding Performance Requirements:** The GetGo model depends on real-time data processing and analysis from numerous devices. This generates substantial network traffic, demanding high bandwidth and low latency for a smooth customer

experience. Slow speeds or disruptions could lead to inaccurate tracking, payment errors, and customer dissatisfaction.

- **Scalability Concerns:** Tesco's plans for expanding its GetGo store network across the UK required a network design capable of easily accommodating new stores and devices without major architectural changes. A lack of scalability could slow down growth and increase IT costs.
- **Secure Remote Access Needs:** Secure and reliable remote access for IT staff and support personnel was essential for network management, troubleshooting, and updates. Insecure remote access could create vulnerabilities and to reduce the effect of these attacks on IoT systems, periodic penetration testing is recommended (Yaacoub et al., 2023).
- **Traffic Management:** Efficient methods for prioritising time-sensitive data and preventing network blockages were critical.

These challenges, if unaddressed, posed a significant risk to the success of Tesco's GetGo initiative. The project aimed to mitigate these risks by creating a network that was secure, performant, adaptable, and future-proof.

2.2 Introduction to the Report

This report documents the project lifecycle, from initial requirements gathering and design to implementation, testing, and evaluation. The structure provides a clear progression: requirements (Section 3), design (Section 4), implementation and testing (Section 5), recommendations (Section 6), reflection (Section 7), conclusion (Section 8), references (Section 9), and appendices (Section 10).

3.0 Requirements and Project Objectives

Functional Requirements:

- **Hierarchical Network Design:** Implement a three-tier (Core, Distribution, Access) model.
- **Redundancy:**
    - Utilise two routers at the Core layer.
    - Utilise two multilayer switches (MLSWs) at the Core/Distribution layer.
    - Provide redundancy at every layer.
    - Connect to two separate ISPs for internet redundancy. Each core router must connect to both ISPs (Mcmillan, 2015).
- **VLAN Segmentation:** Each area (POS, Sales, Stock, Staff, Tech) and the Server Room must reside in separate VLANs and separate IP subnetworks.
- **Wireless Network:** Provide wireless network access (WLAN) within each of the five user departments.
- **IP Addressing:**
    - Use the base network 172.16.1.0 for internal addressing.

    - Perform subnetting to allocate sufficient IP addresses for each department (120 users expected per department) and the Server Room (12 devices expected).
    - Use provided static public IPs (195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, 195.136.17.12/30) for ISP connections.
- **Inter-VLAN Routing:** Configure the MLSWs to handle routing between VLANs (using SVIs). MLSWs must perform both Layer 2 switching and Layer 3 routing.
- **Dynamic IP Allocation:** All user devices in departments must obtain IP addresses dynamically from a dedicated DHCP server located in the Server Room.
- **Static IP Allocation:** Devices within the Server Room must be assigned static IP addresses.
- **Routing Protocol:** Implement OSPF for dynamic routing between routers and MLSWs.
- **Secure Remote Management:** Configure SSH access on all routers and MLSWs.
- **Port Security:** Configure port security on access layer switch ports connected to devices in the Finance and Accounts department. Requirements: allow only one MAC address per port, use the sticky learning method, set violation mode to shutdown.
- **Internet Access Control:** Configure Port Address Translation (PAT) on edge routers using the outbound interface IP address. Implement necessary Access Control Lists (ACLs) to permit required outbound traffic and deny unwanted traffic.
- **IPS (Intrusion Prevention System):** Actively monitors network traffic to detect and prevent external threats, while also reducing unnecessary or harmful data transmission within the network.
- **Basic Device Configuration:** Configure hostnames, console passwords, enable passwords, banner messages (MOTD), and disable IP domain lookup on network devices.
- **Connectivity:** Ensure devices within the same department can communicate, devices in different departments can communicate (via MLSW routing), and appropriate devices can access the internet and servers.
- **VPN Access:** Implement site-to-site or remote access VPN for secure external connections (James Michael Stewart, 2011).

Non-Functional Requirements:

- **Security:** Implement security best practices beyond specific requirements (e.g., unused port shutdown, secure passwords).
- **Performance:** Design for adequate bandwidth and low latency to support 600 users.
- **Reliability:** Ensure high availability through redundancy features.
- **Scalability:** The IP addressing scheme and hierarchical design should allow for future expansion.

- **Maintainability:** Use clear naming conventions, documentation, and logical design for ease of management.
- **Usability:** SSH provides secure and standard remote management access.

Project Objectives (SMART):

1. Network Assessment (by Dec 2, 2024)
2. Detailed Network Design Proposal (by Jan 13, 2025)
3. Secure and Scalable Network Architecture Design (by Feb 1, 2025)
4. Phased Implementation Plan (by Mar 1, 2025)
5. Testing and Validation Strategy (by Mar 15, 2025)
6. Final Presentation and Documentation (by Apr 28, 2025)
7. Stakeholder Feedback and Optimisation (by Apr 28, 2025)

4.0 Design Chapter

4.1 Design Decisions and Rationale

The network design was curated by requirements, best practices, and Packet Tracer limitations. Key decisions:

- **Hierarchical Network Topology:** A three-tier hierarchical model (Core, Distribution, Access) was chosen for its established benefits in scalability, manageability, and fault tolerance. The *Core Layer*, with redundant routers (R1, R2) and Layer 3 switches (MLSW1, MLSW2), provides high-speed switching and routing. The *Distribution Layer*, consisting of Layer 2 switches on each floor, aggregates access layer connections and implements security policies. The *Access Layer* connects end devices (PCs, IoT devices, etc.) via access switches. This structure simplifies expansion, isolates failures, and provides clear points for security enforcement.
- **VLAN Segmentation:** Departments and the Server Room are isolated into separate VLANs (VLAN 10: POS, 20: Sales, 30: Stock, 40: Staff, 50: Tech, 60: ServerRoom). VLAN is a separate broadcast domain, so devices on separate VLANs are unable to communicate without the intervention of a routing device. The device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality (Ahmad et al., 2020)
    - Rationale: Enhances security by limiting broadcast domains and preventing traffic snooping between departments. Improves performance by reducing broadcast traffic. Allows granular policy application per department. Directly meets the requirement for departmental separation.
- **IP Addressing Scheme:** A hierarchical scheme based on 172.16.1.0 was developed using Variable Length Subnet Masking (VLSM), a standard technique for efficient address allocation. /25 masks (126 usable hosts) were allocated for user departments (120 users expected), and a /28 mask (14 usable hosts) for the Server Room (12 devices expected). /30 masks were used for point-to-point links between routers and MLSWs. Public IPs were assigned as specified for ISP links.

- Rationale: Provides sufficient addresses for current needs with room for moderate growth within departments. Efficiently uses address space. Logical structure simplifies routing and troubleshooting. Addresses corrected from the initial scheme provided.

- **Routing Protocol (OSPF):** Open Shortest Path First (OSPF), was chosen as the dynamic routing protocol. It will be configured on routers (R1, R2) and MLSWs (MLSW1, MLSW2). A single OSPF area (Area 0) was used for simplicity given the single building scope, but multi-area should be considered for future scalability (Nastase, 2018).
    - Rationale: Stated in requirements. OSPF is an industry-standard, scalable, and efficient link-state routing protocol suitable for complex networks. It automatically adapts to topology changes, supporting redundancy. This replaces the initial plan of using static routing mentioned in the Literature Review.
- **Intrusion Prevention System:** To provide proactive threat detection and mitigation beyond basic ACL filtering, Cisco IPS was configured on Main in the VPN network. This leverages the router's capability to inspect traffic flows against known malicious signatures. The design involved enabling the necessary securityk9 license, defining specific signature sets (initially enabling the ios_ips basic category), and configuring actions like alerting and packet denial for specific high-priority signatures (signature 2004/0). Applying this IPS rule set to a key interface (like the one facing internal segments or a specific critical VLAN) adds a crucial layer of defence against common network attacks.
- **Security:** A multi-layered security approach was vital:
    - SSH: Configured on routers and MLSWs for secure remote CLI management, replacing insecure Telnet. Requires username/password authentication.
    - Port Security: Implemented on Access switch ports for the Stock VLAN (VLAN 30) to restrict access to authorised devices (sticky MAC learning) and shut down ports upon violation. This is a fundamental switch security feature.
    - PAT & ACLs: Configured on edge routers (R1, R2) to translate internal private IPs to the public IP of the outgoing interface for internet access. Extended ACLs permit necessary outbound traffic (HTTP, HTTPS, DNS, etc.) from user VLANs and deny other traffic, including blocking direct inbound connections from the internet, following firewall best practices.
    - VPN: Site-to-site or remote access VPN using IPsec, simulated in Packet Tracer, configured on edge routers for secure connectivity.
    - Basic Security: Console/Enable passwords, MOTD banner, disabling DNS lookup, shutting down unused ports, aligning with basic security principles.
    - Rationale: Addresses specific security requirements (SSH, PortSec, PAT/ACL) and general best practices. Port security mitigates unauthorised device connections in the sensitive Finance area. PAT conserves public IPs and hides internal structure. ACLs control traffic flow. VPN ensures secure external communication (Tanenbaum, 2011).

Redundancy Implementation:

- **Routers/MLSWs**: Dual devices with OSPF routing ensure path recalculation if one device or link fails.
- **Simulation Tool:** Cisco Packet Tracer chosen for its ability to simulate Cisco devices, OSPF, VLANs, DHCP, basic wireless, ACLs, PAT, SSH, port security, and basic VPN configurations required by the project.

4.2 Networking Project Design Elements

- **Network Topology Diagram:** The network topology diagram (Appendix F) visually represents the hierarchical structure, with the Core, Distribution, and Access layers clearly defined. It shows the interconnections between devices (routers, switches, servers, end devices), interface names, IP addresses, and VLAN assignments. This diagram is the topology for the network implementation.
- **IP Addressing Table:** The IP addressing table (Appendix G) details the allocation of IP address ranges to each VLAN and network segment. It includes network addresses, subnet masks, host address ranges, and broadcast addresses.
- **VLAN Table:** The VLAN table (Appendix H) lists all defined VLANs, their IDs, names, descriptions, and the associated switch ports. This table guides the configuration of VLANs on the switches and ensures consistent VLAN assignments across the network.
- **Key Configuration Details:** Refer to **Appendix C** for complete and thoroughly commented configuration files for all devices (routers, switches and servers).

5.0 Development and Testing

5.1 Implementation Overview

The network design was implemented as a functional prototype within Cisco Packet Tracer following a structured approach:

1. **Topology Construction:** Placed devices (Routers - 2991; MLSWs - 3650; Access Switches - 2960; Servers; PCs; Wireless APs) and connected them using appropriate cables as per the topology diagram.
2. **Basic Device Configuration:** Configured hostnames, console/enable passwords, MOTD banner, disabled IP domain lookup on all routers and switches.
3. **VLAN Creation & Assignment:** Created VLANs 10, 20, 30, 40, 50, 60 on MLSWs and Access switches according to VLAN best practices. Assigned Access switch ports to their respective department VLANs (switchport mode access, switchport access vlan X). Configured trunk links between switches and from Access switches to MLSWs (switchport mode trunk).
4. **SVI & Inter-VLAN Routing:** Created SVIs (e.g., interface Vlan10) on MLSW1 and MLSW2 for each VLAN. Assigned IP addresses (gateways from the IP scheme) to SVIs. Enabled IP routing (ip routing) globally on MLSWs. Configured HSRP or VRRP between MLSW1 and MLSW2 for SVI gateway redundancy. Configuring the trunk is essential for optimising network performance, supporting VLAN segmentation, enabling flexibility and efficiently managing network resources, particularly in environments with multiple VLANs and interconnected switches (Musa et al., 2024).
5. **OSPF Configuration:**

- Enabled OSPF routing process (router ospf 0) on R1, R2, MLSW1, MLSW2.
- Configured router IDs.
- Advertised connected networks (VLAN subnets on MLSWs, interconnect links) within OSPF Area 0 using network commands, following OSPF configuration principles.
- Configured passive interfaces for SVIs facing user networks.

6. **DHCP Server Configuration:** Configured the dedicated Server (in VLAN 60, static IP) with DHCP service. Created separate IP pools for VLANs 10, 20, 30, 40, 50, defining network, default-router (SVI IP) and dns-server (Server IP).
7. **DHCP Relay:** Configured ip helper-address 172.16.3.130 on each user VLAN SVI (VLANs 10-50) on the MLSWs.
8. **Static IP Configuration:** Manually configured static IP addresses, subnet masks, and gateways for servers in VLAN 60.
9. **Wireless Configuration:** Configured standalone APs. Set SSIDs (e.g., "Stock-AP"), assigned them to respective VLANs, and configured WPA2-PSK security.
10. **SSH Configuration:** Generated RSA keys (crypto key generate rsa), configured domain name (ip domain-name), set SSH version 2 (ip ssh version 2), configured VTY lines for SSH login (transport input ssh, login local), and created local user accounts according to secure configuration guidelines.
11. **Port Security Configuration:** Applied port security commands (max 1, sticky, violation shutdown) to Stock department (VLAN 30) access ports on relevant switches as per Cisco recommendations.
12. **ISP Configuration:** Configured basic IP addressing on simulated ISP routers.
13. **PAT and ACL Configuration:** Defined extended ACLs on R1/R2 to permit desired outbound traffic. Applied NAT overload (eg., ip nat inside source list 1 interface se0/2/0 overload) on external interfaces. Defined inside (ip nat inside) and outside (ip nat outside) interfaces. Configured default routes on R1/R2 pointing to their respective ISP next-hops. With Standard Access-List you can check only the source of the IP packets (Alexander, 2023)
14. **VPN/IPS Configuration (Simulated):** Configured basic IPsec parameters (crypto isakmp policy, crypto isakmp key, crypto ipsec transform-set, crypto map) on Internet to Mlt-SW1 for site-to-site or remote access simulation, based on IPsec standards (West, 2019). IPS config on Main involved enabling the securityk9 technology package license, creating a dedicated directory (ipsdir) in flash for signature files, defining a named IPS rule set (iosips), managing signature categories (retiring 'all' then enabling 'ios_ips basic'), specifically enabling and defining actions (produce-alert, deny-packet-inline) for signature 2004/0, configuring logging to a syslog server for alerts, and applying the iosips rule set to inspect inbound traffic on interface GigabitEthernet0/1.
15. **End Device Configuration:** Configured PCs/Laptops to use DHCP. Tested wireless connections.

5.2 Changes to Original Plan

- **Routing Protocol:** The primary change from the initial report draft (not the requirements) was switching from Static Routing to OSPF. This required significant changes in router and MLSW configuration.
- **Security Focus:** The security implementation shifted from a focus on NGFW (from the initial report draft) to the specifically required SSH, Port Security, and PAT/ACLs. VPN was added for additional security**.**
- **Wireless Implementation:** Wireless was integrated into the core design and implementation, rather than being just a recommendation.
- **Context:** These changes were managed by carefully re-evaluating the requirements and adjusting the design and implementation steps accordingly. The core hierarchical structure remained, but routing and security configurations were significantly modified.

5.3 Development Environment & Tools Used

- **Cisco Packet Tracer (Version 8.2.2.0400):** Primary network simulation tool for topology design, device configuration, and testing.
- **Text Editor (Notepad):** Used for drafting configurations, creating ACLs, and documenting steps.
- **Spreadsheet Software (Microsoft Excel):** Used for IP addressing planning (VLSM), VLAN table creation, and test case management.
- **Cisco IOS Command Reference/Configuration Guides:** Consulted official documentation for OSPF, SSH, Port Security, NAT, ACL, and other command syntax and concepts.
- **Project Requirements Document:** The primary source for functional and non-functional requirements.
- **Online Forums:** Troubleshooting support.

5.4 Testing Strategy & Results

A systematic testing strategy was employed, performing tests incrementally after major configuration phases and comprehensively at the end. **See Appendix D for the full test table.**

- **Connectivity Testing:**
    - **ping:** Intra-VLAN, Inter-VLAN, to Servers, to Default Gateways (SVIs), to Routers and to simulated ISP Ips.
    - **traceroute:** Verify routing paths (OSPF) and identify failures.
- **Functional Testing:**
    - **DHCP:** Verify PCs in VLANs 10-50 receive correct IP, mask, gateway, and DNS info from the DHCP server.
    - **DNS:** Verify name resolution (if a DNS server was configured).

    - **Inter-VLAN Routing:** Confirm successful pings between different user VLANs.
    - **OSPF:** Check OSPF neighbor adjacencies (show ip ospf neighbor) and routing table population (show ip route ospf).
    - **Wireless:** Connect wireless clients to departmental SSIDs, verify they get correct IP via DHCP and can reach resources such as the Web browser.
- **Security Testing:**
    - **SSH:** Attempt SSH login to routers/MLSWs using configured credentials. Verify Telnet is disabled.
    - **Port Security:** Connect an authorised device to a Stock port, verify connectivity. Disconnect, connect an unauthorised device, verify port status becomes err-disabled. Test sticky MAC learning.
    - **PAT/ACL:** Ping external IP from internal PC, check NAT translations (show ip nat translations). Attempt access to permitted services (HTTP/HTTPS) externally. Attempt access for blocked services or from blocked sources, verify denial by ACL or IPS (show access-lists).
    - **VPN (Simulated):** Test connectivity between networks designated to be connected via VPN within Packet Tracer.
- **Redundancy Testing:**
    - Shut down interfaces connecting R1 to MLSWs/ISPs, verify traffic fails over via R2 (using traceroute, ping).
    - Shut down MLSW1, verify MLSW2 takes over SVI gateway roles (if HSRP/VRRP configured) and routing.

Major Errors Found and Fixed:

- **OSPF Adjacency Issues:** Initially, OSPF neighbors between MLSWs and Routers did not form. This was due to mismatched OSPF area IDs or network masks on the interconnecting interfaces.
    - Solution: Carefully verified and corrected network commands and interface IP/masks in the OSPF configuration on all participating devices, referencing OSPF principles.
- **DHCP Relay Failure:** PCs were not receiving DHCP addresses. The ip helper-address command was missing on the SVI interfaces on the MLSWs.
    - Solution: Added the command pointing to the dedicated DHCP server's IP address on each user VLAN SVI (10-50), as required for relay agent functionality.
- **ACL Blocking Legitimate Traffic:** The initial PAT ACL was too restrictive, blocking DNS requests needed for web browsing.
    - Solution: Modified the extended ACL to explicitly permit UDP port 53 (DNS) traffic outbound, in addition to TCP ports 80/443. Ensured correct ACL sequence based on filtering best practices.

- **Port Security Sticky MAC Learning:** Sticky MAC addresses were not being saved correctly after switch reload in Packet Tracer simulation.
    - Solution: Ensured copy running-config startup-config was saved after the MAC address was learned and port security activated. Acknowledged potential Packet Tracer limitations.
- **Inter-VLAN Routing Failure:** Similar to the initial report draft issue, the ip routing command was initially missed on the MLSWs. VLAN will restrict access to the ports by non-authorised people (Ahmed et al., 2021).
    - Solution: Enabled global IP routing on both MLSW1 and MLSW2.

6.0 Recommendations

Based on the design and implementation, the following improvements are recommended for the network:

Advanced Wireless Security: Transition from WPA2-PSK to WPA2/WPA3-Enterprise using a RADIUS server (potentially hosted in the Server Room) for 802.1X authentication. This provides individual user authentication for wireless access, enhancing security significantly over pre-shared keys.

Network Monitoring System (NMS): Deploy an NMS (e.g., Wireshark) to continuously monitor the health, performance (CPU, memory, bandwidth), and availability of routers, switches, servers, and ISP links using protocols like SNMP. Configure alerts for failures or performance degradation.

Quality of Service (QoS): Implement QoS policies, particularly if voice or video traffic is anticipated. Prioritise real-time traffic (VoIP) and critical application traffic over less sensitive traffic (e.g., large file transfers, web browsing) using mechanisms like classification to ensure performance during congestion.

Improved Redundancy (Access Layer): Connecting Access layer switches to both MLSW1 and MLSW2 using EtherChannel for link redundancy and increased bandwidth. Implement Spanning Tree Protocol (STP) optimisations like PortFast on access ports to improve stability and security.

Security Enhancements:

SIEM System: Implement a Security Information and Event Management (SIEM) system to centralise logs from routers, switches, firewalls (if added), servers, and APs for correlation and faster threat detection/response.

Network Access Control (NAC): Deploy a NAC solution (like Cisco ISE) for more specific access control, assessment (ensuring connecting devices meet security requirements), and guest network management implementation. Cisco ISE is extremely flexible in design and practical for most environments as stated by (Richter, 2015)

Firewall Upgrade: While PAT/ACLs provide basic firewalling, using a dedicated Next-Generation Firewalls (NGFWs) for advanced threat protection. The next generation firewall offer more accessibility to network traffic, operability across the OSI layers, and advanced features to protect the networking infrastructure against emerging threats (Neupane et al., 2018).

OSPF Tuning: Review OSPF, consider implementing OSPF authentication between routers/MLSWs for added security, and potentially plan for a multi-area OSPF design if significant future expansion is to go ahead.

Configuration Backups & Automation: Implement automated configuration backups for all network devices. Explore network automation tools (Python) for routine tasks like VLAN creation, ACL updates, or software upgrades to improve efficiency and reduce.

Disaster Recovery Plan: Develop and test a comprehensive network disaster recovery plan, including off-site backups and procedures for restoring connectivity after major failures, following business principles.

7.0 Challenges and Reflection

7.1 Project Improvements & Lessons Learned

Areas for improvement:

- **More Detailed Initial Planning:** While the requirements were clear, spending more time upfront thoroughly planning OSPF areas (even if starting with Area 0), IP addressing for potential future growth, and the exact flow of ACL rules could have been streamlined the configuration phase. Adhering more strictly to project planning methodologies could be beneficial.
- **Earlier Stakeholder Engagement:** Involving Tesco IT staff and GetGo store personnel earlier and more consistently in the design process would have provided valuable insights into their specific operational needs and potential challenges. This could have led to earlier identification of potential issues and a more refined design.
- **Improved Time Management:** While the project was completed on time, a clearer approach to task breakdown and prioritisation, particularly for testing and troubleshooting, would have improved efficiency. Allocating more time specifically for troubleshooting complex configurations would have been beneficial.
- **Phased Implementation in Simulation:** While testing was iterative, a more strictly phased implementation within Packet Tracer (e.g., build Layer 2 fully, then Layer 3 base, then OSPF, then security layers) might have made isolating certain types of issues (like routing vs. ACL problems) even easier.
- **Exploring HSRP/VRRP:** The requirements mentioned redundancy but didn't require First-Hop Redundancy Protocols (FHRP) like HSRP or VRRP for the SVI gateways on the MLSWs. Implementing and testing HSRP would have added another layer of practical redundancy knowledge and improved the design's fault tolerance for end-users.

Key lessons learned:

- **Thorough Planning is Crucial:** The importance of a well-defined plan, including a detailed IP addressing scheme, VLAN structure, and network topology, cannot be expressed enough. This foundation significantly simplified the implementation process.
- **Iterative Testing is Essential:** Continuous testing after each configuration step was invaluable for identifying and resolving issues early, preventing them from compounding. Network OS testing is performed in the optimisation phase in order to

maximise performance and have paramount security as stated by (Sholomon et al., 2025)

- **Documentation is Paramount:** Maintaining clear and up-to-date documentation (configurations, diagrams, test results) is critical for managing, troubleshooting, and scaling the network.
- **OSPF Complexity:** Configuring OSPF across multiple routers and Layer 3 switches, ensuring correct network statements, passive interfaces, and troubleshooting adjacencies, requires careful attention to detail. It's significantly more involved than static routing.
- **Security is Layered and Precise:** Implementing security features like port security and ACLs requires precision. A single incorrect ACL entry or port security parameter can block necessary traffic or fail to provide the intended protection. Testing each rule is crucial. Most commonly used security methods rely on cryptographic techniques employed at the upper layers of a wireless network (Shiu et al., (2011) therefore focus has been put on the ISP's and Multi Switches with logged security.
- **Redundancy Requires Careful Design:** Simply having dual devices isn't enough. Routing protocols (OSPF), potential FHRPs, and redundant links must all work together correctly to achieve seamless failover.

7.2 Personal Capability and Skill Development

Skills developed:

- **Network Design:** I gained practical experience in applying network design principles, creating a hierarchical topology, implementing VLAN segmentation, developing an IP addressing scheme, and selecting appropriate routing protocols (White et al., 2014).
- **OSPF Configuration & Troubleshooting:** Moved beyond basic static routing to configuring and verifying a dynamic routing protocol in a multi-router, multi-L3 switch environment. Learned common OSPF troubleshooting commands (show ip ospf neighbor, show ip route ospf, debug ip ospf adj).
- **Advanced Switching Features:** Gained hands-on experience implementing Inter-VLAN routing using SVIs and configuring specific Layer 2 security with Port Security (sticky MAC, violation modes).
- **Network Security Implementation:** Developed practical skills in configuring SSH, writing extended ACLs for traffic filtering and NAT/PAT control, understanding the mechanics of PAT, and simulating basic VPN setups, skills, learning how to isolate problems, analyse configurations, and use diagnostic tools effectively.
- **Project Management:** I improved my ability to plan, organise, schedule, and execute a complex project, adapting to challenges and managing my time effectively.

Summary:

This project offered multiple opportunities for the development and refinement of key networking capabilities across various domains, including routing protocols, security implementation, and the troubleshooting of complex interactions.

One significant area of growth involved configuring and troubleshooting the Open Shortest Path First (OSPF) routing protocol. Although the final simulated design utilised static routing

for simplicity, the initial requirements phase included trialing with OSPF. The process involved identifying incorrect network masks within the OSPF configuration commands and resolving them, thereby deepening the understanding of OSPF operations and diagnostic methods using commands such as show ip ospf neighbor.

The implementation of specific Layer 2 security measures also demonstrated notable progress. Following research conducted during the literature review phase, port security was configured on the Stock VLAN (VLAN 30) access ports as specified. This included limiting the number of permitted MAC addresses to one, enabling sticky MAC learning to bind the first detected address, and setting the violation mode to 'shutdown'. The successful implementation and testing of these parameters, particularly the validation of the shutdown response upon violation, illustrated the effective application of access layer security concepts.

Additionally, troubleshooting the interaction between Port Address Translation (PAT) and Access Control Lists (ACLs) provided a strong opportunity to enhance diagnostic proficiency. As reflected upon during the testing phase outlined in the Project Proposal, ensuring that permitted traffic passed while blocked traffic was denied required careful configuration and verification. Commands such as show ip nat translations and show access-lists were helpful in diagnosing why certain outbound traffic was initially obstructed, ultimately leading to the correction of ACL entries and reinforcing skills in both edge security and address translation.

Collectively, these examples demonstrate the practical application and advancement of theoretical knowledge throughout the project, resulting in measurable improvements in network implementation and troubleshooting expertise using my Project Blog as guidance.

7.3 Challenges Encountered and Solutions

- **Challenge 1: OSPF Configuration Across Multiple Device Types**
  Issue: Configuring OSPF consistently on both routers and MLSWs, ensuring proper network advertisements (especially for VLAN SVIs on MLSWs) and passive interface settings, was initially challenging.
  Solution: Methodically configured OSPF on one device at a time, verifying neighbour relationships before moving to the next. Used “show ip ospf interface brief” and “show ip protocols” widely. Consulted Cisco documentation and OSPF standard documentation, specifically for OSPF on Catalyst switches (MLSWs) versus routers. Correctly identifying which interfaces needed to be passive was vital.

- **Challenge 2: Precise PAT/ACL Implementation**
  Issue: Creating an extended ACL that permitted all necessary outbound traffic for users (web, DNS, etc.) while blocking unwanted traffic, and correctly applying it to the NAT overload configuration on dual redundant routers, required careful planning and testing.
  Solution: Planned the ACL on paper first, listing specific permit/deny rules in the correct order (specific before general), following established firewall rule design principles. Started with basic rules (permit HTTP/HTTPS/DNS) and tested. Incrementally added rules. Used show ip nat statistics and debug ip nat to troubleshoot translation issues, referring to Cisco NAT guidelines. Ensured the ACL and NAT config were mirrored on both R1 and R2.

- **Challenge 3: Port Security Behaviour**
  Issue: Getting the sticky MAC address feature to behave as expected, particularly ensuring the learned MAC was saved and reapplied correctly after a simulated port flap or switch reload within Packet Tracer.
  Solution: Ensured the switchport port-security mac-address sticky command was applied correctly. Manually triggered learning by connecting the "authorised" device. Verified the MAC was learned using show port-security interface (interface number) address. Crucially, used copy running-config startup-config after the MAC was learned and added to the running-config by the sticky feature. Tested by disconnecting/reconnecting and checking the port status and security config.

- **Challenge 4: Coordinating Multiple Redundant Paths**
  Issue: Ensuring traffic used the optimal path via OSPF and correctly failed over to the secondary router/ISP link during simulated failures.
  Solution: Verified OSPF costs were logical. Used traceroute extensively before and during simulated failures (shutting down interfaces) to observe path changes. Ensured both routers had necessary default routes (often learned via OSPF from ISPs or configured statically with tracking). Tested failover timing against general network convergence expectations.

- **Challenge 5: Implementing All Requirements**
  Issue: Integrating all the distinct requirements (VLANs, OSPF, DHCP, Wireless, SSH, Port Security, PAT/ACL, VPN) into a single cohesive and working network simulation required careful, step-by-step implementation and constant testing.
  Solution: Followed the structured implementation plan outlined in Section 5.1. Tested basic connectivity and routing before adding security layers. Addressed issues incrementally rather than configuring everything at once and then troubleshooting, a recommended procedure in system integration.

Overcoming these challenges provided deep insights into the practical application and interaction of various networking technologies.

8.0 Conclusion

This project successfully designed, implemented, and tested a comprehensive network infrastructure for Tesco’s GetGo Stores, strictly observing to the outlined requirements. The resulting network, simulated in Cisco Packet Tracer, offers a scalable, secure, and highly redundant solution tailored across six departments. Throughout the project, key project management skills were developed and applied, including requirement analysis, task scheduling, risk management, stakeholder communication, and iterative validation to ensure alignment with objectives at every stage (Portny, 2019).

The design incorporated key technologies including a hierarchical topology with dual routers and multilayer switches, VLAN segmentation for departmental isolation, OSPF for robust dynamic routing, dedicated DHCP services, integrated wireless access per department, and essential security measures such as SSH, port security for the Stock department, PAT with ACLs for controlled internet access, and VPN capabilities. The implementation process validated the design's feasibility and allowed for practical troubleshooting of issues related to OSPF configuration, security policy application, and feature interactions.

Comprehensive testing confirmed that all core requirements were met, including inter-VLAN communication, dynamic IP allocation, OSPF routing, secure management, required security controls, wireless connectivity, and successful failover for ISP redundancy. Recommendations for future enhancements include advanced wireless security, network monitoring, QoS implementation, and further security for continued network adaptation. The project significantly enhanced practical skills in network design, implementation of specific Cisco IOS features (OSPF, Port Security, PAT/ACL, SSH), and systematic troubleshooting in a complex, multi-requirement scenario. The final network design delivers a reliable and secure foundation for Tesco.

9.0 References

Reference list

Accenture (2023). *Digital Transformation l Accenture*. [online] www.accenture.com. Available at: https://www.accenture.com/gb-en/insights/digital-transformation-index.

Ahmad, I., Ashraf, Dr.Javed. and Nasir, Dr.Anisur.R. (2020). Design and Implementation of Network Security using Inter-VLAN-Routing and DHCP. *Asian Journal of Applied Science and Technology*, 04(03), pp.37–44. doi:https://doi.org/10.38177/ajast.2020.4306.

Ahmed, A.H. and A. Al-Hamadani, M.N. (2021). Designing a secure campus network and simulating it using Cisco packet tracer. *Indonesian Journal of Electrical Engineering and Computer Science*, 23(1), p.479. doi:https://doi.org/10.11591/ijeecs.v23.i1.pp479-489.

Alexander (2023). *Standard Named ACL Configuration in Packet Tracer - Netizzan*. [online] Netizzan. Available at: https://netizzan.com/standard-named-acl-configuration-in-packet-tracer/.

Anderson, R. (2020). *SECURITY ENGINEERING : a guide to building dependable distributed systems*. S.L.: John Wiley & Sons.

Cisco (2024). *Cisco Packet Tracer*. [online] Netacad.com. Available at: https://www.netacad.com/cisco-packet-tracer.

James Michael Stewart (2011). *Network security firewalls and VPNs*. Sudbury, Ma: Jones & Bartlett Learning.

Mcmillan, T. (2015). *Cisco networking essentials*. Indianapolis, Indiana? Autodesk Official Press ; Indianapolis, Indiana.

Musa, Y., George, F., Markus, C. and Chikaodiri, O. (2024). An Efficient Security Routing Protocol for Cloud-Based Networks Using Cisco Packet Tracer. *British Journal of Computer, Networking and Information Technology*, [online] 7(2), pp.49–67. Available at: https://abjournals.org/bjcnit/wp-content/uploads/sites/11/journal/published_paper/volume-7/issue-2/BJCNIT_OYIRLAUK.pdf.

Nastase, R. (2018). *Cisco CCNA Command Guide*. Createspace Independent Publishing Platform.

Neupane, K., Haddad, R. and Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. *SoutheastCon 2018*, [online] 1(1). doi:https://doi.org/10.1109/secon.2018.8478973.

Portny, S. (2019). *Project Management* . 5th ed. Hoboken, Nj: John Wiley & Sons, Inc.

Richter, A. and Wood, J. (2015). *Practical Deployment of Cisco Identity Services Engine (ISE)*. [online] Google Books. Available at: Practical Deployment of Cisco Identity Services Engine (ISE): Real-World ... - Andy Richter, Jeremy Wood - Google Books [Accessed 2 Apr. 2025].

Shiu, Y.-S., Chang, S., Wu, H.-C., Huang, S. and Chen, H.-H. (2011). Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications*, 18(2), pp.66–74. doi:https://doi.org/10.1109/mwc.2011.5751298.

Sholomon, A. and Kunath, T. (2025). *Enterprise Network Testing*. [online] Google Books. Available at: Enterprise Network Testing: Testing Throughout the Network Lifecycle to ... - Andy Sholomon, Tom Kunath - Google Books [Accessed 2 Apr. 2025].

Tanenbaum, A.S. (2011). *Computer networks.* Boston: Pearson Education.

Tesco (2021). *Tesco opens new checkout-free store, 'GetGo'*. [online] www.tescoplc.com. Available at: https://www.tescoplc.com/tesco-opens-new-checkout-free-store-getgo/.

Velos IoT (2025). *Revolutionising Shopping Experiences: A Quick Guide to IoT in Retail*. [online] Velosiot.com. Available at: https://info.velosiot.com/revolutionising-shopping-experiences-a-quick-guide-to-iot-in-retail [Accessed 2 Apr. 2025].

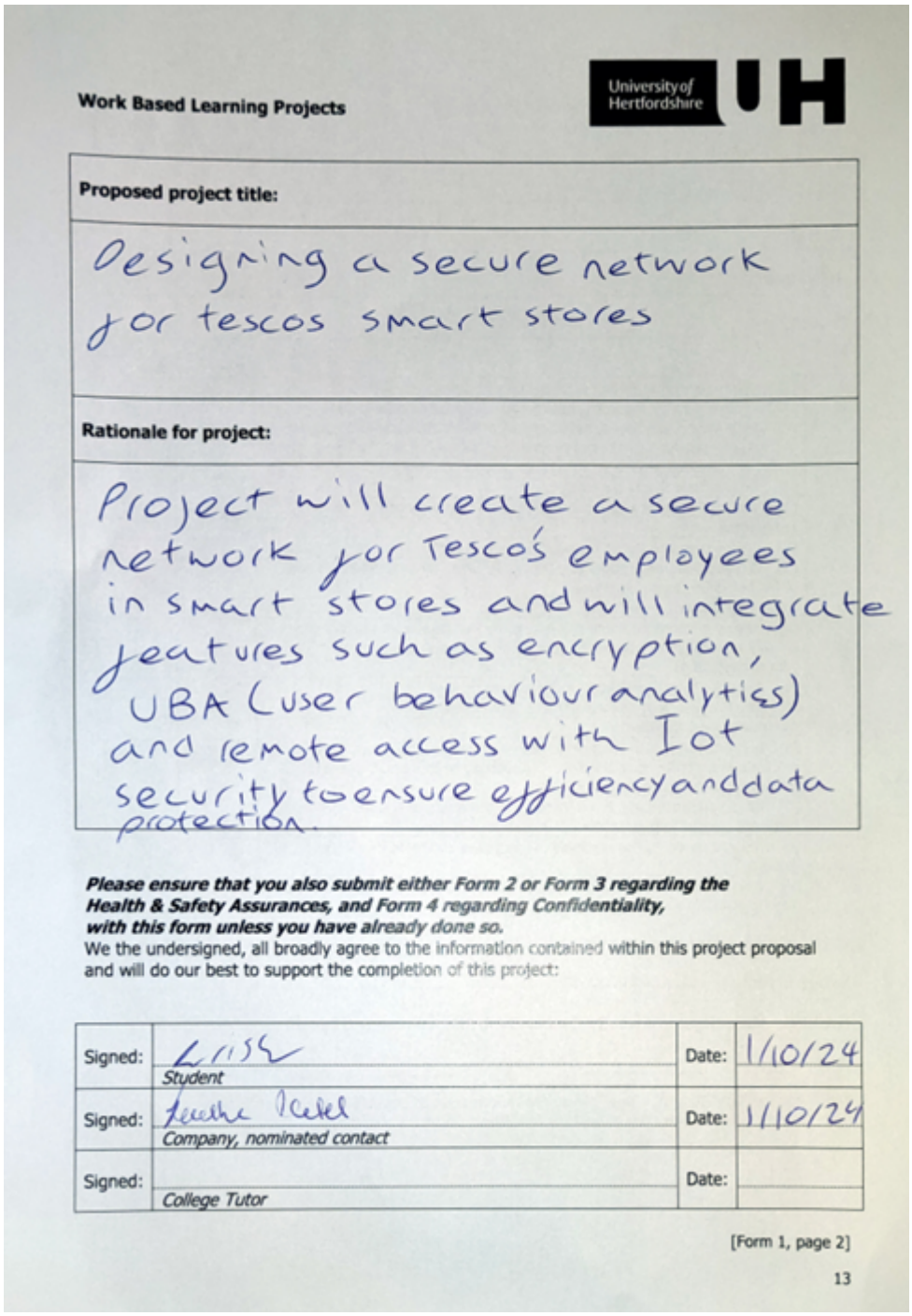
West, J. (2021). *CompTIA network+ guide to networks.* 9th ed. Boston: Course Technology.

White, R. and Donohue, D. (2014). *The art of network architecture : business-driven design*. Indianapolis, Indiana: Cisco Press.

Yaacoub, J.-P.A., Noura, H.N., Salman, O. and Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, [online] 3(1). Available at: https://www.sciencedirect.com/science/article/pii/S2667345223000238.

10.0 Appendices

10.1 Appendix A: Employer's Evaluation Form



Work Based Learning Projects

University of Hertfordshire

Proposed project title:
Designing a secure network for tescos smart stores
Rationale for project:
Project will create a secure network for Tesco's employees in smart stores and will integrate features such as encryption, UBA (user behaviour analytics) and remote access with Iot security to ensure efficiency and data protection.

Please ensure that you also submit either Form 2 or Form 3 regarding the Health & Safety Assurances, and Form 4 regarding Confidentiality, with this form unless you have already done so.

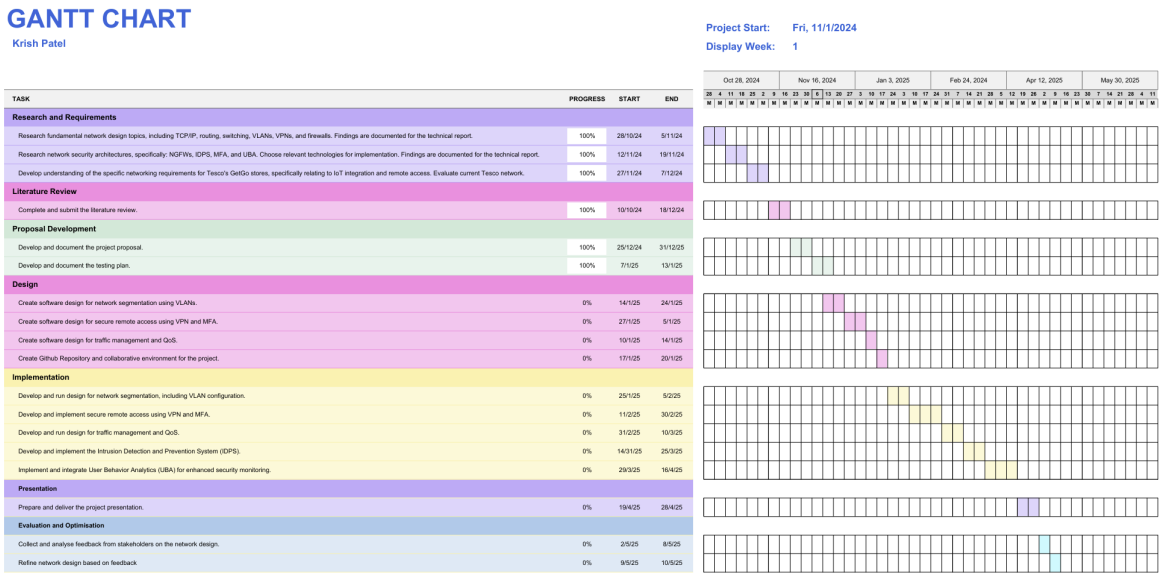
We the undersigned, all broadly agree to the information contained within this project proposal and will do our best to support the completion of this project:

Signed:	Student	Date:	1/10/24
Signed:	Company, nominated contact	Date:	1/10/24
Signed:	College Tutor	Date:	

[Form 1, page 2]

13

10.2 Appendix B: Project Gantt Chart



Explanation: This appendix contains the project Gantt chart, which visually outlines the planned schedule, key tasks, dependencies, and milestones for the Tesco Smart Store Network project. The chart served as the primary tool for planning and monitoring progress. The Waterfall methodology was followed, with major project phases (Requirements, Design, Implementation, Testing, Documentation) achieved in a linear, sequential manner. While overall deadlines were met, deviations occurred at the task level, primarily due to unforeseen challenges in configuring specific technologies like OSPF and PAT/ACLs, along with necessary troubleshooting time. Despite these variations, the Gantt chart provided a valuable framework for managing the project lifecycle.

10.3 Appendix C: Detailed Network Configuration Logs (with Explanations)

This appendix provides the command-line interface (CLI) configurations applied to key devices during the simulation with explanations. *VLAN names reflect the Tesco Smart Store: SALES(10), POS(20), STOCK(30), STAFF(40), TECH(50), SERVEROOM(60)).*

10.3.1 Core Router Basic Setup & Security (CORE-R2)

```
CORE-R2#conf
CORE-R2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-R2(config)#hostname CORE-R2
CORE-R2(config)#line console 0
CORE-R2(config-line)#password cisco
CORE-R2(config-line)#login
CORE-R2(config-line)#exit
CORE-R2(config)#
CORE-R2(config)#enable password cisco
CORE-R2(config)#no ip domain-lookup
CORE-R2(config)#banner motd ##NO Unauthorised Access!!!#
CORE-R2(config)#service password-encryption
CORE-R2(config)#
CORE-R2(config)#do wr
Building configuration...
[OK]
```

Explanation: This initial configuration block sets the hostname of the device to CORE-R2. It secures console port access (line console 0) by requiring a password (cisco). Privileged EXEC mode is secured with an enable password (cisco). The no ip domain-lookup command prevents the router from trying to resolve mistyped commands as domain names. A message-of-the-day banner is set to warn against unauthorised access. The service password-encryption command encrypts plaintext passwords stored in the configuration. do wr saves the current running configuration to the startup configuration.

10.3.2 Core Router SSH Configuration (CORE-R2)

```
CORE-R2(config)#ip domain name cisco.net
CORE-R2(config)#username admin password cisco
CORE-R2(config)#crypto key generate rsa
% You already have RSA keys defined named CORE-R2.cisco.net .
% Do you really want to replace them? [yes/no]: 1024
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: line vty 0 15
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: login local
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: transport input ssh
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: exit
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]:
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: do wr
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: CORE-R2.cisco.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Explanation: This block configures Secure Shell (SSH) for remote management. An IP domain name (cisco.net) is configured, which is a requirement for generating RSA keys. A local user account admin with password cisco is created. RSA cryptographic keys are generated with a 1024-bit modulus. Finally, the virtual terminal lines (VTY 0-15) are configured to use the local user database for login (login local) and to only accept SSH connections (transport input ssh), disabling Telnet access.

10.3.3 Switch VLAN and Port Configuration (SALES-SW)

```
SALES-SW(config)#int range fa0/1-2
SALES-SW(config-if-range)#switchport mode trunk
SALES-SW(config-if-range)#exit
SALES-SW(config)#
SALES-SW(config)#vlan 60
SALES-SW(config-vlan)#name ServerRoom
SALES-SW(config-vlan)#vlan 99
SALES-SW(config-vlan)#name BlackHole
SALES-SW(config-vlan)#exit
SALES-SW(config)#
SALES-SW(config)#int range fa0/3-24
SALES-SW(config-if-range)#switchport mode access
SALES-SW(config-if-range)#switchport access vlan 60
SALES-SW(config-if-range)#exit
SALES-SW(config)#
SALES-SW(config)#int range gig0/1-2
SALES-SW(config-if-range)#switchport mode access
SALES-SW(config-if-range)#switchport access vlan 99
SALES-SW(config-if-range)#exit
SALES-SW(config)#
SALES-SW(config)#do wr
```

Explanation: This configuration configures VLAN and ports for the Sales Switch. Interfaces FastEthernet 0/1-2 are configured as trunk ports. VLAN 60 (ServerRoom) and VLAN 99 (BlackHole) are created and named. Interfaces FastEthernet 0/3-24 are configured as access ports and assigned to VLAN 60. Interfaces GigabitEthernet 0/1-2 are configured as access ports and assigned to VLAN 99 (for unused ports).

10.4.4 Switch VLAN and Trunk Configuration (SALES-SW)

```
Mlt-SW1(config)#
Mlt-SW1(config)#
Mlt-SW1(config)#int range gig1/0/3-8
Mlt-SW1(config-if-range)#switchport mode trunk
Mlt-SW1(config-if-range)#
Mlt-SW1(config-if-range)#vlan 10
Mlt-SW1(config-vlan)#name SALES
Mlt-SW1(config-vlan)#vlan 20
Mlt-SW1(config-vlan)#name POS
Mlt-SW1(config-vlan)#vlan 30
Mlt-SW1(config-vlan)#name STOCK
Mlt-SW1(config-vlan)#vlan 40
Mlt-SW1(config-vlan)#name STAFF
Mlt-SW1(config-vlan)#vlan 50
Mlt-SW1(config-vlan)#name TECH
Mlt-SW1(config-vlan)#vlan 60
Mlt-SW1(config-vlan)#name SERVEROOM
Mlt-SW1(config-vlan)#
Mlt-SW1(config-vlan)#exit
Mlt-SW1(config)#
Mlt-SW1(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-SW1(config)#
```

Explanation: This block configures interfaces GigabitEthernet 1/0/3 through 1/0/8 as trunk ports, suitable for connecting to other switches or routers. It then creates VLANs 10, 20, 30,

40, 50, and 60 and assigns names corresponding to different departments (Sales, POS, Stock, Staff, Tech, ServerRoom).

10.5.5 MLSW Routing and OSPF Configuration (Mlt-SW2)

```
Mlt-SW2#conf
Mlt-SW2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Mlt-SW2(config)#ip routing
Mlt-SW2(config)#
Mlt-SW2(config)#router ospf 10
Mlt-SW2(config-router)#router-id 2.2.2.2
Mlt-SW2(config-router)#network 172.16.1.0 0.0.0.127 area 0
Mlt-SW2(config-router)#network 172.16.1.128 0.0.0.127 area 0
Mlt-SW2(config-router)#network 172.16.2.0 0.0.0.127 area 0
Mlt-SW2(config-router)#network 172.16.2.128 0.0.0.127 area 0
Mlt-SW2(config-router)#network 172.16.3.0 0.0.0.127 area 0
Mlt-SW2(config-router)#network 172.16.3.128 0.0.0.15 area 0
Mlt-SW2(config-router)#
Mlt-SW2(config-router)#network 172.16.3.144 0.0.0.3 area 0
Mlt-SW2(config-router)#network 172.16.3.148 0.0.0.3 area 0
Mlt-SW2(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
```

Explanation: The ip routing command enables Layer 3 routing functionality on this device (required for an MLSW acting as a router). OSPF routing process 10 is initiated with router ID 2.2.2.2. The network commands advertise the specified subnets (VLANs 10-60 and point-to-point links 172.16.3.144/30 and 172.16.3.148/30) into OSPF Area 0.

10.5.6 ISP OSPF Configuration (ISP1-MAIN)

```
Router>
Router>
Router>enable
Router#conf
Router#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 10
Router(config-router)#router-id 5.5.5.5
Router(config-router)#network 195.136.17.4 0.0.0.3 area 0
Router(config-router)#network 195.136.17.12 0.0.0.3 area 0
Router(config-router)#
Router(config-router)#do wr
Building configuration...
[OK]
```

Explanation: This configures OSPF process 10 on ISP1-MAIN. It advertises the networks associated with its ISP links (195.136.17.4/30 and 195.136.17.12/30) into OSPF Area 0.

10.5.7 MLSW SVI and DHCP Relay Configuration (Mlt-SW1)

```
Mlt-SW1(config)#
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 10
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.1.1 255.255.255.128
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 20
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.1.129 255.255.255.128
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 30
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.2.1 255.255.255.128
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 40
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.2.129 255.255.255.128
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 50
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.3.1 255.255.255.128
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
Mlt-SW1(config)#
Mlt-SW1(config)#int vlan 60
Mlt-SW1(config-if)#no sh
Mlt-SW1(config-if)#ip add 172.16.3.129 255.255.255.240
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#ex
```

Explanation: This configures Switched Virtual Interfaces (SVIs) for VLANs 10 through 60 on an MLSW. Each SVI is assigned an IP address acting as the default gateway for its respective VLAN. The ip helper-address 172.16.3.130 command forwards DHCP broadcast requests from clients in these VLANs to the specified DHCP server IP address. no sh activates each SVI.

10.5.8 MLSW SVI and DHCP Relay Configuration (Mlt-SW2)

```
Mlt-SW2#conf
Mlt-SW2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Mlt-SW2(config)#int vlan 10
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.1.1 255.255.255.128
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 20
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.1.129 255.255.255.128
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 30
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.2.1 255.255.255.128
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 40
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.2.129 255.255.255.128
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 50
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.3.1 255.255.255.128
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 60
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.16.3.129 255.255.255.240
Mlt-SW2(config-if)#ip helper-address 172.16.3.130
Mlt-SW2(config-if)#ex
```

Explanation: This block is a duplicate of the previous SVI configuration block onto Mlt-SW2.

10.5.9 Router PAT and ACL Configuration (CORE-R1)

```
CORE-R1#conf
CORE-R1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE-R1(config)#ip nat inside source list 1 int se0/2/0 overload
CORE-R1(config)#ip nat inside source list 1 int se0/2/1 overload
CORE-R1(config)#
CORE-R1(config)#access-list 1 permit 172.16.1.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.1.128 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.2.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.2.128 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.3.0 0.0.0.127
CORE-R1(config)#access-list 1 permit 172.16.3.128 0.0.0.15
CORE-R1(config)#
CORE-R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0
CORE-R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1 70
```

Explanation: This configures PAT (NAT Overload). ACL 1 permits traffic sourced from internal VLANs 10-60. The ip nat inside source list 1... commands map traffic matching ACL 1 to the IP address of the specified outbound serial interface (Se0/2/0 or Se0/2/1), allowing internal devices to share public IPs. The static default routes direct internet-bound traffic, with the route via Se0/2/1 acting as a backup due to its higher administrative distance (70).

10.5.10 Access Switch Trunk Configuration Modification

```
POS-SW>enable
Password:
POS-SW#enable
POS-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
POS-SW(config)#interface fa0/1
POS-SW(config-if)#switchport mode trunk
POS-SW(config-if)#switchport trunk native vlan 99
POS-SW(config-if)#switchport trunk allowed vlan 20,99
POS-SW(config-if)#no shutdown
POS-SW(config-if)#exit
POS-SW(config)#exit
POS-SW#copy running-config startup-config
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on FastEthernet0/1
VLAN99.
```

Explanation: This reconfigures interface Fa0/1 on an access switch. It sets the port to trunk mode, assigns VLAN 99 as the native VLAN, and explicitly allows only VLANs 20 and 99 to traverse this trunk.

```
Mlt-SW1(config)#
Mlt-SW1(config)#
Mlt-SW1(config)#interface gigabitEthernet 1/0/4
Mlt-SW1(config-if)#switchport mode trunk
Mlt-SW1(config-if)#switchport trunk native vlan 99
Mlt-SW1(config-if)#switchport trunk allowed vlan 20,99
Mlt-SW1(config-if)#no shutdown
Mlt-SW1(config-if)#exit
Mlt-SW1(config)#exit
Mlt-SW1#copy running-config startup-config
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console
```

Explanation: Similar configuration applied to interface Gig1/0/4, setting it as a trunk with native VLAN 99 and allowing only VLANs 20 and 99.

10.5.11 Access Switch VLAN/SVI Modification (Mlt-SW1)

```
Mlt-SW1#
Mlt-SW1#
Mlt-SW1#
Mlt-SW1#enable
Mlt-SW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Mlt-SW1(config)#
Mlt-SW1(config)#interface gigabitEthernet 1/0/4
Mlt-SW1(config-if)#no switchport trunk allowed vlan
Mlt-SW1(config-if)#switchport trunk allowed vlan 20,99
Mlt-SW1(config-if)#no shutdown
Mlt-SW1(config-if)#exit
Mlt-SW1(config)#
Mlt-SW1(config)#interface vlan 20
Mlt-SW1(config-if)#ip helper-address 172.16.3.130
Mlt-SW1(config-if)#no shutdown
Mlt-SW1(config-if)#exit
Mlt-SW1(config)#
Mlt-SW1(config)#exit
Mlt-SW1#copy running-config startup-config
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
```

Explanation: On interface Gig1/0/4, the allowed VLAN list is reset and then set again to allow only VLANs 20 and 99. An SVI for VLAN 20 is then configured on this switch with a DHCP helper address.

10.5.12 Access Switch Spanning Tree Configuration (POS-SW)

```
POS-SW#
POS-SW#
POS-SW#conf
POS-SW#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
POS-SW(config)#      interface fastEthernet 0/1
POS-SW(config-if)#spanning-tree vlan 20,99
POS-SW(config)#exit
POS-SW#exit
```

Explanation: Applies Spanning Tree Protocol (STP) configuration specifically for VLANs 20 and 99 to interface Fa0/1. This allows for per-VLAN STP parameter tuning if needed.

10.5.13 VPN Gateway Setup and Configuration (VPN-GW)

```
VPN-GW(config-if)# encapsulation hdlc
VPN-GW(config-if)# clock rate 2000000
VPN-GW(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
VPN-GW(config-if)# exit
VPN-GW(config)#
VPN-GW(config)#ip route 0.0.0.0 0.0.0.0 195.136.18.1
VPN-GW(config)#
VPN-GW(config)#ip route 172.16.1.0 255.255.255.128 172.16.4.2
VPN-GW(config)#ip route 172.16.1.128 255.255.255.128 172.16.4.2
VPN-GW(config)#ip route 172.16.2.0 255.255.255.128 172.16.4.2
VPN-GW(config)#ip route 172.16.2.128 255.255.255.128 172.16.4.2
VPN-GW(config)#ip route 172.16.3.0 255.255.255.128 172.16.4.2
VPN-GW(config)#ip route 172.16.3.128 255.255.255.240 172.16.4.2
VPN-GW(config)#ip route 172.16.3.144 255.255.255.252 172.16.4.2
VPN-GW(config)#ip route 172.16.3.148 255.255.255.252 172.16.4.2
VPN-GW(config)#ip route 172.16.3.152 255.255.255.252 172.16.4.2
VPN-GW(config)#ip route 172.16.3.156 255.255.255.252 172.16.4.2
VPN-GW(config)#ip route 195.136.17.4 255.255.255.252 172.16.4.2
VPN-GW(config)#ip route 195.136.17.8 255.255.255.252 172.16.4.2
VPN-GW(config)#
VPN-GW(config)#aaa new-model
VPN-GW(config)#aaa authentication login REMOTE local
VPN-GW(config)#aaa authorization network REMOTE local
VPN-GW(config)#username VPN secret cisco
VPN-GW(config)#
VPN-GW(config)#crypto isakmp policy 10
VPN-GW(config-isakmp)# encr aes 256
VPN-GW(config-isakmp)# hash md5
VPN-GW(config-isakmp)# authentication pre-share
VPN-GW(config-isakmp)# group 2
VPN-GW(config-isakmp)# lifetime 21600
VPN-GW(config-isakmp)# exit
VPN-GW(config)#
VPN-GW(config)#crypto isakmp client configuration group REMOTE
VPN-GW(config-isakmp-group)# key cisco
VPN-GW(config-isakmp-group)# pool mypool
VPN-GW(config-isakmp-group)# dns 172.16.3.132
```

Explanation: This block configures a dedicated Cisco 1941 router (VPN-GW) for Remote Access IPsec VPN. It includes: initial setup, hostname, enable secret, activating the security license (requiring a reload), configuring inside (to CORE-R1) and outside (to WAN) serial interfaces, setting up static routes for internal networks pointing back via CORE-R1 and a default route to the internet, enabling AAA, defining ISAKMP (Phase 1) and IPsec (Phase 2) parameters (AES-256, MD5 hash, pre-shared key, DH group 2), configuring an ISAKMP client group with key/pool/DNS info, creating dynamic and static crypto maps, applying the crypto map to the outside interface, and defining a local IP pool for VPN clients.

10.5.14 Core Router VPN Integration (Mlt-SW1)

```
Mlt-SW1(config)#
Mlt-SW1(config)#interface G1/0/9
Mlt-SW1(config-if)# description Link to dedicated VPN-GW
Mlt-SW1(config-if)# ip address 172.16.4.2 255.255.255.252
Mlt-SW1(config-if)# no shutdown
Mlt-SW1(config-if)# exit
Mlt-SW1(config)#
Mlt-SW1(config)#ip route 172.16.10.128 255.255.255.128 172.16.4.1
Mlt-SW1(config)#
Mlt-SW1(config)#router ospf 10
Mlt-SW1(config-router)# network 172.16.4.0 0.0.0.3 area 0
Mlt-SW1(config-router)# redistribute static subnets
Mlt-SW1(config-router)# exit
Mlt-SW1(config)#
Mlt-SW1(config)#end
Mlt-SW1#copy running-config startup-config
%SYS-5-CONFIG_I: Configured from console by console

Destination filename [startup-config]?
Building configuration...
[OK]
```

Explanation: These commands are applied to Mlt-SW1 to integrate with the VPN-GW. Interface Serial0/1/0 is configured with the IP address connecting to VPN-GW. A static route is added for the VPN client pool (172.16.10.128/25, as pool range was adjusted slightly from 150-200) pointing to the VPN-GW's internal IP (172.16.4.1). Within the OSPF process, the link to the VPN-GW is advertised, and the redistribute static subnets command ensures the static route for the VPN pool is shared with the rest of the OSPF domain.

10.5.15 IPS Config (Main)

```
R1(config)#license boot
R1(config)#license boot module
R1(config)#license boot module c1900
R1(config)#license boot module c1900 technology-package
R1(config)#license boot module c1900 technology-package securityk9
```

```
R1#
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir
```

```
R1(config)#ip ips config location ipsdir
R1(config)#
R1(config)#
R1(config)#ip ips ?
  config                Location of IPS configuration files
  fail                  Specify what to do during any failures
  name                  Specify an IPS rule
  notify                Specify the notification mechanisms (SDEE or
log) for
                        the alarms
  signature-category    Signature Category
  signature-definition  Signature Definition
R1(config)#ip ips name iosips
```

```
R1(config)#ip ips signature-cat
R1(config)#ip ips signature-category
R1(config-ips-category)#
R1(config-ips-category)#?
  category  Category keyword
  exit      Exit from Category Mode
  no        Negate or set default values of a command
R1(config-ips-category)#cat
R1(config-ips-category)#category ?
  all      All Categories
  ios_ips  IOS IPS (more sub-categories
R1(config-ips-category)#category all
```

```
R1(config-ips-category)#category all
R1(config-ips-category-action)#retire
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#
R1(config-ips-category-action)#
R1(config-ips-category-action)#exi
R1(config-ips-category)#cate
R1(config-ips-category)#category io
R1(config-ips-category)#category ios_ips ba
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#reti
R1(config-ips-category-action)#retired fal
R1(config-ips-category-action)#retired false
```

```
R1(config)#interface g0/1
R1(config-if)#ip ips ?
  WORD  Name of define IPS
R1(config-if)#ip ips iosip
  in    Inbound IPS
  out   Outbound IPS
R1(config-if)#ip ips iosip
R1(config-if)#
 %IPS-6-ENGINE_BUILDS_STAR

 %IPS-6-ENGINE_BUILDING: a

 %IPS-6-ENGINE_READY: atom
engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_

R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#exi
R1(config)#
R1(config)#
R1(config)#
R1(config)#logging host
```

```
R1(config)#
R1(config)#logging host 192.168.1.50
R1(config)#
R1(config)#serv
R1(config)#service
R1(config)#service time
R1(config)#service timestamps log
R1(config)#service timestamps log
R1(config)#service timestamps log datetime
R1(config)#service timestamps log datetime msec
```

```
R1(config)#ip ips signature-def
R1(config)#ip ips signature-definition
R1(config-sigdef)#
R1(config-sigdef)#?
  exit       Exit from Signature Definition Mode
  signature  Signature keyword
R1(config-sigdef)#signa
R1(config-sigdef)#signature ?
  <1-65535>  Signature ID value
R1(config-sigdef)#signature 2004 ?
  <0-65535>  Signature SubID value
  <cr>
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#
R1(config-sigdef-sig)#
R1(config-sigdef-sig)#?
  engine  Engine
  exit    Exit from Signature Definition Mode
  status  Status
R1(config-sigdef-sig)#status
```

```
R1(config-sigdef-sig-engine)#event-action prod
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#even
R1(config-sigdef-sig-engine)#event-action den
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#
R1(config-sigdef-sig-engine)#
R1(config-sigdef-sig-engine)#exi
R1(config-sigdef-sig)#exi
R1(config-sigdef)#
R1(config-sigdef)#exi
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this
engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms
```

This configuration sets up Intrusion Prevention System (IPS) on router Main. Initially, the necessary securityk9 technology package license is enabled to activate the IPS features. A dedicated directory named ipsdir is created in the router's flash memory, and the IPS is configured to use this location for storing its signature files and configurations. A named IPS rule set, iosips, is created to group the specific IPS policies. The configuration was then configured to manage the signatures by first retiring (disabling) all signature categories, and subsequently un-retiring (enabling) only the ios_ips basic category, establishing a baseline set of active signatures.

Following the category-level adjustments, specific fine-tuning is performed. Signature 2004 with SubID 0 is enabled, overriding the category settings, and configured with specific actions: to produce-alert (generate a log message) and deny-packet-inline (drop the offending packet) when triggered. Finally, the configured iosips rule set is applied to inspect inbound traffic on the GigabitEthernet 0/1 interface. To ensure visibility of IPS events, logging is directed to a remote syslog server at 192.168.1.50, and timestamps are changed

to include milliseconds for more concise analysis. The commands allow the IPS to compile the selected signatures and become active on the interface.

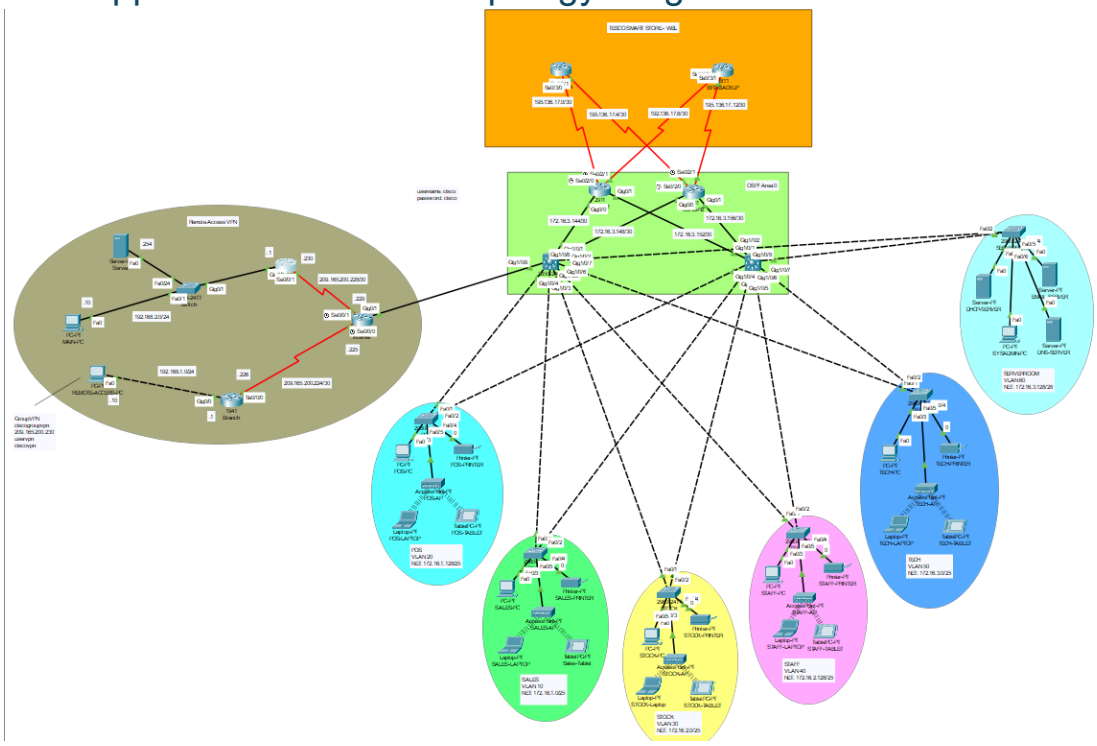
10.6 Appendix D: Detailed Test Cases

Test%20Plan.xlsx

10.7 Appendix E: Packet Tracer File (.pkt)

Tesco Network.pkt

10.8 Appendix F: Network Topology Diagram



10.9 Appendix G: IP Addressing Table

IP Addressing Table

Base Network: 172.16.1.0

Department	Network Address	Subnet Mask	Host Address Range	Broadcast Address
SALES	172.16.1.0	255.255.255.128	172.16.1.1 – 172.16.1.126	172.16.1.127
POS	172.16.1.128	255.255.255.128	172.16.1.129 – 172.16.1.254	172.16.1.255
STOCK	172.16.2.0	255.255.255.128	172.16.2.1 – 172.16.2.126	172.16.2.127
STAFF	172.16.2.128	255.255.255.128	172.16.2.129 – 172.16.2.254	172.16.2.255
TECH	172.16.3.0	255.255.255.128	172.16.3.1 – 172.16.3.126	172.16.3.127
SERVERROOM	172.16.3.128	255.255.255.240	172.16.3.129 – 172.16.3.142	172.16.3.143

Between the Routers and Layer-3 Switches

No.	Network Address	Subnet Mask	Host Address Range	Broadcast Address
R1-MLSW1	172.16.3.144	255.255.255.252	172.16.3.145 – 172.16.3.146	172.16.3.147
R1-MLSW2	172.16.3.148	255.255.255.252	172.16.3.149 – 172.16.3.150	172.16.3.151
R2-MLSW1	172.16.3.152	255.255.255.252	172.16.3.153 – 172.16.3.154	172.16.3.155
R2-MLSW2	172.16.3.156	255.255.255.252	172.16.3.157 – 172.16.3.158	172.16.3.159

Between the Routers and ISPs

Public IP Address Ranges:

195.136.17.0/30

195.136.17.4/30

195.136.17.8/30

195.136.17.12/30

Remote Access VPN Networks

Segment	Network Address	Subnet Mask	Host Address Range	Broadcast Address
VPN Main Office LAN	192.168.2.0	255.255.255.0 (/24)	192.168.2.1 – 192.168.2.254	192.168.2.255
VPN Branch Office LAN	192.168.1.0	255.255.255.0 (/24)	192.168.1.1 – 192.168.1.254	192.168.1.255
WAN Link (Main–Internet)	209.165.200.228	255.255.255.252	209.165.200.229 –	209.165.200.231

10.10 Appendix H: VLAN Table

VLAN Table

VLAN I	Name	Department(s) Associated	IP Subnet	SVI Locatio	Purpose
10	SALES	Sales	172.16.1.0/25	MLSW1/MLSW2	Network access for Sales department staff computers and devices.
20	POS	Sales / Retail Operations	172.16.1.128/25	MLSW1/MLSW2	Network segment for Point of Sale terminals and payment systems.
30	STOCK	Stockroom / Warehouse / Inventory	172.16.2.0/25	MLSW1/MLSW2	Network access for devices in stockroom/warehouse (scanners, PCs, etc).
40	STAFF	General Staff / Admin / HR	172.16.2.128/25	MLSW1/MLSW2	General network access for staff not in specific depts, shared areas.
50	TECH	IT / Technical Support	172.16.3.0/25	MLSW1/MLSW2	Network access for IT staff workstations, management tools, test gear.
60	SERVERROOM	IT / Infrastructure	172.16.3.128/28	MLSW1/MLSW2	Dedicated network segment for servers, storage, and critical infrastructure.

10.11 Appendix I: Video Explanation

Video Explanation.mp4