Tesco GetGo Network Design – Case Study and Requirements

This project involves the design of a secure and scalable network infrastructure for a Tesco GetGo Smart Store. The objective is to support Tesco's next-generation retail model, which incorporates automation and advanced technology to enhance customer experience and improve operational efficiency. The network must be secure, future-proof, and capable of supporting essential functions such as Point of Sale (POS) systems, sales and stock monitoring through IoT devices, staff operations, additional technical equipment, and access to server resources.

To ensure efficiency and security, the network will be structured into six divisions, with each division operating on its own VLAN and subnet:

- POS (Point of Sale) – 100 users
- SALES – 100 users
- STOCK – 100 users
- STAFF – 100 users
- TECH – 100 users
- SERVERROOM – 12 devices

Project Requirements

Both functional and non-functional requirements were considered in the network design. Functional requirements ensured the network supports essential operations like POS and server access through VLANs, inter-VLAN routing, and DHCP. Non-functional requirements focused on scalability, redundancy, and security, incorporating measures like IPS, port security, and secure management via SSH, ensuring the network is reliable and future-proof.

- Use Cisco Packet Tracer to build and simulate the network.
- Follow a hierarchical network design with redundancy at each layer:
    - At least two routers and two multilayer switches for core resilience.
- Ensure internet redundancy via two ISPs, each connected to both routers.
- Enable wireless connectivity in all divisions except SERVERROOM.
- Configure VLANs for each division: POS, SALES, STOCK, STAFF, TECH, and SERVERROOM.
- Deploy Cisco IOS IPS to monitor and block suspicious traffic targeting the VPN and internal network.
- Use the 172.16.1.0/24 network and subnet it appropriately per VLAN.
- Assign public IP blocks for ISP links:
    - 195.136.17.0/30
    - 195.136.17.4/30
    - 195.136.17.8/30

    - 195.136.17.12/30
- Perform essential initial device configurations:
    - Hostnames
    - Console and enable passwords
    - Login banner
    - Disable DNS lookup
- Enable inter-VLAN routing using Switch Virtual Interfaces (SVI).
- Configure a DHCP server in the SERVERROOM for dynamic IP allocation to end-user devices.
- Assign static IPs to SERVERROOM devices.
- Set up OSPF as the dynamic routing protocol on routers and Layer 3 switches.
- Enable SSH access on all core network devices for secure management.
- Apply port security in the SALES VLAN:
    - One device per port
    - Sticky MAC address
    - Violation mode set to shutdown
- Configure PAT (NAT Overload) on the outbound interface of the router:
    - Include the necessary ACL rules.
- Fully test and verify all configurations and connectivity across the network.
- Include a VPN capability for secure remote access in a future phase of the project.

Technologies Implemented

1. Logical topology design in Cisco Packet Tracer
2. Hierarchical architecture with redundancy
3. Physical and logical cabling/interconnection
4. Basic router and switch configuration
5. VLAN segmentation and port mapping
6. Subnetting and address assignment
7. Inter-VLAN Routing (SVI)
8. DHCP for IP leasing
9. SSH for device access security
10. OSPF for dynamic routing
11. PAT (NAT Overload)

12. ACL implementation
13. Port security in SALES
14. Wireless access for all divisions except SERVERROOM
15. ISP configuration and internet access setup
16. Complete network testing and troubleshooting
17. VPN connectivity planned for the next development phase
18. Intrusion Prevention System (IPS) for threat detection and blocking