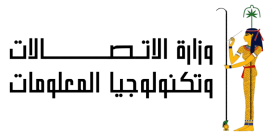
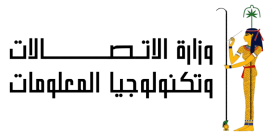
# 



# **Graduation Project Guide**

# 

**Network Design and Security Implementation of a** **Hospital System**

**SUPERVISED BY**

**Dr. Weal Samir**

**PREPARED BY**

**Mohamed Abdo Abdel Sattar**

**-Abdallah Mobarak**

**-Ousaid Ashraf**

**-Ahmed Ghaly**

**-Mohamed Khalil**

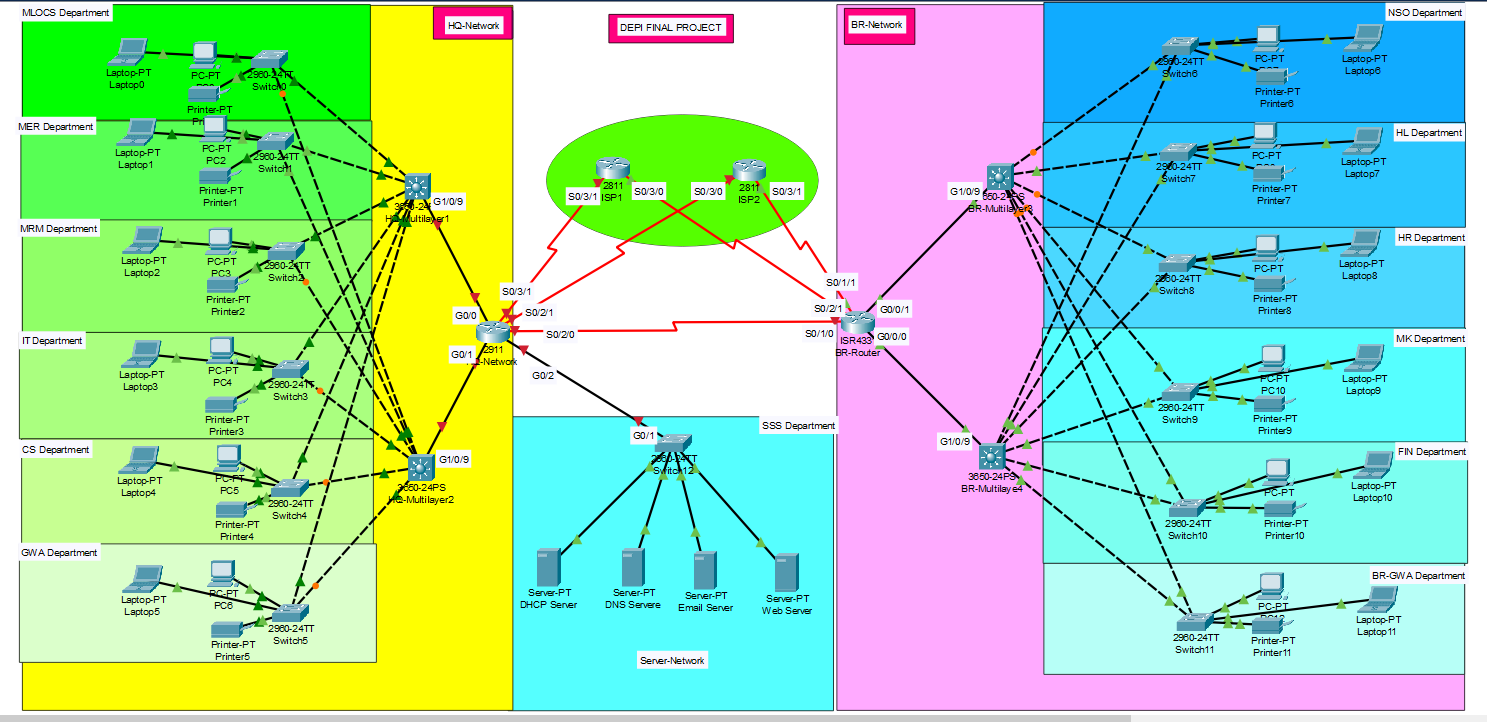
**-Zeyad Mohamed**

# **Case Study**

Hospital System is a well-established Network Design, which offers health solutions and services to its clients. The institution operates in two locations within the same city. Therefore, it has the following departments within its main headquarters Medical Lead Operation & Consultancy Services (MLOCS), Medical Emergency and Reporting (MER), Medical Records Management (MRM), Information Technology (IT), and Customer Service (CS). The branch hospital was designed to share the workloads with the headquarters hence it contains the following departments; Nurses & Surgery Operations (NSO), Hospital Labs (HL), Human resource (HR), Marketing (MK), and Finance (FIN). Each location is also expected to have a Guest/Waiting area (GWA) for patients or visitors.

The network is expected to have a hierarchical model with two already purchased Core routers (one at HQ-Network and one BR-Network) each connecting to two subscribed ISPs. Due to security requirements, it has been decided that all the departments will be on a separate network segment within the same local area network.

1. **Network Topology**

The network topology for Hospital System, as designed in Cisco Packet Tracer, is shown below.

1. **Project Visualization** 
   * Use Cisco Packet Tracer to design and implement the network solution.
   * Use a hierarchical model providing redundancy in the network.
   * Both HQ and Branch routers are expected to be connected using a serial connection.
   * As mentioned earlier, for network cost-effectiveness, each site is expected to have one core router, two multilayer switches, and several access switches connecting each department.
   * Each department is required to have a wireless network for the users.
   * Every department in HQ is estimated to have around 60 users while in Branch is estimated to be 30 users.
   * Each department should be in a different VLAN and a different subnetwork.
   * Provided a base network of 192.168.100.0, and carry out subnetting to allocate the correct number of IP addresses to each department.
   * The company network is connected to the static, public IP addresses (Internet Protocol) 195.136.17.0/30, 195.136.17.4/30, 195.136.17.8/30, and 195.136.17.12/30 connected to the two Internet providers.
   * Configure basic device settings such as hostnames, console password, enable password, banner messages, and disable IP domain lookup.
   * Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
   * The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
   * All devices in the network are expected to obtain an IP address dynamically from the dedicated DHCP servers located in the server room.
   * Devices in the server room are to be allocated IP addresses statically.
   * Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
   * Configure default static routing to enable routers and multilayer switches to forward any traffic that does not match routing table entries. Use next-hop IP addresses.
   * Configure SSH in all the routers and layer three switches for remote login.
   * Configure port-security for the server site department switch to allow only one device to connect to a switch port, use sticky method to obtain mac-address and violation mode shutdown.
   * Configure the extended ACL rule together with site-to-site VPN (IPSec VPN) to create a tunnel and encrypt communication between HQ and the Branch network.
   * Configure PAT to use the respective outbound router interface IPv4 address, and implement the necessary ACL rule.
   * Test Communication, ensure everything configured is working as expected.

**Week 1: Planning and Design**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.

**Week 2: Configuration of Basic Devices**

1. Configuring Basic device settings.
2. Creating VLANs and assigning ports VLAN numbers.
3. Subnetting and IP Addressing.
4. Configuring Inter-VLAN Routing on the Multilayer switches (Switch Virtual Interface).
5. Configuring Dedicated DHCP Server device to provide dynamic IP allocation.
6. NTP and Syslog Server.
7. Configuring switchport security or Port-Security on Server room switch.

**Week 3: Advanced Configuration and Testing**

1. Configuring SSH for secure Remote access.
2. Configuring OSPF as the routing protocol.
3. Configuring NAT Overload (Port Address Translation PAT).
4. Configuring Site-to-Site IPsec VPN.
5. Configuring standard and extended Access Control Lists ACL.
6. Configuring ISP routers.
7. Test and Verifying Network Communication.

**Week 4: Documentation and Presentation**

Document all security configurations, test the network security, and prepare a presentation summarizing the security measures implemented.

Mohamed Abdo Abdel Sattar

1. Subnetting And IP Addressing.
2. Configuring OSPF And Static Route as A Routing Protocols.
3. Configuring Switch Security on All Switches.

**Abstract**

This case study presents the design and implementation of a secure, efficient network for Alexandiria Health Services, a major health provider in Australia. The network covers both headquarters and a branch hospital, aiming to enhance security, communication, and performance. Using Cisco Packet Tracer, the network will be designed based on a hierarchical model with VLANs, OSPF, ACLs, VPN, DHCP, SSH, and other critical technologies to ensure confidentiality, integrity, and availability of data.

# Introduction

Alexandiria Health Services operates in two locations, with the headquarters 20 km away from the branch hospital. The goal is to create a robust and secure network that supports key departments such as Medical Lead Operations, IT, Finance, and others in both locations. The current network relies on third-party services, but the institution now aims to develop its own network infrastructure, covering LAN, WAN, and server-side components.

# Objectives

The objectives of this network design are:  
1. Create a cost-effective and secure network infrastructure.  
2. Ensure secure communication between headquarters and the branch using VPN.  
3. Implement VLANs for each department to improve network segmentation.  
4. Follow the CIA principles of Confidentiality, Integrity, and Availability.  
5. Configure DHCP, DNS, Web, and Email servers to support network services.

# Literature Review

This project applies the hierarchical network model, which is essential for building scalable and secure enterprise networks. VLANs are used to segregate network traffic, while OSPF provides efficient routing between departments. Network security measures such as Access Control Lists (ACLs) and IPsec VPN are crucial for protecting sensitive health data.

# Methodology

The network will be designed using Cisco Packet Tracer and includes the following steps:  
- Subnetting the base network 192.168.100.0 to allocate IP addresses to each department.  
- Creating VLANs for departments such as IT, Medical Records, Finance, and more.  
- Configuring Inter-VLAN routing on multilayer switches to enable communication.  
- Implementing OSPF for dynamic routing and site-to-site IPsec VPN for secure communication between HQ and the branch.  
- Setting up DHCP, DNS, and Web servers at the headquarters.  
- Applying port-security and PAT for additional security.

# Configurations

Key configurations for the network include:  
1. VLAN Creation: Each department is assigned a unique VLAN and subnet.  
2. Inter-VLAN Routing: Multilayer switches are configured for routing between VLANs.  
3. OSPF Routing: Configured for dynamic route advertisement across the network.  
4. VPN Configuration: IPsec VPN to secure communication between HQ and branch.  
5. Access Control Lists: Implemented to control traffic based on IP addresses.  
6. DHCP and DNS Servers: Configured to provide dynamic IP allocation and name resolution.  
7. SSH Configuration: Enabled on all routers and switches for secure remote access.

# Results

The network design successfully achieved secure communication between the headquarters and the branch hospital. All departments are able to communicate efficiently while maintaining security through ACLs, VLAN segmentation, and VPN encryption. Testing confirmed the proper configuration of DHCP, DNS, and web servers. The network is scalable and meets all security requirements.

# Performance Testing

After configuring all the devices and network components, the network was tested for functionality and performance. The following tests were conducted:  
1. VLAN Communication: Devices within each department were able to communicate through their assigned VLANs.  
2. Inter-VLAN Routing: Successfully tested routing between VLANs using the multilayer switches.  
3. DHCP Allocation: Verified that devices in each department were assigned IP addresses dynamically by the DHCP server.  
4. OSPF Routing: Routes were advertised correctly, allowing proper communication between HQ and the branch.  
5. VPN Tunnel: The IPsec VPN tunnel was tested and verified to encrypt traffic between HQ and the branch hospital.  
6. Network Security: ACLs were tested to ensure that only authorized traffic was allowed.

# Conclusion

In conclusion, the network designed for Alexandiria Health Services meets all the specified requirements for a secure, cost-effective, and scalable infrastructure. Future improvements could include the implementation of additional redundancy features or expanding the network to support more locations.

### [مبادرة رواد مصر الرقميه]

Network Design and Security Implementation for Alexandiria Health Services

Project Case Study

Submitted by:

-Mohamed Abdo

-Abdallah Mobarak

-Ousaid Ashraf

-Ahmed Ghaly

-Mohamed Khalil

-Zeyad Mohamed

Supervised by: [ENG:Wael Samir]

Date: [ 18/10/2024]

