Software House Design Network

Presented by Thwet Yin Nyein

3CS-1198

September 2023

Table of Contents

Contents

[Executive Summary 2](#_Toc144938848)

[Part A: Designing a Network 2](#_Toc144938849)

[1. Network Design Requirements 2](#_Toc144938850)

[2. Topology and Subnetwork Design 2](#_Toc144938851)

[3. Network Core Design 2](#_Toc144938852)

[4. Network Design for Configuration and Testing 2](#_Toc144938853)

[5. Network Design Diagram 2](#_Toc144938854)

[Part B: Technologies Used in Network Design 2](#_Toc144938855)

[1. VLAN (Virtual Local Area Network) 3](#_Toc144938856)

[2. Inter-VLAN Routing 3](#_Toc144938857)

[3. OSPF (Open Shortest Path First) 4](#_Toc144938858)

[4. SSH (Secure Shell) 5](#_Toc144938859)

[5. Switch Security 5](#_Toc144938860)

[Part C: Investigation of Network Traffic 5](#_Toc144938861)

[1. Routing inside a VLAN Experimentation 5](#_Toc144938862)

[2. Inter-VLAN Routing Experimentation 5](#_Toc144938863)

[3. OSPF Experimentation 5](#_Toc144938864)

[4. SSH Experimentation 5](#_Toc144938865)

[5. Switch Security Experimentation 5](#_Toc144938866)

[Conclusion 5](#_Toc144938867)

# Executive Summary

The following report details the design and implementation of a network for a software house company (TYN Software House) located at a single site. The network is designed to meet the specific requirements of the company while adhering to provided constraints. This project is divided into three main parts:

- Part A: Designing a Network

- Part B: Technologies Used in Designing a Network

- Part C: Investigation of Network Traffic

Each part will be discussed in detail, including the network design, technologies employed, and the results of experiments conducted. The goal is to create a robust and efficient network that supports the company's operational needs.

# Part A: Designing a Network

## 1. Network Design Requirements

In this network topology, the fundamental elements such as Routers, Switches, Access Points, Personal Computers, Printers, Smartphone, Tablet, Laptop and Cables are used. Specifically, the entire network comprises:

* 3 Routers
* 3 Switches
* 3 Access Points
* 8 Personal Computers
* 8 Printers

The company is a building of three floors; along with 3 Main departments namely Customer Operation, Business Development and Software development in 1st floor, 2nd floor, and 3rd floor respectively.

**Overview of Building Design**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Building Name | TYN Software House | | | |
| 3rd floor | Software Development | Software Development | | QA |
| 2nd floor | Business Development | Finance | Sales & Marketing | Project Management |
| 1st floor | Customer Operation | HR | Help desk | Reception |

Each department has a PC and a Printer respectively; therefore, a total of 8 PCs and 8 Printers for all of the departments. To provide connection between these devices, a switch is installed in each building. All of the end devices are then connected to the switches via Fast Ethernet cables and the switches are connected to their specific routers, too. Furthermore, each building has an access point connected to the switches to allow wireless-capable devices to connect to a wired network.

## 2. Topology and Subnetwork Design

The network is divided into three sub-networks with each one per floor. The routers are connected to each other with Serial DCE cable. A DCE provides a physical connection to a network and forward traffic. Each router is then connected to the switches.

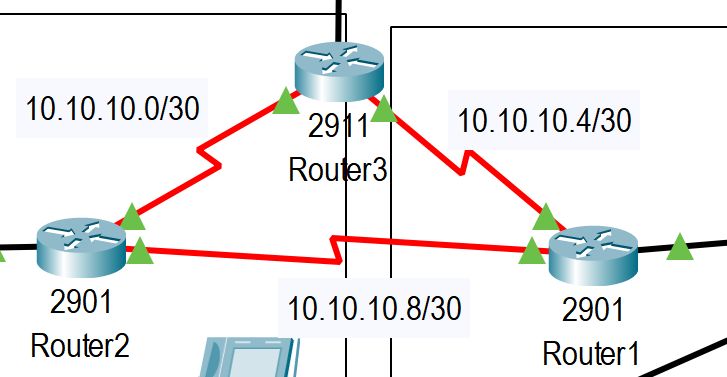
An extended-star physical network topology is applied for this medium-sized company since it is beneficial for short-distance communication which can be used in offices, homes, computer labs, and small buildings where the local area network is established. Another benefit of using a star topology is that all the nodes can be managed from one point which is a central hub. We have designed a hierarchical network with three layers.

1. Access Layer: Comprised of switches to connect end-user devices.
2. Distribution Layer: Responsible for interconnecting VLANs and connecting to the Core Layer.
3. Core Layer: Provides high-speed routing and redundancy.

## 3. Network Core Design

The backbone layer is composed of three routers.

* The network between router1 and router2 is set as 10.10.10.8/30.
* The network between router1 and router3 is set as 10.10.10.4/30.
* The network between router2 and router3 is set as 10.10.10.0/30.

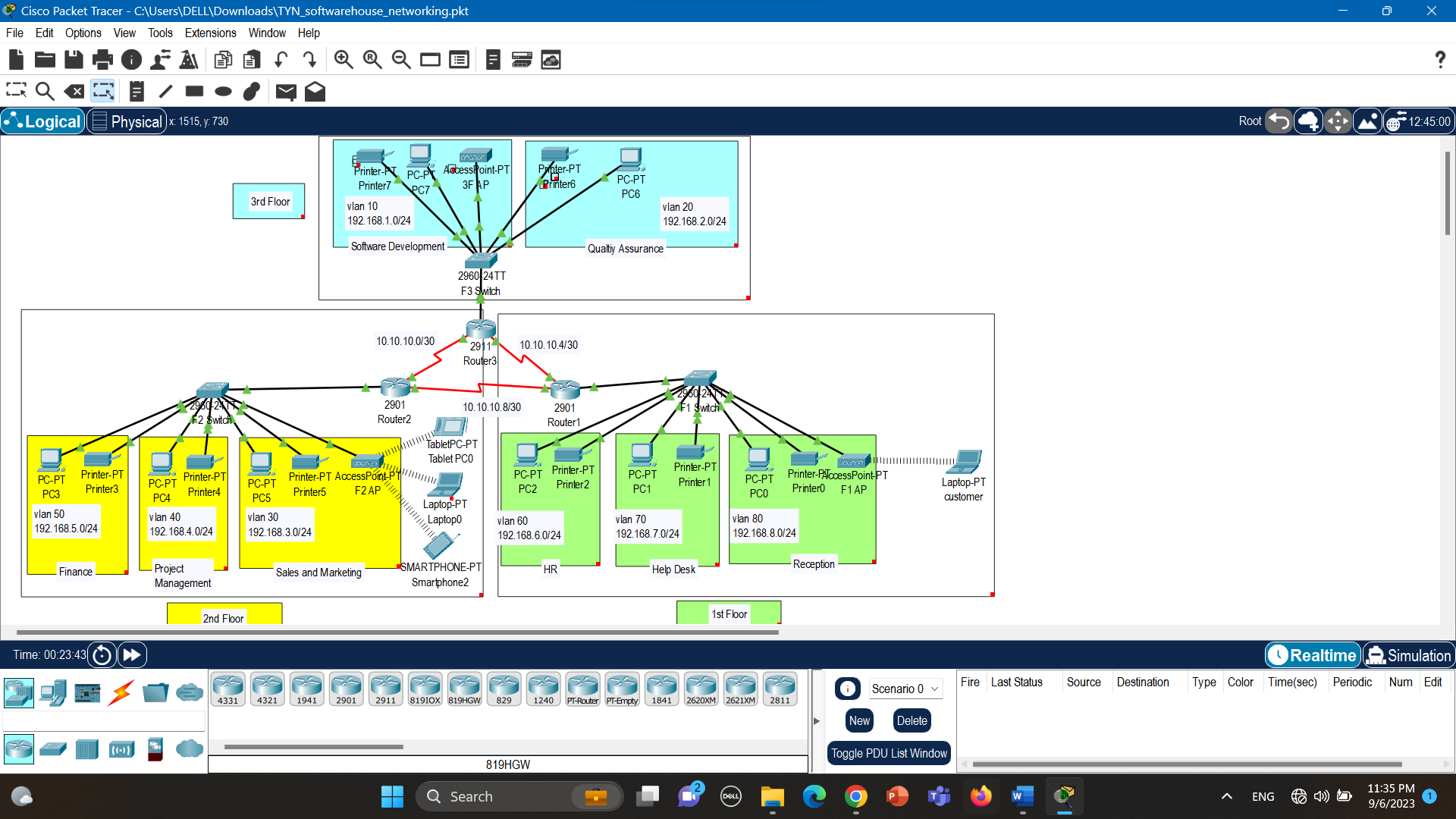


## 4. Network Design for Configuration and Testing

To implement and test this network design, the following steps are taken:

1. Configure and deploy the hardware components, including routers, switches, and servers.
2. Set up VLANs and inter-VLAN routing to ensure efficient communication between departments.
3. Implement OSPF for IPv4 to provide dynamic routing within the campus network.
4. Configure DHCP to assign IP addresses dynamically to end-user devices.
5. Set up security measures such as SSH for secure remote access, port security to restrict unauthorized access, and switch security.

## 5. Network Design Diagram



# Part B: Technologies Used in Network Design

The following technologies are used in this network design:

## 1. VLAN (Virtual Local Area Network)

**VLANs is configured to segment the network based on departments and purposes.**

The DCE Cable between the 3 routers is implemented first and it has been enabled from the shutdown state.

Next, VLANs is configured for each department since it allows different computers and devices to be connected virtually to each other as if they were in a LAN sharing a single broadcast domain. Moreover, it is helpful for organizational use mainly because it can be used to segment a larger network into smaller segments, and it allows only authorized users to have access to networks with highly sensitive information. Each department has been assigned to different VLAN on their respective switches;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Departments** | **VLAN** | **IP Address** | **Subnet Mask** |
|  | Software development | 10 | 192.168.1.0/24 | 255.255.255.252 |
|  | Quality Assurance | 20 | 192.168.2.0/24 | 255.255.255.252 |
|  | Sales and Marketing | 30 | 192.168.3.0/24 | 255.255.255.252 |
|  | Project Management | 40 | 192.168.4.0/24 | 255.255.255.252 |
|  | Finance | 50 | 192.168.5.0/24 | 255.255.255.252 |
|  | HR | 60 | 192.168.6.0/24 | 255.255.255.252 |
|  | Help desk | 70 | 192.168.7.0/24 | 255.255.255.252 |
|  | Reception | 80 | 192.168.8.0/24 | 255.255.255.252 |

## 2. Inter-VLAN Routing

**Inter-VLAN routing is implemented to allow communication between different VLANs.**

The Inter-VLAN routing is configured next. Inter-VLAN routing is the movement of packets across the network between hosts in different network segments. VLANs make it easier for one to segment a network, which in turn improves the performance of the network and makes it more flexible, since they are logical connections.

There are **three** Inter-VLAN routing options: Legacy Inter VLAN Routing, Router on A Stick, Layer 3 Switch Using Switched Virtual Interfaces. In this network topology, Legacy Inter-VLAN Routing is applied.

The legacy inter-VLAN routing connects different physical router interfaces to different physical ports on the switch. The switch ports connected to the router must be placed in access mode.

**DHCP (Dynamic Host Configuration Protocol)**

**Dynamic Host Configuration Protocol is used to assign IP addresses automatically to client devices.**

The Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture. With DHCP, this entire process is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

Every device in the network for the Company is configured to use the dynamic IP address assigned by their respective DHCP servers.

## 3. OSPF (Open Shortest Path First)

**Open Shortest Path First (OSPF) is used as the dynamic routing protocol for IPv4 within the campus network.**

OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) -- that is, protocols aimed at traffic moving around within a larger autonomous system network like a single enterprise's network, which may in turn be made up of many separate local area networks linked through routers. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. All the end devices in this network system for the Apparel Company are successfully configured with OSPF.

## 4. SSH (Secure Shell)

**SSH is used for secure remote access, port security will be configured to prevent unauthorized access, and switch security measures will be implemented.**

To provide a trusted and secure network system, the Secure Shell Protocol (SSH) is implemented in the system. The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network. SSH service was created as a secure replacement for the unencrypted Telnet and uses cryptographic techniques to ensure that all communication to and from the remote server happens in an encrypted manner. It provides a mechanism for authenticating a remote user, transferring inputs from the client to the host, and relaying the output back to the client.

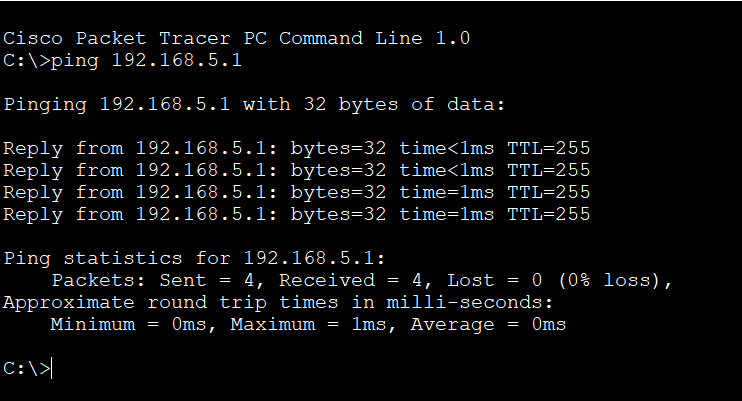
## 5. Switch Security

**A security switch is a hardware device designed to protect computers, laptops, smartphones and similar devices from unauthorized access or operation, distinct from a virtual security switch which offers software protection.** Security switches should be operated by an authorized user only; for this reason, it should be isolated from other devices in order to prevent unauthorized access and it should not be possible to bypass it, in order to prevent malicious manipulation. The simplest form of switch security is using port level security. When using port level security, MAC addresses and number of MAC addresses of the connected devices is controlled.

# Part C: Investigation of Network Traffic

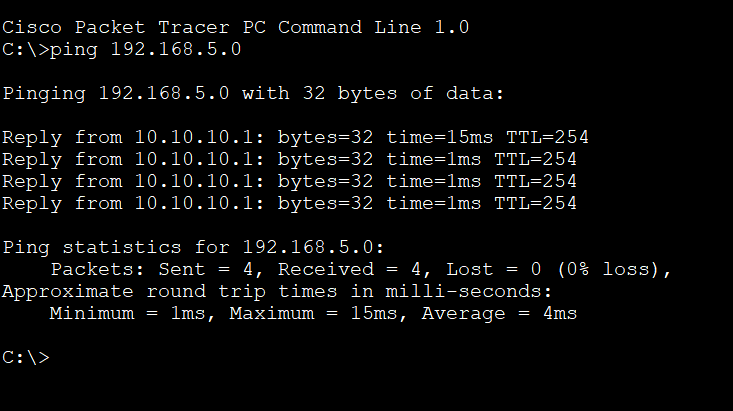
## 1. Routing inside a VLAN Experimentation

Pinging successfully from PC3 to Printer3 from VLAN 50 in Finance Department on 2nd Floor



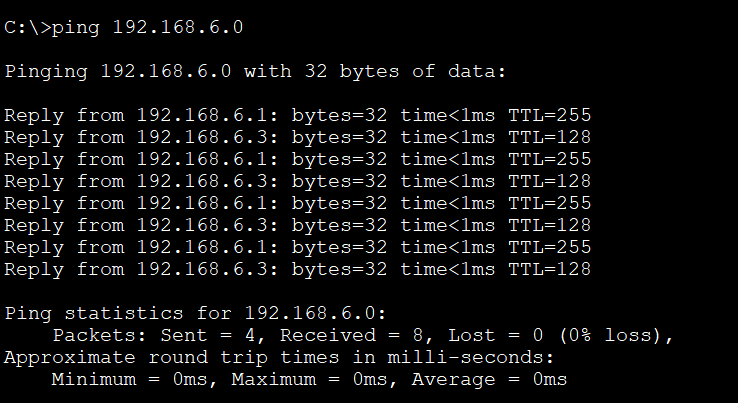
## 2. Inter-VLAN Routing Experimentation

Pinging successfully from PC6 in VLAN 20 (QA) on 3rd Floor to PC3 in VLAN 50 (Finance) on 2nd Floor



## 3. OSPF Experimentation

Pinging successfully from test PC from 3rd floor to Printer3 in Human Resources Department on 1st floor



## 4. SSH Experimentation

tt

## 5. Switch Security Experimentation

rr

# Conclusion

This networking project has yielded achievements, valuable insights, and areas for improvement. Throughout this project, I successfully designed a network for a software house company that meets the specific requirements of the chosen organization. The network was structured into subnetworks, interconnected with a robust core, and configured with a range of technologies, including DHCP, routing protocols, VLANs, and security measures.

By this experiment using Cisco Packet Tracer, I have achieved a deeper understanding of network design principles and their practical application. This project has honed my skills in network configuration, designs, technologies and security measures. This hands-on learning has been invaluable in enhancing my skills and knowledge in network management and security.

While this project has been a valuable learning experience, there are areas where I need to improve my knowledge in networking. Specifically, I could further enhance network performance, scalability, real-time network monitoring with automation. This includes fine-tuning configurations to optimize network traffic management. Additionally, I would like to learn more about real-time monitoring and security assessments which are important for network management to proactively identify and address potential vulnerabilities.

In conclusion, I gained experience and a better understanding of how to brainstorm and create a network for a certain organization. Although I have challenges in my very first individual networking project, the entire experiment has helped me comprehend the concept of networking and identify my limitations and how to improve them.

---

### Part A: Designing a Network

\*\*5. Network Design Diagram:\*\*

![Network Diagram](insert\_network\_diagram\_here.png)

---

### Part B: Technologies Used in Network Design

\*\*1. DHCP, Static, and Default Routing:\*\*

\*\*DHCP:\*\*

- DHCP servers will be deployed in the IT department.

- Dynamic IP address assignment for end-user devices.

- Static IP reservations for servers and network devices.

- Default routes set on core routers for external connectivity.

\*\*2. OSPF for IPv4:\*\*

\*\*OSPF Configuration:\*\*

- OSPF Area 0 (Backbone) at the core layer.

- OSPF Area 1 for each department.

- Appropriate OSPF network statements on routers.

\*\*3. Inter-VLAN Routing and VLAN Configurations:\*\*

\*\*Inter-VLAN Routing:\*\*

- Layer 3 switches used for inter-VLAN routing.

- SVIs configured for each VLAN.

- Appropriate ACLs for traffic control between VLANs.

\*\*4. Security Configurations:\*\*

\*\*SSH:\*\*

- SSH version 2 enabled for secure remote management.

- Access control list (ACL) applied to SSH for authorized hosts.

\*\*Port Security:\*\*

- Port security enabled on access layer switches.

- Maximum MAC address limit set to 2 for end-user ports.

\*\*Additional Security Measures:\*\*

- Firewall and intrusion detection/prevention systems for perimeter security.

- User authentication using RADIUS for remote access.

\*\*5. Network Services from Server Farm:\*\*

\*\*Server Farm Services:\*\*

- File storage and sharing using a NAS server.

- Email services hosted on an Exchange server.

- Web hosting for client projects.

---

### Part C: Investigation of Network Traffic

\*\*1. Experimentation and Simulation:\*\*

\*\*Experiments Conducted:\*\*

- Traffic simulation to test network performance under load.

- Failover testing to ensure core router redundancy functions as expected.

- VLAN isolation testing to confirm logical segmentation.

- SSH access testing for remote management.

\*\*Configuration Details:\*\*

- Provide detailed configurations used for each experiment, including traffic generation tools, scripts, and commands.

\*\*2. Network Traffic Analysis:\*\*

\*\*Traffic Analysis Results:\*\*

- Latency and throughput measurements for various network paths.

- Failover time during core router redundancy testing.

- Successful isolation of VLAN traffic during VLAN testing.

- Secure remote access using SSH validated.

\*\*Recommendations for Improvement:\*\*

- Fine-tuning of OSPF parameters for optimized routing.

- Regular security audits to update ACLs and firewall rules.

- Periodic review of port security settings.

- Implementation of a monitoring solution for real-time network performance tracking.

---

### Conclusion

In conclusion, the network design successfully meets the requirements of the medium-sized marketing agency. It provides scalability, redundancy, and security while accommodating the needs of different departments. The technologies used, including DHCP, OSPF, VLANs, and security measures, contribute to a robust network infrastructure.

Through the network simulations and experiments, we have validated the design's performance and security aspects. While the network design meets current needs, continuous monitoring and periodic reviews will ensure it remains efficient and secure as the organization evolves.

This network design project has provided valuable insights into the complexities of building and maintaining a network for a medium-sized organization, and it emphasizes the importance of aligning technology choices with specific business requirements.