Networking Foundations

CREATING AN ENTERPRISE NETWORK

Diego Acosta Cantú

Cybersecurity

Table of Contents

Introduction

The purpose of this project is to design and test an enterprise-level computer network simulation using Cisco Packet Tracer. The network will be designed with a focus on providing a reliable, secure, and efficient infrastructure to support multiple devices such as workstations, laptops, mobile devices, servers, wireless access points, and firewalls. The project aims to simulate a functional network with components like routers, switches, DHCP and DNS servers, and a web server. It will also involve configuring three separate subnets, a connection to a WAN, and the implementation of essential services like domain name resolution and website hosting. The simulation will be tested to ensure connectivity between all devices and functionality of critical services such as DHCP, DNS, and web hosting.

This project will demonstrate the practical application of network design principles, IP addressing, subnetting, routing, and the integration of key network services. The focus will also be on ensuring scalability, security, and optimal performance for the simulated enterprise network. Through the completion of this project, the importance of proper configuration, troubleshooting, and network testing will be highlighted.

Project Objectives

The objectives of this project are as follows:

1. Design a Complete Network: Develop a network simulation using Cisco Packet Tracer that includes a variety of devices such as workstations, switches, routers, servers, wireless access points, mobile devices, and laptops.

2. Configure Network Components: Properly configure each network device to ensure that workstations, servers, and other devices can successfully communicate with each other through network pings.

3. Subnetting and IP Addressing: Create three separate subnets and assign appropriate IP addresses, using Class A for the WAN and Class C for the local network.

4. Establish WAN Connection: Link the local network to a WAN network and ensure proper routing between the subnets, using optical fiber connections between routers.

5. Set Up DHCP and DNS: Configure the network with a Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) services to provide automatic IP addressing to devices.

6. Configure Web Server and DMZ Zone: Set up a web server and a DMZ (Demilitarized Zone) to host a website, ensuring it is accessible while maintaining proper security configurations.

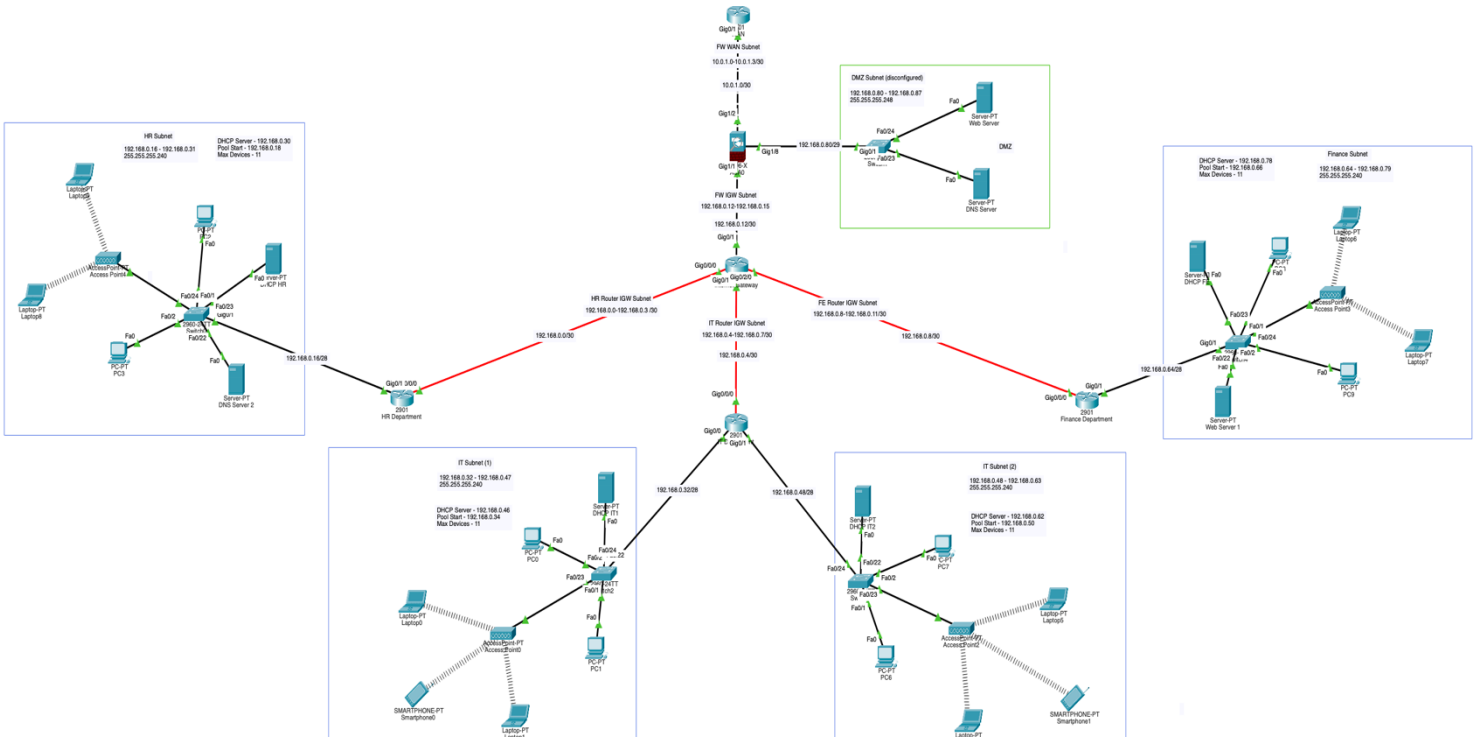
7. Wireless Access and Mobile Devices: Implement wireless access points to provide mobility for devices such as laptops and mobile devices, ensuring they are integrated into the network.

8. Security Implementation: Configure a firewall and ensure it properly protects the network, allowing secure communication while preventing unauthorized access.

9. Testing and Troubleshooting: Conduct thorough testing to verify that all network components are working as expected, including the successful pinging of devices, proper DNS resolution, and website accessibility.

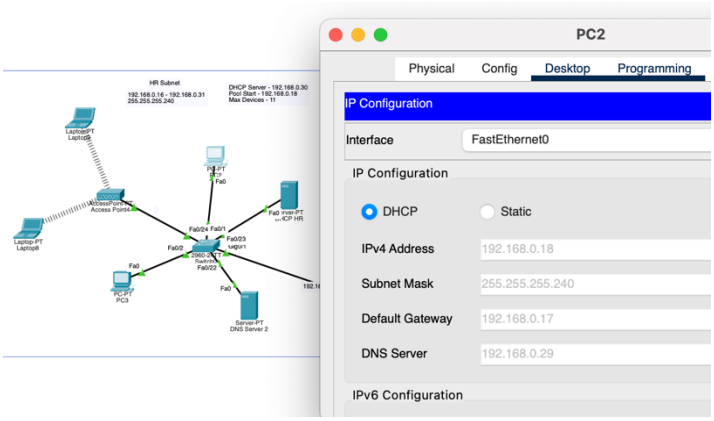
10. Comprehensive Report: Document the network design, configuration process, and testing outcomes in a detailed report, including block diagrams, configuration screenshots, and explanations of technical solutions.

Network Visual Overview

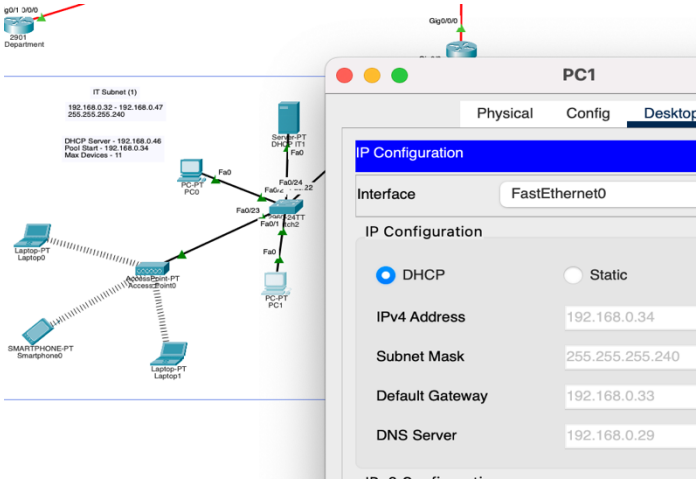


Test Cases

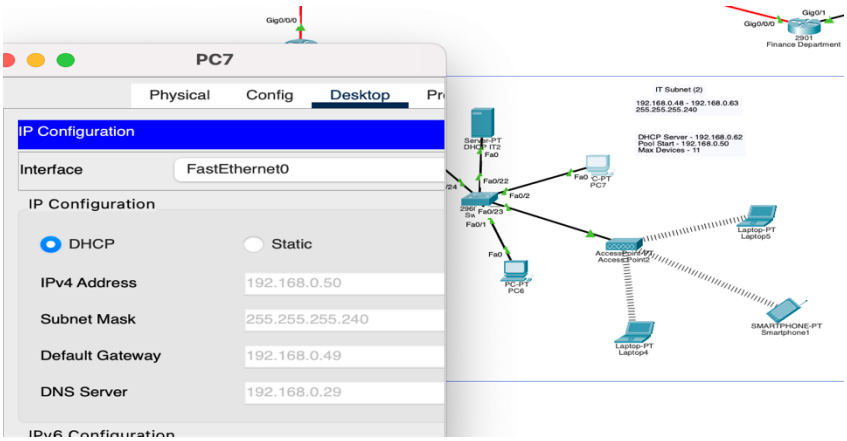
Test Case 1: HR Subnet DHCP



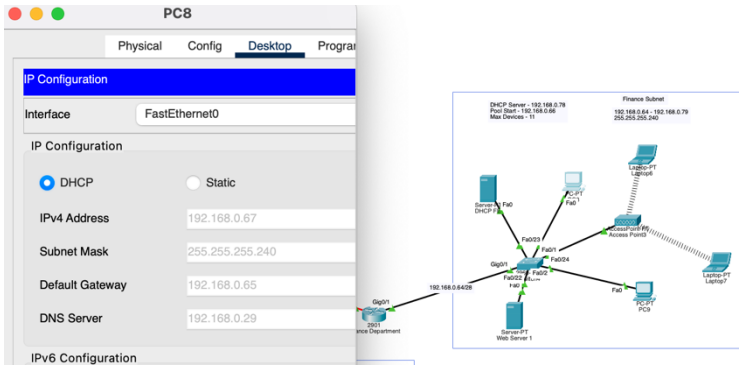
Test Case 2: IT 1 Subnet DHCP Server



Test Case 3: IT 2 Subnet DHCP Server



Test Case 4: Finance Subnet DHCP Server



Test Case 5: HR Subnet PC (192.168.0.18) to IT 1 PC (192.168.0.35) ping

```
C:\>ping 192.168.0.35

Pinging 192.168.0.35 with 32 bytes of data:

Reply from 192.168.0.35: bytes=32 time<1ms TTL=125
Reply from 192.168.0.35: bytes=32 time<1ms TTL=125
Reply from 192.168.0.35: bytes=32 time<1ms TTL=125
Reply from 192.168.0.35: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Test Case 6: HR Subnet PC (192.168.0.18) to IT 2 PC (192.168.0.50) ping

```
C:\>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.50: bytes=32 time<1ms TTL=125
Reply from 192.168.0.50: bytes=32 time<1ms TTL=125
Reply from 192.168.0.50: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Test Case 7: HR Subnet PC (192.168.0.18) to Finance PC (192.168.0.67) ping

```
C:\>ping 192.168.0.67

Pinging 192.168.0.67 with 32 bytes of data:

Reply from 192.168.0.67: bytes=32 time=1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Test Case 8: IT 1 (192.168.0.35) PC to IT 2 PC (192.168.0.50) ping

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.50

Pinging 192.168.0.50 with 32 bytes of data:

Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127
Reply from 192.168.0.50: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

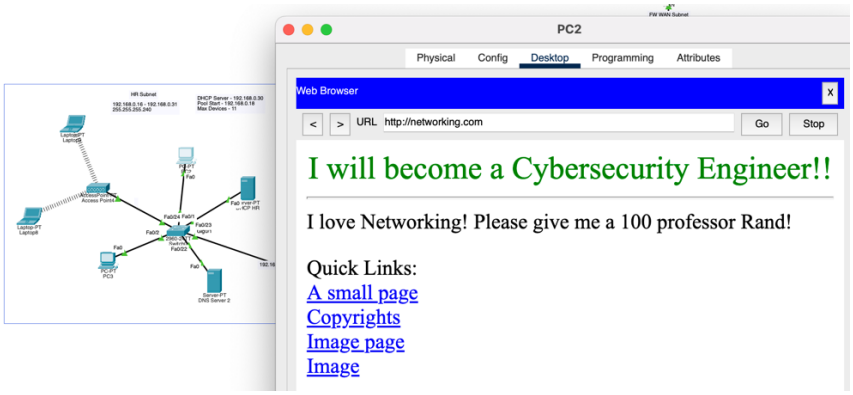
Test Case 9: IT 1 PC (192.168.0.35) to Finance PC (192.168.0.67) ping

```
C:\>ping 192.168.0.67

Pinging 192.168.0.67 with 32 bytes of data:

Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

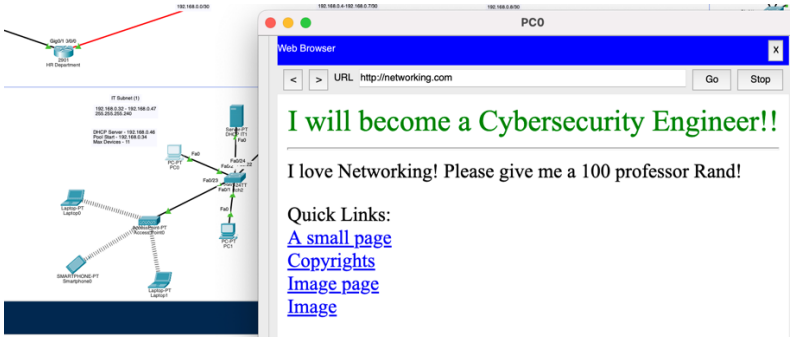
Test Case 10: IT 2 PC (192.168.0.50) to Finance PC (192.168.0.67)ping

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.67

Pinging 192.168.0.67 with 32 bytes of data:

Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125
Reply from 192.168.0.67: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

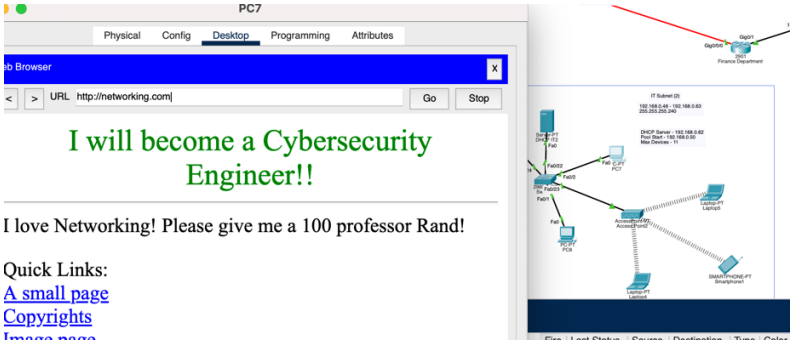
Test Case 11: HR PC (192.168.0.18) to Web Server (192.168.0.77)



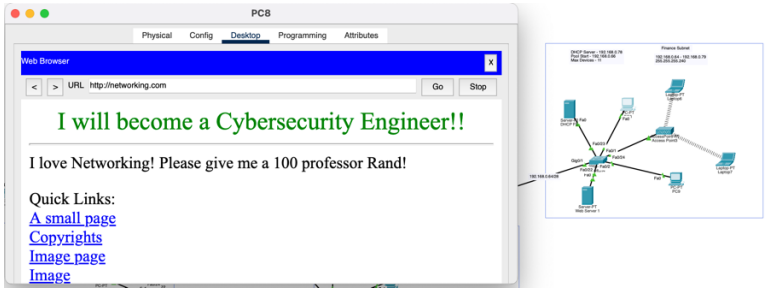
Test Case 12: IT 1 PC (192.168.0.35) to Web Server (192.168.0.77)



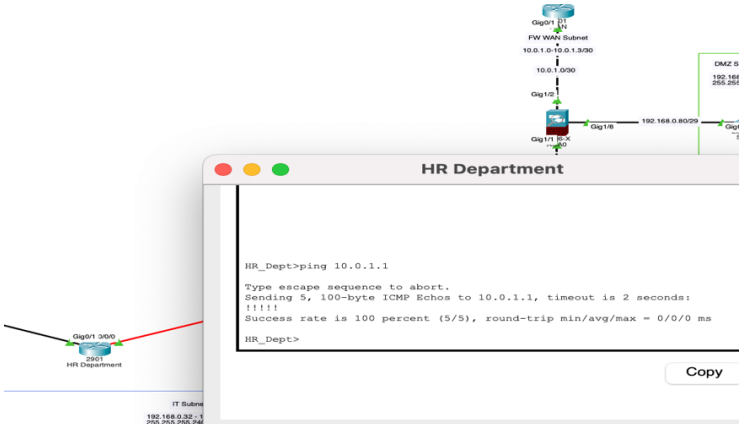
Test Case 13: IT 2 PC (192.168.0.50) to Web Server (192.168.0.77)



Test Case 14: Finance PC (192.168.0.67) to Web Server (192.168.0.77)



Test Case 15: LAN (192.168.0.1) to WAN (10.0.1.1) ping



Test Case 16: HR PC (192.168.0.18) to DNS (192.168.0.29) ping

```
C:\>ping 192.168.0.29

Pinging 192.168.0.29 with 32 bytes of data:

Reply from 192.168.0.29: bytes=32 time<1ms TTL=128
Reply from 192.168.0.29: bytes=32 time=28ms TTL=128
Reply from 192.168.0.29: bytes=32 time=8ms TTL=128
Reply from 192.168.0.29: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 28ms, Average = 9ms
```

Test Case 17: IT 1 PC (192.168.0.35) to DNS (192.168.0.29) ping

```
C:\>ping 192.168.0.29

Pinging 192.168.0.29 with 32 bytes of data:

Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.0.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Test Case 18: IT 2 PC (192.168.0.50) to DNS (192.168.0.29) ping

```
C:\>ping 192.168.0.29

Pinging 192.168.0.29 with 32 bytes of data:

Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time=20ms TTL=125
Reply from 192.168.0.29: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.0.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 5ms
```

Test case 19: Finance PC (192.168.0.67) to DNS (192.168.0.29) ping

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.29

Pinging 192.168.0.29 with 32 bytes of data:

Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125
Reply from 192.168.0.29: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.0.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Network Physical Topology

In general, I chose to simulate a medium sized “Technology Solutions” enterprise network. I realized the best way to organize the physical topology was to use a tree network topology between routers and WAN, a wired star topology within each subnet, each having its respective switch, and an infrastructure topology with Access Points for the wireless network design.

The network is divided into 5 core departments: HR, IT 1, IT 2, and Finance and a DMZ / server farm with DNS and Web servers. Both the HR and Finance departments have their own router, while the two IT departments share the same router.

The three routers are connected to a 4th router that acts as the Internet Gateway, the they are all connected using fiber optic cables. By doing so, it improves the bandwidth, throughput and most importantly is the connection is immune to EMI and can withstand larger distances and harsher environments.

The internet gateway is connected to the LAN’s firewall. The firewall connects to all three, LAN, WAN, and DMZ, it manages traffic between them, and acts as a secure border officer between the LAN and the Internet (Insecure).

I created the DMZ placing the server farm in a separate network segment connected to the firewall.
For the WAN simulation, I couldn’t find a way to configure any of the WAN Emulation devices such as the Cloud-PT. Therefore, I decided to simulate the WAN using a normal router, in this case the 2901 Router.

Components Selection

For the routers, I decided to use 2901 Routers (ideal for a medium-sized enterprise).
One of the problems I encountered during the network design was that, 2901 routers don’t support fiber optics, so I installed an SFP module and a 1000BASE-LX/LH SFP port in each module for the routers to be able to support fiber optics. I installed three modules for the Internet Gateway router because it is the core router meaning it’s connected to all the three LAN routers.

For the firewall, I used a Cisco ASA-5506, and it is connected to both the WAN and the Internet gateway through copper crossover cable, while using a straight through cable to connect to the DMZ. Although using a straight-through cable for the connection between

the routers and the firewall is ideal, upon researching about it, I found out that Cisco Packet Tracer works better by using a crossover cable for that specific connection.

Each department consists of two workstations, an Access Point (Cisco AP-PT), two wireless laptops, and a DHCP server. All of these are connected to a switch directly connected to the department's respective router. Everything is connected through straight-through cable or wireless.

I inlcuded a DHCP server in each subnet after further research, medium-sized enterprise normaly use a DHCP server for each subnet to ensure efficient IP address management, reduce network congestion, and ensure proper address allocation within each subnet, as well as security practices. This simplifies the configuration and maintenance of the network by providing localized DHCP services, improving network performance and reliability.

The HR department has another DNS server, the Finance department has another Web server, and both of the IT departments have an employee mobile device. These are the only differences between each subnet device wise.

For the switches within each subnet, I decided to use Cisco 2960 switches.

In conclusion, I opted for this setup because it's scalable, has enhanced fault tolerance, and uses a hierarchical organization facilitating traffic control.

Network Design and Configuration

Logical Topology

For the logical topology organization, I made use of Variable Length Subnet Mask (VLSM) for subnetting the network. The network is divided into 10 subnets in total including the one between the WAN and the firewall.

Using VLSM is a good practice because it optimizes IP address usage by allowing more efficient allocation of addresses based on the actual number of devices in each subnet. By having used it I reduced the need for excess IP addresses, which can save on purchasing additional IP blocks.

Additionally, VLSM can isolate sensitive devices in smaller subnets, enhancing security by controlling access between network segments.

On the other hand, It provides flexibility in network design, accommodating varying departmental requirements while supporting future scalability as the company grows.

I divided the network as the following:

I used a class A point-to-point link address (10.0.1.0/30) for the WAN and firewall connection. Simulating the LAN's connection to the Internet (WAN).

I used 5 point-to-point link subnets (using a /30 subnet mask) between routers, routers and firewall and between firewall and WAN.

I used 4 /28 subnets one for each department connected to its respective router. (HR, IT 1, IT 2, and Finance departments)

I used a single /29 subnet for the DMZ (server farm).

More specifically:

I used 10.0.1.0/30 for the connection between the WAN router and the Firewall

- Network Address 10.0.1.0/30
- WAN router int g0/1 → 10.0.1.1/30
- Firewall int g1/2 → 10.0.1.2/30
- Broadcast Address 10.0.1.3/30

I used 192.168.0.0/30 for the connection between the HR router and the internet gateway (4th router).

- Network Address 192.168.0.0/30
- Internet Gateway int g0/0/0 → 192.168.0.1/30
- HR router int g0/0/0 → 192.168.0.2/30
- Broadcast Address 192.168.0.3/30

I used 192.168.0.4/30 for the connection between the IT router and the Internet gateway.

- Network Address 192.168.0.4/30
- Internet Gateway int g0/1/0 → 192.168.0.5/30
- IT router int g0/0/0 → 192.168.0.6/30
- Broadcast Address 192.168.0.7/30

I used 192.168.0.8/30 for the connection between the finance department and the internet gateway.

- Network Address 192.168.0.8/30

- Internet Gateway int g0/2/0 → 192.168.0.9/30
- Finance router int g0/0/0 → 192.168.0.10/30
- Broadcast Address 192.168.0.11/30

I used 192.168.0.12/30 for the connection between the internet gateway and the firewall.

- Network Address 192.168.0.12/30
- Internet Gateway int g0/1 → 192.168.0.13/30
- Firewall int g1/1 → 192.168.0.14/30
- Broadcast Address 192.168.0.15/30

I used 192.168.0.16/28 for the HR department

- Network Address 192.168.0.16/28
- HR default gateway int g0/1 → 192.168.0.17/28
- HR last usable IP address → 192.168.0.30/28
- Broadcast Address 192.168.0.31/28

I used 192.168.0.32/28 for the IT 1 department

- Network Address 192.168.0.32/28
- IT 1 default gateway int g0/0 → 192.168.0.33/28
- HR last usable IP address → 192.168.0.46/28
- Broadcast Address 192.168.0.47/28

I used 192.168.0.48/28 for the IT 2 department

- Network Address 192.168.0.48/28
- IT 2 default gateway int g0/1 → 192.168.0.49/28
- HR last usable IP address → 192.168.0.62/28
- Broadcast Address 192.168.0.63/28

I used 192.168.0.64/28 for the Finance department

- Network Address 192.168.0.64/28
- Finance default gateway int g0/1 → 192.168.0.65/28
- HR last usable IP address → 192.168.0.78/28
- Broadcast Address 192.168.0.79/28

I used 192.168.0.80/29 for the DMZ

- Network Address 192.168.0.80/29
- HR default gateway int g0/1 → 192.168.0.81/29
- HR last usable IP address → 192.168.0.86/29
- Broadcast Address 192.168.0.87/29

Subnetting

When subnetting, I used a single class C network (192.168.0.0) for the whole enterprise, working with only 256 addresses. Before starting, I performed an subnet analysis by hand to get the exact amount of ip addresses needed in each subnet based on specifications but open to future scalability:

- HR department: 2 workstations, 2 laptops, 2 servers, 1 router + 2 (network and broadcast addresses) = 9
    - Having 9 devices means the best fitting subnet mask is the /28 giving me 16 addresses in total with 14 usable addresses.

- IT 1 department: 2 workstations, 2 laptops, 1 server, 1 mobile device, 1 router + 2 (network and broadcast addresses) = 9
    - Having 9 devices means the best fitting subnet mask is the /28 giving me 16 addresses in total with 14 usable addresses.

- IT 2 department: 2 workstations, 2 laptops, 1 server, 1 mobile device, 1 router + 2 (network and broadcast addresses) = 9
    - Having 9 devices means the best fitting subnet mask is the /28 giving me 16 addresses in total with 14 usable addresses.

- Finance department: 2 workstations, 2 laptops, 2 servers, 1 router + 2 (network and broadcast addresses) = 9
    - Having 9 devices means the best fitting subnet mask is the /28 giving me 16 addresses in total with 14 usable addresses.

- HR Router to Internet Gateway Router connection: 2 routers + 2 (network and broadcast addresses)
    - Having 2 devices means the best fitting subnet mask is the /30 giving me 4 addresses in total with 2 usable addresses.

- IT Router to Internet Gateway Router connection: 2 routers + 2 (network and broadcast addresses)
    - Having 2 devices means the best fitting subnet mask is the /30 giving me 4 addresses in total with 2 usable addresses.

- Finance Router to Internet Gateway Router connection: 2 routers + 2 (network and broadcast addresses)

    - Having 2 devices means the best fitting subnet mask is the /30 giving me 4 addresses in total with 2 usable addresses.

- *16 + 16 + 16 + 16 + 8 + 4 + 4 + 4 + 4 = 88 used IPs in total*
- *256 – 88 = 168 remaining IPS for future use.*

Routers Configuration

For the Routers configuration I opted to use static routes since I all of them are operating within the same LAN, they are not many enough to use the OSPF protocol, and using RIP is too old-fashioned. By doing this, troubleshooting will be easier and straightforward.

HR, IT, and Finance Routers

In these routers I included static routes to reach the Internet gateway router, and routing between themselves. Although static routes can be added via CLI, I opted adding them via the GUI interface for simplicity.

HR Router → 0.0.0.0/0 via 192.168.0.1
IT Router → 0.0.0.0/0 via 192.168.0.5
Finance Router → 0.0.0.0/0 via 192.168.0.9

Internet Gateway Router

For the IGW I included static routes towards every one of the inside subnets, towards the DMZ, and towards the Internet (WAN).

- 192.168.0.16/28 via 192.168.0.2
- 192.168.0.32/28 via 192.168.0.6
- 192.168.0.48/28 via 192.168.0.6
- 192.168.0.64/28 via 192.168.0.10
- 10.0.1.0/30 via 192.168.0.14
- 0.0.0.0 0.0.0.0 via 192.168.0.14

Firewall Configuration

For the firewall, I configured it to assume its int g1/1 (LAN interface) is the LAN's inside network.

CLI commands:

- en

- conf t
- int g1/1
- nameif INSIDE
- security-level 100
- do wr
- ex

By doing this I ensured the INSIDE interface is trusted with 100 security level meaning the firewall will process traffic coming from this interface.
On the other hand, I configured int g1/2 (WAN interface) to act as the outside network.
CLI commands:

- int g1/2
- nameif OUTSIDE
- security-level 0
- do wr
- ex

After that, I configured int 1/8 (DMZ interface) as a DMZ isolated network segment.
CLI commands:

- int g1/8
- nameif DMZ
- security-level 70
- do wr
- ex

Finally, I configured each of the interfaces static routes.
CLI commands

- route OUTSIDE 0.0.0.0 0.0.0.0 10.0.1.1
- route INSIDE 0.0.0.0 0.0.0.0 192.168.0.13
- route DMZ 0.0.0.0 0.0.0.0 192.168.0.81

Servers Configuration

DHCP Servers

For the DHCP servers I assigned each one of them a static address matching its respective subnet, enabled the DHCP server status, and configured the subnets respective DHCP pool and starting from the subnet's 3rd available IP address (the one after the default gateway of each subnet) and set a max device limit to 11 (based on the available IP addresses of each subnet).

HR DHCP

- Static Address → 192.168.0.30
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.17
- Start IP Address → 192.168.0.18
- Subnet Mask → 255.255.255.240
- Max Users → 11

IT 1 DHCP

- Static Address → 192.168.0.46
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.33
- Start IP Address → 192.168.0.34
- Subnet Mask → 255.255.255.240
- Max Users → 11

IT 2 DHCP

- Static Address → 192.168.0.62
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.49
- Start IP Address → 192.168.0.50
- Subnet Mask → 255.255.255.240
- Max Users → 11

Finance DHCP

- Static Address → 192.168.0.78
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.65
- Start IP Address → 192.168.0.66
- Subnet Mask → 255.255.255.240
- Max Users → 11

Web Server

Servers already have http and https server status enabled by default so the only thing I did was to assign it a static address, and customize the already created HTML files in the packet tracer web server.

- Static Address → 192.168.0.77
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.65

- DNS Server → 192.168.0.29

DNS Server

For the DNS server, I assigned a static IP address and enabled DNS server status in the "services" tab and added the already created web server address.

- Static Address → 192.168.0.29
- Subnet Mask → 255.255.255.240
- Default Gateway → 192.168.0.17
- "Services" Tab
- Web Server Address → 192.168.0.77
- URL → www.networking.com

Access Points Configuration

Configuring the APs was really simple and straigthforward, I only had to access each of the APs port 1 set up the SSID (AP's wireless network connection's name), enable the WPA2 with a PSK, select the encryption type, in this case the AES which is the least vulnerable one, and set up a password. Although presenting a great security risk for the network, for simplicity, I used 12345678 as the password for every one of the network's APs. I tried following network security best practices and disable SSID broadcast but I don't think it's possible in Packet Tracer.

Wireless Configuration

To enable wireless functions and access to the network, I changed all of the laptops default NIC with a wireless NIC module. For this to work, I had to first turn off the device, take of the default module, install the wireless NIC and turn the device on again. Then I had to connect all of the wireless devices to the APs using its respective subnet AP's SSID and use the PSK.

Technical Solution

Why this Solution?

For the project, I chose the used topologies and network design because united they provide the three most important factors in networking.

1. Scalability: Fiber optics between routers allow the network to scale easily as more devices or subnets are added.

2. Security: A firewall and DMZ protect critical services and prevent unauthorized access. Static routing enhances security by controlling traffic flow between departments and external networks.

3. Efficiency: Static IP addressing and DHCP pools ensure efficient and accurate IP assignment, while static routes optimize network traffic and performance.

I chose that design because it meets the needs for scalability, security, and performance. It follows established network design principles, such as hierarchy, segmentation, and security, all of which are crucial for a medium-sized enterprise.

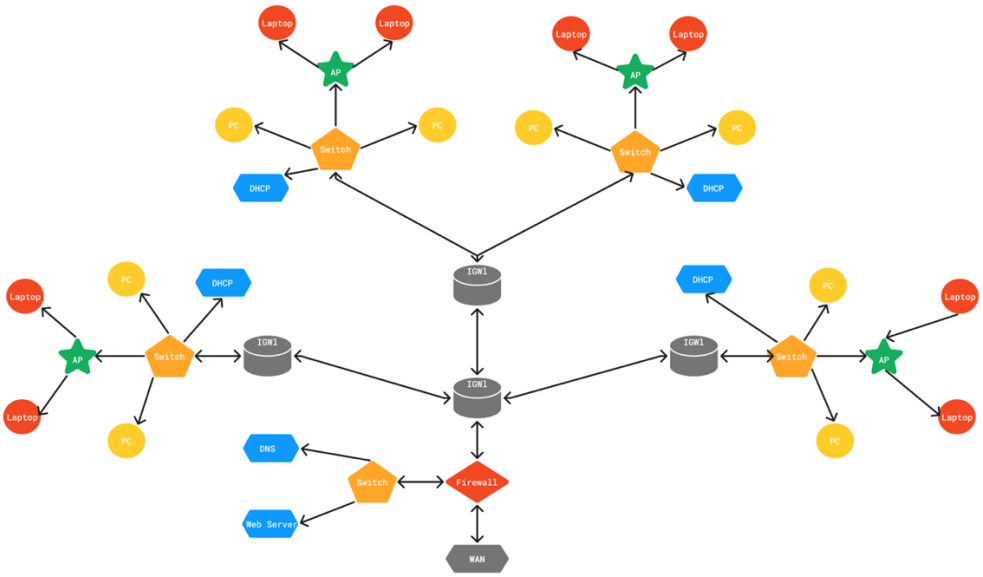
Other reasons why I chose eveything include:

Hierarchical Network Design: By dividing the network into departments and using dedicated routers for each, this design minimizes congestion and streamlines routing. The central Internet Gateway router handles external communication, while the department routers manage internal connectivity.

VLSM Subnetting: Variable Length Subnet Masking (VLSM) allows for efficient allocation of IP addresses based on the number of devices in each subnet, reducing waste and improving performance.
Security Through Firewalls and DMZ: The firewall secures the network from external threats, and the DMZ isolates external-facing services like the web and DNS servers, ensuring that only authorized traffic can access the internal network.

Centralized DHCP and DNS: With DHCP servers in each subnet, devices can automatically obtain IP addresses and resolve domain names quickly, enhancing overall network efficiency.

Explanation via Block Diagram



Department Routers: Each department (HR, IT 1, IT 2, Finance) has a dedicated router and subnet, ensuring traffic is controlled and resources are allocated without interference.

Firewall: Positioned between the internal network and the WAN, the firewall ensures that only authorized traffic can pass through. It also isolates the DMZ, which contains external-facing services such as web and DNS servers.

DMZ: The DMZ is separated from the internal network, allowing external users to access services like the web and DNS servers while keeping internal systems secure.

WAN Connection: The WAN router simulates the connection between the enterprise network and the external internet, enabling communication with outside systems.
Switches: Each department has a switch connecting workstations, wireless access points, and other devices within the subnet, facilitating communication within the network.

Project Portfolio

Suggested Hardware, Software, and Support (after sale)

Hardware

1. Routers: The Cisco 2901 routers are used for routing within the network. They offer scalability for medium-sized enterprise environments and can support the addition of an SFP module to enable fiber optic connectivity. Their reliability in handling

point-to-point connections and high-throughput routing makes them ideal for this project.

2. Switches: Cisco 2960 switches are selected for their fault tolerance, hierarchical design, and scalability. These switches can efficiently handle traffic distribution within the departments, providing reliable connections for both wired and wireless devices.

3. Firewall: The Cisco ASA-5506 is deployed to protect the network by controlling traffic between the internal network, the DMZ, and the WAN. It provides robust security features including VPN support and advanced threat protection.

4. Servers: For DNS, DHCP, and web hosting, dedicated servers are configured with static IP addresses. The servers ensure reliable and consistent performance, managing services such as dynamic IP addressing, name resolution, and web hosting efficiently.

Software

1. Cisco Packet Tracer: The network simulation software is used for designing and testing the entire network. It allows for a virtual setup and troubleshooting of devices such as routers, switches, firewalls, and servers.

2. Operating Systems for Servers: The network employs industry-standard software for servers to run services such as DNS and DHCP. This ensures compatibility with a wide range of devices and provides a stable platform for the network's core services.

3. Firewall Software: Cisco ASA software is utilized for the firewall configuration, providing a secure gateway and segmentation between the internal network, the DMZ, and the external Internet connection.

After-Sale Support

1. Network Maintenance and Updates: After-sale support will include regular updates to software and firmware to ensure that network devices remain secure and perform optimally. Cisco's software tools and systems can be integrated for ongoing monitoring and management.

2. Hardware Support and Warranty: The Cisco devices used in this project come with manufacturer warranties and support options. After-sale technical assistance will be available to address any hardware failures or troubleshooting needs.

3. Technical Assistance and Training: Users can access Cisco's technical support for detailed troubleshooting. Additionally, training programs can be offered to employees to ensure they are proficient in managing and maintaining the network infrastructure.

Service Catalog

Service Type	Description	Device	Quantity	Cost	Total Cost
Service Catalog					
Network routing	Static routing and dynamic routing between departments, internet, and DMZ	Cisco 2901 Routers	5	$955	$4775
Network Security	Firewall to manage traffic and protect the network	Cisco ASA-5506	1	$1000	$1000
Switches					
Servers	Servers providing Web hosting, DHCP and DNS.	Cisco MTBF	8	$2000	$16000
Access Points	Allow wireless devices to connect to the network via RF signals.	Cisco AP-PT	4	$20	$80
Workstations	Handles complex tasks with high processing power and memory	Average PC and Laptop	20	$1000	$20000
Retired Services	Connects devices, forwarding data within a network.	2960 Switch	5	$1500	$7500
Legacy Equipment	Older PC's replaced by wireless Laptops	IBM PC XT (1983)	10	N/A	N/A