Simple Network (Packet Tracer)

Course Name: IT Platforms
Done By: Botirjon Salokhiddinov
Instructor: professor Rand Kouatly
Date: 15.07.2025

---

1. Introduction

This project demonstrates the practical design, step-by-step configuration, and thorough testing of a corporate network using Cisco Packet Tracer. The aim is to deliver seamless connectivity and reliable access to essential IT services (DHCP, DNS, Web) for both wired and wireless clients, while enforcing security through an enterprise firewall. The process included careful planning, network segmentation, dynamic routing, and a full security policy—mirroring the expectations of a real-world IT department.

2. Project Objectives

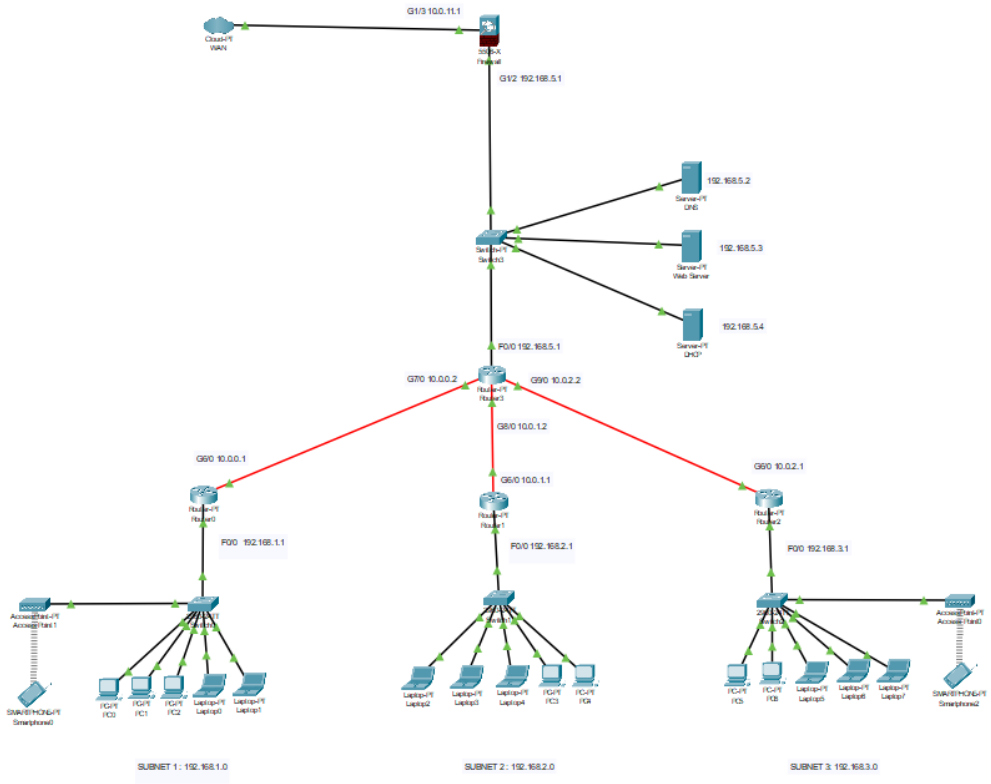
The objectives of this project are as follows:

- Design a scalable and segmented network that serves multiple departments and devices, including **wireless/mobile users**
- Implement **dynamic routing** (RIP v2) for robust connectivity across all subnets
- Enforce network security using an ASA **firewall**, restricting unauthorized access between segments and to the server subnet
- Deploy core network services: **automated IP management (DHCP), DNS** for hostname resolution, and an internal web server
- Demonstrate mobile and wireless connectivity for modern work environments

- Document all steps, configurations, and troubleshooting, providing a professional and reproducible reference

3. Network Topology

The implemented network topology reflects a typical secure enterprise network, segmented for scalability and security.



3.1– WAN Connection (Cloud): At the top, the network connects to an external WAN through Router 4 (Fast Ethernet 0/0 10.0.11.2), providing simulated internet connectivity for testing purposes.

3.2-Firewall (ASA): The ASA firewall sits between the WAN and the core of the enterprise network, enforcing security policies for all inbound and outbound traffic. The firewall connects to the main distribution switch via Gigabit Ethernet ½ 192.168.5.1 and to the WAN via Gigabit Ethernet 1/3 10.0.11.1

3.3 - Core Switch (Switch 4): The central switch aggregates connections from all server resources (DNS, WEB, DHCP servers) and acts as a distribution point for the core subnet (192.168.5.0/24)

3.4 – Server Farm: Three dedicated servers are connected to the core switch:

3.4.1 DNS Server: provides internal name resolution

3.4.2 WEB Server: hosts the intranet web application

3.4.3 DHCP Server: manages IP address assignments for all end devices

3.5 – Main Router (Router 4): Located centrally, this router connects the server subnet (Fast Ethernet 0/0 192.168.5.1) to the three main user segments through three separate routers, creating a secure DMZ for server resources

3.6 – User Segments (Routers 1,2,3):

3.6.1 Router 1: connects user LAN1 (192.168.1.0/24), including PCs, laptops, an access point, and a smartphone

3.6.2 Router 2: connects user LAN2 (192.168.2.0/24) with multiple laptops and PCs

3.6.3 Router 3: connects user LAN3 (192.168.3.0/24), again with end devices and wireless access

3.7 – Switches and End Devices: Each subnet contains a switch aggregating connections to various PCs, laptops, and wireless access points. Wireless connectivity is simulated with smartphones and access points, providing mobile access to the network

3.8 – Routing: All routers use dynamic routing (RIP v2) for automatic route propagation between subnets, and the firewall is configured to allow/deny access as per security policies.

4. Device Inventory

Device Type	Hostname	Purpose / Role	Model	Interfaces
Router	Router1,Router2, Router3, Router4	Interconnect subnets	2911/K9	G0/0, G0/1
Switch	Switch1, Switch2 Switch3, Switch4	LAN aggregation	2960-24TT	Fa0/1, Fa0/24
Firewall	ASA0	Security, segmentation	ASA 5505-PT	G1/1, G1/2, G1/3
Server	DHCP	DHCP for all clients	Server-PT	Fa0
Server	DNS	DNS for name resolution	Server-PT	Fa0
Server	WEB	Internet Web hosting	Server-PT	Fa0
Access Point	AP1	Wireless Coverage	WRT300N	Fa0
End Device	PC1, PC2, …	User workstations	PC-PT	Fa0
End Device	Smartphones	Wireless user	PT-smartphone	WIFI

5. IP Addressing and Subnet Design

A logical IP addressing plan was developed to segment the network for security, manageability, and scalability. Each subnet supports current and future growth, while unique gateway addresses ensure correct routing

Segment	Subnet Address	Subnet Mask	Gateway Address	Ex Device IPs
User LAN 1	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.10, … 11
User LAN 2	192.168.2.0/24	255.255.255.0	192.168.2.1	192.168.2.10, … 11
User LAN 3	192.168.3.0/24	255.255.255.0	192.168.3.1	192.168.3.10, … 11
Server Subnet (DMZ)	192.168.5.0/24	255.255.255.0	192.168.5.1	192.168.5.10, … 11
Wireless LAN	192.168.10.0/24	255.255.255.0	192.168.10.1	192.168.10.10, … 11
Inter-routers links	10.1.1.0/30	255.255.255.0	10.1.1.1 1.2	Point to point

This structure prevents address overlap and enables straightforward configuration of routing, firewall, and DHCP pools

6. Device Configuration Steps

6.1 – Initial Device connections:

a) Connect all routers, switches, firewalls, and servers as shown in the topology diagram
b) Use straight-through cables between switches and routers, and between switches

and servers

c) Use cross-over or serial links for router-to-router connections if required

6.2 – Basic Device Configuration:

a) Set Hostnames and assign IP addresses to all router and server interfaces as per the addressing table

```
Router1(config)# hostname Router1
Router1(config)# interface f0/0
Router1(config-if)# ip address 192.168.1.1 255.255.255.0
Router1(config-if)# no shutdown
```

6.3 – DHCP Configuration:

a) Configure a DHCP Pool on the DHCP server for each subnet

b) Set **ip-helper-address** on each router's LAN interface pointing to the DHCP server's IP

```
Router1(config)# interface f0/0
Router1(config-if)# ip helper-address 192.168.5.4
```

6.4 – DNS Server Configuration:

a) Add A records for web server, other key hosts, and test name resolution from clients

6.5 – Web Server Configuration:

a) Upload HTML welcome page to the server's www root

b) Test HTTP access from client PCs using the server's IP or registered DNS name

6.6 – Dynamic Routing:

a) On all routers, enable RIP v2 and advertise all directly connected networks

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
Router(config-router)# network 192.168.5.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
```

6.7 – ASA Firewall Configuration:

a) Assign interfaces to security levels and IPs

b) Configure access rules to permit traffic from inside to outside

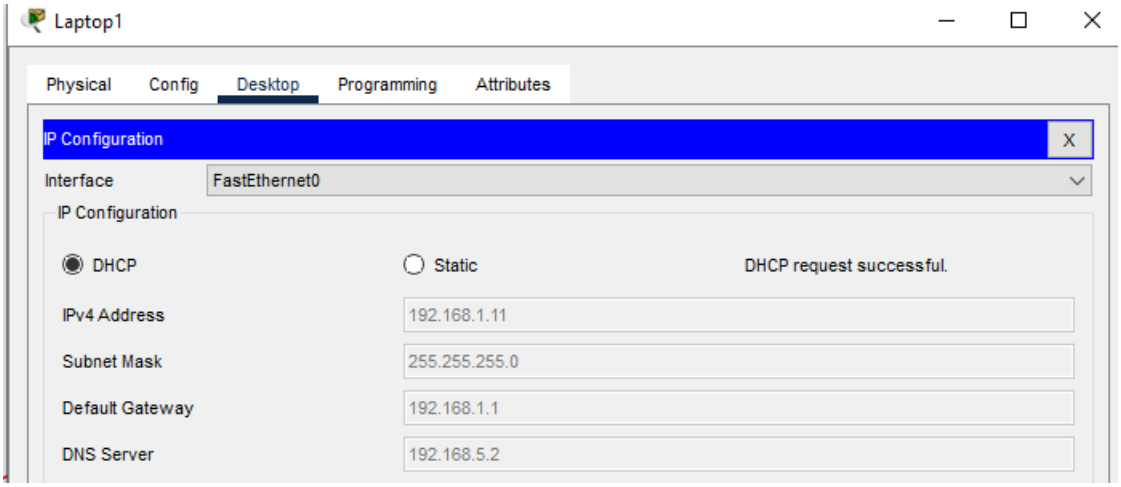
```
access-list OUTSIDE_IN extended permit tcp any host 192.168.5.3 eq 80
access-list OUTSIDE_IN extended permit udp any host 192.168.5.4 eq 67
access-group OUTSIDE_IN in interface outside
```

6.8 – Wireless Configuration:

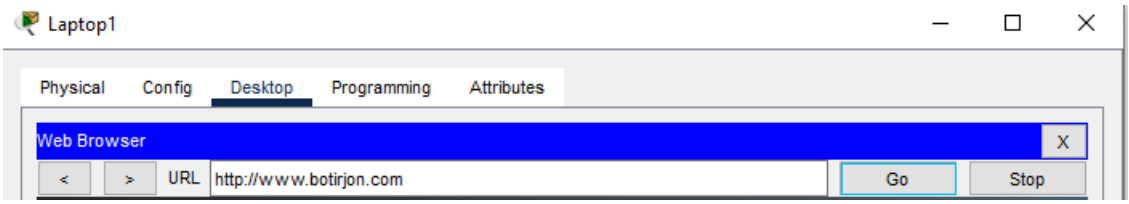
a) Set SSIDs on access points and connect smartphones/clients using the correct wireless settings

7. Testing and Troubleshooting

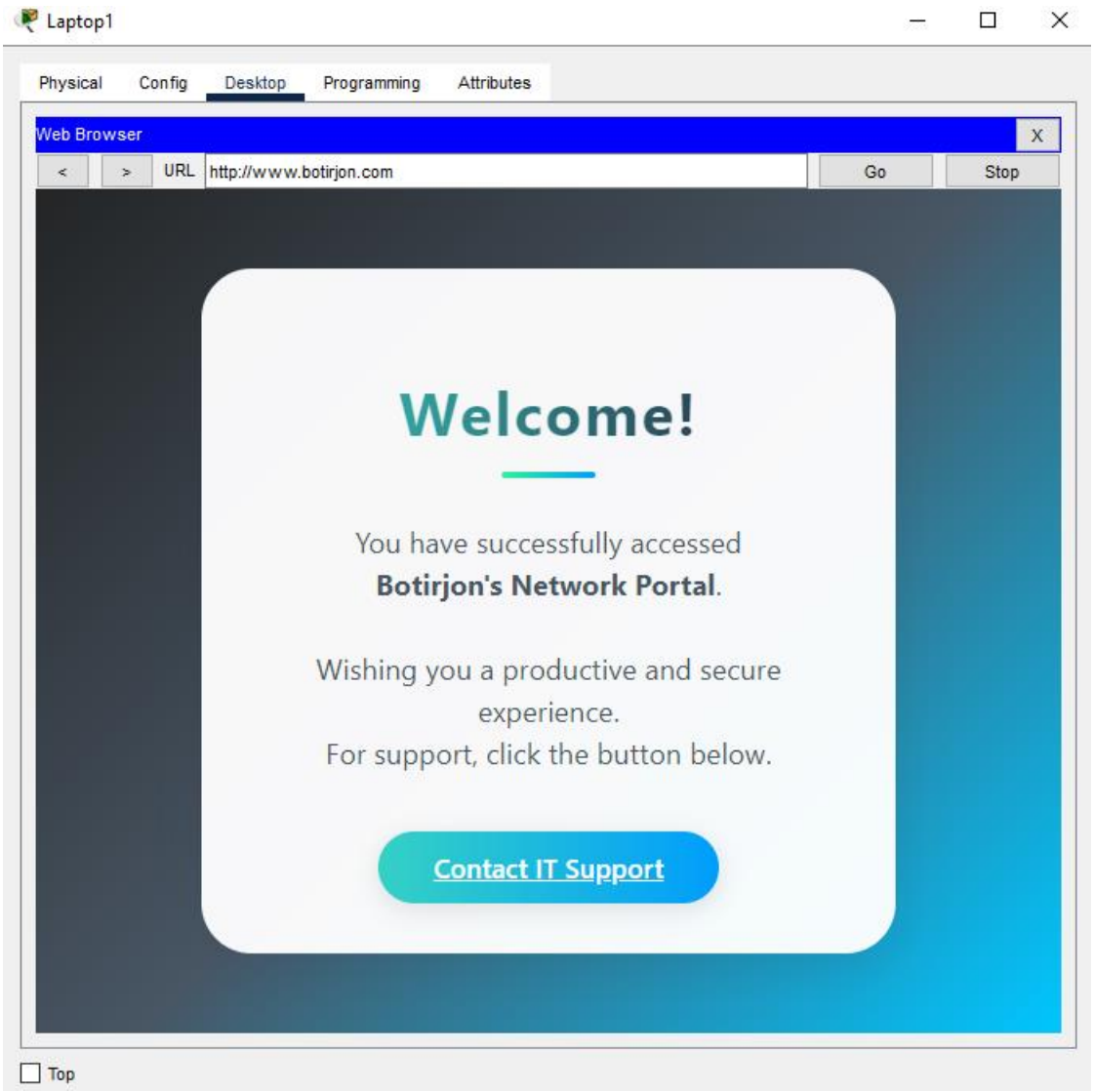
7.1 -DHCP: Ensure all PCs/laptops receive IP addresses and default gateways via DHCP.



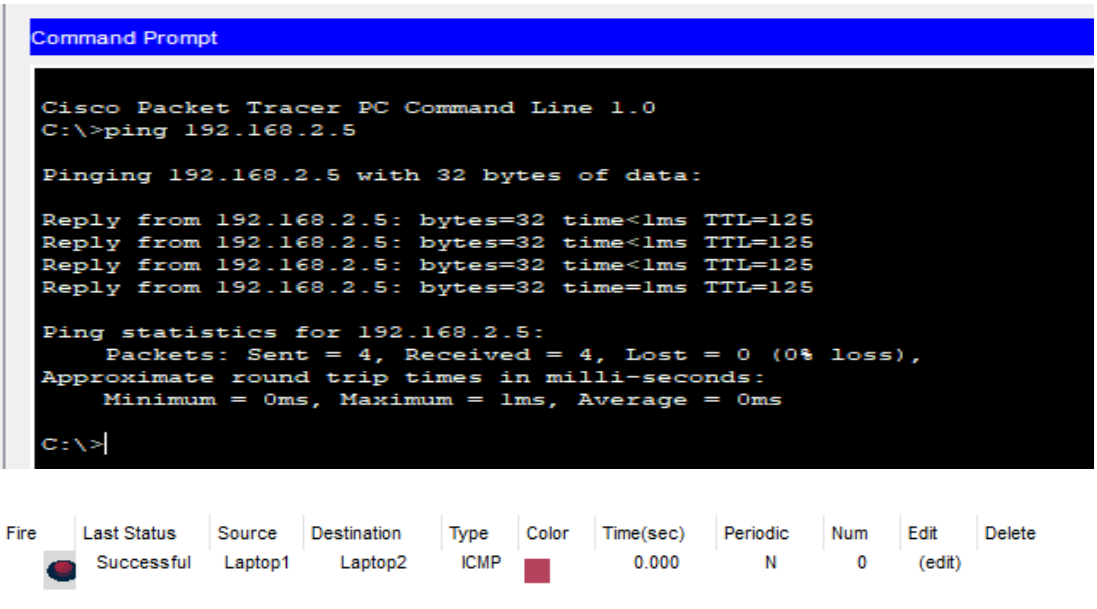
7.2 – DNS: From a client, run `nslookup` for your web server domain—ensure correct resolution



7.3 – WEB: Open a browser, enter the web server's domain or IP—your welcome page should appear



7.4 –Connectivity: Ping between subnets and to all servers, ensure successful replies



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop1	Laptop2	ICMP		0.000	N	0	(edit)	

8. Conclusion

This project demonstrates the planning, configuration, and testing of a multi-segmented, secure enterprise network in Cisco Packet Tracer. The implemented network provides robust separation between user, server, and WAN resources, with automated IP management, name resolution, dynamic routing, and firewall protection—mirroring real-world best practices.