Reamohetse Ntetshe 06 Nov 2025

Cisco Network Infrastructure Project Documentation

Project Overview

This project presents the design and configuration of a **Cisco Packet Tracer-based network infrastructure** simulating a small-scale enterprise environment.
The main focus was to implement **secure communication and service accessibility** between multiple servers and end-user clients using Cisco devices.

The network includes:

- A **DNS server** for hostname resolution
- Multiple **Web servers** hosting internal and external web services (HTTP/HTTPS)
- Three **PC clients** configured to use the DNS service to access the web servers by domain name
- A central **router** acting as the gateway and security enforcement point
- Layer 2 switches providing connectivity between devices

The entire network was designed and tested in **Cisco Packet Tracer**, focusing on both **functionality and security hardening** through configuration commands and logical segmentation.

Project Objectives

The primary goals of this project were:

- ☑ To design a functional and secure Cisco network supporting DNS and HTTP communication
- ☑ To configure and test name resolution using a local DNS server
- ☑ To allow clients (PCs) to access multiple web servers via domain names
- ☑ To implement proper IP addressing and subnetting for different segments
- ☑ To apply **security configurations** that enhance trust, mitigate spoofing, and ensure network stability

Network Topology Description

The topology consists of a **core router** connected to multiple subnets via switch infrastructure.
Each subnet serves a specific purpose:

Network	Purpose	Example IP Range
Server Network	Hosts DNS and Web servers	192.168.10.0/24
Client Network	Connects user PCs	192.168.20.0/24
Management / Admin Network	For secure management traffic	192.168.30.0/24

The **DNS server** holds records for all internal servers (Web1, Web2, API services).
Client PCs send DNS requests to the DNS server to resolve names to IP addresses, enabling access to hosted web applications.

Devices and Roles

Device	Role	Description
Router	Core gateway	Provides inter-VLAN routing, IP addressing, and security features
Switches	Access layer	Connect servers and clients to the router

DNS Server	Name resolution	Resolves all internal server hostnames and APIs
Web Servers	HTTP/HTTPS hosting	Host web and API services accessible by clients
Client PCs	End devices	Access web services using domain names configured through DNS

Configuration Summary

Below are the key configuration areas implemented across the network:

1. DNS Server Configuration
    a. Configured using the Packet Tracer **Services → DNS** feature
    b. Added A-records for all internal web and API domains:
        i. ramo.com → 192.168.30.13
        ii. fds.ramo.com → 192.168.30.12
        iii. cs.ramo.com → 192.168.30.11
    c. PCs were assigned the DNS server IP either manually or via DHCP
2. Web Server Configuration
    a. Assigned **static IPs**
    b. Enabled **HTTP service**
    c. Deployed simple HTML pages and simulated API endpoints
    d. Accessible through DNS names
3. Router Configuration
    a. Configured **multiple routed interfaces** for each subnet:

```
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown

interface GigabitEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
```

    b. Enabled IP routing for inter-network communication
    c. Applied **security configurations** like:
        i. ip dhcp snooping
        ii. ip arp inspection
        iii. ip proxy-arp
        iv. Access control on untrusted interfaces
4. Client Configuration
    a. Configured with IP addresses and DNS server IP
    b. Tested name resolution using `nslookup` and web access using Packet Tracer's browser

Security Focus Areas

Security was a **primary goal** of this project.

The following features and best practices were implemented:

Security Feature	Purpose
Dynamic ARP Inspection (DAI)	Prevent ARP spoofing and poisoning attacks
DHCP Snooping	Secure DHCP assignments and validate bindings
Port Security	Limit MAC addresses per switch port
Access Control Lists (ACLs)	Control access between networks
Proxy ARP Management	Prevent unwanted ARP replies and restrict routing misuse
Trusted Interfaces	Proper use of ip arp inspection trust for uplinks
DNS Hardening	Limited DNS access to internal clients only

Testing and Verification

To confirm correct functionality:

1. DNS Resolution
    a. PCs successfully resolved `ramo.com`, `cs.ramo.com`, and `fds.ramo.com` to their correct IPs.
2. Web Access
    a. Browsers on PCs accessed pages and APIs hosted by the web servers.
3. Ping Tests
    a. Cross-network connectivity verified using ICMP.
4. Security Tests
    a. Verified ARP spoofing protection using DAI logs.
    b. Confirmed DHCP snooping binding table entries.

This Cisco Packet Tracer project demonstrates how a **secure, service-based network** can be designed and implemented using core routing, DNS configuration, and web server integration.
By combining DNS, HTTP, and network security features such as DAI and DHCP snooping, this simulation provides a practical foundation for understanding enterprise network design and protection techniques.

The project highlights:

- Proper configuration hierarchy (Router → Switch → Server → Client)
- Secure device communication using internal DNS
- Enforcement of best-practice security configurations

Author: *Reamohetse Ntetshe*
Platform: Cisco Packet Tracer
Focus: Security, DNS Configuration, Routing, and Web Service Implementation
Date: 06 November 2025