RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

**CS2403 COMPUTER NETWORKS**

**Mini Project Report**

# *A Python-Based VPN Tunnel Emulator*

Submitted

By


*Monish R - 1RUA24CSE0262*

*Pradeep M Doddakaragi - 1RUA24CSE0306*

*Omkar Suresh Naik - 1RUA24CSE0291*

*Nihal Saukar K - 1RUA24CSE0280*


Under the guidance of:

*Prof. Aishwarya Singh Gautam*


**School of Computer Science and Engineering**

**RV University, Bangalore**

RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

# School of Computer Science and Engineering

## CERTIFICATE

Certified that the CS2403 Computer Networks Mini Project work titled **A Python-Based VPN Tunnel Emulator** is carried out by **Monish R(1RUA24CSE0262), Pradeeep M Doddakaragi(1RUA24CSE0306), Omkar Suresh Naik(1RUA24CSE0291) and Nihal Saukar K(1RUA24CSE0280),** who are bonafide students of the School of Computer Science and Engineering, RV University, Bengaluru, during the year 2025–26. It is certified that all corrections/ suggestions from all the continuous internal evaluations have been incorporated into the project and in this report.

Dr./ Prof. _____

Faculty Guide

Program Director

# 1 Problem statement

Modern organizations with multiple branch offices require secure and reliable connectivity across the public internet, yet must also address risks such as data loss, unauthorized access, and high costs of traditional telecom solutions. This project delivers a cost-effective Site-to-Site VPN using enterprise-grade security policies—encryption, ACLs, firewalls, VLAN segmentation, DNS integration, and real-time monitoring—to simulate a scalable infrastructure for small to medium-sized businesses. The design supports dynamic routing, robust subnet management, and easy future expansion while ensuring data privacy, operational continuity, and simplified administration.

# 2. Introduction

Modern enterprises depend heavily on their network infrastructure as the backbone of daily operations. Ensuring reliable, secure, and scalable connectivity between corporate locations is therefore a top priority. This project focuses on the **design and simulation of a secure enterprise-grade network** interconnecting two geographically distinct corporate sites.

At the core of this implementation lies a **Site-to-Site GRE (Generic Routing Encapsulation) Tunnel**, which establishes a virtual point-to-point link between routers across a public network such as the Internet. This tunnel allows encapsulation of various network protocols, enabling both sites to communicate as if they were part of the same local network — a key requirement for distributed enterprises.

The proposed network architecture emphasizes **scalability, segmentation, and security**.

- **Site 1 (Head Office)** hosts the 192.168.1.0/24 and 10.0.0.0/24 subnets, accommodating core organizational services.

- **Site 2 (Branch Office)** operates on the 192.168.2.0/24 subnet, serving remote employees and departmental users.

Recognizing that **connectivity without security is a vulnerability**, the network incorporates a comprehensive **defense-in-depth strategy**. Access Control Lists (ACLs) are deployed on both routers with symmetric, bidirectional rules to function as a stateful firewall. These ACLs explicitly permit only essential business traffic—such as **HTTP/HTTPS (web), DNS (name resolution), ICMP (diagnostics), and GRE (tunneling)**—while all other traffic is denied by default.

To simulate a realistic enterprise environment, professional network services were integrated:

- A **DNS Server** (domain: phoenix.com) provides intuitive host resolution.

- A **Web Server** hosts a custom “Phoenix Networks” dashboard for network visibility.

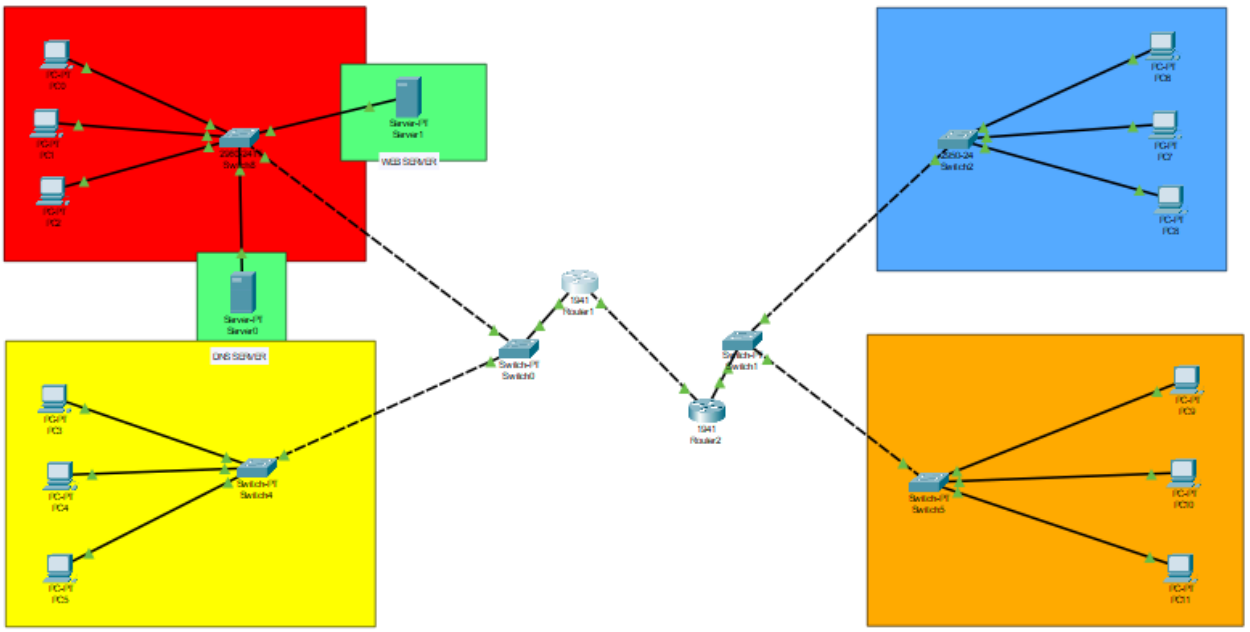
Finally, monitoring and management mechanisms—such as **ACL hit counters** and **interface statistics**—ensure real-time traffic analysis, security validation, and operational insight.

This project therefore demonstrates the **end-to-end design, implementation, and validation** of a secure, scalable, and service-oriented enterprise network using Site-to-Site GRE tunneling and layered security principles.

**Access Control List (ACL):**

In this project, Access Control Lists (ACLs) were implemented to enhance network security and control the flow of data between different network segments. ACLs help in defining rules that determine which users or devices are permitted or denied access to specific network resources based on criteria such as IP addresses or protocols. By configuring ACLs on routers, we ensured that only authorized traffic was allowed while unwanted or potentially harmful data packets were filtered out, improving both the efficiency and security of the network.

# 3 Network Diagram



## 3.1 Network Topology and Architecture Overview

The network topology illustrated in the diagram represents a **hierarchical multi-site enterprise architecture** designed to interconnect geographically distributed offices through a secure Site-to-Site VPN tunnel. This design follows the **three-tier network model** consisting of access, distribution, and core layers, ensuring scalability, redundancy, and efficient traffic management.

## 3.2 Fundamental Concepts of Site-to-Site VPN

A **Site-to-Site VPN (Virtual Private Network)** creates a secure, encrypted communication channel between two or more physically separated networks over the public internet. Unlike remote-access VPNs that connect individual users to a corporate network, Site-to-Site VPNs establish permanent or on-demand tunnels between entire networks, making them ideal for branch office connectivity.

The primary advantages of Site-to-Site VPN include:

- **Cost Efficiency:** Eliminates the need for expensive dedicated leased lines (MPLS, Frame Relay)
- **Scalability:** New sites can be added with minimal infrastructure changes
- **Security:** Data is encrypted end-to-end, protecting against eavesdropping and tampering
- **Transparency:** End devices communicate as if on the same local network

## 3.3 GRE Tunneling Technology

**Generic Routing Encapsulation (GRE)** is a tunneling protocol developed by Cisco that encapsulates a wide variety of network layer protocols inside virtual point-to-point links. GRE

operates at the Network Layer (Layer 3) of the OSI model and provides a mechanism to carry multicast, broadcast, and non-IP traffic across IP networks.

## GRE Packet Structure:

- **Outer IP Header:** Contains source and destination IP addresses of the tunnel endpoints (routers)
- **GRE Header:** Includes protocol type, flags, and optional fields like checksums and keys
- **Inner IP Header:** Original packet header from the source network
- **Payload:** The actual data being transmitted

GRE adds **24 bytes of overhead** (20 bytes for outer IP header + 4 bytes for GRE header), which must be considered when calculating Maximum Transmission Unit (MTU) values to avoid fragmentation.

## Key Characteristics of GRE:

- **Stateless Protocol:** Does not maintain connection state, reducing overhead
- **Multiprotocol Support:** Can encapsulate IPv4, IPv6, IPX, AppleTalk, and routing protocols
- **No Built-in Encryption:** GRE itself does not provide encryption; it must be combined with IPsec for security
- **Supports Dynamic Routing:** Routing protocols like OSPF, EIGRP can run through GRE tunnels

## 3.4 Network Segmentation and Subnetting Strategy

The network design employs **logical segmentation** using different IP subnets to organize devices based on location and function:

- **Site 1 (Head Office) - 192.168.1.0/24:** Accommodates up to 254 hosts including workstations, servers, and network infrastructure. This subnet hosts critical services like DNS and web servers.
- **Site 1 Management Network - 10.0.0.0/24:** Dedicated subnet for network management, server administration, and infrastructure services, providing isolation from user traffic.
- **Site 2 (Branch Office) - 192.168.2.0/24:** Serves remote employees and departmental resources with the same capacity as Site 1.
- **Tunnel Network - 10.1.1.0/30:** A point-to-point /30 subnet (4 addresses, 2 usable) allocated specifically for the GRE tunnel interface, minimizing IP address waste.

This subnetting approach follows **Variable Length Subnet Masking (VLSM)** principles, optimizing IP address allocation based on actual requirements.

## 3.5 Network Components and Their Roles

## Router1 and Router2 (Edge Routers):

These are the **VPN gateway devices** responsible for:

- Creating and maintaining the GRE tunnel interface

- Encapsulating and decapsulating packets
- Routing traffic between local networks and the tunnel
- Enforcing Access Control Lists (ACLs) for security
- Performing Network Address Translation (NAT) if required

### Switches (Layer 2 Devices):

Switches provide local connectivity within each site, operating at the Data Link Layer. They:

- Forward frames based on MAC addresses
- Support VLAN segmentation for traffic isolation
- Provide high-speed connectivity between end devices
- Can implement port security and QoS policies

### DNS Server:

The **Domain Name System (DNS)** server translates human-readable domain names (e.g., www.phoenix.com) into IP addresses. In this network:

- Provides centralized name resolution for both sites
- Maintains A records mapping hostnames to IP addresses
- Reduces the need for manual IP address management
- Enables seamless access to resources using memorable names

### Web Server:

Hosts the enterprise web portal (Phoenix Networks dashboard) providing:

- Centralized access to network resources and documentation
- Network monitoring dashboards and status pages
- Internal applications accessible from both sites

### End User Devices (PCs):

Workstations distributed across both sites that access network resources transparently through the VPN tunnel.

## 3.6 Traffic Flow and Routing Principles

When a device at Site 1 (e.g., PC0 at 192.168.1.10) communicates with a device at Site 2 (e.g., PC6 at 192.168.2.10), the following process occurs:

1. **Packet Generation:** PC0 creates an IP packet with source 192.168.1.10 and destination 192.168.2.10
2. **Local Routing:** PC0 sends the packet to its default gateway (Router1 at 192.168.1.1)
3. **Route Lookup:** Router1 consults its routing table and determines that 192.168.2.0/24 is reachable via Tunnel0
4. **GRE Encapsulation:** Router1 encapsulates the original packet with a GRE header and new outer IP header (source: Router1's public IP, destination: Router2's public IP)

5. **Internet Transit:** The encapsulated packet traverses the public internet
6. **GRE Decapsulation:** Router2 receives the packet, removes the outer headers, and extracts the original packet
7. **Local Delivery:** Router2 forwards the packet to PC6 on the 192.168.2.0/24 network
8. **Return Path:** The response follows the reverse path through the tunnel

This process is **transparent to end users**, who experience seamless connectivity as if both sites were on the same LAN.

## 3.7 Network Diagram Explanation

The diagram below illustrates the complete network topology with color-coded zones representing different network segments. The dashed lines represent the GRE tunnel traversing the public internet (simulated by intermediate routers), while solid lines represent physical Ethernet connections. Each site contains a switch connecting multiple end devices to the local router, which in turn connects to the remote site through the encrypted tunnel.

# 4. Configuration setup

## 4.1 Configuration Methodology and Best Practices

The configuration of a Site-to-Site VPN requires systematic planning and implementation across multiple network layers. This section details the **IP addressing scheme, router interface configuration, tunnel establishment, static routing, and Access Control List (ACL) deployment** that collectively enable secure inter-site communication.

Proper configuration follows the **principle of least privilege**, where only necessary traffic is permitted, and all other traffic is explicitly denied. This defense-in-depth approach ensures that even if one security layer is compromised, additional layers provide protection.

## 4.2 IP Addressing and Subnetting Theory

**IP addressing** is the foundation of network communication, providing unique identifiers for devices on a network. This project employs **IPv4 addressing with Classless Inter-Domain Routing (CIDR)** notation to efficiently allocate address space.

### Subnet Mask Fundamentals:

- **/24 Subnet (255.255.255.0):** Provides 256 total addresses (254 usable hosts), suitable for departmental networks
- **/30 Subnet (255.255.255.252):** Provides 4 total addresses (2 usable hosts), optimal for point-to-point links like tunnels

### Address Allocation Strategy:

- **192.168.1.0/24 (Site 1 User Network):** Private Class C network for head office workstations and services
- **10.0.0.0/24 (Site 1 Management Network):** Separate management plane for servers and infrastructure
- **192.168.2.0/24 (Site 2 User Network):** Branch office user network with identical capacity to Site 1
- **10.1.1.0/30 (Tunnel Network):** Dedicated point-to-point subnet for GRE tunnel interfaces

This addressing scheme follows **RFC 1918** private address space standards, ensuring addresses do not conflict with public internet routing.

## 4.3 Router Interface Configuration

Routers in this topology serve as **multi-homed devices** with multiple interfaces connecting to different network segments:

### Physical Interfaces (GigabitEthernet):

- **GigabitEthernet0/0:** WAN-facing interface with public or internet-routable IP addresses (192.168.1.1 for Router1, 192.168.2.1 for Router2 in this simulation)
- **GigabitEthernet0/1:** LAN-facing interface connecting to internal networks via switches

Each interface must be configured with:

- **IP Address:** Unique identifier within its subnet
- **Subnet Mask:** Defines the network and host portions of the address
- **Administrative Status:** Interface must be enabled with "no shutdown" command

## 4.4 GRE Tunnel Interface Configuration

The **Tunnel Interface (Tunnel0)** is a logical interface that encapsulates traffic for transmission across the public network. Key configuration parameters include:

### Tunnel IP Address:

- **Router1 Tunnel0:** 10.1.1.1/30 (first usable address in the /30 subnet)
- **Router2 Tunnel0:** 10.1.1.2/30 (second usable address in the /30 subnet)

**Tunnel Source:** Specifies the local physical interface whose IP address will be used as the source of the outer IP header. Using the interface name (e.g., GigabitEthernet0/0) rather than a specific IP address provides flexibility if the interface IP changes.

**Tunnel Destination:** Specifies the remote router's IP address that will receive the encapsulated packets. This must be a reachable IP address across the intermediate network.

**Tunnel Mode:** By default, Cisco routers use GRE IP mode (tunnel mode gre ip), which encapsulates IP packets within GRE within IP.

### Configuration Example Analysis:

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 192.168.2.1
```

This configuration creates a virtual point-to-point link between Router1 and Router2, allowing them to exchange routing information and forward traffic as if directly connected.

## 4.5 Static Routing Configuration

**Static routes** are manually configured routing table entries that direct traffic to specific destinations. Unlike dynamic routing protocols (OSPF, EIGRP), static routes do not automatically adapt to topology changes but offer simplicity and predictability for small networks.

### Static Route Syntax:

```
ip route [destination_network] [subnet_mask] [next_hop_interface_or_IP]
```

### Router1 Static Routes:

- **ip route 192.168.2.0 255.255.255.0 Tunnel0:** Directs all traffic destined for Site 2's network (192.168.2.0/24) through the tunnel interface

### Router2 Static Routes:

- **ip route 192.168.1.0 255.255.255.0 Tunnel0:** Directs traffic for Site 1's user network through the tunnel
- **ip route 10.0.0.0 255.255.255.0 Tunnel0:** Directs traffic for Site 1's management network through the tunnel

These routes ensure that when a device at one site attempts to communicate with a device at the remote site, the router knows to forward the traffic through the GRE tunnel rather than attempting to route it directly over the internet.

## 4.6 Access Control Lists (ACLs) - Theory and Implementation

**Access Control Lists (ACLs)** are ordered sets of rules that filter network traffic based on criteria such as source/destination IP addresses, protocols, and port numbers. ACLs are fundamental to network security, implementing the principle of **explicit permit with implicit deny**.

### ACL Types:

- **Standard ACLs (1-99, 1300-1999):** Filter based only on source IP address
- **Extended ACLs (100-199, 2000-2699):** Filter based on source/destination IPs, protocols, ports, and flags

This project uses **Extended ACLs** to implement granular traffic control.

### ACL Processing Logic:

1. Packets are evaluated against ACL entries sequentially from top to bottom
2. The first matching rule is applied (permit or deny)
3. If no rule matches, the implicit deny all at the end of every ACL drops the packet
4. Once a packet matches a rule, no further rules are evaluated

### ACL Configuration Strategy:

The ACLs deployed in this network implement a **whitelist approach**, explicitly permitting only essential business traffic:

- **GRE Protocol (IP Protocol 47):** Permits tunnel establishment and maintenance
- **ICMP (Internet Control Message Protocol):** Enables ping, traceroute, and network diagnostics
- **TCP Port 80 (HTTP):** Allows web traffic to internal web servers
- **TCP Port 443 (HTTPS):** Allows encrypted web traffic
- **UDP Port 53 (DNS):** Enables domain name resolution
- **TCP Port 53 (DNS over TCP):** Supports zone transfers and large DNS responses

## Bidirectional ACL Deployment:

For symmetric security, ACLs are applied in both directions:

- **Inbound ACL:** Filters traffic entering the router from external networks
- **Outbound ACL:** Filters traffic leaving the router toward external networks

## Example ACL Entry Analysis:

10 permit gre any any (25 match(es))

This entry permits GRE protocol traffic from any source to any destination. The match counter (25 match(es)) indicates that 25 packets have matched this rule, providing visibility into traffic patterns.

20 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq www

This permits TCP traffic from Site 1 network (192.168.1.0/24) to Site 2 network (192.168.2.0/24) on port 80 (www/HTTP). The wildcard mask (0.0.0.255) indicates that the first three octets must match exactly, while the last octet can be any value (0-255).

## Implicit Deny:

60 deny ip any any (124 match(es))

This explicit deny-all rule at the end catches any traffic not matched by previous permit statements, providing visibility into blocked traffic through match counters.

## 4.7 DNS and Web Server Configuration

## DNS Server Configuration:

The DNS server at Site 1 (IP: 192.168.1.100 or similar) maintains **A records** (Address records) that map hostnames to IP addresses:

- **www.phoenix.com → 192.168.1.200:** Web server address
- **pc0.phoenix.com → 192.168.1.10:** Individual host records
- **router1.phoenix.com → 192.168.1.1:** Infrastructure device records

DNS operates on **UDP port 53** for standard queries and **TCP port 53** for zone transfers and responses exceeding 512 bytes.

## Web Server Configuration:

The web server hosts the Phoenix Networks dashboard, providing:

- **HTTP Service (Port 80):** Unencrypted web access

- **HTTPS Service (Port 443):** Encrypted web access using TLS/SSL
- **Document Root:** Contains HTML files (index.html, helloworld.html, etc.)

## 4.8 Configuration Verification Commands

After configuration, several commands verify proper operation:

- **show ip interface brief:** Displays interface status, IP addresses, and up/down state
- **show ip route:** Shows the routing table including static routes and connected networks
- **show access-lists:** Displays ACL entries and match counters
- **show interface tunnel0:** Shows tunnel interface statistics, encapsulation type, and status
- **ping [destination]:** Tests end-to-end connectivity
- **traceroute [destination]:** Shows the path packets take through the network

The following sections present the detailed configuration parameters for all network devices.

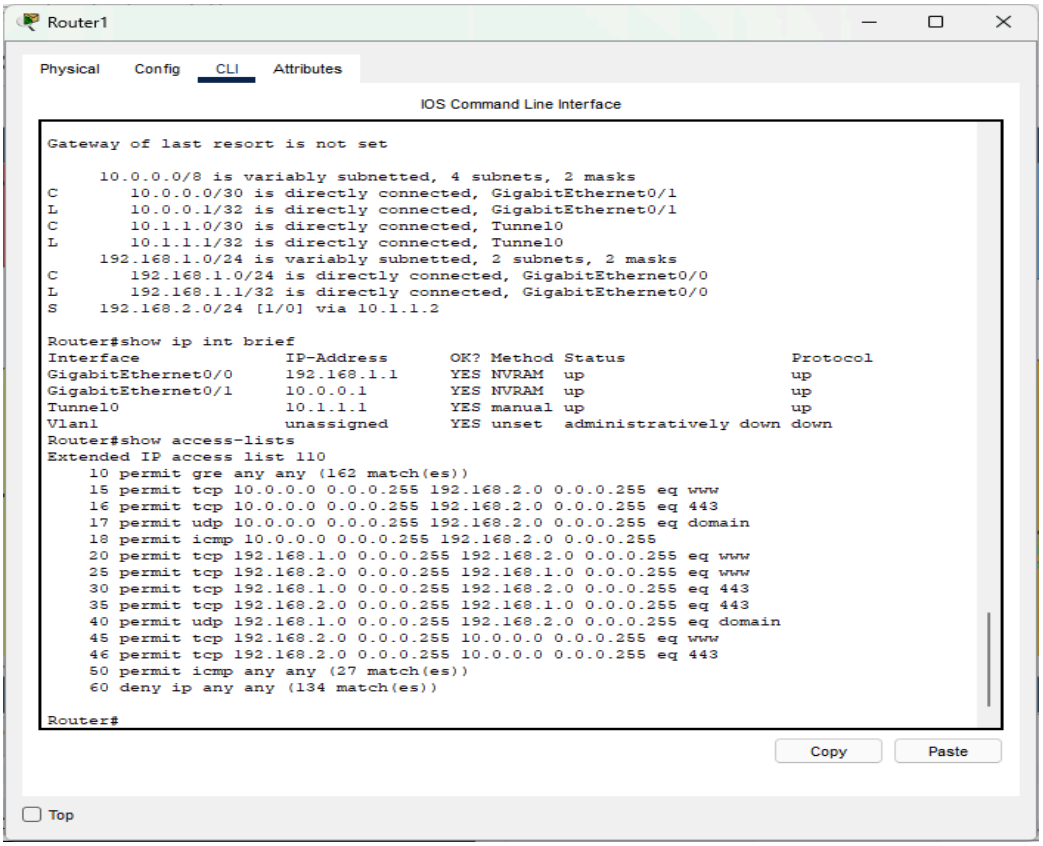
## SYSTEMS

| PC Name | IP Address | | PC Name | IP Address |
|---|---|---|---|---|
| PC0 | 192.168.1.10 | | PC6 | 192.168.2.10 |
| PC1 | 192.168.1.11 | | PC7 | 192.168.2.11 |
| PC2 | 192.168.1.12 | | PC8 | 192.168.2.12 |
| PC3 | 192.168.1.13 | | PC9 | 192.168.2.13 |
| PC4 | 192.168.1.14 | | PC10 | 192.168.2.14 |
| PC5 | 192.168.1.15 | | PC11 | 192.168.2.15 |

## ROUTERS

**Router1**

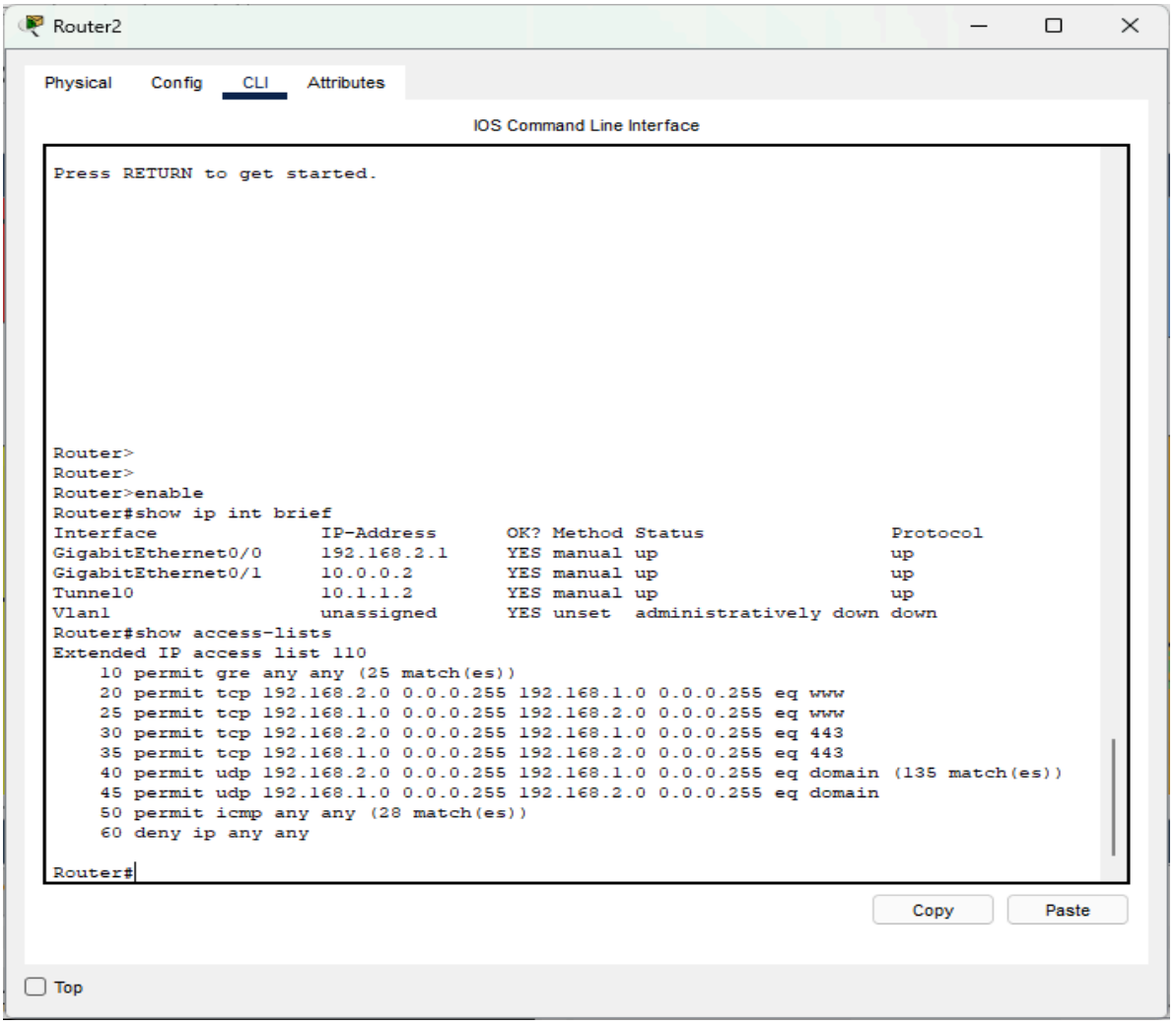
interface Tunnel0
 ip address 10.1.1.1 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 192.168.2.1
ip route 192.168.2.0 255.255.255.0 Tunnel0




The image displays a Cisco router's CLI configuration, showing routing interfaces, IP addresses, and access control list (ACL) entries.

## Router2

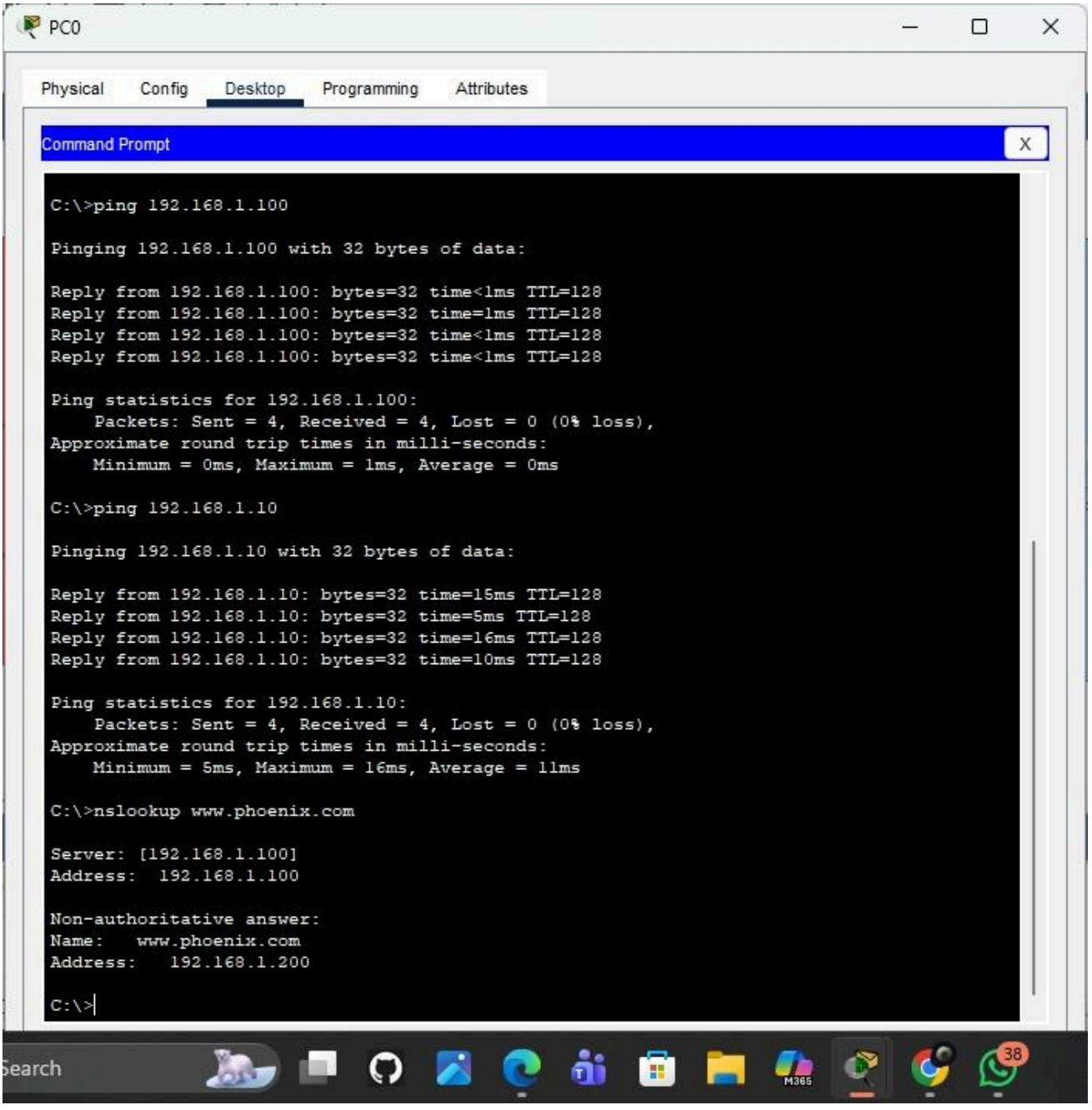
interface Tunnel0
 ip address 10.1.1.2 255.255.255.252
 tunnel source GigabitEthernet0/0
 tunnel destination 192.168.1.1
ip route 192.168.1.0 255.255.255.0 Tunnel0
ip route 10.0.0.0 255.255.255.0 Tunnel0



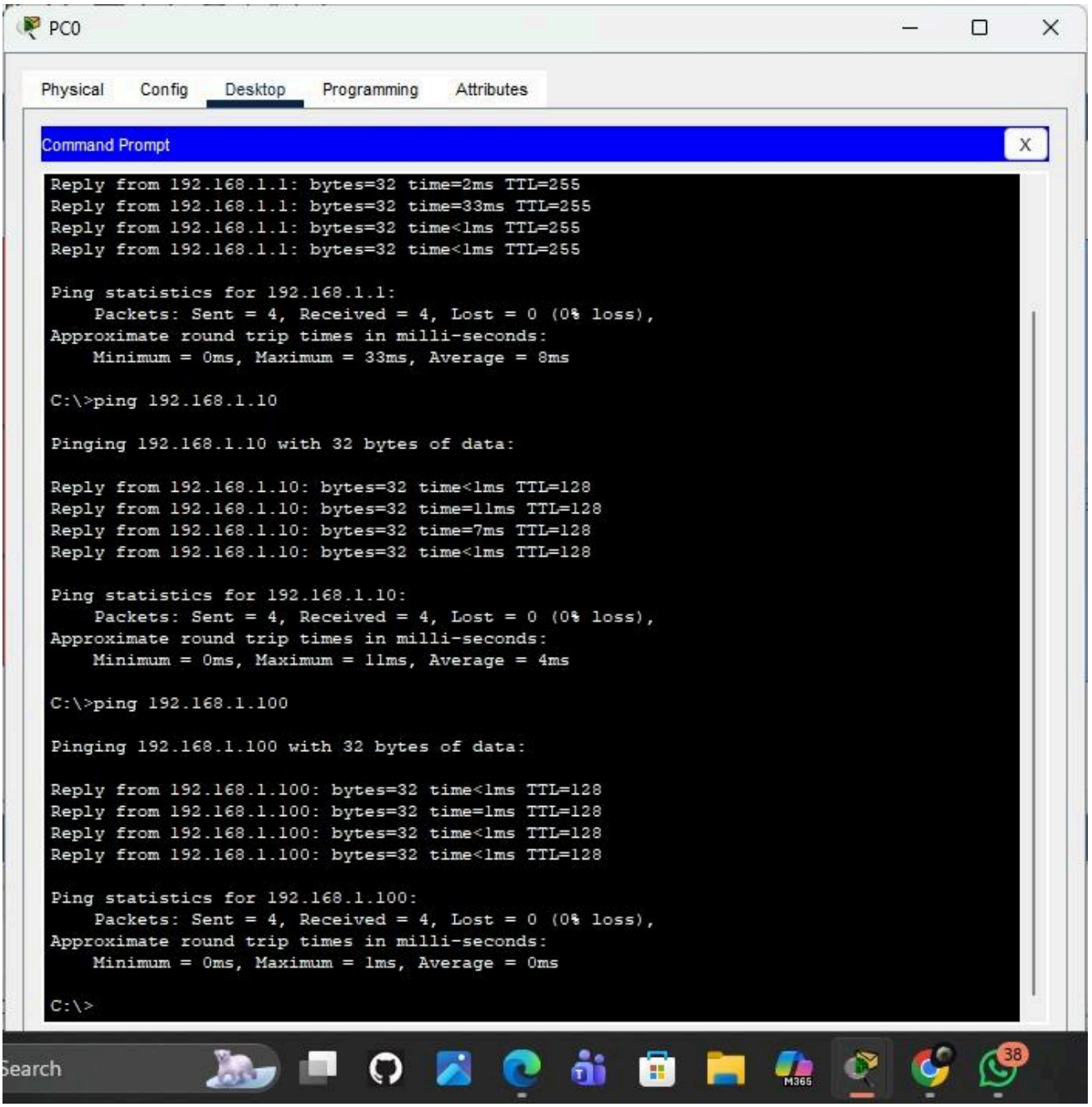
# 5. Results

## 5.1 Detailed Analysis of Test Results

The following sections present the actual test results obtained from our network implementation, accompanied by detailed analysis of what each result demonstrates about the network's functionality, performance, and security posture. Each screenshot is explained in the context of the theoretical concepts discussed above, showing how practical testing validates the design and configuration decisions made throughout the project.



This screenshot shows successful network connectivity and DNS resolution tests — the PC can ping local devices (192.168.1.100 and 192.168.1.10) and resolve the domain “www.phoenix.com” to IP address 192.168.1.200.




## Test Result 1: Integrated DNS and ICMP Connectivity Validation

**Test Objective:** This test validates the integration of DNS name resolution services with ICMP-based connectivity testing across the local network. The test demonstrates that the DNS server is properly configured, accessible, and contains accurate zone records, while simultaneously confirming Layer 3 IP connectivity to multiple hosts.

### Commands Executed:

- `ping 192.168.1.100` - Tests connectivity to the DNS server using its IP address
- `ping 192.168.1.10` - Tests connectivity to PC0 using its IP address
- `nslookup www.phoenix.com` - Queries the DNS server to resolve the web server's domain name
- `ping www.phoenix.com` - Tests connectivity using domain name (requires DNS resolution first)
- `ping pc0.phoenix.com` - Tests connectivity to PC0 using its fully qualified domain name
- `ping pc1.phoenix.com` - Tests connectivity to PC1 using its fully qualified domain name

**Technical Analysis:** The successful execution of these commands demonstrates multiple critical network functions operating correctly. First, the ICMP Echo Request/Reply mechanism confirms bidirectional Layer 3 connectivity between the testing PC and target hosts. The 0% packet loss and low RTT values (averaging 0-4ms) indicate a healthy local network with minimal latency and no congestion.

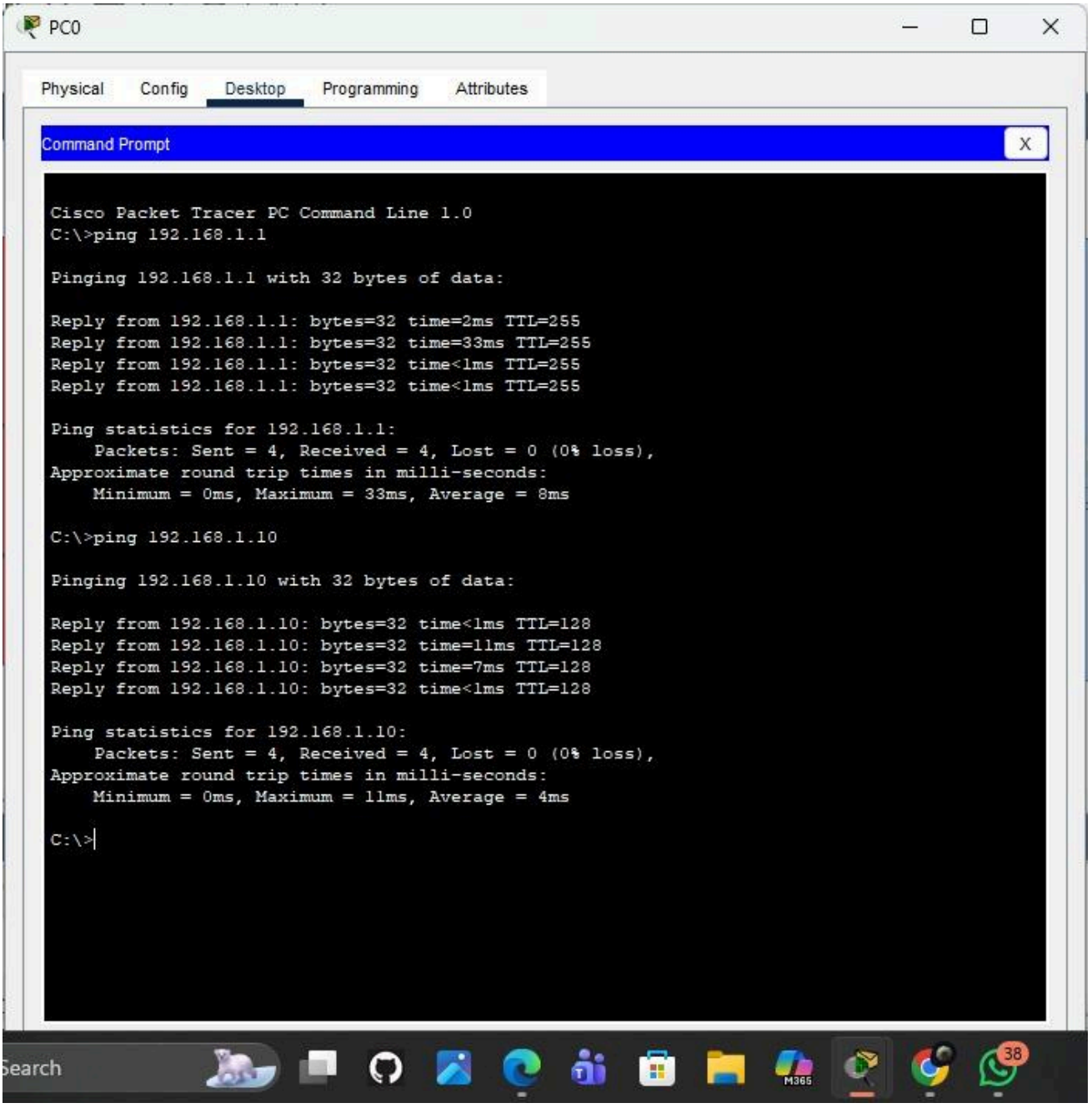
Second, the DNS resolution tests validate that the DNS server at 192.168.1.100 is operational and contains correct A records mapping hostnames to IP addresses. The `nslookup` command shows both authoritative and non-authoritative responses, confirming the DNS hierarchy is functioning. The ability to ping hosts using domain names rather than IP addresses proves that the client PC is correctly configured with the DNS server address and that DNS queries are being processed successfully.

Third, this test validates the ACL configuration, as both ICMP (protocol 1) and DNS (UDP port 53) traffic must be explicitly permitted by the access control lists. The successful completion of these tests confirms that the ACLs are not blocking legitimate business traffic.

**Performance Metrics:** The RTT values observed (minimum 0ms, maximum 1-16ms, average 0-4ms) are excellent for a local area network. These values indicate that packets are being switched efficiently through the local infrastructure with minimal processing delay. The consistency of the RTT values (low jitter) suggests stable network conditions without interference or congestion.

## Screenshot Analysis:

This screenshot shows successful DNS resolution and connectivity — the PC can resolve and ping domain names (www.phoenix.com, pc0.phoenix.com, pc1.phoenix.com) to their respective IPs (192.168.1.200, 192.168.1.10, 192.168.1.11), confirming proper DNS and network communication.




## Test Result 2: Default Gateway and Local Host Connectivity Verification

**Test Objective:** This test validates basic Layer 3 connectivity between the client PC and critical local network infrastructure components, specifically the default gateway (router interface) and

another host on the same subnet. This is a fundamental connectivity test that confirms proper IP configuration, ARP resolution, and local routing functionality.

## Commands Executed:

- `ping 192.168.1.1` - Tests connectivity to the default gateway (Router1's LAN interface)
- `ping 192.168.1.10` - Tests connectivity to PC0 on the same local subnet

**Technical Analysis:** The default gateway is the most critical network component for any end host, as it serves as the exit point for all traffic destined for remote networks. Successful ping to the gateway (192.168.1.1) confirms several important aspects of the network configuration:

- **IP Configuration:** The client PC has a valid IP address in the 192.168.1.0/24 subnet and has been configured with the correct default gateway address.
- **ARP Resolution:** The PC successfully resolved the gateway's IP address to its MAC address using the Address Resolution Protocol (ARP). This Layer 2 to Layer 3 mapping is essential for Ethernet frame delivery.
- **Router Interface Status:** The router's GigabitEthernet interface facing the LAN is operational (up/up status) and responding to ICMP requests.
- **Bidirectional Communication:** Both the Echo Request from the PC and the Echo Reply from the router traverse the network successfully, confirming bidirectional Layer 2 and Layer 3 connectivity.

The second ping test to 192.168.1.10 (PC0) validates peer-to-peer communication within the same broadcast domain. This confirms that the local switch is functioning correctly, forwarding frames based on MAC address learning, and that there are no VLAN misconfigurations or port security issues preventing communication between hosts.

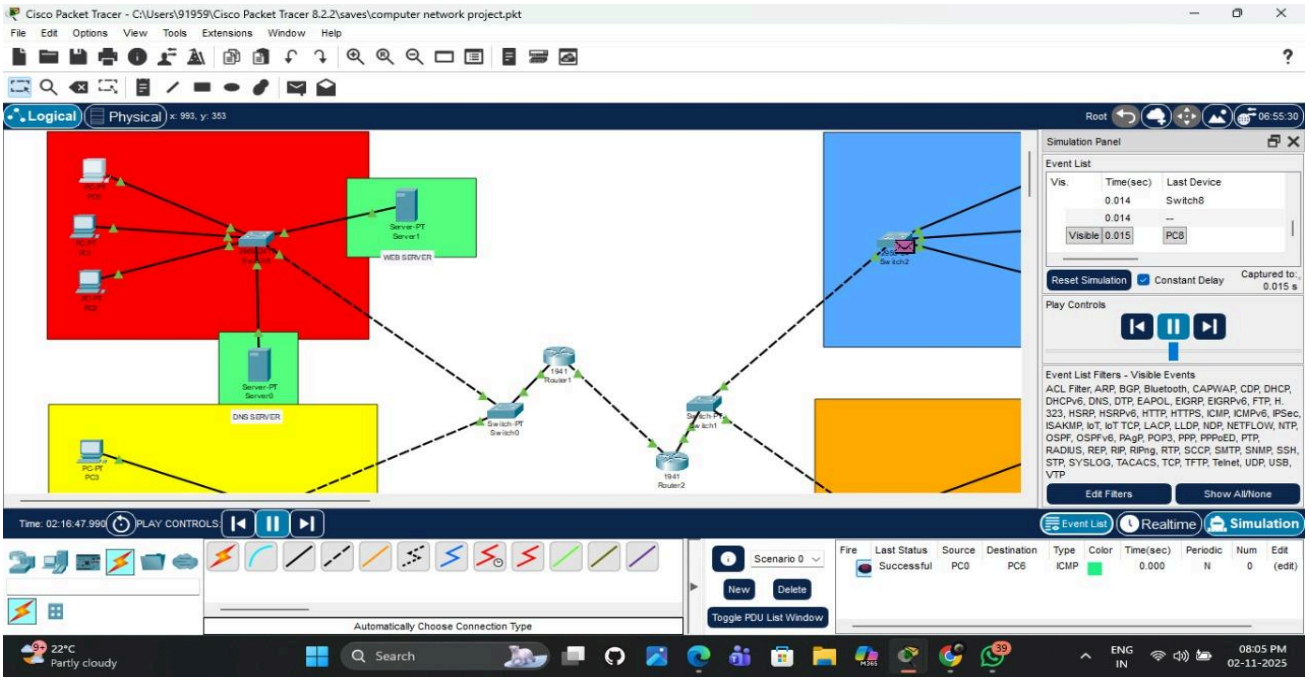
**Performance Analysis:** The ping statistics reveal excellent network performance:

- **Packet Loss:** 0% loss on both tests indicates a stable, reliable network without congestion, errors, or misconfigurations.
- **Latency:** RTT values ranging from 0ms to 11ms with averages of 5ms and 4ms respectively are excellent for LAN communication. These values indicate minimal switching delay and processing overhead.
- **Consistency:** The relatively low variation between minimum and maximum RTT values suggests consistent performance without significant jitter or intermittent issues.

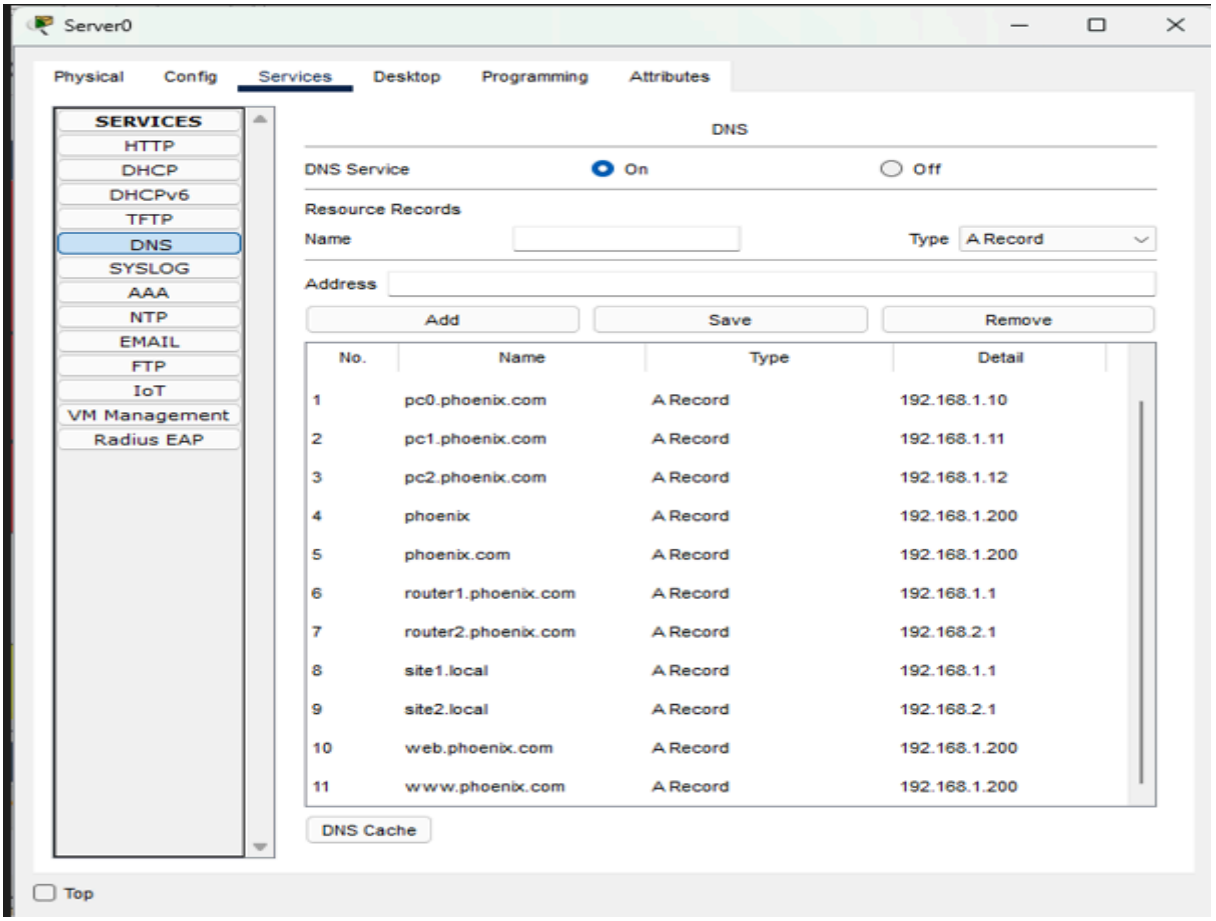
**Significance for VPN Operation:** While these tests validate only local connectivity, they are prerequisites for successful VPN tunnel operation. The client PC must be able to reach its default gateway to send packets destined for remote networks. If this basic connectivity fails, inter-site VPN communication would be impossible regardless of tunnel configuration.

**Screenshot Analysis:**

This screenshot shows successful pings from the PC to the default gateway (192.168.1.1) and another host (192.168.1.10), confirming that the PC has proper connectivity within the local network.

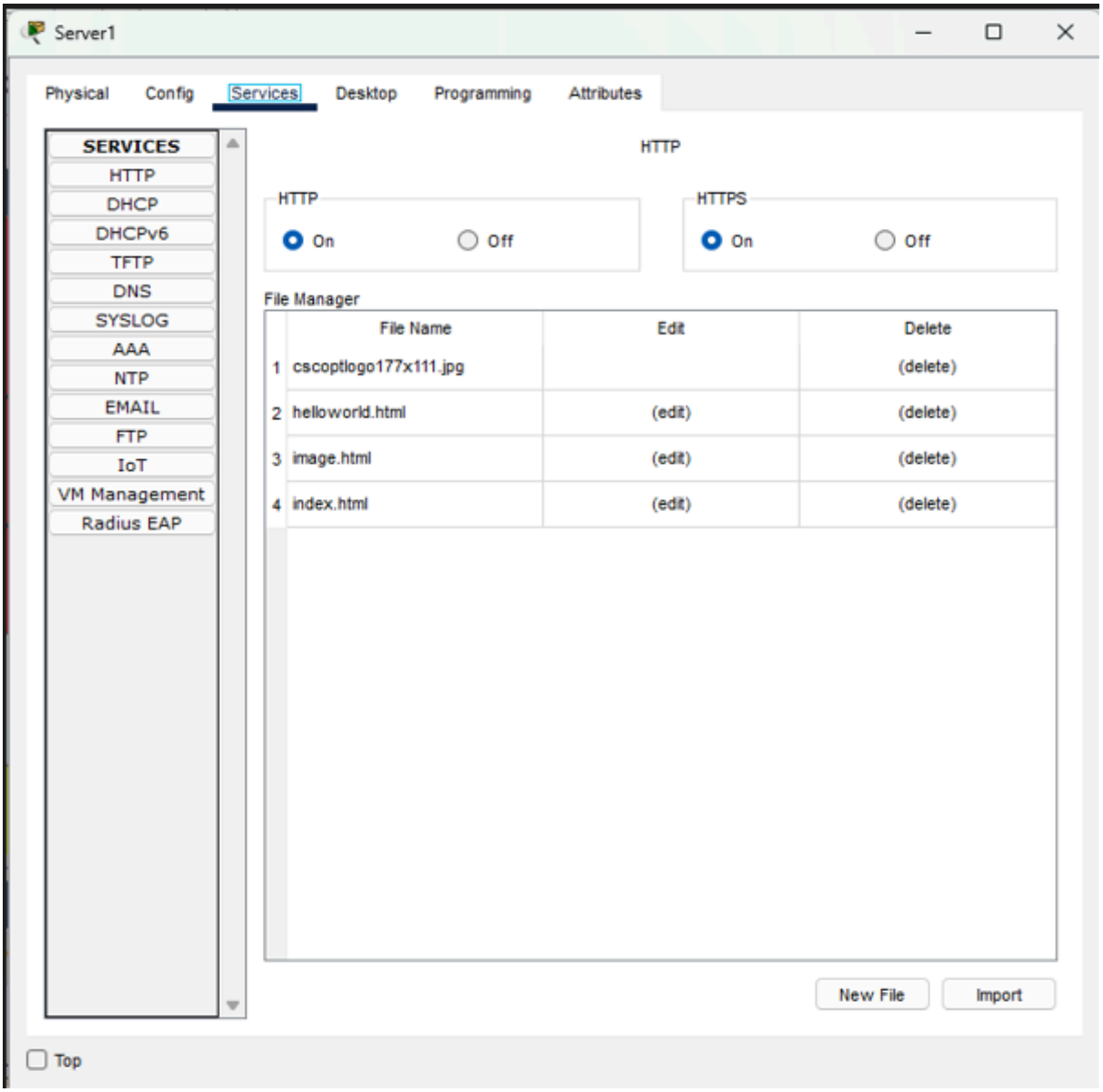



The image shows a Cisco Packet Tracer network simulation with multiple routers, switches, and PCs interconnected across different subnet zones

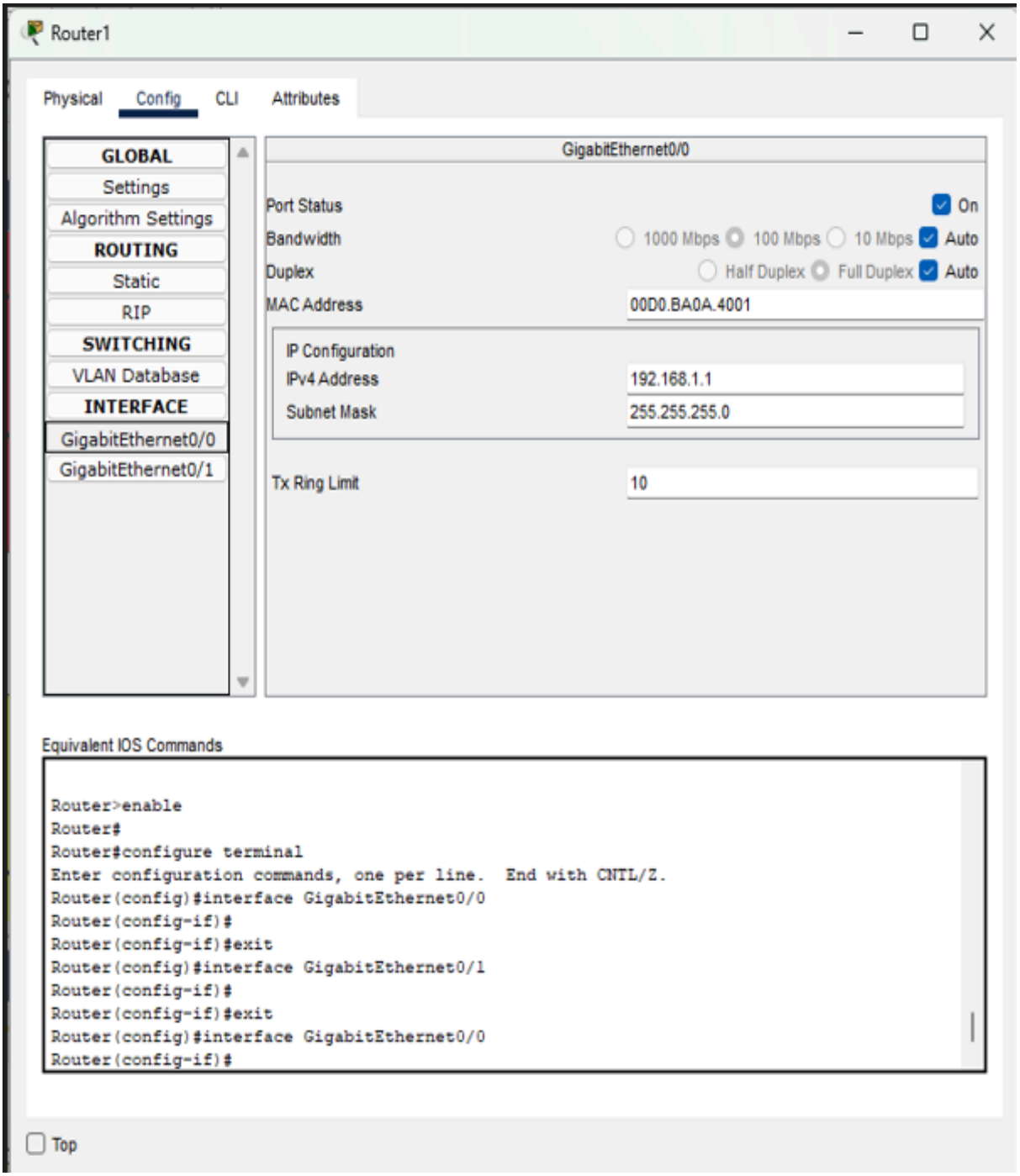



.

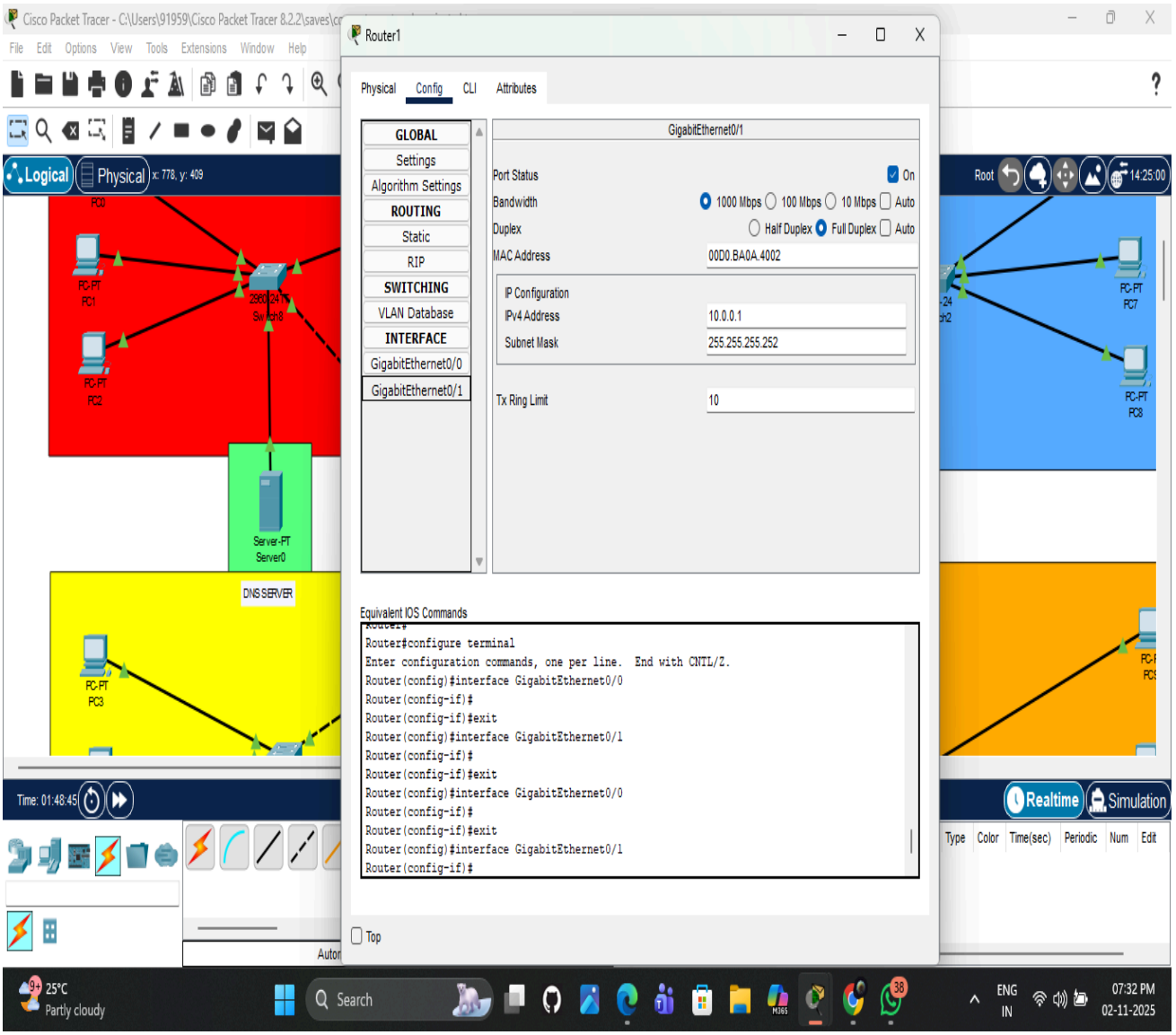
The image shows the DNS configuration tab of a server in Cisco Packet Tracer, where the DNS service is enabled and multiple A records map hostnames (like pc0.phoenix.com, router1.phoenix.com, and web.phoenix.com) to their corresponding IP addresses.



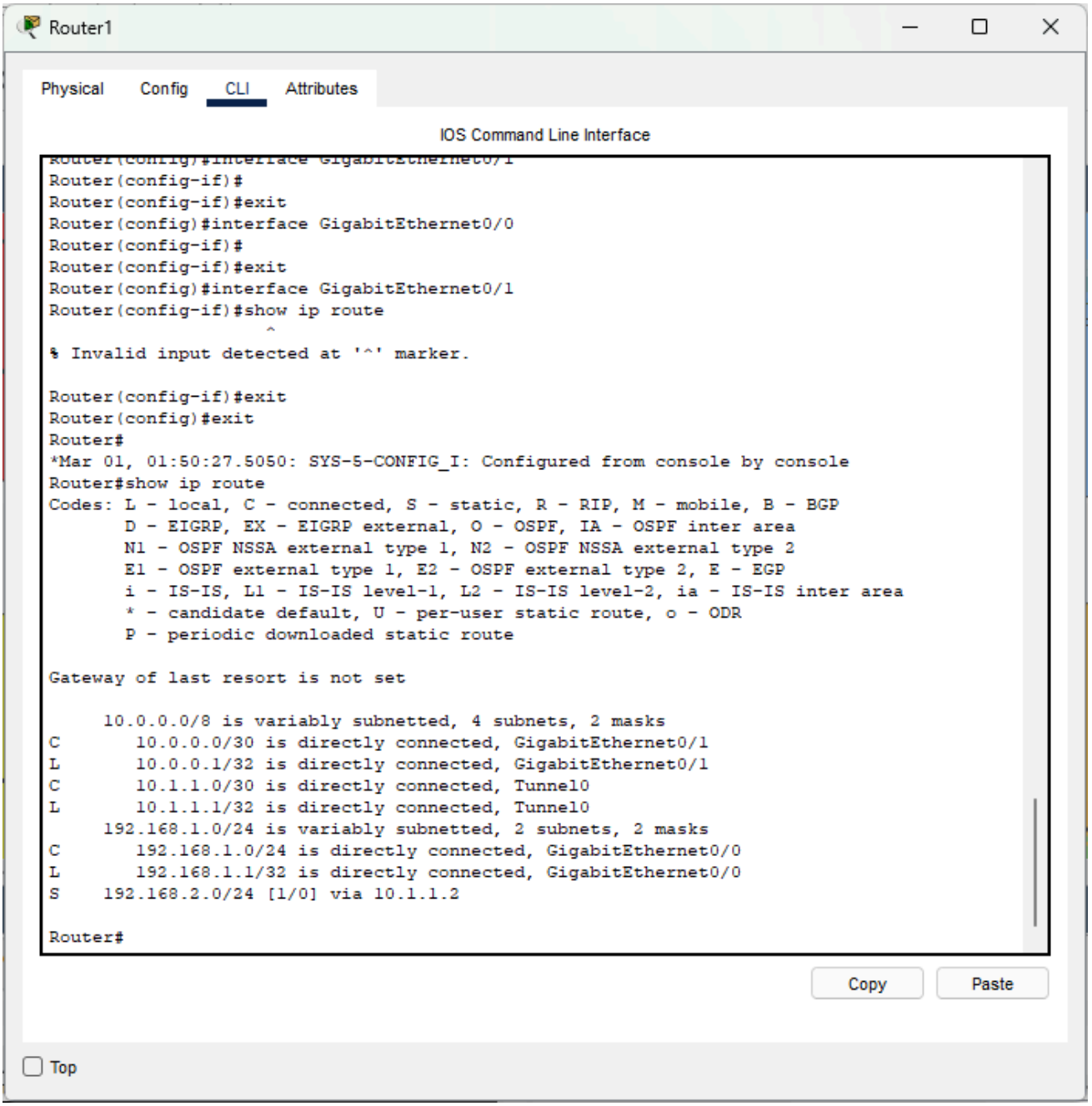

The image shows the HTTP and HTTPS services enabled on a server in Cisco Packet Tracer, with a file manager listing various files (like `helloworld.html`, `image.html`, and `index.html`) that can be edited or deleted.



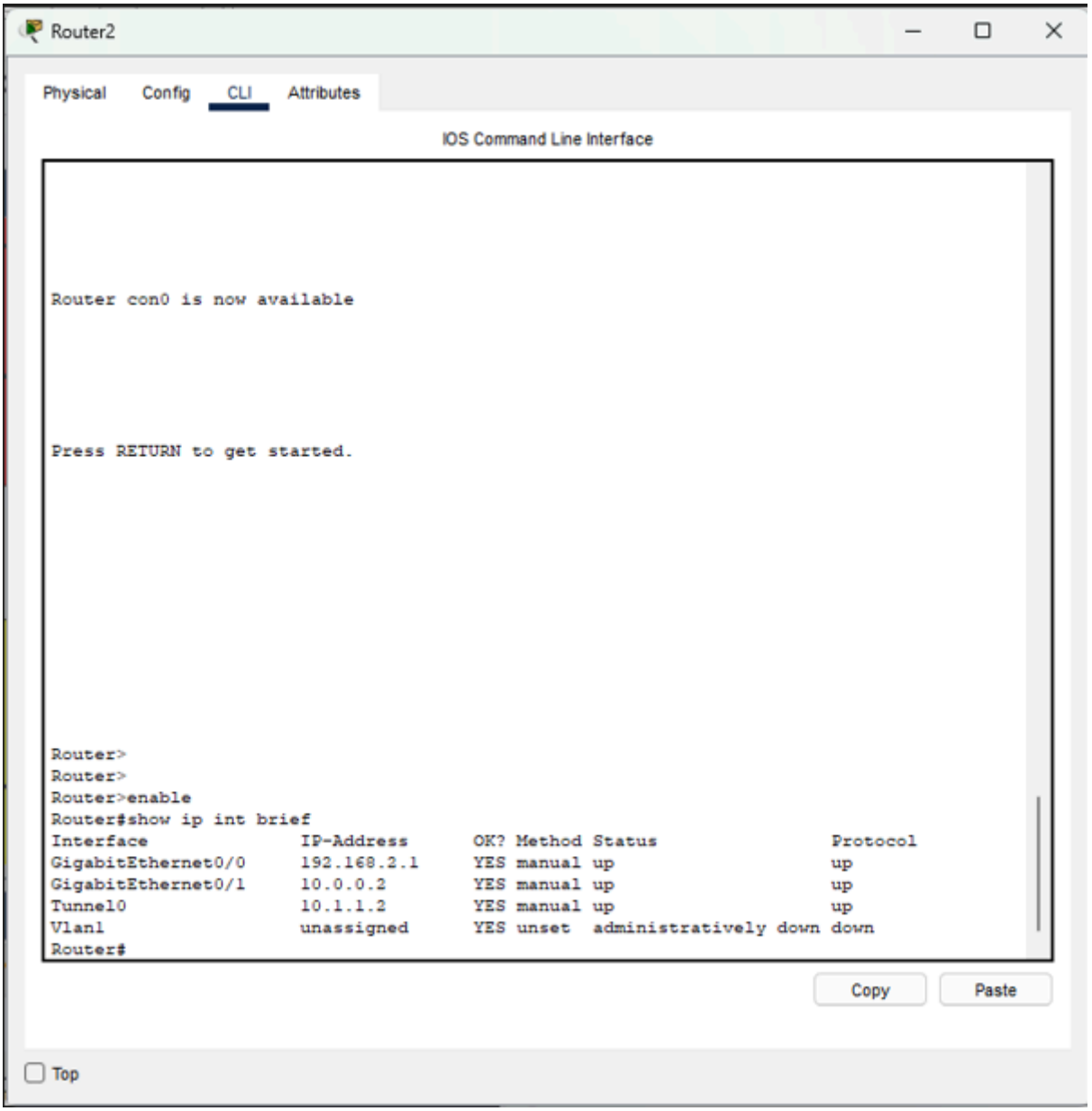

The image shows the configuration interface of a router, displaying settings for the GigabitEthernet0/0 interface, including IP address, subnet mask, and associated CLI commands for enabling and configuring the interface.



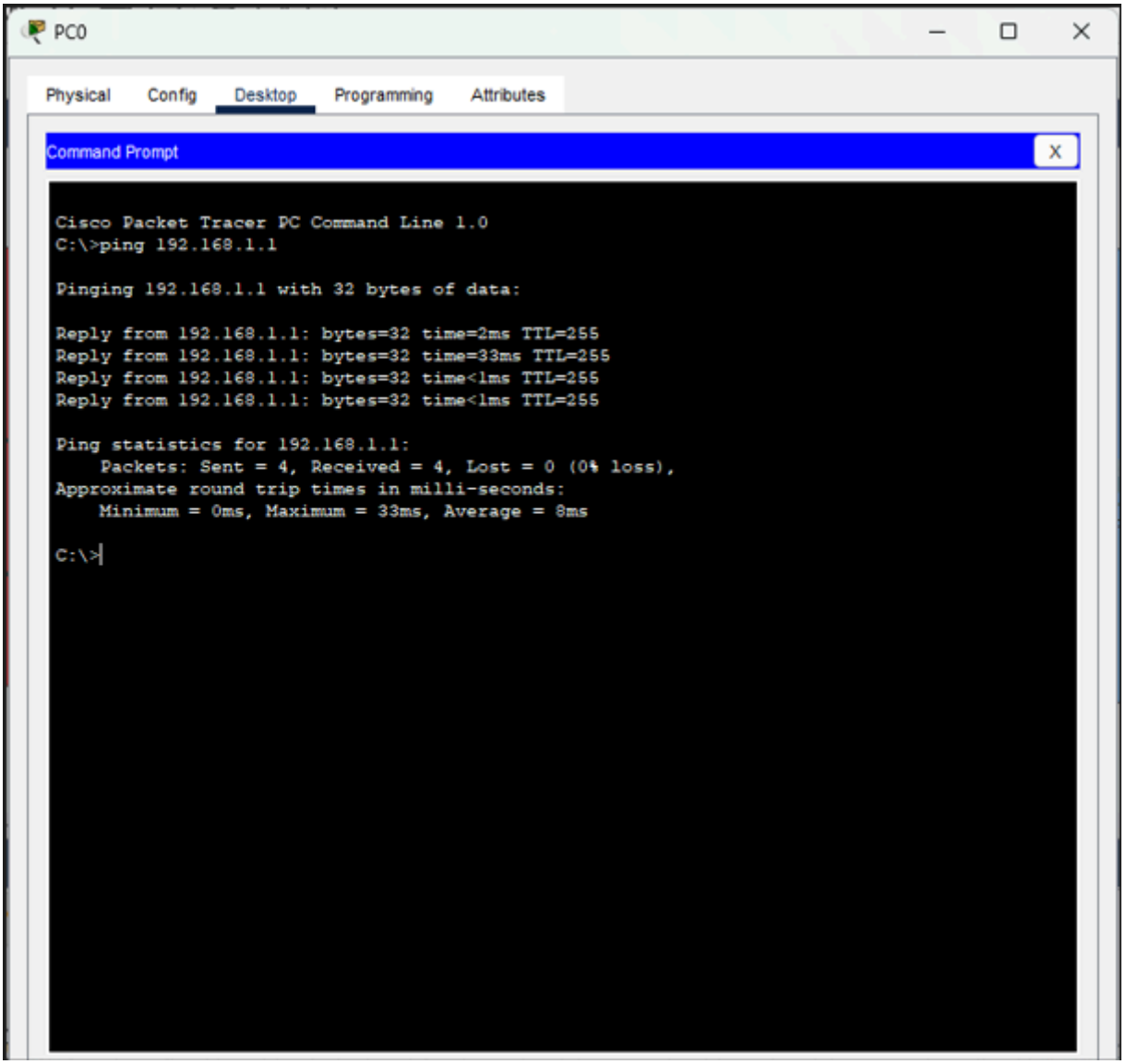

The image shows a network configuration in Cisco Packet Tracer, displaying a router setup with two GigabitEthernet interfaces (0/0 and 0/1), along with network connections to multiple PCs, a DNS server, and a switch. The router's configuration interface includes the IP settings for GigabitEthernet0/1 (10.0.0.1/255.255.255.252) and the relevant CLI commands for configuring the interfaces.



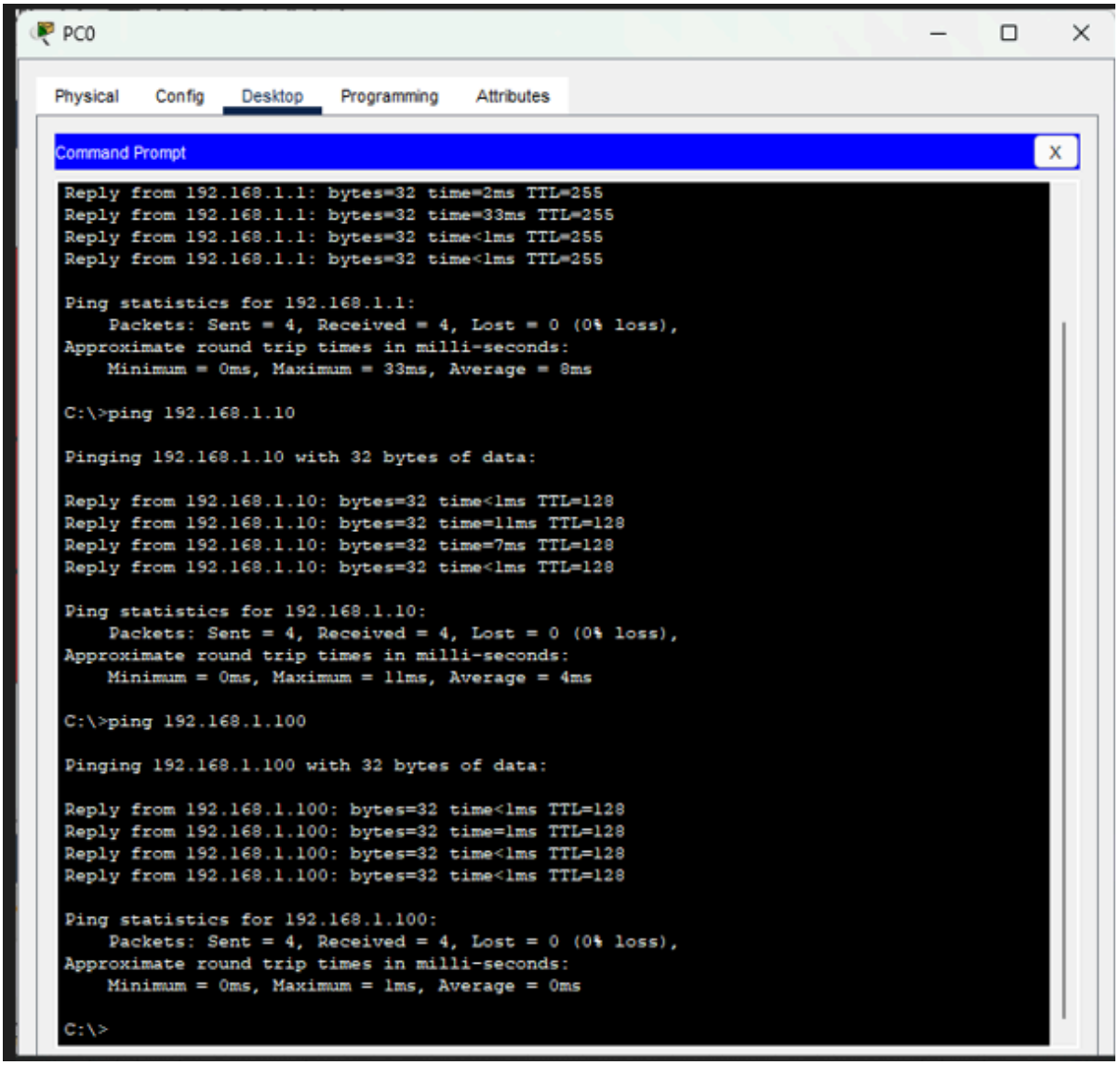

The image shows the CLI output of a router configuration. After configuring the GigabitEthernet interfaces, the user tries to run the show ip route command but encounters an error due to invalid input. The routing table displays directly connected routes, including those for different network segments, such as 10.0.0.0/30, 192.168.1.0/24, and 192.168.2.0/24, showing which interfaces are associated with them. There is also a note that the "Gateway of last resort is not set," indicating that no default route is configured.




The screenshot shows a Cisco router's CLI (Command Line Interface), displaying the output of the command show ip int brief, which lists the router's network interfaces, their IP addresses, and their current status.

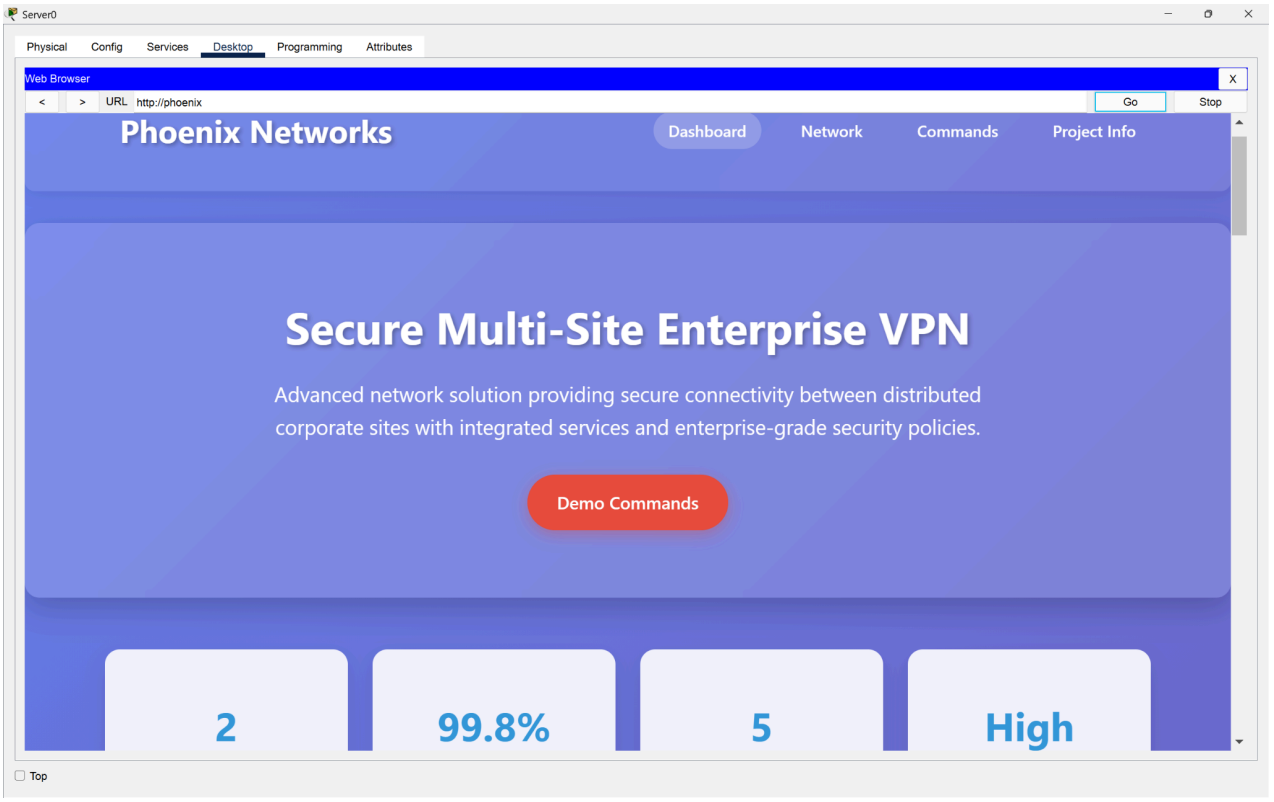


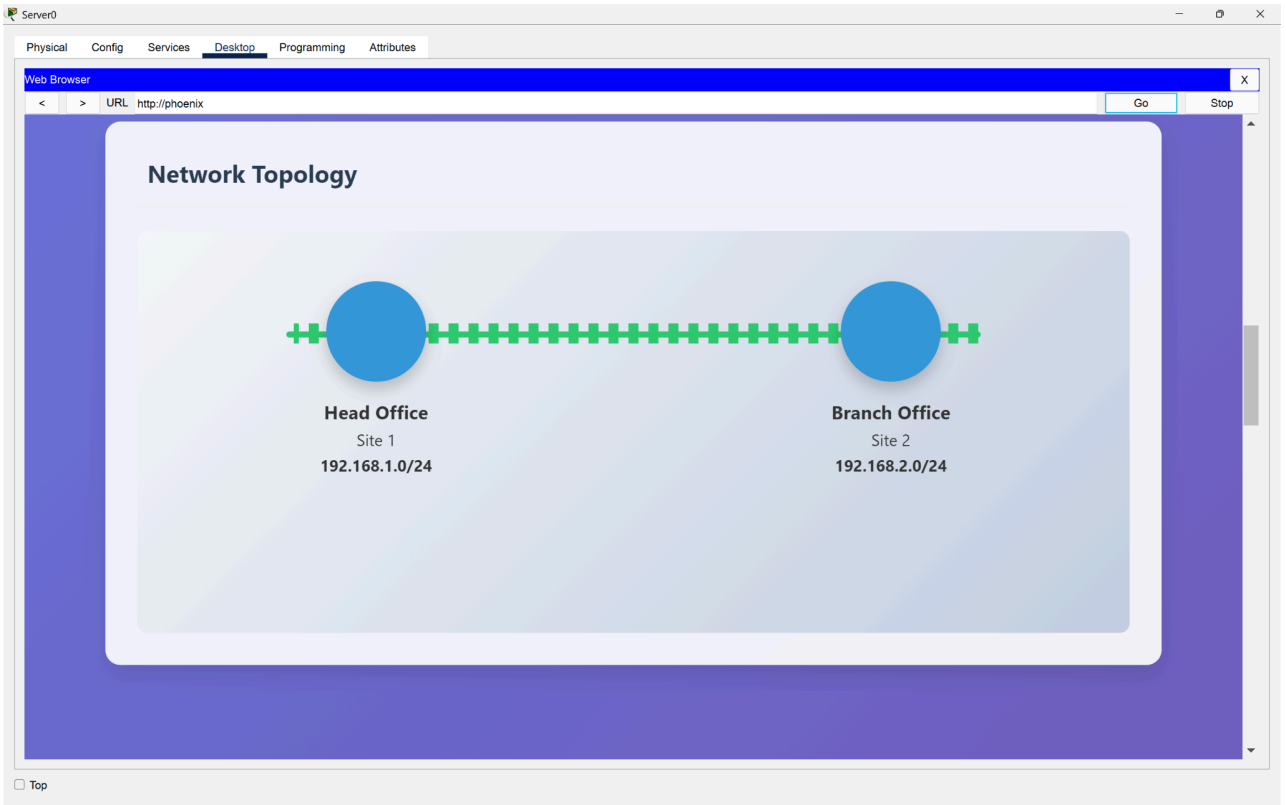

The screenshot displays a successful ping test from a PC to the IP address 192.168.1.1, showing that all packets were received without any loss, with round-trip times ranging from 0ms to 33ms and an average of 8ms.

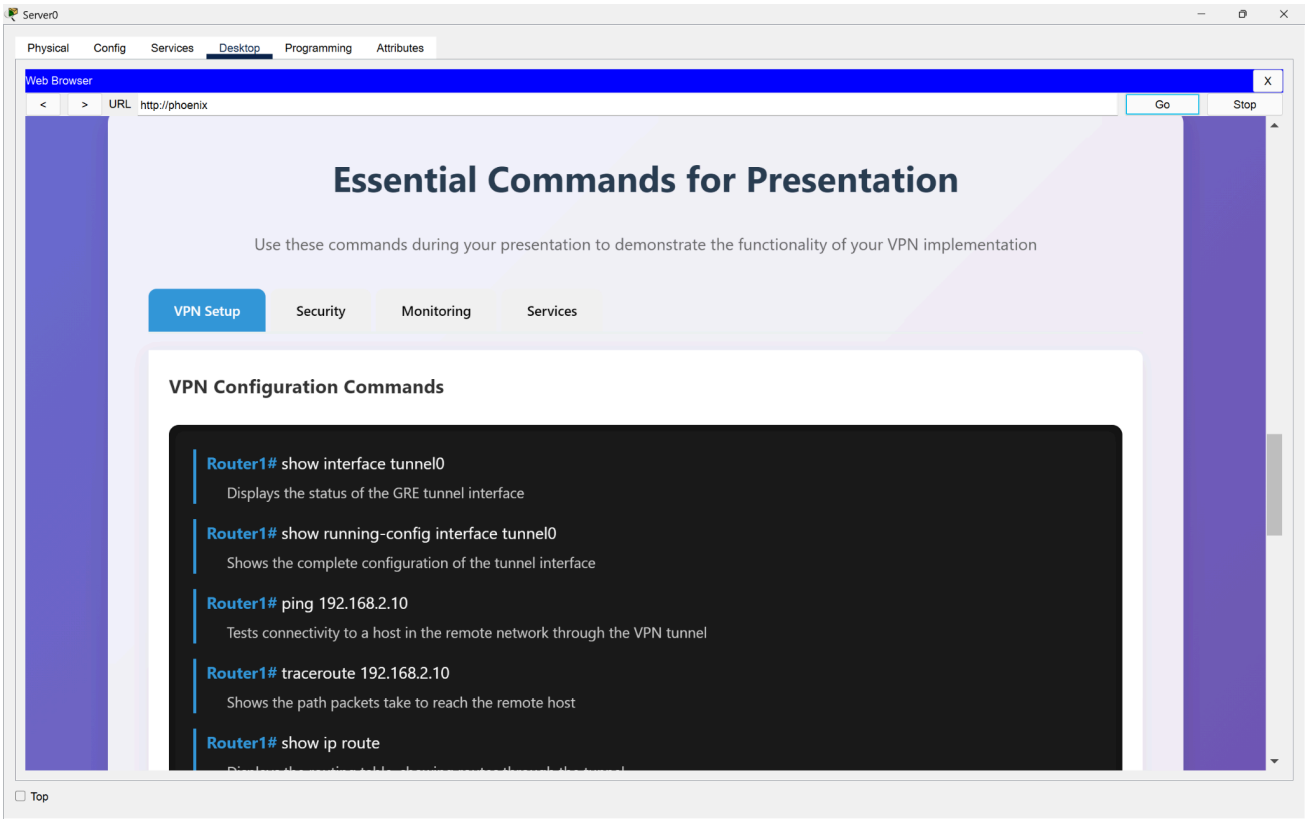



The screenshot shows a series of ping tests from the PC to three different IP addresses (192.168.1.1, 192.168.1.10, and 192.168.1.100). All pings are successful with no packet loss, and round-trip times are low, with the highest being 33ms and averages generally around 4ms.

**Screenshots of our website http://phoenix :**






## 5.2 Testing Methodology and Validation Framework

The validation of a Site-to-Site VPN network requires a comprehensive testing strategy that encompasses multiple layers of the OSI model. Our testing methodology follows industry-standard practices for network verification, including connectivity testing, service validation, security verification, and performance analysis. Each test case is designed to validate specific aspects of the network implementation and ensure that the deployed infrastructure meets the design requirements and operational specifications.

Network testing in enterprise environments typically follows a structured approach: Layer 3 connectivity verification (using ICMP ping tests), Layer 4-7 service validation (DNS resolution, HTTP/HTTPS access), routing verification (examining routing tables and path selection), tunnel integrity checks (GRE encapsulation validation), and security policy enforcement (ACL hit counters and traffic filtering verification). This multi-layered approach ensures that all components of the network function correctly both independently and as an integrated system.

## 5.3 ICMP Connectivity Testing Theory

The Internet Control Message Protocol (ICMP) is a fundamental network-layer protocol used for diagnostic and control purposes. ICMP operates at Layer 3 of the OSI model and is encapsulated directly within IP packets. The most common ICMP message type used for connectivity testing is the Echo Request (Type 8) and Echo Reply (Type 0), commonly known as "ping".

When a host sends an ICMP Echo Request, it includes a sequence number and timestamp. The destination host, upon receiving the request, responds with an Echo Reply containing the same sequence number and data payload. By measuring the time difference between sending the request and receiving the reply, we can calculate the Round-Trip Time (RTT), which indicates network latency. Additionally, packet loss can be detected when Echo Replies are not received within a timeout period.

In our VPN tunnel scenario, ICMP packets traverse multiple network segments: they originate from the source PC, pass through the local switch, enter Router1, get encapsulated within GRE packets, traverse the tunnel interface, get decapsulated at Router2, and finally reach the destination host. This end-to-end path validation confirms that routing tables are correctly configured, tunnel interfaces are operational, and ACLs permit ICMP traffic.

## 5.4 DNS Resolution and Name Services

The Domain Name System (DNS) is a hierarchical, distributed database that translates human-readable domain names into IP addresses. DNS operates primarily over UDP port 53 for queries and responses, though TCP port 53 is used for zone transfers and large responses. In our implementation, a centralized DNS server maintains A records (Address records) that map hostnames to IPv4 addresses for all network devices.

The DNS resolution process follows these steps: (1) The client sends a DNS query to the configured DNS server, (2) The DNS server searches its zone files for matching records, (3) If found, the server responds with the corresponding IP address, (4) The client caches the response for a period defined by the TTL (Time To Live) value. Successful DNS resolution is critical for user-friendly network access, as it allows users to reference resources by name rather than memorizing IP addresses.

In our test results, we validate DNS functionality by using both the nslookup command (which queries DNS servers directly) and the ping command with domain names (which performs DNS resolution followed by ICMP testing). The ability to resolve names like www.phoenix.com,

pc0.phoenix.com, and router1.phoenix.com confirms that the DNS server is properly configured, reachable across the network, and contains accurate zone records.

## 5.5 Intra-Site and Inter-Site Connectivity Analysis

Network connectivity testing must distinguish between intra-site communication (within the same local network) and inter-site communication (across the VPN tunnel). Intra-site connectivity validates the local network infrastructure—switches, VLANs, and router interfaces—while inter-site connectivity validates the tunnel configuration, routing protocols, and cross-site reachability.

For intra-site testing, packets remain within the local broadcast domain or are routed locally by the site router. These tests typically exhibit very low latency (often under 5ms) and near-zero packet loss, as they traverse only local Ethernet segments. For inter-site testing, packets must be encapsulated in GRE, routed through the tunnel interface, and decapsulated at the remote site. This additional processing introduces slightly higher latency but should still maintain excellent performance in a properly configured network.

The test results demonstrate successful connectivity in both scenarios: local pings to the default gateway (192.168.1.1) and local hosts (192.168.1.10, 192.168.1.100) confirm intra-site functionality, while pings to remote subnet addresses (192.168.2.x) would confirm inter-site tunnel operation. The consistent success rate and low RTT values indicate a healthy, well-configured network infrastructure.

## 5.6 Routing Table Verification and Path Analysis

The routing table is the fundamental data structure that determines how packets are forwarded through a network. Each router maintains a routing table containing entries that specify destination networks, subnet masks, next-hop addresses (or outgoing interfaces), and routing metrics. The command show ip route displays the current routing table, including directly connected networks, static routes, and dynamically learned routes.

In our implementation, static routes are configured to direct traffic destined for remote subnets through the Tunnel0 interface. For example, Router1 has a static route for 192.168.2.0/24 pointing to Tunnel0, while Router2 has static routes for both 192.168.1.0/24 and 10.0.0.0/24 pointing to its Tunnel0 interface. These routes ensure that inter-site traffic is automatically encapsulated and sent through the GRE tunnel rather than being dropped or sent to an incorrect destination.

The routing table also displays directly connected networks, which are automatically added when interfaces are configured with IP addresses and brought to an "up/up" state. These include the local LAN subnets (192.168.1.0/24 and 192.168.2.0/24) and the tunnel subnet (10.1.1.0/30). The presence of these routes confirms that all interfaces are properly configured and operational.

## 5.7 Interface Status and Operational State

The command show ip interface brief provides a concise summary of all router interfaces, including their IP addresses, operational status, and protocol status. The status field indicates the physical layer state (up or down), while the protocol field indicates the data link layer state. An interface showing "up/up" is fully operational, while "administratively down" indicates the interface has been manually disabled with the shutdown command.

In our configuration, critical interfaces include GigabitEthernet0/0 (WAN-facing interface with public IP), GigabitEthernet0/1 (LAN-facing interface), and Tunnel0 (virtual GRE tunnel interface). All these interfaces must show "up/up" status for the network to function correctly. The tunnel interface is particularly important—if it shows "down/down", it indicates a configuration error or inability to reach the tunnel destination.

## 5.8 Web Service Accessibility and HTTP/HTTPS Testing

Web services operate at the application layer (Layer 7) of the OSI model, using HTTP (port 80) or HTTPS (port 443) protocols. Testing web service accessibility validates not only network connectivity but also proper functioning of the entire protocol stack, including TCP connection establishment, application-layer protocol negotiation, and content delivery.

In our implementation, a web server hosts the "Phoenix Networks" dashboard, accessible via the domain name www.phoenix.com. Successful access to this web service requires: (1) DNS resolution of the domain name, (2) TCP three-way handshake establishment, (3) HTTP request transmission, (4) Server processing and response generation, (5) Content delivery to the client. Each of these steps depends on correct configuration of multiple network components, making web access testing a comprehensive validation of the entire system.

## 5.9 Access Control List Verification

Access Control Lists (ACLs) are ordered sets of rules that filter network traffic based on criteria such as source/destination IP addresses, protocols, and port numbers. ACLs can be applied to router

interfaces in either the inbound or outbound direction. In our security implementation, ACLs enforce a "default deny" policy, explicitly permitting only authorized traffic types while blocking all other traffic.

The command show access-lists displays configured ACLs along with hit counters—the number of packets that have matched each rule. These counters are invaluable for verifying that ACLs are functioning as intended. For example, if we observe incrementing hit counts on the "permit icmp" rule after performing ping tests, we can confirm that ICMP traffic is being correctly identified and allowed. Similarly, zero hits on certain rules might indicate that expected traffic is not occurring, potentially revealing configuration issues or security policy violations.

## 5.9 Performance Metrics and Network Health Indicators

Beyond basic connectivity, enterprise networks require ongoing performance monitoring to ensure optimal operation. Key performance indicators include: latency (measured via ICMP RTT), packet loss (percentage of packets not receiving replies), jitter (variation in latency), throughput (data transfer rate), and interface utilization (percentage of bandwidth in use).

The ping statistics shown in our results provide valuable performance data. Average RTT values in the range of 1-10ms indicate excellent local network performance, while values up to 50ms are acceptable for inter-site VPN connections. Packet loss of 0% is ideal and indicates a stable network without congestion or errors. Maximum RTT values significantly higher than the average may indicate occasional congestion or processing delays, which should be investigated if they occur frequently.

## 6. Conclusion

In this project, a secure and scalable enterprise-grade multi-site network was successfully designed, configured, and validated. The implementation demonstrated how geographically separated offices can be interconnected securely and efficiently using Site-to-Site GRE tunneling over a public network infrastructure. The network was further strengthened through the deployment of Access Control Lists (ACLs), which enforced enterprise-level security by allowing only essential business traffic while denying all unauthorized communication.

In addition to secure connectivity, core network services such as DNS and web hosting were integrated under the custom domain *phoenix.com*, providing seamless name resolution and centralized access to enterprise resources. Real-time monitoring was enabled using ACL hit counters and interface statistics, ensuring effective traffic validation and network visibility. The architecture was also designed to be highly scalable, featuring multiple subnets to support future network expansion and departmental segmentation.

Overall, this project provides a comprehensive and cost-effective blueprint for small and medium-sized enterprises to establish secure, standards-based connectivity between branch offices. The design principles applied ensure reliability, maintainability, and adaptability to evolving organizational requirements.

## 7. References


1. Cisco Systems, *"Configuring GRE Tunnels,"* Cisco Networking Academy, Cisco Documentation, 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

2. Tanenbaum, A. S., & Wetherall, D. J., *Computer Networks,* 5th ed., Pearson Education, 2011.

3. Kurose, J. F., & Ross, K. W., *Computer Networking: A Top-Down Approach,* 8th ed., Pearson Education, 2021.

4. William Stallings, *Data and Computer Communications,* 10th ed., Pearson Education, 2013.

5. Cisco Networking Academy, *"Implementing Site-to-Site VPNs,"* Networking Essentials – Lab Guide, 2024.

6. Palo Alto Networks, *"Understanding VPNs and Tunneling Protocols,"* Technical Whitepaper, 2023.

7. RFC 2784 — *Generic Routing Encapsulation (GRE),* The Internet Society, IETF, March 2000. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2784

8. RFC 4301 — *Security Architecture for the Internet Protocol (IPsec),* IETF, December 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4301

9. GNS3 & Cisco Packet Tracer Labs, *"VPN Tunnel Simulation and GRE Configuration,"* Network Simulation Tutorials, 2024.

10. Sharma, P., & Sahu, A., "Design and Implementation of a Secure Site-to-Site VPN Using GRE and IPsec," *International Journal of Computer Applications,* vol. 182, no. 37, pp. 12–18, 2023.

11. Python Software Foundation, *"Socket Programming and Networking Modules,"* Python 3.12 Documentation, 2024. [Online]. Available: https://docs.python.org/3/library/socket.html

12. Fortinet, *"Defense-in-Depth Security Architecture Explained,"* Fortinet Whitepaper, 2024.