ADVANCED NETWORK SECURITY

Simulation and Verification of HTTP and DNS Services in a Secured Network Environment"

CHANDRA SHEKHAR VENKATARAMA REDDY-11618700

NAGA VENKATA SAI NITIESH ANURAG PREPARA-11660912

KRISHNA SAI CHEGGOJU-11646472

Agenda

- Introduction
- Network Component
- Network Configuration
- Data Flow
- Simulation Results
- Challenges and Solution
- Conclusion

INTRODUCTION

In today's interconnected world, secure and efficient communication is the backbone of any modern network. Our project focuses on implementing and verifying a robust network topology featuring critical services like HTTP and DNS. By configuring routers, switches, and servers, we simulate a real-world environment where devices communicate seamlessly while ensuring data integrity and reliability.

The objective is to:
- Build a scalable and functional network infrastructure.
- Configure essential services like HTTP and DNS to handle requests efficiently.
- Analyze and verify the data flow using network simulation tools.

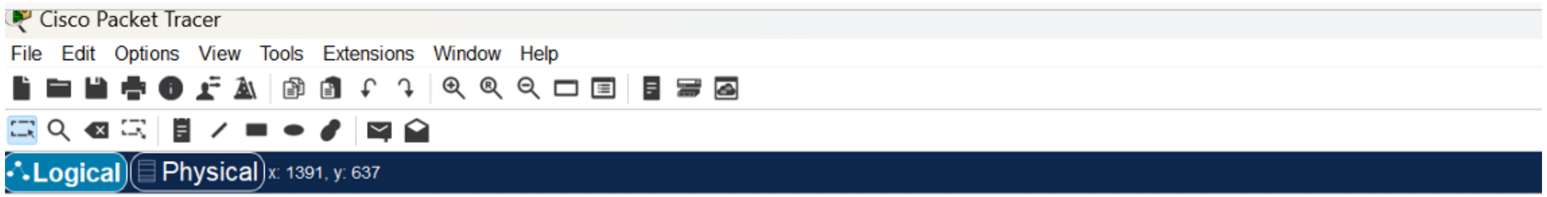
This project not only enhances our understanding of network design and configuration but also demonstrates practical solutions to real-world challenges in advanced networking and security.

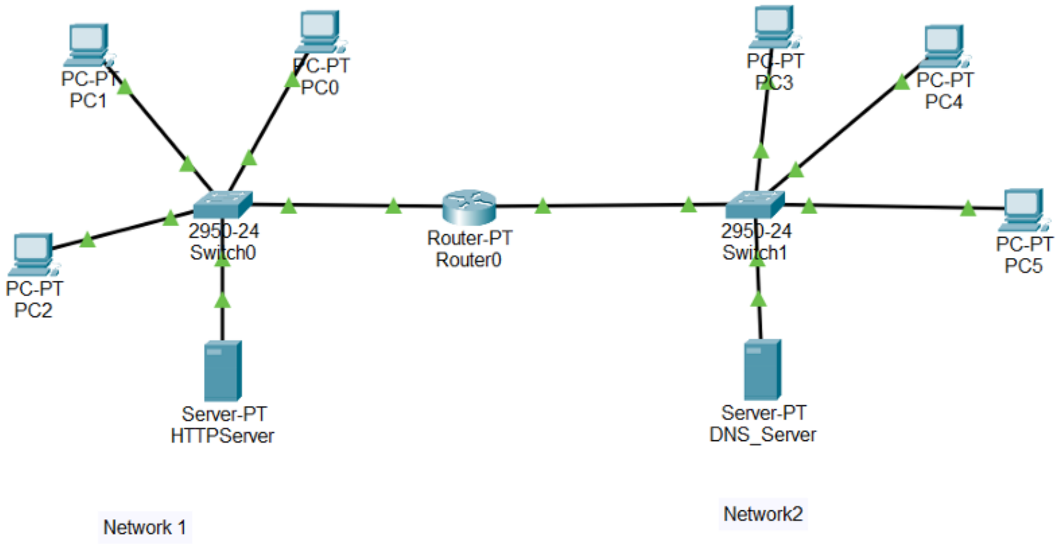
NETWORK COMPONENT

- **Routers**: Connect and manage traffic between different networks.
- **Switches**: Facilitate device communication within the same network.
- **HTTP Server**: Responds to web requests from client devices.
- **DNS Server**: Resolves domain names into IP addresses.
- **PCs**: Represent clients sending DNS and HTTP requests.

NETWORK CONFIGURATION

- Each PC and server is assigned a unique IP address.
- Configuration of routers for packet forwarding.
- DNS server setup to resolve domain names.
- HTTP server setup to respond to requests.
- Proper routing tables and switching mechanisms are implemented

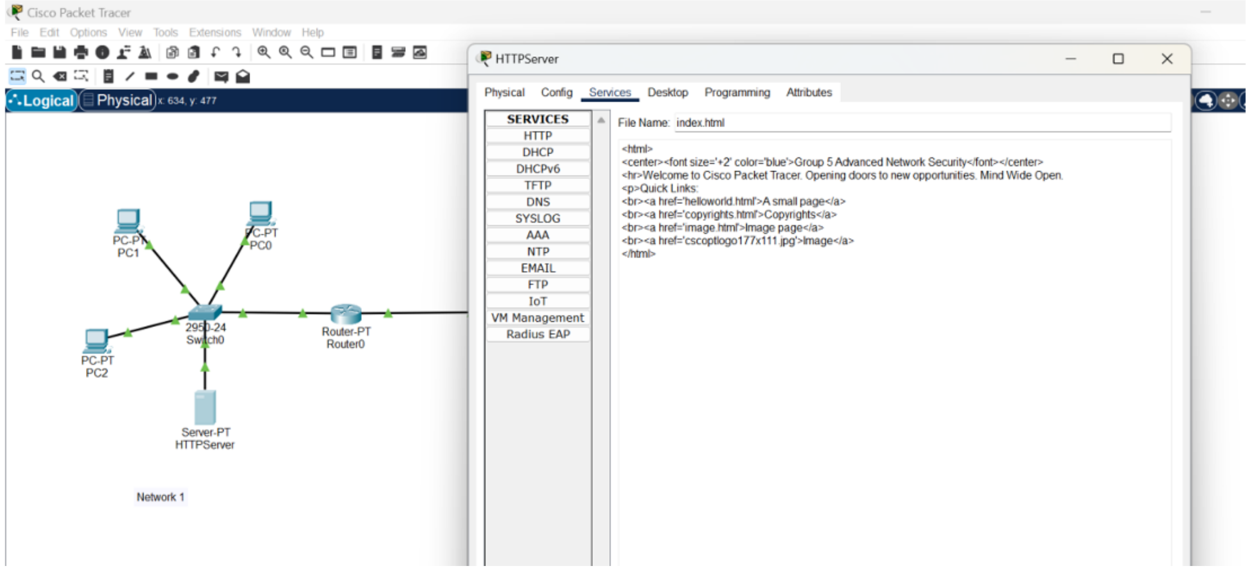




- Network consists of two LANs (Network1 and Network2).
- Networks are interconnected via a router (Router0).
- Includes HTTP and DNS servers for functionality

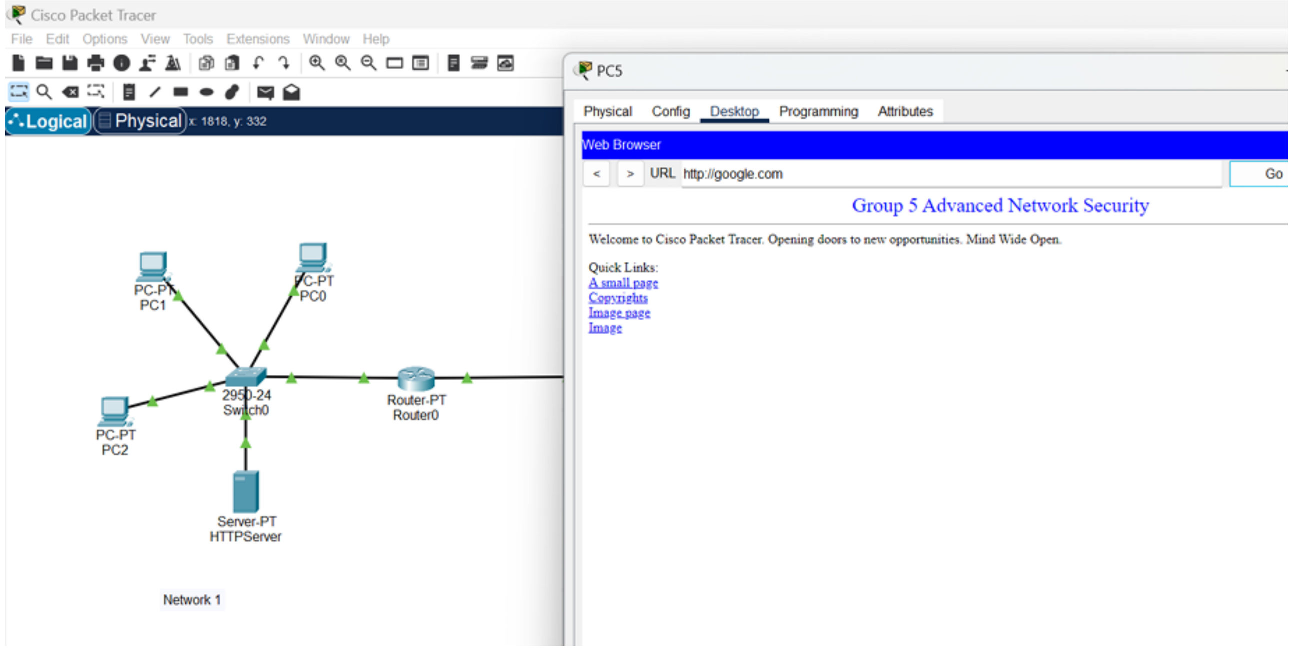
DATA FLOW

- **Step 1**: DNS Request
- PC sends a domain name query to the DNS server.
- DNS server responds with the resolved IP address.
- **Step 2**: HTTP Request
- PC uses the resolved IP to send a request to the HTTP server.
- HTTP server processes and responds to the request.
- Data traverses through configured routers and switches.



File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Group 5 Advanced Network Security</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

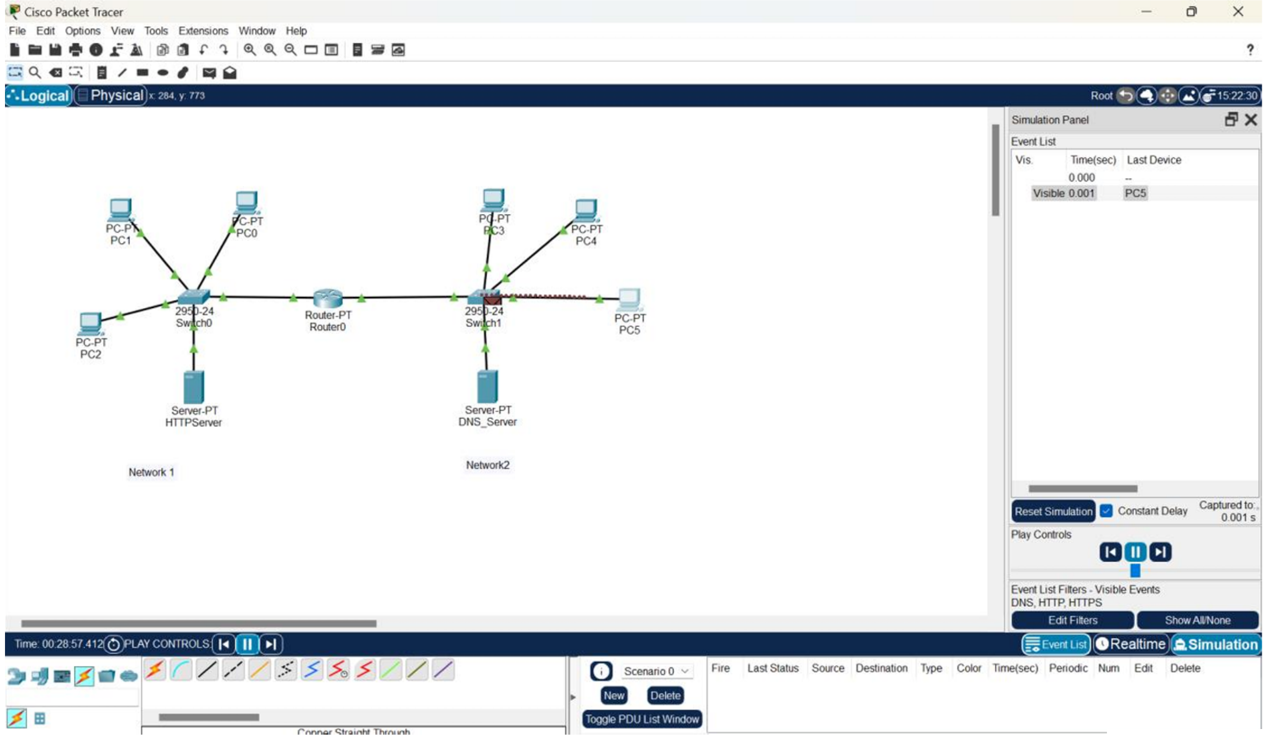


URL http://google.com

Group 5 Advanced Network Security

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



Event List

Vis.	Time(sec)	Last Device
	0.000	--
Visible	0.001	PC5

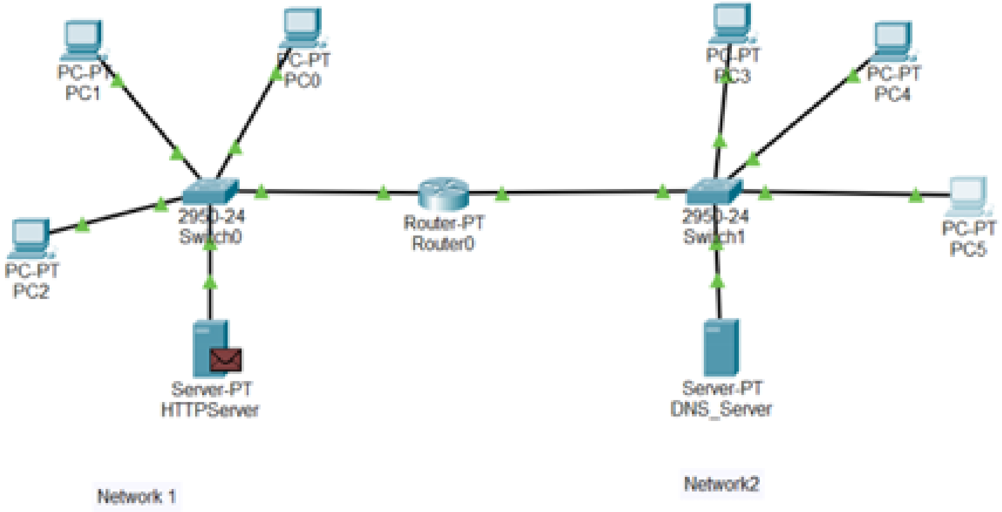
☑ Constant Delay

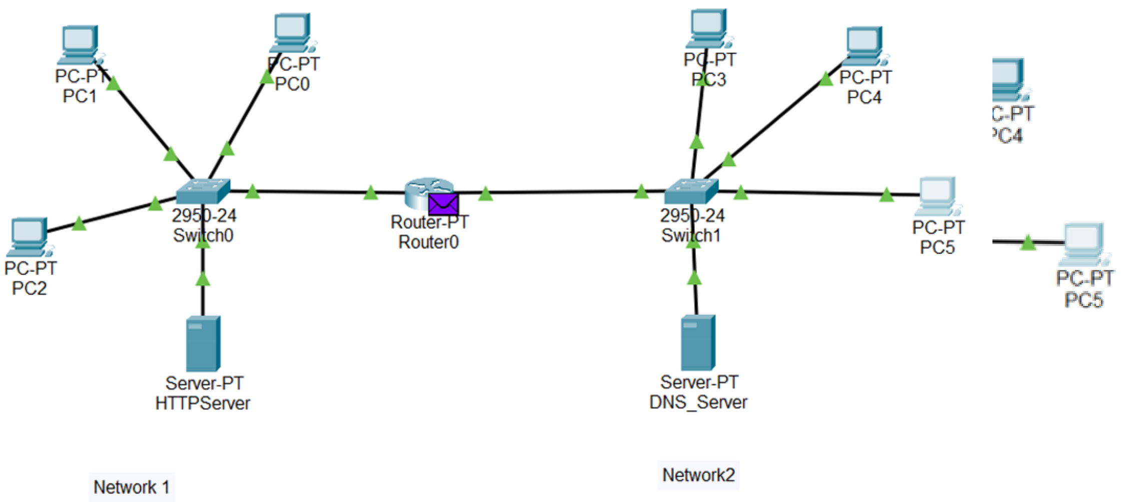
Captured to: 0.001 s

Event List Filters - Visible Events
DNS, HTTP, HTTPS

Time: 00:28:57.412

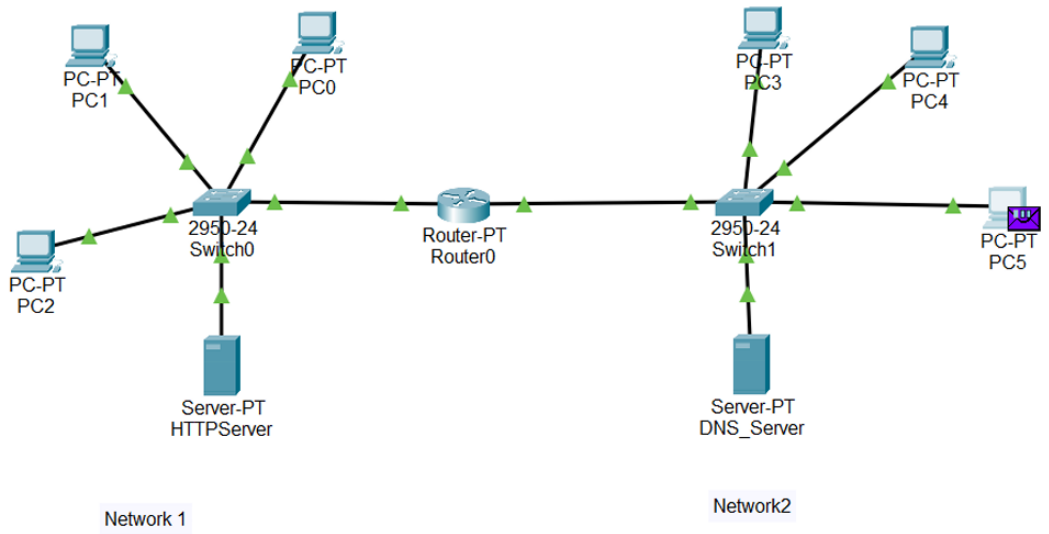
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

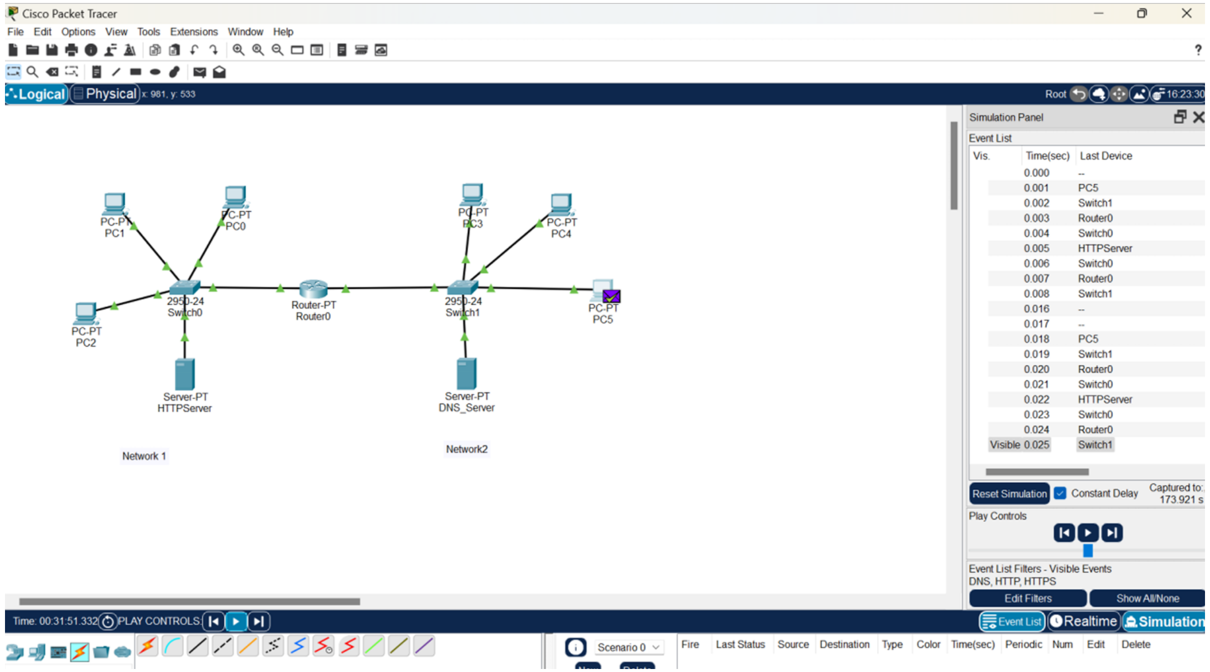




Network 1

Network2





Event List

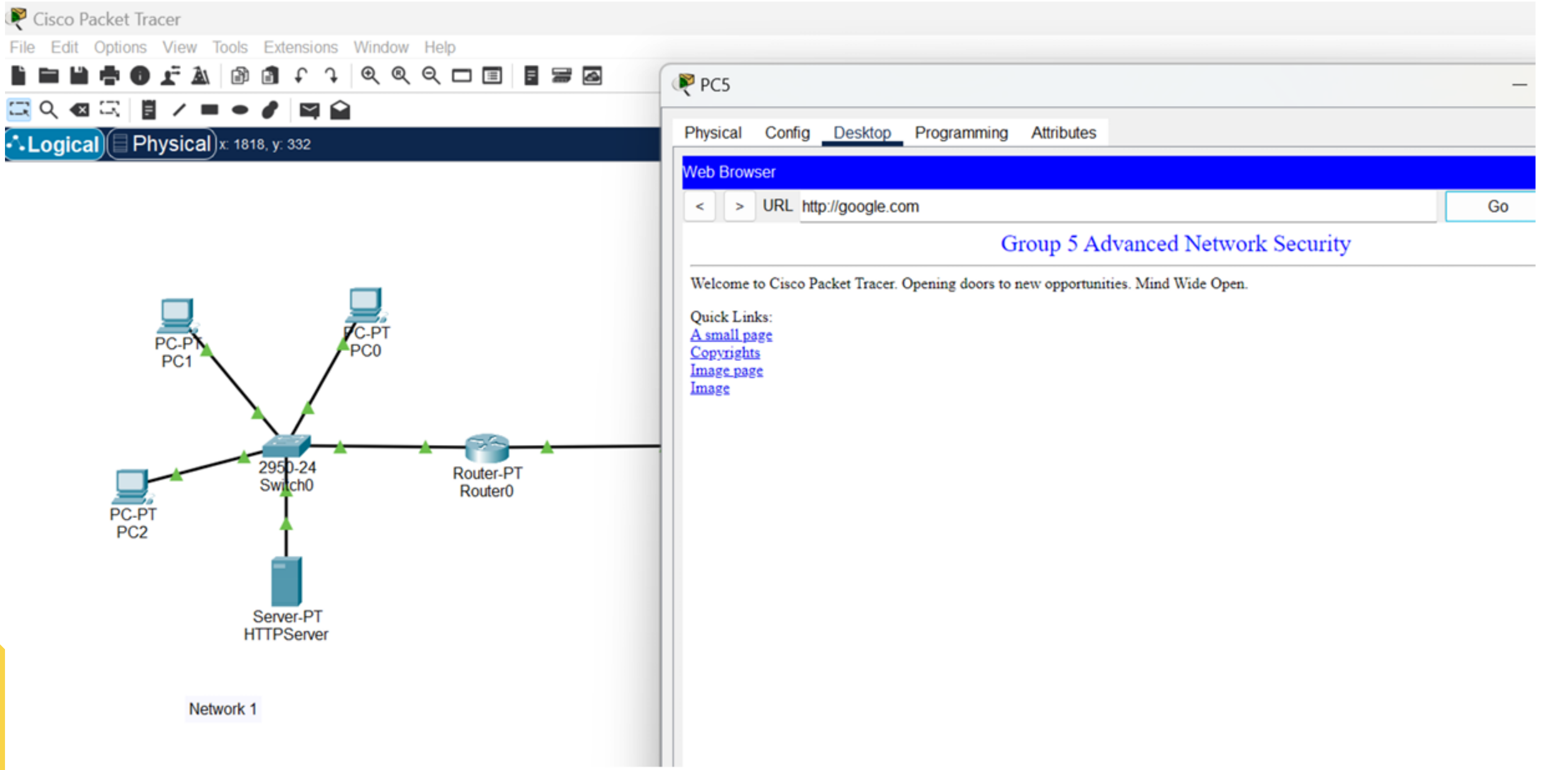
Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC5
	0.002	Switch1
	0.003	Router0
	0.004	Switch0
	0.005	HTTPServer
	0.006	Switch0
	0.007	Router0
	0.008	Switch1
	0.016	--
	0.017	--
	0.018	PC5
	0.019	Switch1
	0.020	Router0
	0.021	Switch0
	0.022	HTTPServer
	0.023	Switch0
	0.024	Router0
Visible	0.025	Switch1

☑ Constant Delay

Captured to: 173.921 s

Event List Filters - Visible Events
DNS, HTTP, HTTPS

- **Successful Connection:** Client PC (PC5) connected to the HTTP server via HTTPS.
- **Browser View:** The custom webpage "Group 5 Advanced Network Security" loaded successfully, confirming server functionality.
- **Traffic Encryption:** HTTPS ensures all data transmitted between clients and the server is encrypted.
- **Security Implementation:** TLS was successfully deployed on the HTTP server to enable HTTPS.



URL http://google.com

Group 5 Advanced Network Security

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

SIMULATION RESULTS

- **Successful HTTPS Communication:** Clients in both networks accessed the HTTP server securely via https://, ensuring encrypted traffic.
- **TLS Encryption Validation:** Packet inspection confirmed traffic on port 443 is encrypted, while HTTP (port 80) is blocked.
- **Access Control:** Router ACLs enforced HTTPS-only access, denying unencrypted HTTP connections.
- **DNS Integration:** DNS server resolved domain names correctly, enabling seamless HTTPS requests.

IMPLEMENTED FIREWALL

1. **Placement in the Topology:**

    1. The firewall was deployed between Router0 and the HTTP/DNS servers to control traffic

    entering and exiting each network.

2. **Access Control Rules (ACLs):**

    1. **Permit HTTPS (port 443):** Only encrypted HTTPS traffic is allowed to the HTTP server.

    2. **Block HTTP (port 80):** Prevents unencrypted traffic, enforcing secure communication.

    3. **Permit DNS (port 53):** Allows domain name resolution traffic to and from the DNS server.

    4. **Deny All Other Traffic:** Ensures no unauthorized access to other ports or services.

ACL Configuration:

- On Router0:

```
access-list 101 permit tcp any any eq 443
access-list 101 permit udp any any eq 53
access-list 101 deny ip any any
```

- Applied the ACL to the interface connected to the server:

```
interface GigabitEthernet0/0 ip access-group 101 in
```

CHALLENGES AND SOLUTIONS

Challenges:

- Configuring DNS and HTTP services correctly.
- Assigning IP addresses without conflicts.
- Ensuring efficient routing and switching.

Solutions:

- Systematic configuration and testing.
- Troubleshooting routing paths and server responses.

CONCLUSION

- ❑ Successfully simulated network topology with working DNS and HTTP services
- ❑ Verified secure and efficient communication between devices.
- ❑ Highlighted practical applications of routers, switches, and IP configuration.

Thank you