Cisco Network Academy
Virtual Internship Program 2025
Cyber Shield : Defending the Network

PROJECT REPORT PREPARED IN ALIGNMENT WITH THE CISCO VIP 2025

CYBER SECURITY INDUSTRY PROBLEM STATEMENT.

Submitted By
Akshay Sahadeo Sannakki
akshaysannakki24@gmail.com
STU67e41cdf1c9721743002847

1. Objectives

The project aims to fulfill multiple academic and technical objectives. These objectives were defined keeping in mind both the existing challenges of the college network and the requirements of modern cybersecurity practices.

1) Functional Objectives :
   - Ensure smooth inter-departmental communication.
   - Provide centralized data access for administration.
   - Improve reliability and scalability of the network.

2) Security Objectives :
   - Protect critical services (DNS, FTP, Web servers) from unauthorized access.
   - Introduce VLANs to segment departments and limit lateral movement.
   - Deploy ACLs and firewall policies to block malicious traffic.

3) Scalability Objectives :
   - Create a design that supports future expansion of labs and offices.
   - Support both wired and wireless connectivity.

4) Remote Access Objectives :
   - Enable secure faculty remote access through VPN or identity-aware solutions.
   - Support hybrid access models for students and faculty.

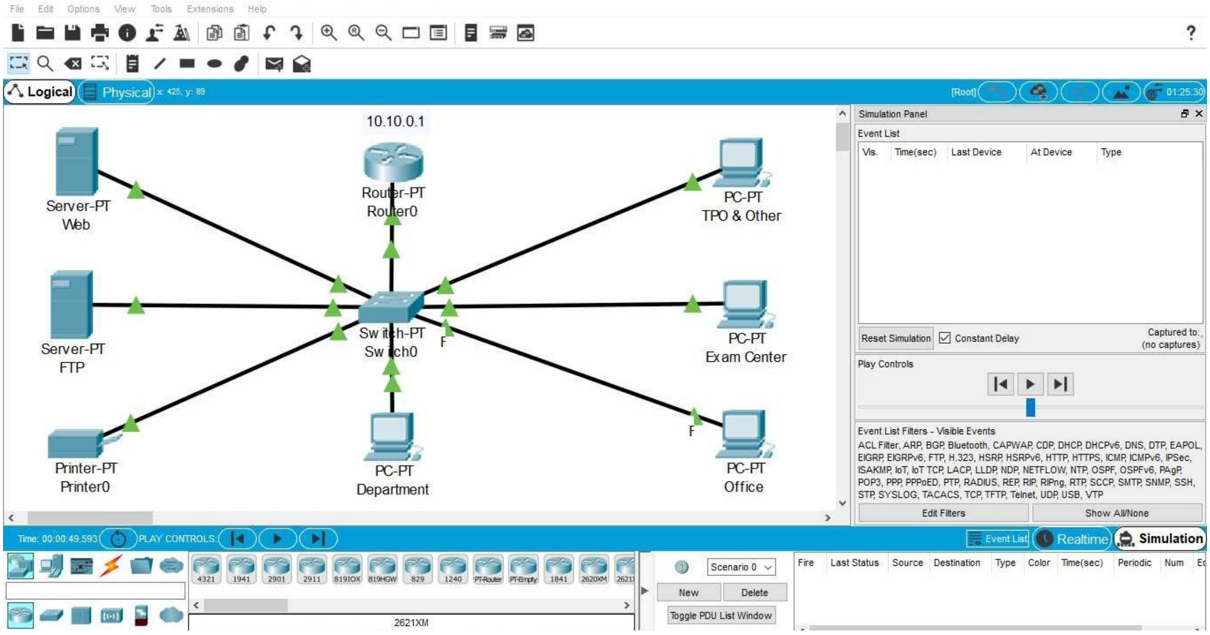
5) Policy Objectives :
   - Implement intelligent access policies to restrict non-academic content.
   - Ensure role-based and time-based access rules are enforced.

2. Existing Infrastructure Analysis

The current network infrastructure in the college has several limitations that prevent it from being secure, efficient, and scalable.

The following points summarize the issues :

1) Flat Network : All devices, including labs, offices, and administration, are in the same broadcast domain, increasing risks of broadcast storms and lack of isolation.
2) Static IP Assignment : Each device is manually assigned an IP, making it difficult to manage and prone to conflicts.
3) Outdated Switches : Existing switches do not support advanced monitoring or SNMP.
4) Lack of Remote Access : Administrators cannot access the network remotely to monitor or fix issues.
5) Security Gaps : No firewall, IDS/IPS, or content filtering exists.
6) Redundant Server Rooms : Multiple server rooms waste power and management resources.



Reset Simulation ☑ Constant Delay

Captured to:
(no captures)

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

3. Proposed Secure Network Design

1) VLANs & Segmentation :
   - Departments such as IT, Computer Science, Office, Principal Room, Internet Lab, and Server Room are separated into VLANs with dedicated IP subnets.
   - This improves traffic isolation and security.

2) RIP Routing :
   - RIP protocol is used between routers for dynamic routing.
   - Provides automatic route updates and easier scalability.

3) Server Placement :
   - DNS, Web, and FTP servers are hosted in a secure Server Room VLAN.
   - Controlled via firewall and ACLs.

4) Security Enhancements :
   - ACLs applied at routers and switches.
   - Deployment of a firewall for external and internal traffic monitoring.
   - IDS/IPS planned for detecting intrusions.

5) Hybrid Access :
   - VPN gateways configured for faculty remote access.
   - Secure SASE-based proxy for cloud-aware access policies.

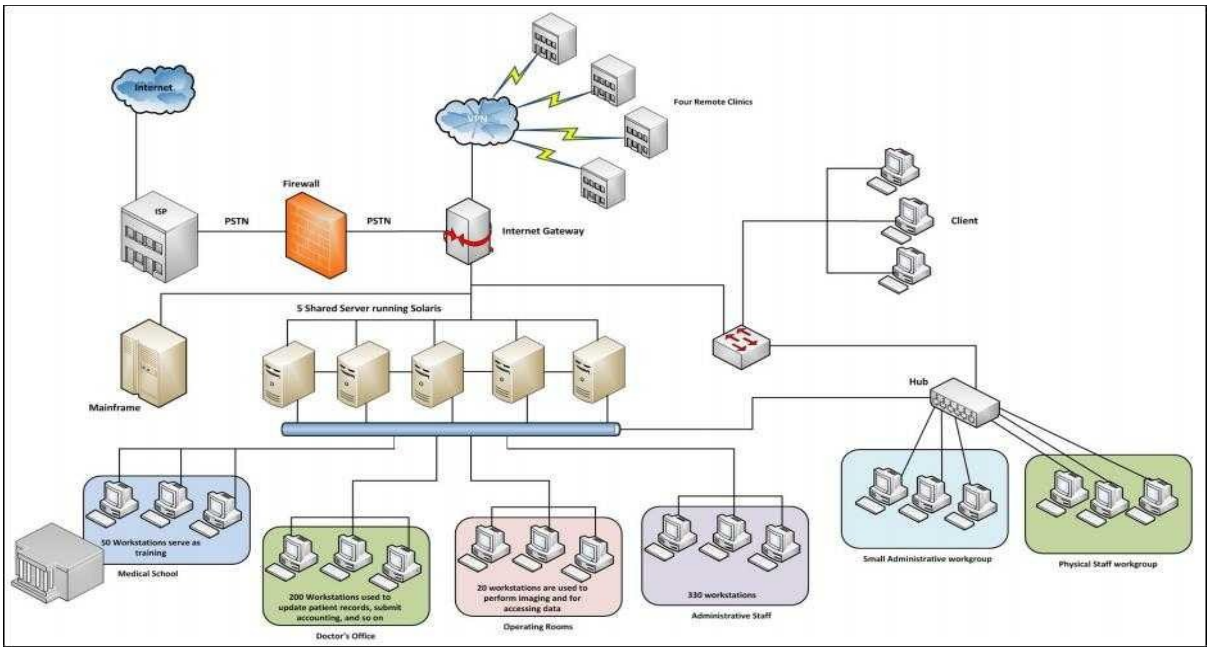
6) Devices :
   - Cisco Catalyst 6500/4500 switches with VSS.
   - Cisco Aironet 1140 APs for wireless connectivity.

Part 1 : Security Assessment & Attack Surface Analysis

1) Threats :
    - Insider threats (students accessing restricted areas).
    - Malware spreading across a flat network.
    - DoS attacks due to lack of traffic filtering.
    - Unauthorized access to server data.

2) Attack Surface :
    - Servers (DNS, Web, FTP) are exposed without strong security.
    - Switches without ACLs allow unrestricted communication.
    - Lack of VLAN segmentation means compromised PCs affect the whole network.

3) Countermeasures :
    - Introduce VLANs with ACLs.
    - Firewalls with IDS/IPS at core routers.
    - Strong authentication policies.
    - Centralized logging and monitoring of traffic.
    - Regular audits and penetration testing.


Internet
VPN
Four Remote Clinics
Firewall
ISP
PSTN
PSTN
Internet Gateway
Client
5 Shared Server running Solaris
Mainframe
Hub
50 Workstations serve as training
Medical School
200 Workstations used to update patient records, submit accounting, and so on
Doctor's Office
20 workstations are used to perform imaging and for accessing data
Operating Rooms
330 workstations
Administrative Staff
Small Administrative workgroup
Physical Staff workgroup

Part 2 : Hybrid Access Architecture

A secure hybrid access model is designed to support flexible faculty work and student access.

1) Role-Based Segmentation :
    - Faculty VLAN with remote access.
    - Student VLAN with controlled access.
    - Guest VLAN with restricted access.

2) Remote Access Solutions :
    - VPN (IPSec/SSL) for faculty.
    - SASE for cloud-based secure access.
    - Identity-aware proxy for authenticati

3) Policy Enforcement :
    - Faculty can access research repositories, teaching tools.
    - Students restricted to academic portals.
    - Guests allowed internet-only access.

4) Authentication :
    - Username/password with multi-factor authentication.
    - Role-based identity verification.

Part 3 : Smart Web Access Policy

Students misuse the network for streaming, torrenting, and bypassing restrictions. A smart access policy is created.

1) Policy Framework :
   - DNS filtering to block malicious and social domains.
   - L7 firewall rules to block torrent/gaming.
   - Time-based rules (stricter in class hours).
   - Role-based rules (faculty vs student vs guest).

2) Policy Enforcement Example Table :

User Type	Time	Allowed	Blocked
Faculty	24x7	All academic & research	None
Student	Class Hours	Academic portals	Social media & gaming
Student	Off Hours	Academic + limited social	Torrent & illegal sites
Guest	24x7	Internet only	All internal services

3) Monitoring :
   - Logs of all DNS/firewall violations.
   - Alerts for suspicious circumvention attempts.
   - Reports to admin weekly.

4. Testing & Results (Packet Tracer Implementation)

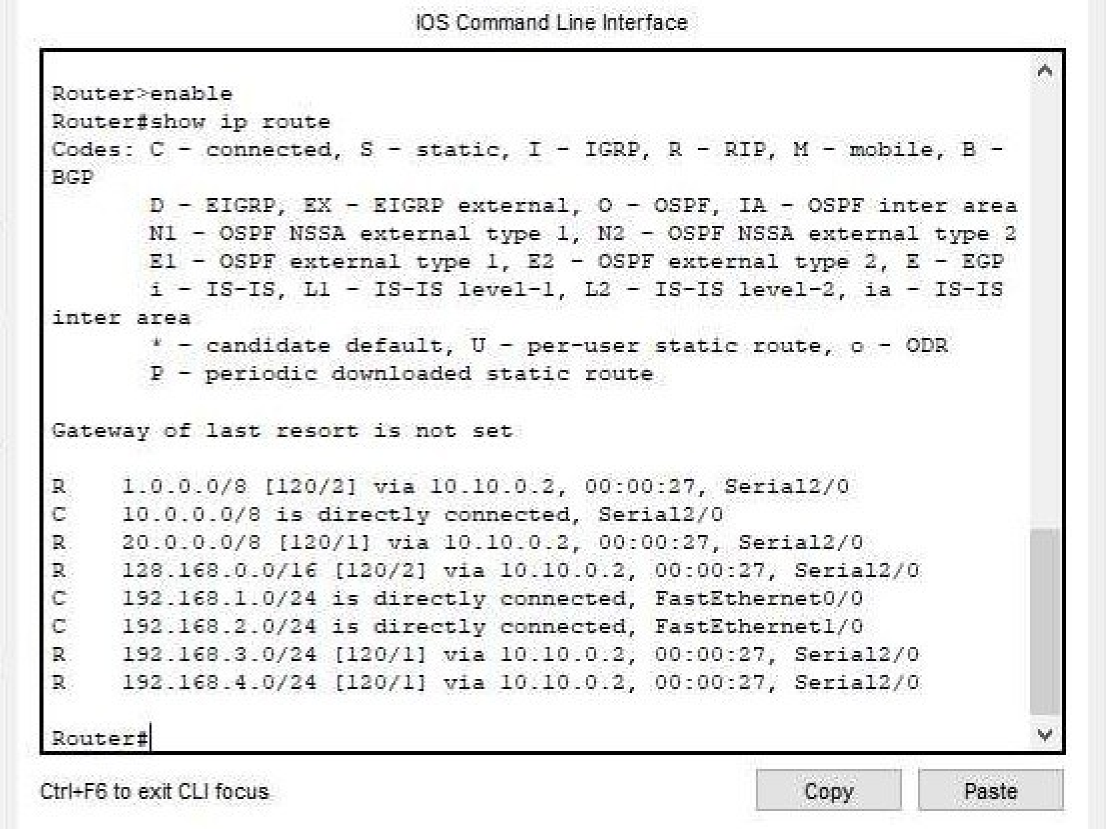
Testing was conducted in Cisco Packet Tracer to validate the design.

1) Test Cases :
   - VLAN Communication:
   - Ping between IT Lab and Computer Lab successful.
   - Unauthorized cross-VLAN blocked by ACL.

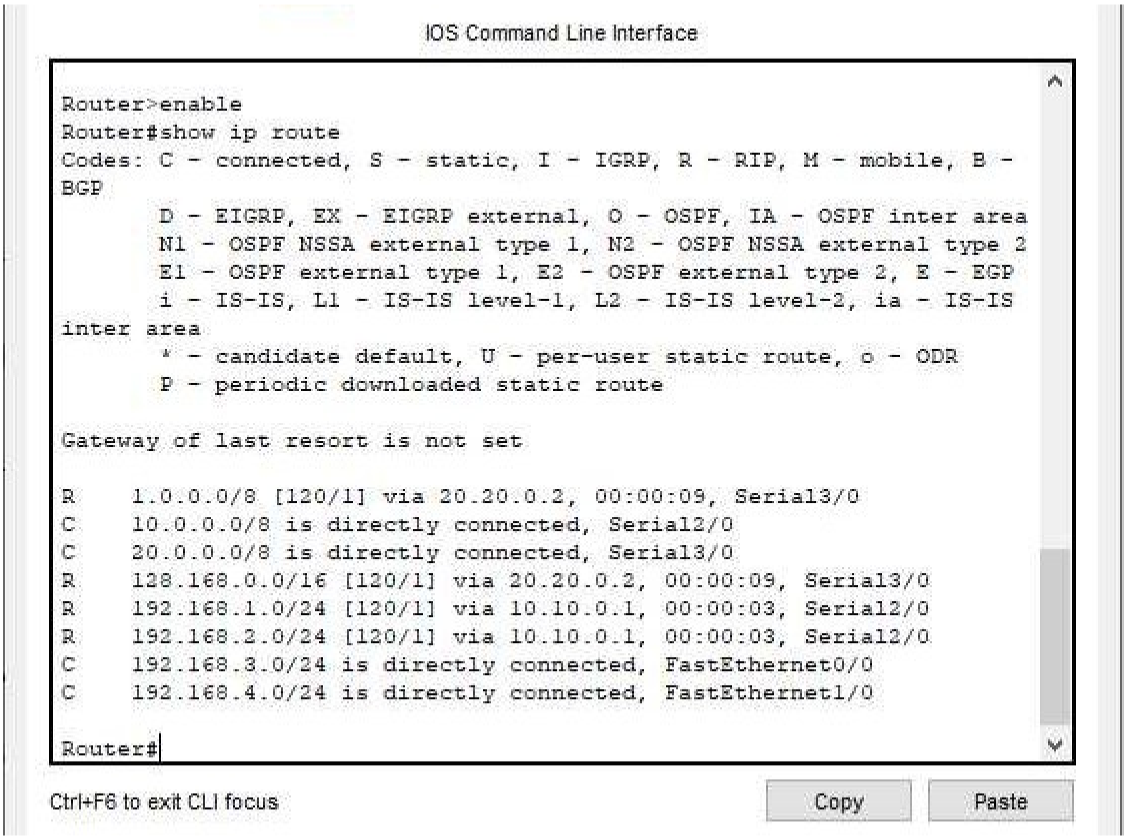
2) Server Access :
   - DNS, Web, and FTP servers accessible only by permitted VLANs.
   - Unauthorized users denied access.

3) VPN Access :
   - Faculty connected remotely using VPN tunnel.
   - Verified access to teaching tools securely.

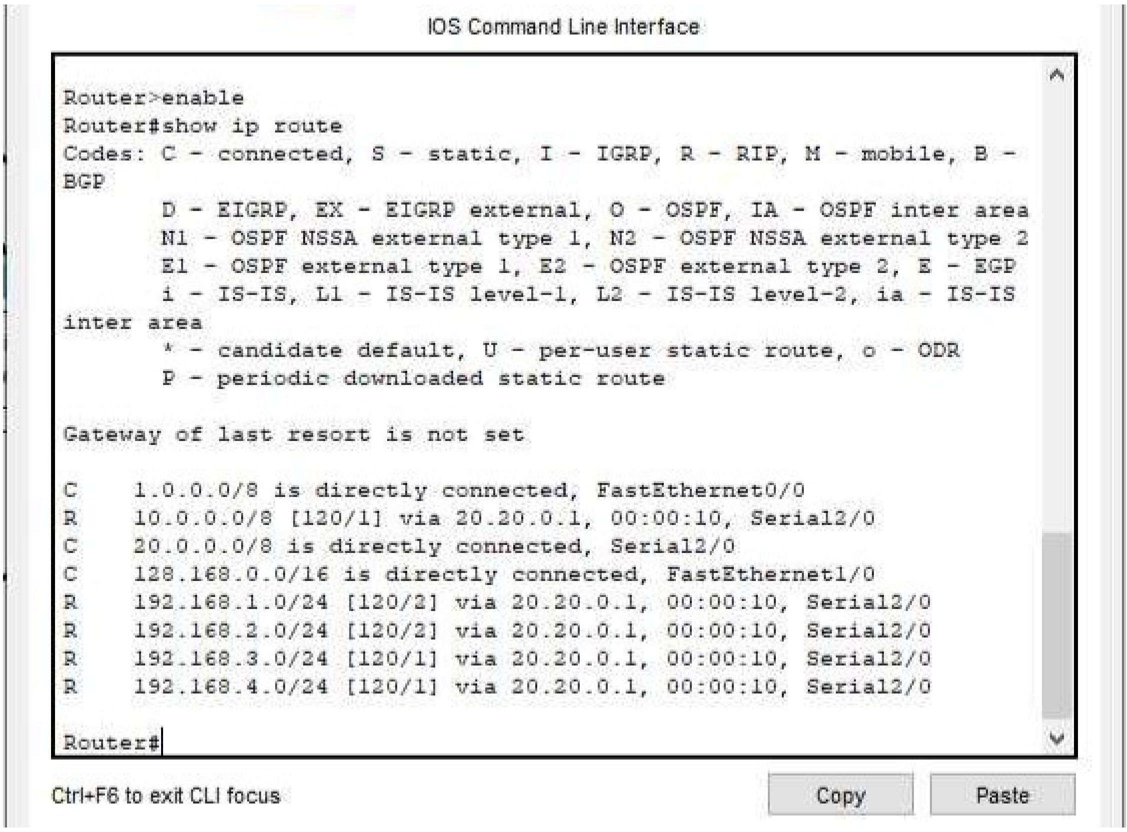
4) Policy Enforcement :
   - Students blocked from accessing torrents.
   - Time-based restriction simulated for class hours.
   - Logging showed alerts when bypass attempts made.



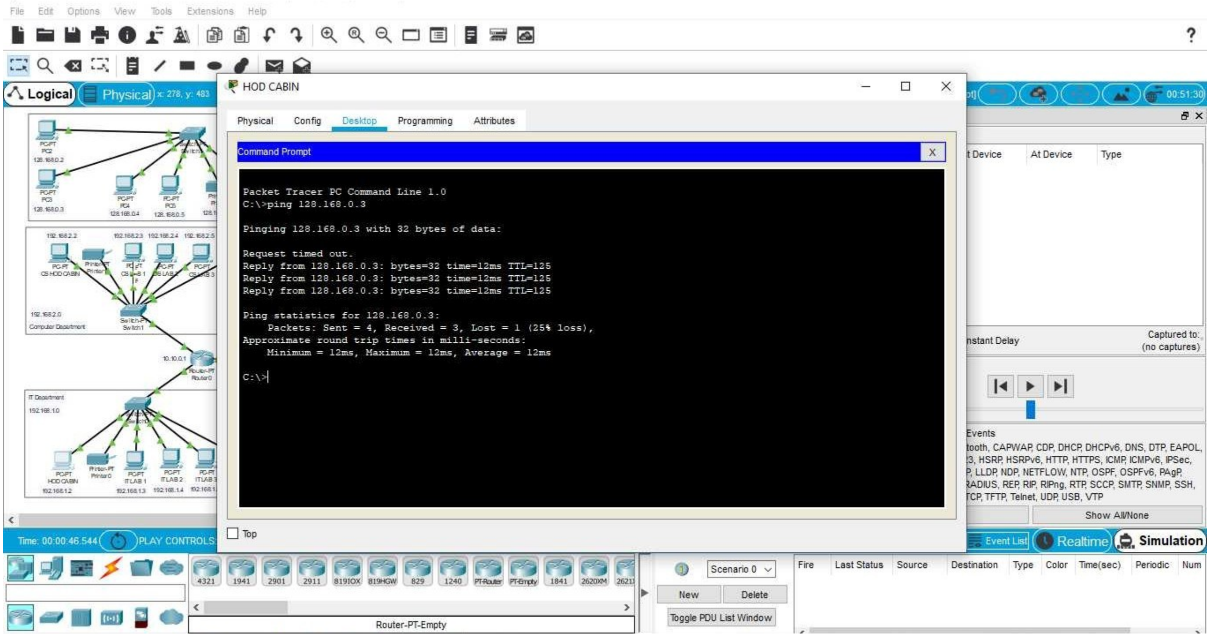
```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    1.0.0.0/8 [120/2] via 10.10.0.2, 00:00:27, Serial2/0
C    10.0.0.0/8 is directly connected, Serial2/0
R    20.0.0.0/8 [120/1] via 10.10.0.2, 00:00:27, Serial2/0
R    128.168.0.0/16 [120/2] via 10.10.0.2, 00:00:27, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet1/0
R    192.168.3.0/24 [120/1] via 10.10.0.2, 00:00:27, Serial2/0
R    192.168.4.0/24 [120/1] via 10.10.0.2, 00:00:27, Serial2/0

Router#
```



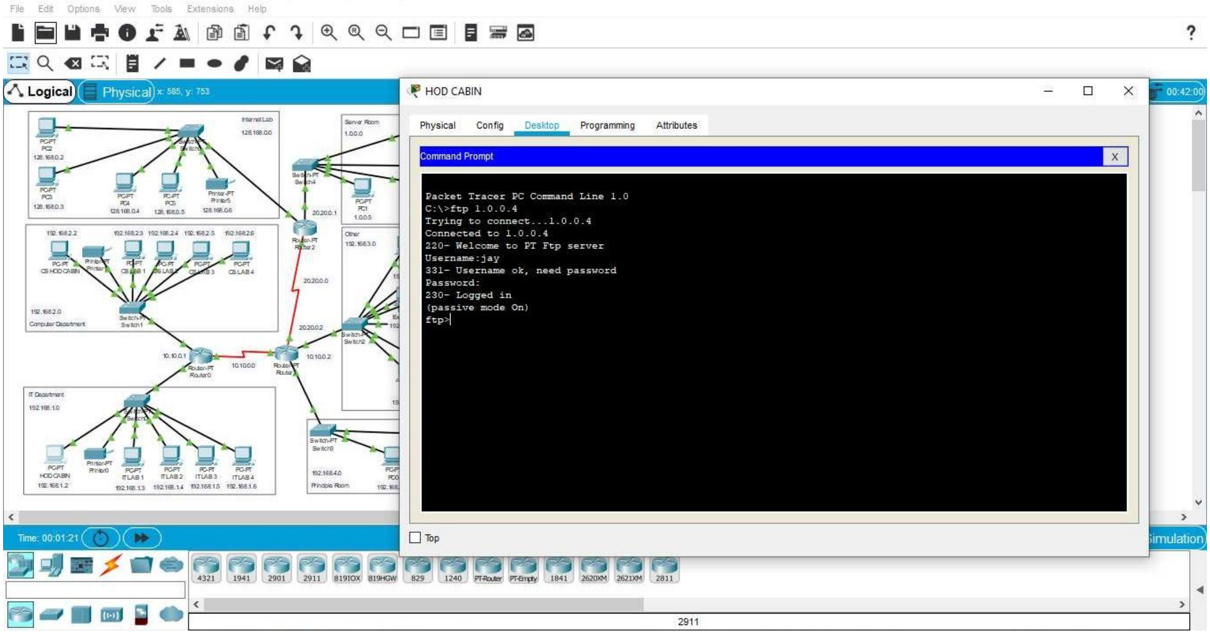
```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    1.0.0.0/8 [120/1] via 20.20.0.2, 00:00:09, Serial3/0
C    10.0.0.0/8 is directly connected, Serial2/0
C    20.0.0.0/8 is directly connected, Serial3/0
R    128.168.0.0/16 [120/1] via 20.20.0.2, 00:00:09, Serial3/0
R    192.168.1.0/24 [120/1] via 10.10.0.1, 00:00:03, Serial2/0
R    192.168.2.0/24 [120/1] via 10.10.0.1, 00:00:03, Serial2/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0

Router#
```



```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, FastEthernet0/0
R    10.0.0.0/8 [120/1] via 20.20.0.1, 00:00:10, Serial2/0
C    20.0.0.0/8 is directly connected, Serial2/0
C    128.168.0.0/16 is directly connected, FastEthernet1/0
R    192.168.1.0/24 [120/2] via 20.20.0.1, 00:00:10, Serial2/0
R    192.168.2.0/24 [120/2] via 20.20.0.1, 00:00:10, Serial2/0
R    192.168.3.0/24 [120/1] via 20.20.0.1, 00:00:10, Serial2/0
R    192.168.4.0/24 [120/1] via 20.20.0.1, 00:00:10, Serial2/0

Router#
```

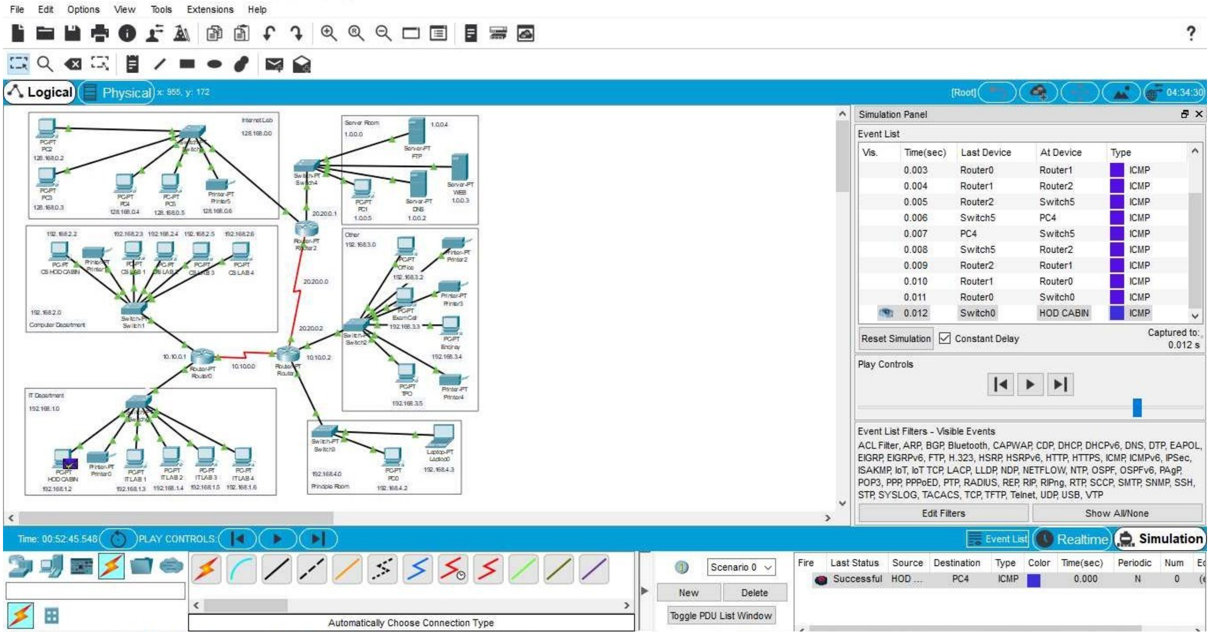


```
Packet Tracer PC Command Line 1.0
C:\>ping 128.168.0.3

Pinging 128.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.3: bytes=32 time=12ms TTL=125
Reply from 128.168.0.3: bytes=32 time=12ms TTL=125
Reply from 128.168.0.3: bytes=32 time=12ms TTL=125

Ping statistics for 128.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\>
```



```
Packet Tracer PC Command Line 1.0
C:\>ftp 1.0.0.4
Trying to connect...1.0.0.4
Connected to 1.0.0.4
220- Welcome to PT Ftp server
Username:jay
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Final University College Network detailed topology diagram



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.003	Router0	Router1	ICMP
	0.004	Router1	Router2	ICMP
	0.005	Router2	Switch5	ICMP
	0.006	Switch5	PC4	ICMP
	0.007	PC4	Switch5	ICMP
	0.008	Switch5	Router2	ICMP
	0.009	Router2	Router1	ICMP
	0.010	Router1	Router0	ICMP
	0.011	Router0	Switch0	ICMP
	0.012	Switch0	HOD CABIN	ICMP

Reset Simulation ☑ Constant Delay

Captured to:
0.012 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
●	Successful	HOD ...	PC4	ICMP	■	0.000	N	0	(e