ONL3_ISS5_S2_Huawei network administrator

UNVERSITY SYSTEM NETWORK

Team members:

El Sayed EL Tablawy El Sayed

Fahd Abdelaziz Taher

Samy Awad Samy

Mostafa Nasser Mohamed

Malek Khaled Abo El Maged

Project Report: Intercollege Network Integration

1. Introduction

This project demonstrates the design and implementation of an integrated network infrastructure connecting **two colleges** within a university system.
The goal is to create a scalable, secure, and efficient network environment that supports routing, switching, security services, management, and user segmentation across multiple departments.

The design follows real-world enterprise network standards and includes:

- Dynamic Routing Protocols (OSPF, ISIS, BGP, and MPLS)
- VLAN segmentation and Inter-VLAN routing
- AAA, NAT, SNMP, and VPN services
- RSTP/MSTP for Layer 2 redundancy
- Network security layers and DMZ structure

---

2. Project Objectives

1. Connect two separate college networks into a unified university system.
2. Provide secure communication between departments, students, staff, and external users.
3. Ensure high availability using redundancy protocols.

4. Apply routing technologies to optimize internal and external connectivity.
5. Implement network security to protect sensitive university resources.
6. Provide centralized services such as management, AAA, and NAT.

---

3. Network Architecture Overview

The network is divided into **multiple functional zones**, each represented by VLANs and routing domains.
The topology includes:

A. Core Layer

- Devices R1–R6 form the backbone responsible for:
  - OSPF
  - ISIS
  - BGP
  - MPLS + LDP
  - Static Routing
- The core ensures fast and resilient communication between both colleges.

B. Distribution Layer

- Layer 3 switches (LSW10, LSW11, LSW12, LSW13, etc.) route traffic between VLANs.
- Inter-VLAN routing is implemented.
- Redundancy ensured through RSTP / MSTP.

C. Access Layer

- Multiple access switches serve end users:
    - Students
    - Campus security
    - IT security
    - Management
    - Staff
    - External users

Each group is isolated using VLANs:

- VLAN 10 → Campus Security
- VLAN 20 → IT Security
- VLAN 30 → Management
- VLAN 40 → Staff
- VLAN 50 → External Users
- VLAN 60 → Students

Every VLAN has its own gateway through the L3 switch.

---

4. Addressing & VLAN Structure

Each college is assigned unique subnet ranges.
Examples:

- Students Network: **60.0.60.1 / 60.1.60.1**
- Staff Network: **40.0.40.1 / 40.1.40.1**
- Management: **30.0.30.1 / 30.1.30.1**

- IT Security: **20.0.20.1 / 20.1.20.1**
- Campus Security: **10.0.10.1 / 10.1.10.1**
- External: **50.0.50.1 / 50.1.50.1**

This segmentation improves security, reduces broadcast domains, and supports policy-based control.

---

5. Routing Technologies

The project integrates multiple routing protocols for optimized communication:

1. OSPF (Open Shortest Path First)

Used for internal routing inside the college networks.

2. ISIS

Used in specific backbone segments for high-speed internal connectivity.

3. BGP (Border Gateway Protocol)

Used between major routers to exchange routes between the two colleges or external networks.

4. MPLS + LDP

Provides:

- Traffic engineering
- Fast reroute
- Support for VPN services across the university backbone

---

6. Security Implementation

Security is applied at various layers:

A. AAA (Authentication, Authorization, Accounting)

Ensures controlled access for administrators and users.

B. NAT

Provides address translation to protect internal subnets.

C. Firewall Zone

Includes:

- FW2
- VPN Gateway (Cloud1)
  Used for:
- Remote user access
- Secure external connectivity

D. ACLs

To restrict inter-VLAN communication based on policy.

E. DMZ

Hosts services such as:

- DNS
- Web servers
- SNMP management

---

7. Switching Features

The switching layer uses:

1. VLANs

To isolate departments and users.

2. Inter-VLAN Routing

To allow controlled communication between VLANs via L3 switches.

3. RSTP

Provides fast link failure recovery.

4. MSTP

Used where multiple VLAN groups require redundancy spanning multiple switches.

---

8. Network Services

The design supports the following services:

- **SNMP**: For monitoring network devices.
- **DNS**: For resolving university domain names.
- **DMZ Servers**: Hosting external and internal services.
- **VPN**: Secure connectivity for remote users.
- **Campus and IT security zones** for controlling access.

---

9. End-User Connectivity

Different user groups connect through access switches.
Each user device belongs to a specific VLAN and has access only to the resources allowed for its department.

For example:

- **Students**: Internet and LMS access, but restricted from staff and management.

- **IT Security**: Full control for monitoring.
- **Staff**: Administrative systems.
- **External Users**: Restricted guest Wi-Fi access.

---

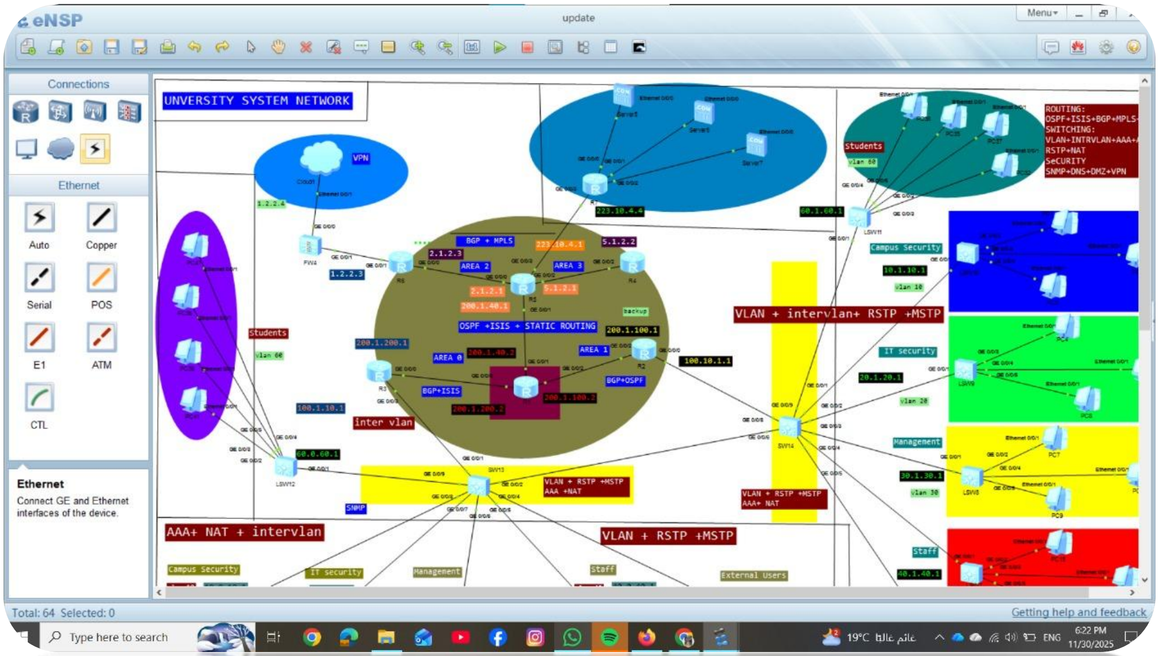
10. Conclusion

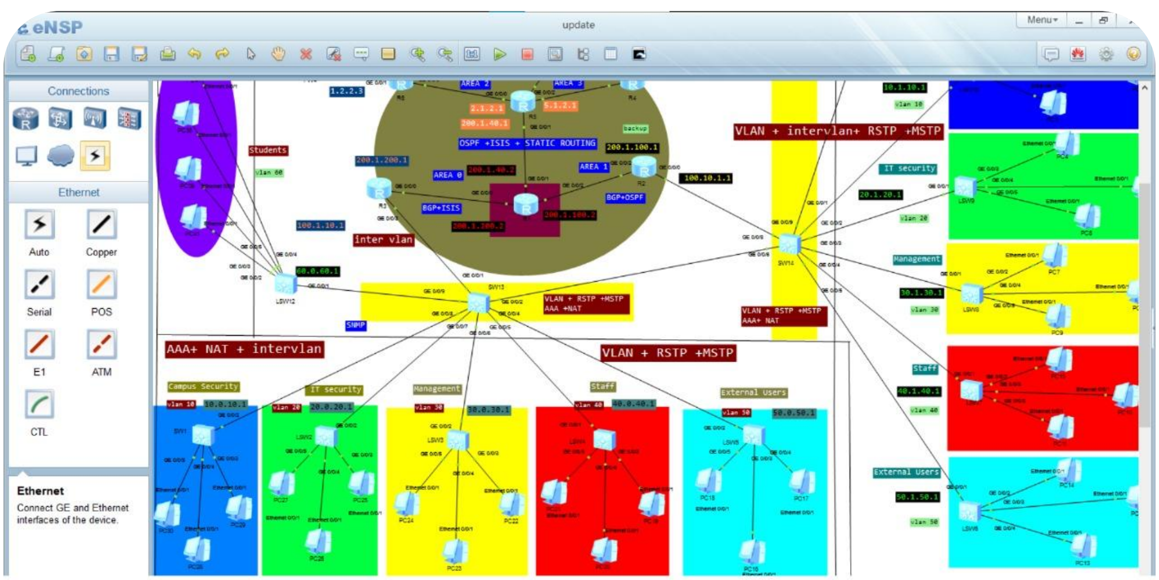
This project successfully demonstrates a comprehensive, enterprise-grade network connecting two colleges under one university system. The network is scalable, secure, and structured according to industry standards, using advanced routing and switching technologies.

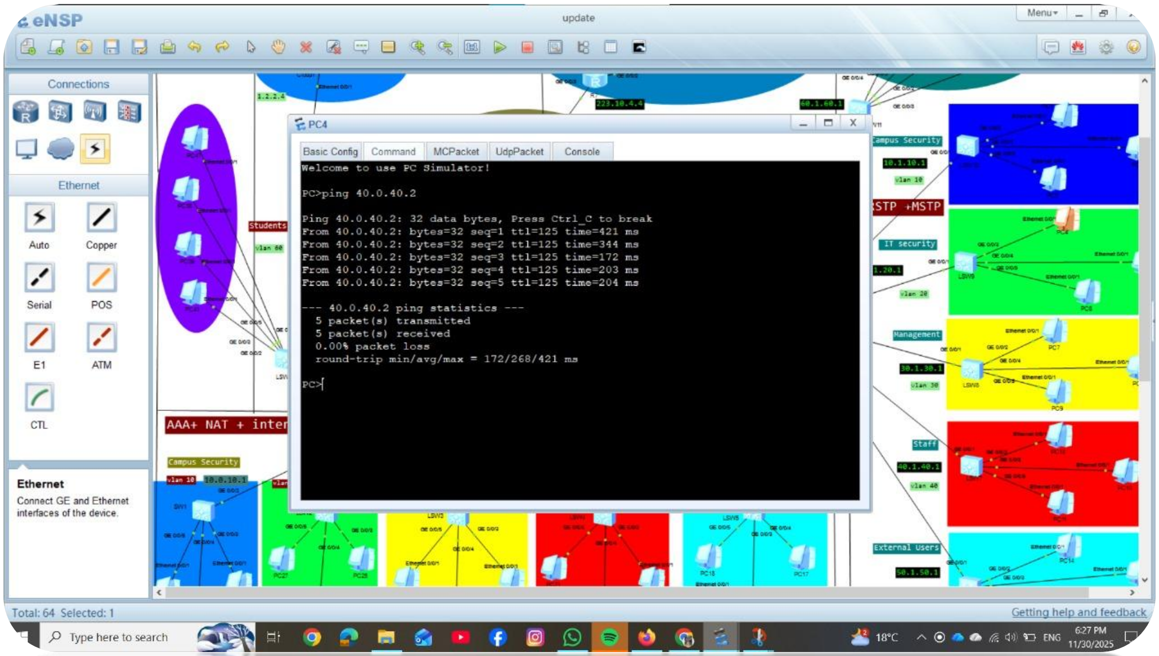
The design ensures:

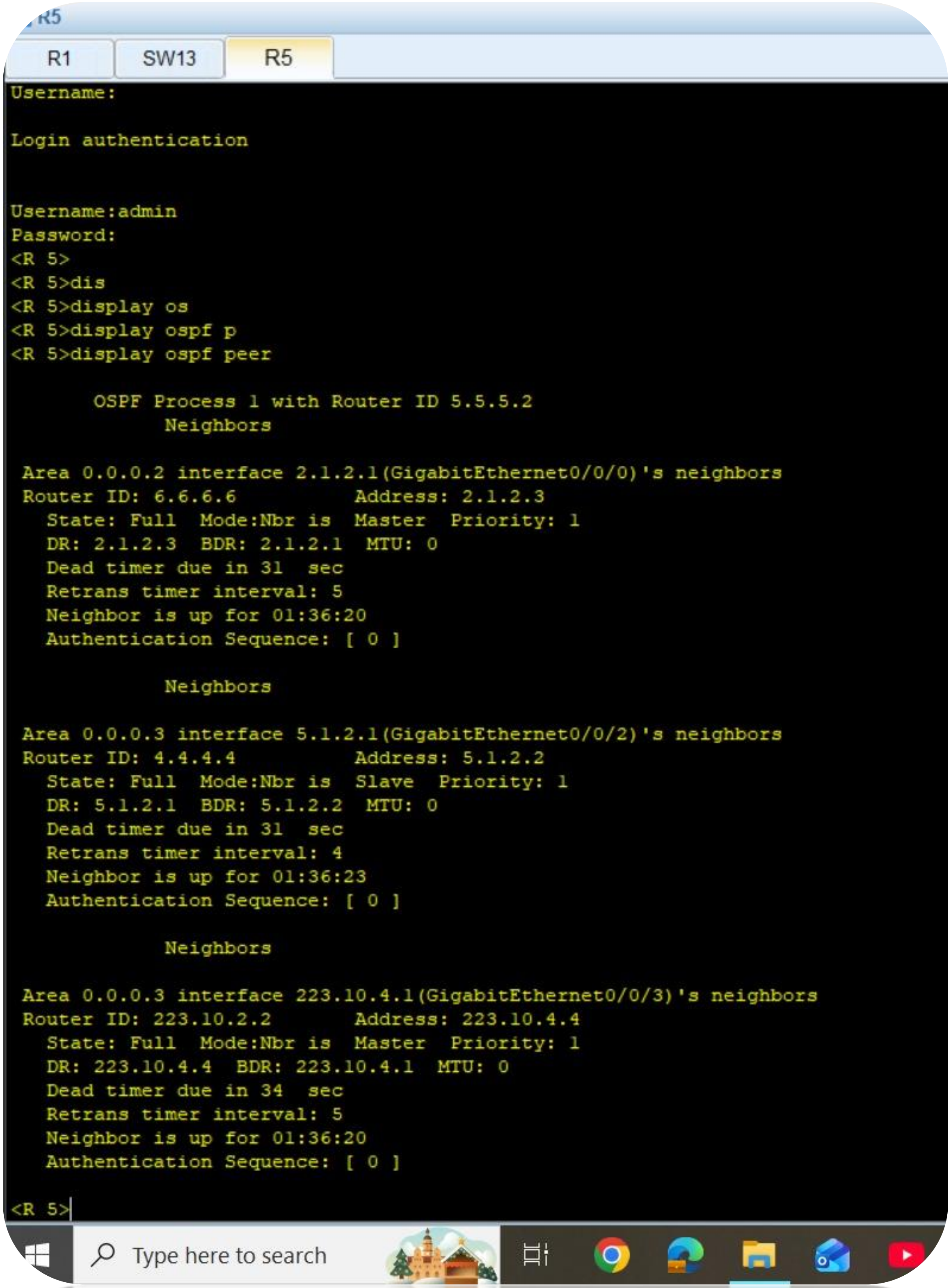
- Efficient communication
- High availability
- Strong security
- Clear segmentation
- Professional management of users and services

This network model can serve as a blueprint for real educational institutions.


eNSP
update
Connections
Ethernet
Auto
Copper
Serial
POS
E1
ATM
CTL
Ethernet
Connect GE and Ethernet interfaces of the device.
UNVERSITY SYSTEM NETWORK
VPN
BGP + MPLS
AREA 2
AREA 3
OSPF +ISIS + STATIC ROUTING
AREA 0
AREA 1
BGP+ISIS
BGP+OSPF
inter vlan
Students
VLAN + intervlan+ RSTP +MSTP
Campus Security
IT security
Management
Staff
VLAN + RSTP +MSTP
AAA +NAT
VLAN + RSTP +MSTP
AAA+ NAT
AAA+ NAT + intervlan
VLAN + RSTP +MSTP
External users
SNMP
ROUTING:
OSPF+ISIS+BGP+MPLS
SWITCHING:
VLAN+INTRVLAN+AAA+
RSTP+NAT
SeCURITY
SNMP+DNS+DMZ+VPN
Total: 64 Selected: 0
Getting help and feedback
Type here to search
19°C
ENG
6:22 PM
11/30/2025


eNSP
update
Connections
Ethernet
Auto
Copper
Serial
POS
E1
ATM
CTL
Ethernet
Connect GE and Ethernet interfaces of the device.
OSPF +ISIS + STATIC ROUTING
AREA 0
AREA 1
BGP+ISIS
BGP+OSPF
inter vlan
Students
VLAN + intervlan+ RSTP +MSTP
IT security
Management
Staff
External users
VLAN + RSTP +MSTP
AAA +NAT
VLAN + RSTP +MSTP
AAA+ NAT
AAA+ NAT + intervlan
VLAN + RSTP +MSTP
Campus Security
IT security
Management
Staff
External users
SNMP


eNSP
update
Connections
Ethernet
Auto
Copper
Serial
POS
E1
ATM
CTL
Ethernet
Connect GE and Ethernet interfaces of the device.
PC4
Basic Config
Command
MCPacket
UdpPacket
Console
Welcome to use PC Simulator!
PC>ping 40.0.40.2
Ping 40.0.40.2: 32 data bytes, Press Ctrl_C to break
From 40.0.40.2: bytes=32 seq=1 ttl=125 time=421 ms
From 40.0.40.2: bytes=32 seq=2 ttl=125 time=344 ms
From 40.0.40.2: bytes=32 seq=3 ttl=125 time=172 ms
From 40.0.40.2: bytes=32 seq=4 ttl=125 time=203 ms
From 40.0.40.2: bytes=32 seq=5 ttl=125 time=204 ms
--- 40.0.40.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 172/268/421 ms
PC>
Campus Security
IT security
Management
Staff
External users
Students
AAA+ NAT + inter
Total: 64 Selected: 1
Getting help and feedback
Type here to search
18°C
ENG
6:27 PM
11/30/2025



```
R1    SW13    R5
Username:

Login authentication


Username:admin
Password:
<R 5>
<R 5>dis
<R 5>display os
<R 5>display ospf p
<R 5>display ospf peer

       OSPF Process 1 with Router ID 5.5.5.2
             Neighbors

 Area 0.0.0.2 interface 2.1.2.1(GigabitEthernet0/0/0)'s neighbors
 Router ID: 6.6.6.6          Address: 2.1.2.3
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 2.1.2.3  BDR: 2.1.2.1  MTU: 0
   Dead timer due in 31  sec
   Retrans timer interval: 5
   Neighbor is up for 01:36:20
   Authentication Sequence: [ 0 ]

             Neighbors

 Area 0.0.0.3 interface 5.1.2.1(GigabitEthernet0/0/2)'s neighbors
 Router ID: 4.4.4.4          Address: 5.1.2.2
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 5.1.2.1  BDR: 5.1.2.2  MTU: 0
   Dead timer due in 31  sec
   Retrans timer interval: 4
   Neighbor is up for 01:36:23
   Authentication Sequence: [ 0 ]

             Neighbors

 Area 0.0.0.3 interface 223.10.4.1(GigabitEthernet0/0/3)'s neighbors
 Router ID: 223.10.2.2       Address: 223.10.4.4
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 223.10.4.4  BDR: 223.10.4.1  MTU: 0
   Dead timer due in 34  sec
   Retrans timer interval: 5
   Neighbor is up for 01:36:20
   Authentication Sequence: [ 0 ]

<R 5>
```

PC25

Basic Config | Command | MCPacket | UdpPacket | Console

```
Ping 60.1.60.2: 32 data bytes, Press Ctrl_C to break
From 60.1.60.2: bytes=32 seq=1 ttl=125 time=500 ms
From 60.1.60.2: bytes=32 seq=2 ttl=125 time=234 ms
From 60.1.60.2: bytes=32 seq=3 ttl=125 time=250 ms
From 60.1.60.2: bytes=32 seq=4 ttl=125 time=250 ms
From 60.1.60.2: bytes=32 seq=5 ttl=125 time=172 ms

--- 60.1.60.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 172/281/500 ms

PC>ping 50.1.50.2

Ping 50.1.50.2: 32 data bytes, Press Ctrl_C to break
From 50.1.50.2: bytes=32 seq=1 ttl=125 time=547 ms
From 50.1.50.2: bytes=32 seq=2 ttl=125 time=265 ms
From 50.1.50.2: bytes=32 seq=3 ttl=125 time=219 ms
From 50.1.50.2: bytes=32 seq=4 ttl=125 time=250 ms
From 50.1.50.2: bytes=32 seq=5 ttl=125 time=250 ms

--- 50.1.50.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 219/306/547 ms

PC>ping 30.1.30.3

Ping 30.1.30.3: 32 data bytes, Press Ctrl_C to break
From 30.1.30.3: bytes=32 seq=1 ttl=125 time=313 ms
From 30.1.30.3: bytes=32 seq=2 ttl=125 time=203 ms
From 30.1.30.3: bytes=32 seq=3 ttl=125 time=219 ms
From 30.1.30.3: bytes=32 seq=4 ttl=125 time=171 ms
From 30.1.30.3: bytes=32 seq=5 ttl=125 time=204 ms

--- 30.1.30.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 171/222/313 ms

PC>
```