CISCO Networking Academy

# Enterprise Network Infrastructure Enhancement

**UTM Faculty of Computing Expansion (Block N28B) - Phase 2**

**Author:** Aiman Nurzharfan Bin Mohd Ali Yusni

# Table of Contents

# 1. Introduction & Scope

## 1.1 Background

The initial phase of this project, detailed in the Network Design Report, focused on the physical layer (Layer 1) requirements for Block N28B. This included feasibility studies, hardware procurement, structured cabling planning, and cost analysis required by the university curriculum.

## 1.2 Project Evolution (Personal Initiative)

This document details Phase 2, a personal initiative to transform the physical design into a fully functional, logically segmented, and secure enterprise network simulation. Moving beyond static planning, this phase implements advanced Layer 2 and Layer 3 protocols to simulate a real-world production environment.

**Key enhancements include:**

- **Dynamic Routing**: Transitioning from static routing to OSPF for network-wide convergence.
- **Traffic Isolation**: Implementing VLANs to secure data at the switch level.
- **Security Policy Enforcement**: Using Extended ACLs to protect critical assets (Video Conference Room) and restrict high-risk zones (Student Lounge).
- **Internet Connectivity**: Configuring NAT/PAT to allow private internal subnets to communicate with external ISP networks.

## 2. Network Topology

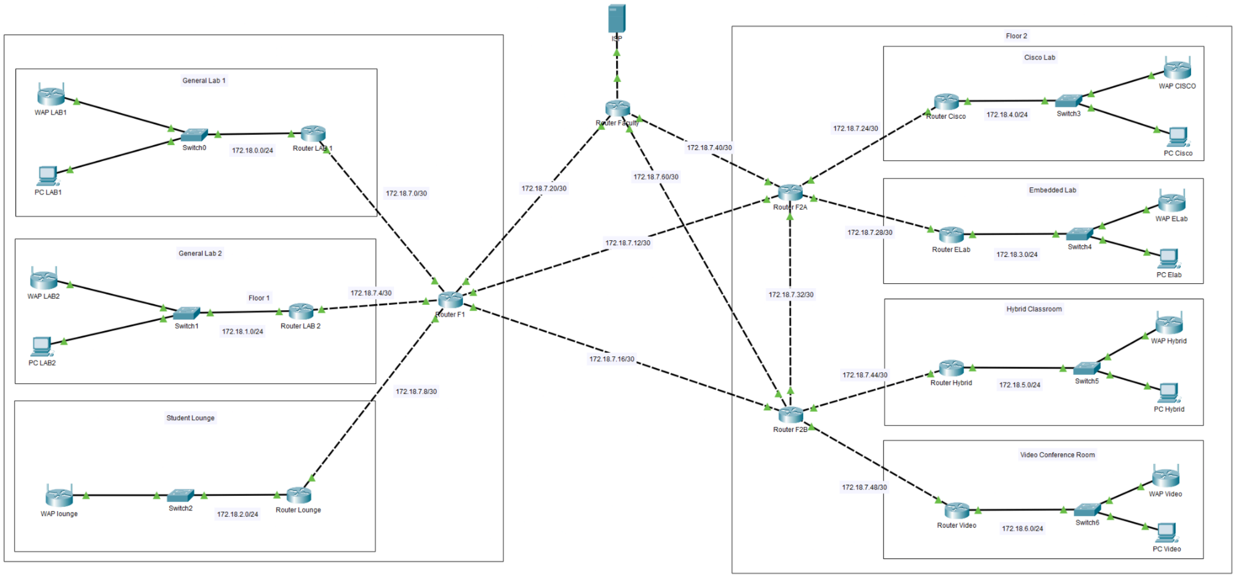

Image 2.1 : Network Topology

This logical topology utilizes a hierarchical star design, connecting the Faculty Core Router to distinct distribution layers for the Ground Floor and Second Floor. This structure ensures fault isolation and simplifies management.

## 2.1 Interface Configuration & IP Addressing

The network utilizes a hierarchical IP addressing scheme based on Variable Length Subnet Masking (VLSM). The following tables detail the interface assignments for the Ground Floor, Second Floor, and the Core Edge, ensuring efficient address allocation and logical separation.

**Section 1: Ground Floor (Floor 1 Distribution)**
This segment covers the General Purpose Labs, Student Lounge, and the Floor 1 Distribution Router (F1).

| Device Name | Interface | Connection / Description | IP Address | Subnet Mask | Network Address |
|---|---|---|---|---|---|
| **Router F1** | Gig2/0 | Link to Lab 1 | 172.18.7.1 | 255.255.255.252 | 172.18.7.0 |
| | Gig1/0 | Link to Lab 2 | 172.18.7.5 | 255.255.255.252 | 172.18.7.4 |
| | Gig0/0 | Link to Lounge | 172.18.7.9 | 255.255.255.252 | 172.18.7.8 |
| | Gig4/0 | Link to F2A (Backbone) | 172.18.7.13 | 255.255.255.252 | 172.18.7.12 |
| | Gig3/0 | Link to F2B (Backbone) | 172.18.7.17 | 255.255.255.252 | 172.18.7.16 |
| | Gig5/0 | Uplink to Faculty | 172.18.7.21 | 255.255.255.252 | 172.18.7.20 |
| **Router LAB 1** | Gig0/0 | Uplink to F1 | 172.18.7.2 | 255.255.255.252 | 172.18.7.0 |
| | Gig0/1 | LAN Gateway | 172.18.0.1 | 255.255.255.0 | 172.18.0.0 |
| **Router LAB 2** | Gig0/0 | Uplink to F1 | 172.18.7.6 | 255.255.255.252 | 172.18.7.4 |
| | Gig0/1 | LAN Gateway | 172.18.1.1 | 255.255.255.0 | 172.18.1.0 |
| **Router Lounge** | Gig0/0 | Uplink to F1 | 172.18.7.10 | 255.255.255.252 | 172.18.7.8 |
| | Gig0/1 | LAN Gateway | 172.18.2.1 | 255.255.255.0 | 172.18.2.0 |

**Section 2: Second Floor (Floor 2 Distribution)**
This segment covers the Specialized Labs (Embedded, Cisco), Hybrid Classrooms, Video Conference Room, and the redundant Floor 2 routers (F2A & F2B).

| Device Name | Interface | Connection / Description | IP Address | Subnet Mask | Network Address |
|---|---|---|---|---|---|
| **Router F2A** | Gig1/0 | Link to Cisco Lab | 172.18.7.25 | 255.255.255.252 | 172.18.7.24 |
| | Gig0/0 | Link to Embedded Lab | 172.18.7.29 | 255.255.255.252 | 172.18.7.28 |
| | Gig2/0 | Link to F1 | 172.18.7.14 | 255.255.255.252 | 172.18.7.12 |
| | Gig3/0 | Link to F2B | 172.18.7.33 | 255.255.255.252 | 172.18.7.32 |
| | Gig4/0 | Uplink to Faculty | 172.18.7.41 | 255.255.255.252 | 172.18.7.40 |
| **Router ELab** | Gig0/0 | Uplink to F2A | 172.18.7.30 | 255.255.255.252 | 172.18.7.28 |
| | Gig0/1 | LAN Gateway | 172.18.3.1 | 255.255.255.0 | 172.18.3.0 |
| **Router Cisco** | Gig0/0 | Uplink to F2A | 172.18.7.26 | 255.255.255.252 | 172.18.7.24 |
| | Gig0/1 | LAN Gateway | 172.18.4.1 | 255.255.255.0 | 172.18.4.0 |
| **Router F2B** | Gig1/0 | Link to Hybrid Class | 172.18.7.45 | 255.255.255.252 | 172.18.7.44 |
| | Gig0/0 | Link to Video Room | 172.18.7.49 | 255.255.255.252 | 172.18.7.48 |
| | Gig2/0 | Link to F1 | 172.18.7.18 | 255.255.255.252 | 172.18.7.16 |
| | Gig3/0 | Link to F2A | 172.18.7.34 | 255.255.255.252 | 172.18.7.32 |
| | Gig4/0 | Uplink to Faculty | 172.18.7.61 | 255.255.255.252 | 172.18.7.60 |
| **Router Hybrid** | Gig0/0 | Uplink to F2B | 172.18.7.46 | 255.255.255.252 | 172.18.7.44 |
| | Gig0/1 | LAN Gateway | 172.18.5.1 | 255.255.255.0 | 172.18.5.0 |
| **Router Video** | Gig0/0 | Uplink to F2B | 172.18.7.50 | 255.255.255.252 | 172.18.7.48 |
| | Gig0/1 | LAN Gateway | 172.18.6.1 | 255.255.255.0 | 172.18.6.0 |

**Section 3: Core Layer & Internet Edge**

This segment details the Main Faculty Router which handles inter-floor routing and the NAT connection to the ISP.

| Device Name | Interface | Connection / Description | IP Address | Subnet Mask | Network Address |
|---|---|---|---|---|---|
| **Router Faculty** | Gig0/0 | Downlink to F1 | 172.18.7.22 | 255.255.255.252 | 172.18.7.20 |
| | Gig1/0 | Downlink to F2A | 172.18.7.42 | 255.255.255.252 | 172.18.7.40 |
| | Gig2/0 | Downlink to F2B | 172.18.7.62 | 255.255.255.252 | 172.18.7.60 |
| | Gig3/0 | **WAN / ISP Link**<br>(NAT Outside) | 200.200.200.2 | 255.255.255.252 | 200.200.200.0 |
| **ISP Server** | NIC | Service Provider Gateway | 200.200.200.1 | 255.255.255.252 | 200.200.200.0 |

## 3. Technical Implementation

### 3.1 Dynamic Routing (OSPF)

To ensure scalability and fault tolerance, Open Shortest Path First (OSPF) was deployed across the Core and Distribution layers. Unlike static routing, OSPF allows the routers to automatically learn new paths and re-route traffic if a link fails.

- **Area**: Single Area OSPF (Area 0 / Backbone).
- **Configuration**: All 13 routers participate in OSPF Process 1.
- **Benefit**: Enables full connectivity between Floor 1 (General Labs) and Floor 2 (Specialized Labs) without manual route maintenance.

### 3.2 Network Segmentation (VLANs)

To reduce broadcast domains and improve local security, Virtual Local Area Networks (VLANs) were standardized across all access switches. This ensures that only authorized physical ports have access to the routing infrastructure.

| VLAN ID | Name | Purpose |
|---|---|---|
| **1** | Default | Management / Unused Ports (Security disabled) |
| **10** | **DATA** | Authorized User Traffic (Labs, Faculty, Staff) |

- **Implementation:** Ports `Fa0/1` through `Fa0/10` and the Uplink `Gig0/1` are assigned to **VLAN 10**.
- **Security Benefit:** "Port Security by Separation." Any device plugged into unauthorized ports (Fa0/11-24) remains in VLAN 1 and cannot communicate with the Router Gateway or the Internet.

### 3.3 Interface Configuration & IP Addressing

To simulate real-world internet connectivity, Port Address Translation (PAT) was configured on the Faculty Core Router. This hides internal topology details from the public internet while providing connectivity.

- **Inside Network**: 172.18.0.0/20 (Private Internal).
- **Outside Interface**: GigabitEthernet 3/0 (Connected to ISP Server).
- **Mechanism**: NAT Overload allows hundreds of internal student devices to share a single Public IP (200.200.200.2) when accessing external resources.

# 4. Security Policies (ACLs)

Security was prioritized by implementing "Bouncer" and "Restriction" policies using Extended Access Control Lists (ACLs). These rules enforce strict traffic flow control based on user roles and room functions.

## 4.1 Policy Definitions

| Policy Name | Source Location | Target / Destination | Action / Behavior |
|---|---|---|---|
| **Video Room Isolation** | **External**<br>(Any Lab) | **Video Room**<br>(172.18.6.0) | **BLOCK INBOUND:** Prevents unauthorized connections from initiating contact with the Video Room.<br>**PERMIT OUTBOUND:** Allows Video Room to initiate calls and receive replies. |
| **Student Lounge Restriction** | **Student Lounge**<br>(172.18.2.0) | **Internal Labs**<br>(172.18.0.0/16) | **BLOCK INTERNAL:** Students cannot access sensitive areas (Embedded Lab, Cisco Lab, Staff PCs).<br>**PERMIT INTERNET:** Students can still access the Internet. |

## 5. Testing & Verification

The following validation procedures were executed to confirm network stability and policy enforcement. These tests ensure the network meets all operational and security requirements.

### Test 1: OSPF Convergence

- Objective: Verify that routers automatically learn paths to remote subnets.
- Method: Run `show ip route` on the Faculty Router.
- Success Criteria: The routing table displays `O` (OSPF) entries for all subnets (172.18.0.0 through 172.18.6.0).

### Test 2: VLAN Isolation

- Objective: Verify that devices on unauthorized switch ports cannot access the network.
- Method: Move a PC cable from Port 1 (VLAN 10) to Port 15 (VLAN 1).
- Success Criteria: The PC loses connectivity to its Gateway (Ping `172.18.0.1` fails / Request Timed Out).

### Test 3: Security Policy Enforcement (ACLs)

**A. Video Room "Bouncer" Test:**

- Attack Simulation: From General Lab 1, attempt to Ping Video Room PC (`172.18.6.10`).
  - *Result:* Destination Host Unreachable (Blocked by Router).
- Functionality Check: From Video Room PC, attempt to Ping General Lab 1.
  - *Result:* Reply Received (Traffic allowed out, reply allowed in).

**B. Student Lounge Restriction Test:**

- Intrusion Simulation: From Student Lounge PC, attempt to Ping Cisco Lab.
  - *Result:* Destination Host Unreachable (Blocked at Source).
- Access Check: From Student Lounge PC, attempt to Ping Internet ISP (`200.200.200.1`).
  - *Result:* Reply Received (Internet access permitted).

### Test 4: Internet Connectivity (NAT)

- Objective: Verify internal private IPs are translated to public IPs.
- Method: Ping the ISP Server (`200.200.200.1`) from an internal Lab PC, then inspect the Faculty Router.
- Command: `show ip nat translations`
- Success Criteria: The table lists internal local IPs (e.g., `172.18.0.10`) mapping to the global outside IP (`200.200.200.2`).