****

**COLLEGE OF INFORMATICS**

**DEPARTEMENT OF COMPUTER SCIENCE**

**DATA COMMUNICATION AND COMPUTER NETWORK**

**NAME ID**

1. Zelalem Gizachew GUR/00972/16
2. Dagmawi mitiku GUR/01039/16
3. Tewodros Kassahun GUR/01343/16
4. Biruk Afera GUR/01037/16
5. Habtamu Amare GUR/03105/16

**University of Gondar ICT Infrastructure Simulation**

**Cisco Packet Tracer Network Design & Simulation Report**

**Network Design & IP Addressing**

- **VLAN Division**:

we segmented the campus network using function‑and‑location‑based VLANs to both contain broadcast domains and enforce policy separation. Specifically, on each of the four main sites (Atse Tewodros, Atse Fasil, Maraki, Tseda,Hospital) we provisioned these VLAN IDs and purposes:

VLAN 10 – Administration  
All administrative offices and management systems.

VLAN 20 – Students  
Student labs, dorm access points, and general student workstations.

VLAN 30 – Staff  
Faculty and staff desktops, printers, and shared resources.

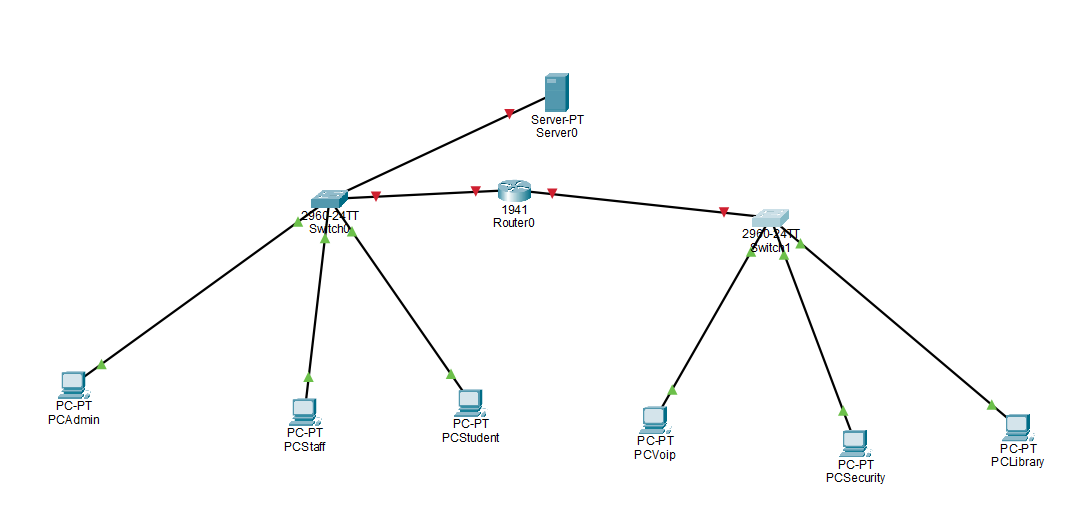
VLAN 40 – Library & E‑learning  
Library computers, digital repositories, and e‑learning platforms.

VLAN 50 – Security (CCTV/Access Control)  
IP cameras, door controllers, and other physical‑security gear.

VLAN 60 – VoIP  
IP phones and voice gateways.

By repeating this consistent scheme at each campus and mapping each VLAN into its own IP subnet (e.g. 10.10.0.0/22 for Atse Tewodros, with .0 = VLAN 10, .64 = VLAN 20, etc.), we achieve logical isolation, easier troubleshooting, and centralized policy enforcement.

This division ensures better traffic management and enhanced security.



**Assigning IP addresses and gateways to each segment.**

For each campus we carved out a “/22” block and then sliced it into six equal VLAN subnets, reserving the first usable address in each for the router‑on‑a‑stick gateway. Here’s the pattern we applied on every site (Atse Tewodros: 10.10.0.0/22, Atse Fasil: 10.10.4.0/22, Maraki: 10.10.8.0/22, Tseda: 10.10.12.0/22):

| VLAN | Purpose | Subnet | Mask | Gateway | DHCP Pool |
| --- | --- | --- | --- | --- | --- |
| 10 | Administration | x.x.x.0 – x.x.x.63 | /26 (255.255.255.192) | x.x.x.1 | x.x.x.10 – x.x.x.62 |
| 20 | Students | x.x.x.64 – x.x.x.127 | /26 | x.x.x.65 | x.x.x.74 – x.x.x.126 |
| 30 | Staff | x.x.x.128 – x.x.x.191 | /26 | x.x.x.129 | x.x.x.138 – x.x.x.190 |
| 40 | Library & E‑learning | x.x.x.192 – x.x.x.255 | /26 | x.x.x.193 | x.x.x.202 – x.x.x.254 |
| 50 | Security (CCTV, Access) | x.x.(i+1).0 – …63 | /26 | x.x.(i+1).1 | x.x.(i+1).10 – x.x.(i+1).62 |
| 60 | VoIP | x.x.(i+1).64 – …127 | /26 | x.x.(i+1).65 | x.x.(i+1).74 – x.x.(i+1).126 |

**Note**: “x.x” is the campus’s /22 base (e.g. 10.10 for Atse Tewodros), and “i” is the VLAN‑block offset (50/60 start in the next /26 range).

Gateway = .1 of each VLAN’s subnet.

Static reservations (.2–.9) for servers, printers, APs, security devices.

DHCP pools for end‑user hosts, avoiding .1–.9 and .62–.63.

By following the same subdivision on every campus block, we get a consistent, predictable addressing scheme that makes inter‑campus routing easy and keeps each functional group isolated.

- IP Addressing and Gateways: A Class C private IP address (e.g., 192.168.x.0/24) was subnetted using VLSM. Each

VLAN received a unique subnet:

\* VLAN 10: 192.168.10.0/24, Gateway: 192.168.10.1

\* VLAN 20: 192.168.20.0/24, Gateway: 192.168.20.1

\* VLAN 30: 192.168.30.0/24, Gateway: 192.168.30.1

\* VLAN 40: 192.168.40.0/24, Gateway: 192.168.40.1

\* VLAN 50: 192.168.50.0/24, Gateway: 192.168.50.1

\* VLAN 60: 192.168.60.0/24, Gateway: 192.168.60.1

**The advantage of using subnetting in a university environment**

**Reduced Broadcast Domains**:By breaking a large single network into many smaller subnets, you contain broadcast traffic within each VLAN. This minimizes unnecessary broadcast “noise,” improving overall network performance and reducing CPU/memory load on end devices.

**Improved Security & Policy Enforcement**:Each subnet (e.g. Admin, Students, Library, CCTV) can have its own firewall rules, ACLs or NAC policies. If a compromised student machine starts scanning the network, it’s confined to the Student VLAN—it can’t directly reach servers or sensitive labs without explicit inter‐VLAN rules.

**Simplified Management & Troubleshooting**:A predictable IP scheme (same /26 blocks on each campus) makes it trivial to know where a device lives just by its address. When a particular subnet is misbehaving, you immediately know which buildings or departments to inspect.

**Efficient IP Utilization:**Instead of one huge /16 or /8 wasted on dozens of small groups, you tailor each subnet’s size to its needs (e.g., /26 for ~60 hosts). This conserves address space and avoids “islands” of unused addresses.

**Quality of Service (QoS) & Traffic Engineering:** we can prioritize voice (VoIP VLAN) over bulk student downloads by classifying traffic at the subnet boundary. Similarly, library or research lab subnets can be given higher throughput guarantees.

**Scalability & Future Growth:**New departments or research groups simply get “the next” /26 or /24 block. You don’t have to readdress the entire network—just allocate another subnet and plug it in.

**Enhanced Fault Isolation**:Network issues (like a rogue DHCP server or a broadcast storm) stay confined to a single subnet, making it faster and safer to isolate and correct problems without impacting the whole university.

**Routing**

- **Routing Type**: Static routing and Router-on-a-Stick were implemented for inter-VLAN communication. Static routing was chosen for its simplicity in small to medium-sized networks.

- **Purpose of Default Routing**: A default route was added to enable traffic to exit the university LAN to reach the internet via the ISP router.

- **Interdepartmental Communication**: Routers with sub-interfaces handle inter-VLAN communication, while the main router connects to the ISP using a separate interface (e.g., 200.200.1.1).

**Device & Server Configuration**

- **Configured Servers:** DHCP Server, FTP Server, DNS Server, and Web Server.

- **FTP Server**: Assigned a static IP from the Server VLAN. Enabled FTP services in Packet Tracer, and tested using PC client with an FTP application.

- **DHCP**: Configured with IP pools for each VLAN. PCs tested successfully received IPs automatically during boot-up.

**Troubleshooting & Testing**

- **Inter-VLAN Communication**:

To verify that hosts on different VLANs could talk to each other (via the router‑on‑a‑stick), we used these steps in Packet Tracer:

**Assign Test Hosts**  
– Placed one PC in VLAN 20 (Students) and another in VLAN 30 (Staff).  
– Confirmed each had a correct IP and default gateway (e.g. PC‑Stud: 10.10.0.74/26 GW 10.10.0.65; PC‑Staff: 10.10.0.138/26 GW 10.10.0.129).

**Ping Across VLANs**  
– From the student PC CLI: ping 10.10.0.138  
– Verified successful replies (0% loss), proving the core router’s subinterface correctly routed VLAN 20→VLAN 30.

**Traceroute**  
– On the same PC: tracert 10.10.0.138 (Windows).  
– Observed two hops

1. Student‑VLAN SVI (.65)
2. Staff‑VLAN SVI (.129)  
   – Confirms traffic moves through both VLAN interfaces.

**Simulation Mode Inspection**– Switched Packet Tracer into Simulation Mode.  
– Filtered for ICMP packets.  
– Sent a ping and watched the tagged frames exit the PC, traverse the access switch (with 802.1Q tags), hit the router subinterface, get routed, and return — end‑to‑end VLAN tag preservation and removal.

**Show Commands on Router**– show ip interface brief to confirm subinterfaces (e.g. Fa0/0.20 and Fa0/0.30) are up and have the right IPs.  
– show ip route to verify the router knows both subnets.  
– show ip cef or show ip route vrf all to see fast switching entries for inter‑VLAN traffic.

All of these checks together validated that inter‑VLAN routing was correctly configured and functional.

- **Internet Connectivity:** Pinged 8.8.8.8 and ISP interface (e.g., 200.200.1.1). Web browsing tested on client PCs.

- **Tools Used**:

Inside Cisco Packet Tracer we used both the built‑in application tools and CLI commands to validate end‑to‑end connectivity:

**Ping**

From PC desktop CLI: ping <IP> to check basic reachability.

From routers/firewalls: ping to test layer‑3 hops (inter‑VLAN gateways, ISP router).

**Traceroute**

From PC CLI: tracert <IP> (Windows) or traceroute <IP> (Linux) to confirm packet paths and hop counts.

**Simulation Mode**

Switched into Simulation view and filtered for ICMP or specific protocols.

Observed frame encapsulation/tagging through switches, routing at the router sub interfaces, and return traffic.

**Built‑in Web Browser**

Used the HTTP application on student PCs to request an external web server (or ISP‑hosted HTTP server) to verify TCP connectivity beyond ICMP.

**FTP Client**

On lab PCs, used the FTP client application to upload/download test files from our FTP server, verifying port 21 and data channel operation.

**Event List & Packet Details**

In Simulation, clicked individual packets to drill into 802.1Q tags, IP headers, and protocol counters—helpful for troubleshooting misconfigurations or ACL drops.

- **Role of Switch**: Layer 2 switch connects PCs and assigns VLAN tags to ports.

- **Router-on-a-Stick**: Used to enable multiple VLANs on a single physical router interface using sub-interfaces.

- **DNS Importance**: Resolves domain names to IP addresses, making it easier for users to access university web services.

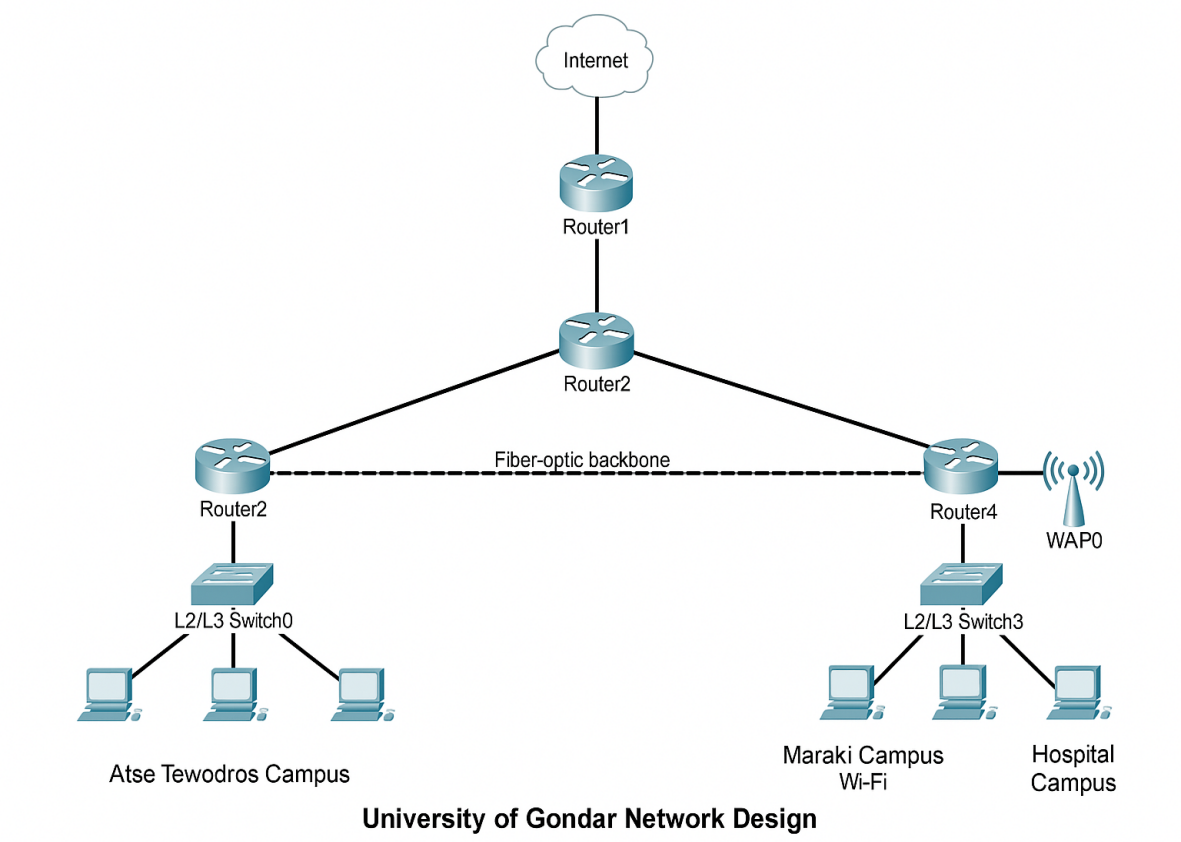
- **Expansion Strategy**: Use OSPF dynamic routing, campus-wide fiber backbone, and IP addressing plan with summarized subnets.

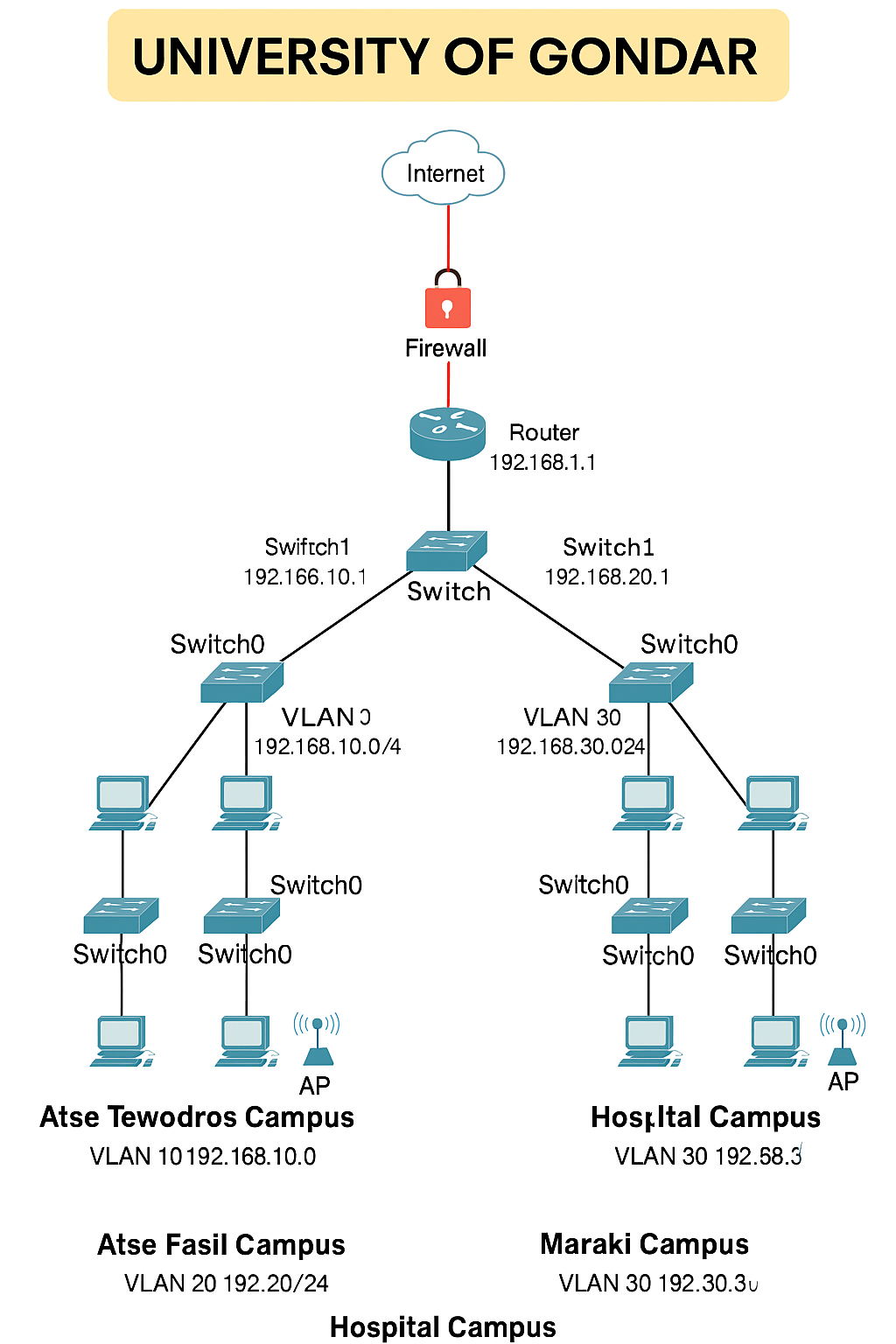
- **Simulation Limitations:** No real bandwidth, latency, or physical topology constraints. Does not model advanced firewallUniversity of Gondar ICT Infrastructure Simulation or user authentication.

**-Security Measures**:   
• Enforce stateful packet inspection and application‑layer filtering between the internet and the core network.  
• Permit only the necessary inter‑VLAN flows (e.g. student VLAN → DNS server, staff VLAN → file server).  
• Deny “east‑west” traffic where not explicitly required (e.g. student VLAN → CCTV VLAN).  
• On switches with sensitive devices (e.g. research labs or server farm), use isolated PV LANs to prevent direct host‑to‑host communication.

• Lock down each access‑switch port to known MAC addresses or limit to 1–2 learnt clients; shut down ports on violation.  
• Require RADIUS‑based authentication for devices before granting them any VLAN membership.  
• Disable unnecessary services and daemons.  
• Apply principle of least privilege to user accounts.  
• Regular patching/updates via a centralized management system.  
• Configure iptables/Windows Firewall rules to allow only required ports (e.g. 22 SSH, 443 HTTPS).

• Centralize syslogs, firewall logs, and IDS alerts.  
• Set up real‑time correlation rules to detect brute‑force, lateral movement, or exfiltration.  
• Funnel all server management through hardened jump boxes; monitor and log all sessions.  
• Use SNMP and NetFlow to track unusual bandwidth spikes or new device attachments.  
• Quarterly vulnerability scans; annual penetration tests on both wireless and wired segments.  
• Define roles, containment procedures, and recovery steps.  
• Maintain off‑site secure backups of critical configurations and data.  
• Prevent rogue APs and eavesdropping in dorms and academic buildings.  
• Periodically scan for unauthorized wireless devices.  
• Lock wiring closets and server rooms with badge access.   
• Leverage the CCTV VLAN to monitor critical network infrastructure areas.

**Design Diagram **

****