UNIVERSITY OF GONDAR

COLLAGE OF INFORMATICS

DEPERTMENT OF COMPUTER SCIENCE

Networking Assignment

No	NAME		ID
1.	Bezawit	Bekele	01106/16
2.	Bezawit	Degu	02084/15
3.	Hawlet	Husen	02850/16
4.	Kalkidan	Ayalew	02775/16
5.	Sada	Murad	02912/16

SUMMITTED TO:HAILU

S SUMMITTEDDATE:19/6/2025

Table of Contents

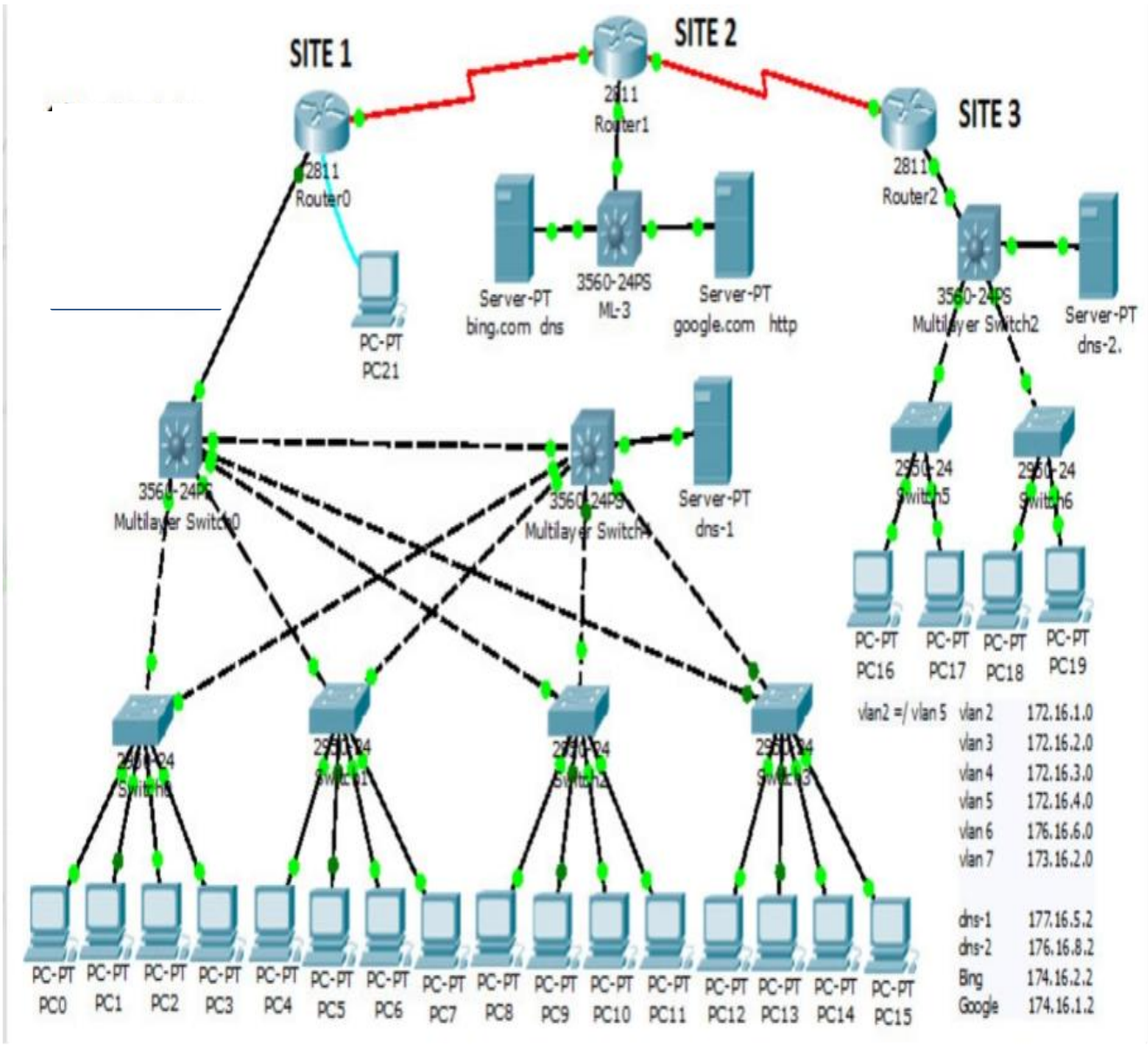
Introduction

This document presents a comprehensive analysis of the network topology depicted in the accompanying diagram, which is conceptualized as a foundational representation of **Gondar University's campus network infrastructure**. This design illustrates a strategic approach to connecting geographically and functionally distinct operational areas—designated as Site 1, Site 2, and Site 3—to form a cohesive, resilient, and scalable university-wide network.

Our analysis will delve into the core architectural and implementation decisions underpinning this infrastructure. Specifically, we will examine **how network segments (VLANs) are strategically designed and divided** to ensure efficient traffic flow, enhance security across various university departments, and simplify network administration. We will further detail the **methodology for assigning IP addresses and default gateways** to each of these logical segments, which is critical for seamless internal communication and resource accessibility. A pivotal aspect of this network's functionality is its **routing implementation**, and we will explain the chosen routing protocols—whether static, dynamic, or default—and the rationale behind these selections for both intra-campus and external (ISP) connectivity. Finally, we will identify and discuss the roles of the **various servers configured within the topology**, highlighting their essential contributions to providing core network services for the university community.

analysis of the network segmentation strategy, specifically focusing on the utilization of Virtual Local Area Networks (VLANs), as depicted in the provided Cisco Packet Tracer diagram for a multi-site network infrastructure. While the original diagram labels the sites generically, for the purpose of this analysis, we will conceptually align this design with a potential University of Gondar campus network structure, comprising various distinct operational areas or buildings.

The primary objective of network segmentation, through the implementation of VLANs, is to enhance network security, optimize performance by reducing broadcast domains, and simplify network management and troubleshooting across different functional units or user groups within the university environment.


SITE 1
SITE 2
SITE 3
2811
Router0
2811
Router1
2811
Router2
PC-PT
PC21
Server-PT
bing.com dns
3560-24PS
ML-3
Server-PT
google.com http
3560-24PS
Multilayer Switch2
Server-PT
dns-2.
3560-24PS
Multilayer Switch0
3560-24PS
Multilayer Switch1
Server-PT
dns-1
2950-24
Switch5
2950-24
Switch6
PC-PT
PC16
PC-PT
PC17
PC-PT
PC18
PC-PT
PC19
vlan2 =/ vlan 5
vlan 2 172.16.1.0
vlan 3 172.16.2.0
vlan 4 172.16.3.0
vlan 5 172.16.4.0
vlan 6 176.16.6.0
vlan 7 173.16.2.0
dns-1 177.16.5.2
dns-2 176.16.8.2
Bing 174.16.2.2
Google 174.16.1.2
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
PC-PT
PC8
PC-PT
PC9
PC-PT
PC10
PC-PT
PC11
PC-PT
PC12
PC-PT
PC13
PC-PT
PC14
PC-PT
PC15

Network Design & IP Addressing

➢ divide network segments (VLANs)

Overview of Network Topology

The provided diagram illustrates a three-site network design, each interconnected via routing devices over what appears to be a Wide Area Network (WAN) backbone. Each site features core networking devices, including Routers and Multilayer Switches, which are fundamental to implementing a robust VLAN strategy.

- **Site 1:** Appears to be a primary academic or administrative building, hosting numerous PCs and multiple access switches.
- **Site 2:** Serves as a central server farm or data center, housing critical network services such as DNS and HTTP servers.
- **Site 3:** Represents another academic or departmental
- with end-user devices.

Network Segmentation Strategy (VLANs and Subnets)

The network segmentation strategy in this design is primarily based on the logical division of the network into VLANs, each assigned a specific IP subnet. This approach enables traffic isolation and controlled communication between different segments via routing.

Explicitly Defined VLANs (As per Diagram Annotations):

The diagram explicitly references several VLANs, indicating their direct implementation in the network:

- **VLAN 2:**
  - **Status:** Explicitly identified.
  - **Conceptual Purpose (University Context):** While the diagram does not provide an IP subnet or specific function, in a university setting, this VLAN could potentially be assigned to:
    - **Management Traffic:** For secure access to network devices' management interfaces.
    - **IoT Devices:** For Building Management Systems (BMS), smart sensors, or other Internet of Things devices within a campus building.
    - **Specific Departmental Devices:** For a small, specialized departmental network.
  - **Note:** The annotation "vlan 2 =/= vlan 5" clearly signifies that this is a distinct, isolated segment from VLAN 5, requiring a Layer 3 device (Multilayer Switch or Router) for inter-VLAN communication.
- **VLAN 3:**
  - **Associated IP Subnet:** `172.16.2.0`

    - **Conceptual Purpose (University Context):** This VLAN, being associated with a specific IP subnet, is a primary operational segment. In the context of a university, it would most likely be used for:
        - **Student Labs:** Computers in various teaching labs across campus, providing a standardized environment.
        - **General Classroom PCs:** Desktops used by students in lecture halls or shared study areas.
        - **General Administrative Staff:** Standard workstations for non-specialized administrative roles.
    - **Location:** Given its appearance near `PC0-PC5` in Site 1, it is highly probable that this VLAN is predominantly configured within **Site 1**, with its inter-VLAN routing handled by the `Multilayer Switch` in that site.
- **VLAN 5:**
    - **Status:** Explicitly identified.
    - **Conceptual Purpose (University Context):** Similar to VLAN 2, its specific function and IP details are not provided. In a university context, VLAN 5 could serve as:
        - **Faculty Workstations:** Dedicated and more secure access for academic staff.
        - **Library Resources:** PCs and terminals within the university library, potentially with specific access policies.
        - **Visitor Kiosks:** For public information points with limited network access.

➢ assigned IP addresses and gateways to each segment

Explain how IP addresses and default gateways would be assigned to each segment, based on the network diagram provided and standard networking practices. This explanation assumes the context of a university infrastructure as discussed previously.

The fundamental principle is that **each VLAN (network segment) needs its own unique IP subnet**, and a **default gateway** within that subnet to allow devices to communicate with other segments.

IP Address and Gateway Assignment Strategy

The assignment of IP addresses and default gateways in this network would follow a structured approach to ensure logical organization, prevent conflicts, and enable seamless communication between segments.

1. IP Addressing Scheme (Conceptual)

Given the specific IP addresses seen for servers and the `vlan 3` subnet, it appears a private IP addressing scheme is in use, likely from the `172.16.0.0/16` range or other private ranges (`10.0.0.0/8`, `192.168.0.0/16`). A hierarchical approach would be used:

- **Major Network Blocks for Sites:** Each site might be assigned a larger block of IP addresses to sub-divide.

    - **Site 1:** Could be `172.16.0.0/22` (or a similar block)
    - **Site 2 (Servers):** Could be `174.16.0.0/22` (or a similar block - though `174.x.x.x` is a public range, it's used privately in this Packet Tracer example)
    - **Site 3:** Could be `172.16.4.0/22` (or a similar block)
    - **WAN Interconnects:** Separate small subnets (e.g., `/30` or `/29`) for router-to-router links.
- **Subnetting for VLANs:** Within each major site block, smaller subnets would be allocated for individual VLANs. A subnet mask like `/24` (255.255.255.0) is common for user VLANs, providing 254 usable IPs. Server VLANs might be smaller, e.g., `/27` or `/28`, if fewer IPs are needed.

2. IP Address and Gateway Assignment for Each Segment (Based on Image Data)

Let's break down the assignment for the segments explicitly or implicitly identified in the image:

A. Explicitly Mentioned VLANs:

- **VLAN 3 (Network: `172.16.2.0/24`)**
    - **IP Address Range:** `172.16.2.1` through `172.16.2.254`
    - **Default Gateway:** `172.16.2.1`
    - **How Assigned:**
        - **Default Gateway:** The IP address `172.16.2.1` would be configured on a **Switched Virtual Interface (SVI)** on the **Multilayer Switch** in Site 1 (or the nearest Multilayer Switch responsible for routing this VLAN). This SVI (`interface vlan 3`) acts as the Layer 3 termination point for VLAN 3, enabling devices in VLAN 3 to reach other VLANs or networks.
        - **End Devices (e.g., PC0-PC5):** PCs in this VLAN would be configured to obtain IP addresses automatically via **DHCP**. The DHCP server would be set up to hand out IP addresses from the `172.16.2.0/24` range, with `172.16.2.1` as their default gateway. Alternatively, they could be manually configured (static IP).
- **VLAN 2 & VLAN 5** (Details not shown, assumed similar structure to VLAN 3)
    - **Conceptual IP Subnet:**
        - VLAN 2: e.g., `172.16.1.0/24` (assuming it's a separate segment from VLAN 3)
        - VLAN 5: e.g., `172.16.3.0/24` (assuming it's another distinct segment)
    - **Default Gateway:**
        - VLAN 2: e.g., `172.16.1.1`
        - VLAN 5: e.g., `172.16.3.1`
    - **How Assigned:**
        - **Default Gateways:** SVIs (`interface vlan 2`, `interface vlan 5`) on the relevant Multilayer Switch would be configured with these IP addresses.

- **End Devices:** Devices in VLAN 2 and VLAN 5 would receive IPs from their respective subnets via DHCP or static assignment, with their respective SVI IP as the gateway.
-

B. Implied Server/Service Segments (Likely VLANs):

These segments are identified by the distinct IP addresses of the servers in Site 2. In a real university network, these would almost certainly be placed in separate VLANs.

- **Bing Server Segment (IP: `174.16.2.2`)**
  - **Conceptual IP Subnet:** `174.16.2.0/28` (or similar, providing a small number of IPs)
  - **Default Gateway:** `174.16.2.1`
  - **How Assigned:**
    - **Default Gateway:** An SVI (`interface vlan <Server_Bing_VLAN_ID>`) on the **Multilayer Switch in Site 2** would be configured with `174.16.2.1`.
    - **Server (bing.com dns):** The server `174.16.2.2` would be configured with a **static IP address**, its subnet mask (e.g., 255.255.255.240), and its default gateway (`174.16.2.1`).
- **Google Server Segment (IP: `174.16.1.2`)**
  - **Conceptual IP Subnet:** `174.16.1.0/28`
  - **Default Gateway:** `174.16.1.1`
  - **How Assigned:**
    - **Default Gateway:** An SVI (`interface vlan <Server_Google_VLAN_ID>`) on the **Multilayer Switch in Site 2** would be configured with `174.16.1.1`.
    - **Server (https://www.google.com/search?q=google.com http):** The server `174.16.1.2` would be configured with a **static IP address**, its subnet mask, and its default gateway (`174.16.1.1`).
- **DNS-1 Server Segment (IP: `177.16.5.2`)**
  - **Conceptual IP Subnet:** `177.16.5.0/28`
  - **Default Gateway:** `177.16.5.1`
  - **How Assigned:** Similar to the other servers: SVI on a Multilayer Switch for the gateway, static IP on the server.
- **DNS-2 Server Segment (IP: `176.16.6.2`)**
  - **Conceptual IP Subnet:** `176.16.6.0/28`
  - **Default Gateway:** `176.16.6.1`
  - **How Assigned:** Similar to the other servers: SVI on a Multilayer Switch for the gateway, static IP on the server.

C. WAN Interconnect Segments (Between Routers):

- **Router-to-Router Links:** Each physical serial or Fast Ethernet/Gigabit Ethernet interface connecting two routers (e.g., `Router0` to `Router1`, `Router1` to `Router2`) would represent its own point-to-point network segment.
  - **Conceptual IP Subnet:** Small subnets like `/30` (2 usable IPs) are common, e.g., `192.168.10.0/30`.

- **Default Gateway:** Not applicable in the same way as for end-user segments. Routers communicate directly via routing protocols .
- **How Assigned:** Each router interface connected to another router would have a **static IP address** assigned from the shared subnet for that specific link. For example, `Router0's` interface could be `192.168.10.1/30` and `Router1's` interface `192.168.10.2/30`.

3. Role of DHCP and Static Assignment

- **DHCP (Dynamic Host Configuration Protocol):** Most end-user devices (PCs, laptops, IP phones) would obtain their IP address, subnet mask, default gateway, and DNS server information dynamically from a **DHCP server**. This server would be configured with separate "scopes" (pools of IP addresses) for each VLAN. The DHCP server's IP address would likely be one of the Infrastructure VLAN's servers or a configured service on a router.
- **Static Assignment:** Critical network infrastructure devices (Routers, Multilayer Switches' management interfaces, Servers) are typically assigned **static IP addresses**. This ensures they always have the same, predictable address for management and service delivery.

4. Inter-VLAN Routing (Gateways in Action)

The `Multilayer Switches` are critical for the gateways. For any device in a VLAN (e.g., a PC in VLAN 3), its default gateway is the IP address of the SVI configured on the Multilayer Switch for that VLAN (`172.16.2.1` for VLAN 3). When a device needs to communicate with a device in *another* VLAN or network (e.g., a PC in VLAN 3 wants to access the Google server in its own segment), it sends the traffic to its default gateway (the SVI). The Multilayer Switch then performs the Layer 3 routing to forward the packet to the correct destination network.

This structured assignment ensures that all devices have the necessary network parameters to communicate within their segment and reach other segments through their designated gateways.

➢ advantage of using subnetting in a university environment

1. Improve network performance and speed

A single broadcast packet sends out information that reaches every device connected to that network because each device has an entry point into the network. A large number of entry points, however, can negatively impact internetwork switching device performance, as well as your network's overall performance.

Another issue with broadcast packets is that they can spam every device within a network, even devices that aren't relevant to the task at hand, which can strain a network's capacity and cause it to collapse.

But subnetting enables you to ensure that information remains in the subnetted network or broadcast domain, which allows other subnets to maximize their speed and effectiveness. Subnetting also divides your network's broadcast domains, enabling you to better control traffic flow, thus increasing network performance!

A word of caution, though. You're better off limiting traffic to a single subnet instead of letting it move from subnet to subnet. So, you should limit the number of devices on your subnet whenever possible, along with controlling the traffic flow between subnets. Doing this will improve your network's speed and performance.

2. Reduce network congestion

Subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion. Through strategic placement of subnets, you can help reduce your network's load and more efficiently route traffic.

So, what happens to a large network with no subnets? Every computer would see broadcast packets from all the computers and servers on the network, resulting in the switches having to move all that traffic to the appropriate ports. This leads to increased congestion, reduced network performance, and slower response times.

However, using a router to move traffic between subnets results in no broadcast traffic or any information that doesn't need to be routed being moved to other subnets. Because the amount of traffic within each subnet is reduced, the speed of each subnet is increased, which eases network congestion.

3. Boost network security

You might be thinking, "What if a device in my network is comprised?" By splitting your network into subnets, you can control the flow of traffic using ACLs, QoS, or route-maps, enabling you to identify threats, close points of entry, and target your responses more easily.

You also can split your network using routers to connect subnets though the configuration of ACLs on the routers and switches. As a result, devices in a subnet are unable to access the entire network.

Another option is to limit access to resources on wireless clients, ensuring that valuable information isn't easily accessible in remote locations.

4. Control network growth

When you're planning and designing a network, size is something that needs to be taken into consideration. One of the key benefits of subnetting is that it enables you to control the growth of your network.

You can use a popular host formula to determine the size of your network. Take the number of zeros in the mask of your subnet when converted to binary, take two to the power of that number, then minus two — and then you will have the number of possible hosts for that subnet mask. That was a bit of a doozy, so here is a more in depth explanation of the host formula.

Your next step is to figure out the expected growth of the network, which in most cases will be based heavily on the physical size of your building. For example, will the number of devices needed remain steady or could it eventually double? If so, you will need to adjust the equation for the host formula accordingly, in order to determine the proper IP address space for your network.

Routing

➢ Kind of routing implement

- **Dynamic Routing (EIGRP or OSPF):** A dynamic routing protocol like EIGRP (Enhanced Interior Gateway Routing Protocol) or OSPF (Open Shortest Path First) would be used between the core routers (`Router0`, `Router1`, `Router2`) and potentially extending to the Multilayer Switches. This allows for scalability, fault tolerance, and automatic route updates.
- **Default Routing:** A default route would be configured on the router connecting the university network to the Internet. This enables devices to access destinations outside the campus

➢ kind of routing did implement

Why Dynamic Routing (EIGRP/OSPF)

1. **Scalability:**
   - **University Context:** A university network (like the multi-site one in your diagram) is typically large and constantly growing. New departments, buildings, or services are added regularly.
   - **Benefit:** With dynamic routing, you don't have to manually configure routes for every new network segment. Routers automatically learn and update routing tables as the network expands or changes. This saves immense administrative effort and reduces the chance of configuration errors.

2. **Fault Tolerance and Redundancy:**
    - **University Context:** Network uptime is critical for a university. Students, faculty, and staff rely on the network for learning, research, administration, and communication. A network outage can severely disrupt operations.
    - **Benefit:** Dynamic routing protocols can quickly detect network failures (e.g., a router or a link going down). They can then rapidly converge and calculate alternative paths to reach destinations. This ensures that traffic can reroute around failures, minimizing downtime.
3. **Automatic Route Updates:**
    - **University Context:** Network changes (adding or removing segments, modifying IP addresses) are inevitable.
    - **Benefit:** When a change occurs, dynamic routing protocols automatically update all participating routers' routing tables. This eliminates the need for manual intervention, prevents routing black holes, and ensures consistent network reachability.
4. **Optimal Path Selection:**
    - **University Context:** With multiple sites and potentially multiple links between them (even if not fully meshed in this simplified diagram, it's a common university design), there might be several paths to a destination.
    - **Benefit:** Dynamic routing protocols use metrics (like bandwidth, delay, reliability, load, cost) to determine the best (most efficient) path to a destination. This helps ensure optimal performance and resource utilization.

Why Default Routing?

1. **Internet Access:**
    - **University Context:** A primary function of any modern university network is to provide robust access to the Internet for research, online learning, communication, and general web Browse.
    - **Benefit:** A default route (`0.0.0.0 0.0.0.0`) tells the router, "If you don't have a specific route for a destination, send the traffic to this next hop." This is essential for reaching destinations outside the university's internal network (i.e., the entire Internet) without having to list millions of individual routes.
2. **Simplified Routing Tables (for external routes):**
    - **University Context:** The Internet's routing table contains hundreds of thousands of routes.
    - **Benefit:** Without a default route, your internal routers would theoretically need a route for every network on the Internet, which is impossible and impractical. A default route dramatically simplifies routing tables within your campus network for all external traffic.
    -

Why NOT Static Routing (for the main internal routing)?

1. **Lack of Scalability:**
    - **University Context:** As explained, universities grow constantly.
    - **Problem:** If you used static routing, every time a new network segment was added or removed, you would have to manually go into *every single router* in the campus network and add or delete static routes. This is tedious, time-consuming, and highly prone to errors.
    -
2. **No Automatic Redundancy:**
    - **University Context:** Static routes are fixed.
    - **Problem:** If a link or a router goes down, static routes *do not* automatically update or reroute traffic. Network connectivity would be lost until an administrator manually reconfigured the routes, leading to significant downtime.
3. **High Administrative Overhead:**
    - **University Context:** Maintaining complex static routes across a large network requires immense manual effort and careful documentation.
    - **Problem:** It becomes very difficult to manage, troubleshoot, and ensure consistency, especially in a dynamic environment like a university.

While static routing might be used for specific, very simple scenarios (e.g., a single route to a specific server farm or a backup route), it is **not suitable for the primary internal routing protocol** in a multi-site, dynamic university network like the one implied by your diagram. The complexity and need for uptime strongly favor dynamic routing.

➢ the purpose of default routing

Enabling Internet Access (Accessing Unknown Networks):

The primary purpose of a default route in this university topology is to allow any device within the campus network to reach destinations **outside of its own network structure**, specifically the **Internet**.

The Internet is a vast network with millions of different destinations (IP addresses). It's impossible and impractical for every router within the university (like `Router0`, `Router1`, `Router2`) to know a specific route to every single destination on the Internet.

A default route acts as a "catch-all" or "last resort" route. It tells a router: "If you receive a packet for a destination network that is *not* explicitly listed in your routing table (i.e., it's not one of the university's internal networks), then forward that packet to this specific next-hop IP address." This next hop would be the router (likely the one connected to the Internet Service Provider - ISP).

Simplifying Routing Tables:

Without a default route, a router would need to learn specific routes for every possible external network it might need to reach. This would make routing tables massive and cumbersome to manage.

By using a default route, the routing tables of the internal university routers remain cleaner and more efficient. All traffic destined for "anywhere else" (the Internet) is simply directed to the designated Internet-facing router, which then handles the forwarding to the ISP.

Default routing improves network reliability by providing a backup route in case of network failures If a primary route fails, the default route can be used to forward packets to their intended destinations.

A default gateway is a crucial component in a computer network that facilitates communication between different networks. It allows devices on separate networks to connect and communicate with one another seamlessly Default routing provides a "last resort" route for packets that don't match any specific route in the routing table. It ensures that packets are not dropped and can reach their intended destination.

If a packet is received on a routing device, the device first checks to see if the IP destination address is on one of the device's local subnets. If the destination address is not local, the device checks its routing table. If the remote destination subnet is not listed in the routing table, the packet is forwarded to the next hop toward the destination using the default route. The default route generally has a next-hop address of another routing device, which performs the same process. The process repeats until a packet is delivered to the destination.

- **routers communicate between departments and the ISP**

How Routers Communicate within Departments (Intra-Campus)

Within the university's campus network, communication between different departments or logical segments (VLANs) happens through a combination of **Inter-VLAN Routing** on Multilayer Switches and **Dynamic Routing Protocols** on the dedicated routers.

1. **Inter-VLAN Routing (on Multilayer Switches):**
    - **Scenario:** When a device in one department's VLAN (e.g., a student PC in VLAN 3 in Site 1) needs to communicate with a device in *another* VLAN within the same campus (e.g., a faculty member's PC in VLAN 101 within Site 1, or even a server in Site 2's server VLAN), the traffic first hits its default gateway.
    - **Mechanism:** The default gateway for each VLAN is typically a **Switched Virtual Interface (SVI)** configured on the **Multilayer Switch** (`3560-24PS` in Site 1, Site 2, and Site 3). The Multilayer Switch performs **Layer 3 routing** between these different VLANs that are directly connected to it or its access switches.
    - **Example:** If a PC in VLAN 3 (172.16.2.x) wants to talk to a server in a server VLAN (e.g., 174.16.1.x), it sends the packet to its default gateway (the SVI for VLAN 3 on its Multilayer Switch). That Multilayer Switch then looks at its routing table, finds the

route to the server's network, and forwards the packet to the appropriate interface or next-hop (which might be another Multilayer Switch or a Router).

2. **Dynamic Routing Protocols (Between Routers and potentially Multilayer Switches):**
    - **Mechanism:** These routers run a **Dynamic Routing Protocol** (like EIGRP or OSPF).
    - **Scenario:** For communication between entirely separate physical sites (Site 1, Site 2, Site 3) or large network segments that are not directly connected to the same Multilayer Switch performing inter-VLAN routing, the dedicated routers (`Router0`, `Router1`, `Router2`) come into play.
        - They **exchange routing information** with each other, automatically learning about all the network segments (VLANs and their subnets) that exist within the entire university campus.
        - When `Router0` (Site 1) receives a packet destined for a network in `Site 3`, it looks up the destination in its routing table. The dynamic routing protocol ensures `Router0` knows that the path to `Site 3` is via `Router1` (or directly via `Router2` if a direct link exists and is preferred).
        - The routers then forward the packet across the appropriate WAN link (the red lines in your diagram, typically serial connections) to the next-hop router until it reaches the destination site.

How Routers Communicate with the ISP (External)

Communication with the ISP involves the **Internet Edge Router** and the **Default Route**.

1. **Internet Edge Router:**
    - **Location:** One of the university's main routers (`Router0`, `Router1`, or `Router2` would be designated as the **Internet Edge Router**, or a dedicated perimeter router might be used, though not explicitly shown in detail). This router has a physical connection (e.g., a serial link or Gigabit Ethernet link) directly to the ISP's router.
    - **IP Addressing:** The interface on the Internet Edge Router connected to the ISP would be configured with an IP address from a small, dedicated subnet provided by the ISP (this might be a public IP range, or a private range used between the customer and ISP).

2.Default Route :

- **Mechanism:** On the **Internet Edge Router**, a **Default Route** (`ip route 0.0.0.0 0.0.0.0 [ISP _Router _IP]`) is configured. This tells the router: "For any network not explicitly known in my routing table (i.e., anything on the Internet), send the traffic to the ISP's router at `[ISP_ Router _IP]`."
- **Internal Routing:** Within the university's internal network, the dynamic routing protocol would typically advertise this default route to all other internal routers. This means every router in the university would know that to reach the Internet, it should forward traffic towards the designated Internet Edge Router

Device & Server Configuration.

- **servers did you configure**

DNS Servers (Domain Name System):

DNS servers act like phonebooks for the internet. When you type a website name (like https://www.google.com/url?sa=E&source=gmail&q=google.com) into your browser, your computer asks a DNS server for the corresponding IP address (like 174.16.1.2). Without DNS, you'd have to remember long numerical IP addresses for every website you want to visit.

Examples from image Server-PT bing.com DNS This server would be responsible for resolving the domain name "bing.com" to its IP address. So, if a PC on the network wanted to access Bing, it would query this server (or another DNS server configured to know about it).Server-PT dns-1 (IP 177.16.5.2): This is a general DNS server that would likely handle various domain name lookups for devices within the network. Server-PT dns-2 (IP 176.16.6.2): Another general DNS server, possibly serving a different segment or acting as a backup/secondary DNS server. Web Server (HTTP Server).A web server stores website files (HTML, CSS, images, etc.) and delivers them to web browsers when requested. When you type a website address, your browser sends an HTTP request to the web server, and the server responds by sending the website's content back to your browser. Example from image Server-PT google.com http (IP 174.16.1.2): This server is configured to host the "https://www.google.com/url?sa=E&source=gmail&q=google.com" website. If a user on the network tried to access "https://www.google.com/url?sa=E&source=gmail&q=google.com", their browser would connect to this server at IP address 174.16.1.2, and the server would send back the Google homepage.

- **configured the FTP server and tested**

DNS Servers 'Server-PT bing.com DNS`, `Server-PT dns-1`, `Server-PT dns-2`

Web Server 'Server-PT google.com http` If an FTP server were configured, you would typically see a device labeled as "FTP Server" or a server with an "FTP" service explicitly enabled and indicated on the topology. Since it's not visible, we cannot explain its configuration or testing based solely on this image. If there were an FTP server, the general steps for configuring and testing it in Cisco Packet Tracer would be:

1. FTP Server Configuration (Hypothetical):

Add a Server Device: Drag a "Server" device from the End Devices section onto the Packet Tracer topology. Assign IP Address: Click on the server, go to the "Desktop" tab, then "IP Configuration," and assign a static IP address, subnet mask, and default gateway that fits the network's addressing scheme (e.g., 172.16.x.x for a server in Site 2's segment). Enable FTP Service: Go to the "Services" tab, select "FTP," and turn the service "On."

Create Users: Add usernames and passwords for FTP access (e.g., `user1` / `password123`). You would also define permissions (read, write, delete, list, rename). Create Files (Optional): You could

create some dummy text files on the server's "Storage" or "Desktop" (via the "Text Editor" tool) to test file transfer.

FTP Server Testing (Hypothetical):

From a PC (e.g., PC0, PC21, PC16):

Click on a client PC.

Go to the "Desktop" tab.

Select "Command Prompt."

Type `ftp <FTP_Server_IP_Address>` (e.g., `ftp 172.16.x.y`).

Enter the username and password when prompted.

Once logged in, you could use FTP commands like:

`dir` or `ls`: To list files on the FTP server.

`get <filename>`: To download a file from the server to the client PC.

`put <filename>`: To upload a file from the client PC to the server.

`bye`: To exit the FTP session.

From a Web Browser (less common for full FTP, but sometimes supported for file listing):

On a client PC, go to the "Desktop" tab and open "Web Browser."

Type `ftp://<FTP_Server_IP_Address>` in the URL bar. This might allow basic file listing if the server is configured for it, but typically a command-line FTP client or a dedicated FTP application is used for full functionality.

1. Configuration of an FTP Server in Cisco Packet Tracer:

* Add a Server: Drag and drop a "Server-PT" device from the End Devices menu onto the topology.

* Assign an IP Address:

* Click on the server.

* Go to the "Desktop" tab and select "IP Configuration."

* Enter a static IP address (e.g., 192.168.1.10), subnet mask, and a default gateway (the IP address of the router interface connected to the server's network).

* Enable and Configure FTP Service:

  * Click on the server.

  * Go to the "Services" tab and select "FTP."

  * Ensure the "FTP Service" is "On."

  * Create User Accounts: Define usernames and passwords for FTP access. For each user, select the desired permissions (Write, Read, Delete, Rename, List). For example:

    * Username: `user1`

    * Password: `cisco`

    * Permissions: Check all boxes (Write, Read, Delete, Rename, List) to allow full access.

  * Click "Add" to save the user.

* Create Files (Optional but good for testing): You can create simple text files on the server itself (e.g., using the Text Editor in the Desktop tab) to test uploads and downloads later

2. Testing the FTP Server in Cisco Packet Tracer:

From a Client PC:

  * Go to a PC (e.g., PC0 from Site 1).

  * Go to the "Desktop" tab and select "Command Prompt."

  * Test Connectivity (Ping): First, verify network connectivity to the FTP server by pinging its IP address.

 ping <FTP_ Server _IP_ Address>

   (e.g., `ping 192.168.1.10`)

* Connect to FTP:** Once ping is successful, use the `ftp` command followed by the server's IP address ftp <FTP_ Server _IP _Address (e.g., `ftp 192.168.1.10`)

  * Login: You will be prompted for a username and password. Enter the credentials you configured on the FTP server (e.g., `user1` and `cisco`).

  * List Files Once logged in, you can list the files on the FTP server using the `dir` or `ls` command.

* Upload a File: To upload a file from the PC to the FTP server, you first need to create a file on the PC (using Text Editor in the Desktop tab) and then use the `put` command.

put <filename.txt>(e.g., `put mytestfile.txt`)

* Download a File: To download a file from the FTP server to the PC, use the `get` command

get <filename_on_server.txt

(e.g., `get serverfile.txt`)

* Disconnect: To exit the FTP session, type `bye` or `quit`

* Verification on the FTP Server

* After uploading a file from a client, you can go back to the FTP server's "Services" tab, select "FTP," and check the file list to confirm the uploaded file appears there.

* Similarly, if a file was downloaded, you could verify its presence on the client PC's "Desktop" via the "Text Editor" or "Command Prompt" (using `dir`).

➢ DHCP work test automatic IP assignment

it's not possible to definitively state how DHCP works or if automatic IP assignment was tested because: No DHCP Servers are Explicitly Labeled: While there are DNS servers (bing.com dns, https://www.google.com/search?q=google.com http, dns-2), none of the servers or devices are explicitly labeled as a DHCP server. DHCP functionality is typically provided by a dedicated DHCP server or configured on a router or multilayer switch. No IP Address Ranges for DHCP: The diagram provides static IP addresses for some VLANs in Site 3 and for DNS servers, but it doesn't show any configured DHCP pools or scopes for the PCs (PC0-PC15 in Site 1 and PC16-PC19 in Site 3).Lack of Configuration Details: Cisco Packet Tracer allows for detailed configuration of devices. Without looking at the configuration of the routers, multilayer switches, or any potential servers, we cannot determine if DHCP services are enabled, what IP ranges are being assigned, or if the PCs are configured to obtain IP addresses automatically (DHCP client).To determine if DHCP is implemented and how it works, we would need to:

Examine the Configuration of the Routers (Router0, Router1, Router2): Routers are common places to configure DHCP server functionality for their connected networks/VLANs.

Examine the Configuration of the Multilayer Switches (3560-24PS, 3560-24PS ML-3, 3560-24PS Multilayer Switch2): Multilayer switches can also act as DHCP servers, especially for VLANs they route. Look for a Dedicated DHCP Server: Although not explicitly labeled, one of the "Server-PT" devices could be configured as a DHCP server. Check PC IP Configurations: Within Packet Tracer, you can click on each PC and check its IP configuration settings. If it's set to "DHCP," then automatic IP assignment is being attempted. Therefore, based only on the visual information in the diagram, we cannot

answer whether DHCP is working or if automatic IP assignment was tested. The diagram shows the physical and logical layout of the network but not the detailed service configurations.

Troubleshooting and Testing

➢ verify inter-VLAN communication

Inter-VLAN communication is the process by which devices on different Virtual Local Area Networks (VLANs) can communicate with each other. Since VLANs segment a network, a Layer 3 device (like a router or a Layer 3 switch) is required to route traffic between them. From the diagram, the key components for inter-VLAN communication verification are primarily within Site 3 and potentially through the Multilayer Switches. Here's a brief explanation of how inter-VLAN communication would be verified:

VLAN Configuration Verification:

Confirmation of VLANs on Switches: Ensure that VLANs (VLAN 2, 3, 4, 5, 6, 7 as listed for Site 3) are correctly created on the Multilayer Switch (3560-24PS Multilayer Switch2) and the access switches (2950-24 Switch5, 2950-24 Switch6).Port Assignment to VLANs: Verify that the access ports on Switch5 and Switch6 connected to PCs (PC16-PC19) are correctly assigned to their respective VLANs (e.g., PC16's port is in VLAN 2, PC17's in VLAN 3, etc.).

Trunking Configuration: Confirm that the links between the access switches (Switch5, Switch6) and the Multilayer Switch2 are configured as trunk ports. Trunking allows traffic from multiple VLANs to traverse a single link.

Layer 3 Routing (SVI) Verification on Multilayer Switch: The "3560-24PS Multilayer Switch2" is crucial here. As a multilayer switch, it can perform inter-VLAN routing using Switched Virtual Interfaces (SVIs).SVI Creation: Verify that SVIs are created for each VLAN (VLAN 2, 3, 4, 5, 6, 7) on the Multilayer Switch2, and that each SVI has an IP address (e.g., a gateway IP for that VLAN, like 172.16.1.1 for VLAN 2).Routing Table: Check the routing table on the Multilayer Switch2 to ensure it has routes for all configured VLAN networks.

IP Address and Gateway Configuration on PCs:

PC IP Addresses: Confirm that the PCs in Site 3 (PC16-PC19) have IP addresses within their respective VLAN subnets (e.g., PC16 with 172.16.1.x, PC17 with 172.16.2.x).Default Gateway: Crucially, ensure that each PC's default gateway is configured to the IP address of its respective VLAN's SVI on the Multilayer Switch2. For example, PC16's default gateway should be 172.16.1.1 (assuming this is the SVI IP for VLAN 2).Verification Steps (Actual Testing):Ping Tests Intra-VLAN Ping: First, test communication within a VLAN (e.g., if there were two PCs in VLAN 2, ping between them). This confirms basic connectivity within the VLAN .Inter-VLAN Ping: The primary test is to ping from a PC in one VLAN to a PC in a different VLAN within Site 3 (e.g., PC16 in VLAN 2 to PC17 in VLAN 3)

Ping to Gateway: Ping from a PC to its own default gateway (the SVI IP on the multilayer switch). This verifies the PC can reach its router for inter-VLAN communication. Traceroute Perform a traceroute

from one PC to another in a different VLAN. This command will show the path the packet takes, and you should see the traffic being routed through the Multilayer Switch2's SVI IP.

Mechanism for Inter-VLAN Communication:

The core of inter-VLAN communication in this topology relies on Layer 3 devices (routers and multilayer switches).Site 3: This site explicitly shows multiple VLANs (VLAN 2, 3, 4, 5, 6, 7) with different IP subnets (e.g., 172.16.1.0, 172.16.2.0, etc.).

The presence of a Multilayer Switch (3560-24PS Multilayer Switch2) is key here. Multilayer switches have Layer 3 routing capabilities. They can have Switch Virtual Interfaces (SVIs) configured for each VLAN, allowing them to route traffic directly between VLANs connected to that same switch. This is more efficient than "router-on-a-stick" for intra-site inter-VLAN routing.

Alternatively, if routing isn't configured on the multilayer switch, the Router2 (2811) would perform "router-on-a-stick" routing for these VLANs, where a single physical link to the multilayer switch carries traffic for all VLANs as a trunk, and the router has sub-interfaces for each VLAN. Given the multilayer switch , the former is more likely.

Between Sites (e.g., Site 1 to Site 3): For inter-VLAN communication across different sites, the routers (Router0, Router1, Router2) are responsible.

Traffic originating from a VLAN in Site 1 and destined for a VLAN in Site 3 would first be routed by Router0 (or the multilayer switch in Site 1) to the inter-site WAN links.

Router1 would then route the traffic between the sites.

Finally, Router2 (or the multilayer switch in Site 3) would route the traffic to the destination VLAN in Site 3.

How Verification Would Be Performed (Not shown in diagram, but standard practice):To verify inter-VLAN communication, the following steps are commonly performed in Cisco Packet Tracer Ping Test Intra-site (e.g., within Site 3) From a PC in VLAN 2 (e.g., PC16) try to ping a PC in VLAN 3 (e.g., PC17). If the multilayer switch is correctly configured for inter-VLAN routing, this ping should be successful.

Inter-site (e.g., Site 1 to Site 3): From a PC in Site 1 (e.g., PC0) try to ping a PC in Site 3 (e.g., PC16). This verifies that traffic can traverse VLANs within Site 1, go through Router0, Router1, Router2, and then be routed to the target VLAN in Site 3.Also, pinging servers (e.g., Server-PT https://www.google.com/search?q=google.com http from any PC) would test routing across multiple segments and potentially inter-site links. Traceroute Running a traceroute command from a PC to a destination in a different VLAN or site would show the path the packets take, allowing you to see if the routing is occurring as expected through the routers and multilayer switches. Simulation Mode (in Packet Tracer):

Packet Tracer's simulation mode is an excellent visual verification tool. You can send a PDU (Packet Data Unit) from one PC to another across different VLANs and observe the packet's journey, seeing it

traverse switches, hit the Layer 3 device (router/multilayer switch) for routing, and then be forwarded to the destination VLAN. show Commands (on devices):

On Switches show vlan brief To confirm VLAN creation and port assignments. show interfaces trunk: To verify that links between switches and between switches/routers are configured as trunks, allowing multiple VLANs to pass through. On Routers/Multilayer Switches (acting as Layer 3 devices)show ip route: To check the routing table and ensure routes to all VLAN subnets are present. show ip interface brief: To confirm IP addresses and status of SVI interfaces (on multilayer switches) or sub-interfaces (on routers for router-on-a-stick).

➢ test connectivity to the internet (ISP router)

The red lines connecting Router0 (Site 1), Router1 (Site 2), and Router2 (Site 3) represent the WAN (Wide Area Network) links between the company's own sites. These are internal connections, not an external internet connection via an ISP. If there were an ISP router and an internet connection, here's how connectivity would typically be tested Identify the ISP Router and Gateway: The diagram would need to show a fourth router, often labeled "ISP Router" or similar, connected to one of the company's routers (most likely Router1 in Site 2, as it appears to be the central hub). There would also be a default route configured on the company's router pointing to the ISP router's IP address. Verify Default Route: On the company router connected to the ISP (e.g., Router1), you would use the command show ip route to ensure there's a default route (0.0.0.0 0.0.0.0 [next-hop IP or exit interface]) pointing towards the ISP. Ping Public IP Addresses From any PC in the network, you would try to ping a well-known public IP address (e.g., Google's DNS server: 8.8.8.8 or 8.8.4.4).If NAT (Network Address Translation) is configured on the edge router (the one connected to the ISP), you'd verify that it's translating internal private IP addresses to a public IP address before sending traffic to the internet. Ping Public Domain Names From any PC, you would try to ping a public domain name (e.g., ping google.com or ping cisco.com).This also tests DNS resolution. If DNS resolution fails but pinging public IPs works, then the DNS server configuration might be an issue. The diagram does show some DNS servers (bing.com DNS, https://www.google.com/url?sa=E&source=gmail&q=google.com http, dns-2), which would be used for internal and potentially external name resolution. Access Web Pages From a PC, try to access a public website via a web browser (e.g., http://www.google.com). This tests end-to-end connectivity, including DNS resolution and HTTP/HTTPS traffic. Traceroute to Public Destination Run a traceroute command from a PC to a public IP or domain name. This would show the path the packets take, including passing through the company's edge router and then the ISP's network. Finally, the provided diagram does not depict an internet connection or an ISP router, so testing connectivity to the internet cannot be addressed based on this specific image. The current setup focuses on internal company network connectivity.

➢ tools did you use inside Packet Tracer to test communication

Based on the diagram and common practices in Cisco Packet Tracer, the primary tools used to test communication are Ping Command How it's used: This is the most fundamental and frequently used tool. You would open the "Command Prompt" (or "Terminal") application on any PC (e.g., PC0, PC21, PC16) within Packet Tracer. From there, you would type ping <destination IP address>.What it tests:

End-to-End Connectivity: Whether a packet can successfully reach a destination device (another PC, a server, or a router interface) and receive a reply.

IP Addressing: Confirms that the source and destination devices have correct IP addresses and subnet masks. Routing Ensures that routers and multilayer switches have the correct routes to forward traffic between different subnets/VLANs and across the inter-site WAN links. Firewall/ACL Issues (if configured): Can indirectly indicate if a packet is being blocked. Examples based on diagram ping 172.16.2.0 (from PC16 in VLAN 2 to PC17 in VLAN 3 to test inter-VLAN routing within Site 3).ping 174.16.1.2 (from PC0 in Site 1 to the Google server in Site 2 to test inter-site routing).ping 177.16.5.2 (from PC19 in Site 3 to the dns-1 server to test routing from Site 3 to Site 2).Web Browser How it's used: You would open the "Web Browser" application on any PC in Packet Tracer. In the address bar, you would type the IP address or domain name of a web server. What it tests HTTP/HTTPS Connectivity Verifies if web services are reachable.

DNS Resolution (if using domain names): Ensures that DNS servers are correctly configured and can resolve domain names to IP addresses. The diagram shows Server-PT bing.com DNS and Server-PT google.com http, indicating potential web servers or DNS servers that could be accessed. Examples based on diagram Type http://google.com or the IP address of the "Server-PT https://www.google.com/url?sa=E&source=gmail&q=google.com http" into a PC's web browser to see if the web page loads. This would test DNS resolution if the domain name is used, and then HTTP connectivity.

Trace route (or Tracert):How it's used: Similar to ping, this command is run from the "Command Prompt" on a PC: tracert <destination IP address or domain name>.What it tests Path Discovery: Shows the hops (routers/Layer 3 switches) that packets take to reach a destination. Routing Path Verification: Helps identify if packets are taking the expected path and where delays or failures might be occurring along the route. Examples based on diagram:

tracert <IP address of PC16> (from PC0) would show the path through Router0, Router1, Router2, and finally the Multilayer Switch2.Simulation Mode (Packet Tracer specific):How it's used: This is a visual tool available in the Packet Tracer interface. You switch from "Real time" mode to "Simulation" mode. You can then click the "Add Simple PDU" tool (the open envelope icon) to send a test packet from a source device to a destination device. What it tests Step-by-step Packet Flow: Allows you to see exactly how a packet traverses the network, hitting each device, making routing decisions, and being forwarded. Troubleshooting: Highly effective for visualizing where packets are dropped or misrouted, helping to pinpoint configuration errors (e.g., incorrect VLAN assignments, missing routes, trunking issues).Examples based on diagram: You could send a PDU from PC21 to PC18 and watch it move from Router0 to Router1, then to Router2, and finally through Multilayer Switch2 to PC18, observing each routing decision.

➢ the role of a switch in this simulation

the role of a switch in this simulation is primarily to facilitate local area network (LAN) communication within each site and to connect end devices (like PCs and servers) to the larger network infrastructure. Here's a breakdown of the specific roles of the different types of switches shown:

1. Multilayer Switches (e.g., 3560-24PS Multilayer Switch, 3560-24PS ML-3, 3560-24PS Multilayer Switch2):Core Distribution within a Site: These switches likely act as the central distribution points within Site 1, Site 2, and Site 3. They connect to the routers and to other lower-level switches, forming the backbone of the internal site network.

Layer 3 Routing (Inter-VLAN Routing): As "Multilayer Switches," they are capable of performing Layer 3 (IP) routing in addition to Layer 2 (MAC address) switching. This means they can route traffic between different VLANs configured within the same site, without needing to send that traffic up to the main router. This improves efficiency and reduces router load for intra-site communication.

VLAN Support: They are responsible for creating and managing Virtual Local Area Networks (VLANs). The presence of "VLAN 2" through "VLAN 7" in the Site 3 information strongly suggests that these multilayer switches are segmenting the network into different broadcast domains. This enhances security, reduces broadcast traffic, and allows for better network organization.

High-Speed Connectivity: They provide high-speed connections to other network devices, including other switches, servers, and potentially directly to high-demand end devices.

2. Standard Layer 2 Switches (e.g., 2950-24 Switch0, Switch1, Switch2, Switch3, Switch5, Switch6):End Device Connectivity (Access Layer): These switches are positioned at the access layer of the network. Their primary role is to provide physical connection points for end devices such as PCs (PC0-PC19). Each PC is plugged directly into a port on one of these switches.

MAC Address Learning and Forwarding: They learn the MAC addresses of connected devices and build a MAC address table. When a frame arrives, the switch looks up the destination MAC address in its table and forwards the frame only out of the specific port where the destination device is located, thus preventing unnecessary traffic on other ports.

Broadcast Domain Management (within a VLAN): Within a single VLAN, these switches forward broadcast frames to all ports within that VLAN.

Ethernet Communication: They enable standard Ethernet communication (data link layer) between the connected end devices within the same broadcast domain (VLAN).Facilitating Local Communication: They enable devices within the same local network (and often the same VLAN) to communicate with each other efficiently.

➢ the purpose of Router-on-a-Stick

the purpose of "Router-on-a-Stick" would be to enable inter-VLAN routing within a single site using only one physical interface on the router connected to a multilayer switch. Here's a more detailed explanation:

VLANs and Broadcast Domains: As observed in the diagram (especially the Site 3 information with VLANs 2, 3, 4, 5, 6, and 7), Virtual Local Area Networks (VLANs) are used to segment the network into separate broadcast domains. Devices within the same VLAN can communicate directly (Layer 2). However, devices in different VLANs cannot communicate with each other at Layer 2, even if they are

on the same physical switch. They require a Layer 3 device (a router or a Layer 3 switch) to route traffic between them.

The Challenge of Inter-VLAN Routing: Traditionally, to enable communication between multiple VLANs using a router, you would need a separate physical interface on the router for each VLAN. This means if you have 10 VLANs, your router would need 10 physical Ethernet ports, each connected to an access port on the switch configured for that specific VLAN. This approach quickly becomes inefficient and costly, as routers typically have a limited number of physical interfaces. Router-on-a-Stick Solution: Router-on-a-Stick (often abbreviated as "RoaS") overcomes this limitation. It involves Single Physical Connection: Connecting a single physical interface on the router to a switch.

Trunk Link: This single physical connection is configured as a trunk link on both the router's interface and the switch port it's connected to. A trunk link can carry traffic for multiple VLANs by using 802.1Q encapsulation (VLAN tagging).

Sub interfaces: On the router, the single physical interface is logically divided into multiple sub interfaces. Each sub interface is configured to handle traffic for a specific VLAN. For example, GigabitEthernet0/0.10 for VLAN 10, GigabitEthernet0/0.20 for VLAN 20, and so on. Default Gateways: Each sub interface is assigned an IP address that acts as the default gateway for devices in its corresponding VLAN.

How it Works (Packet Flow):When a device in VLAN A wants to communicate with a device in VLAN B, it sends the packet to its default gateway, which is the router's sub interface for VLAN A. The switch, configured with a trunk link to the router, forwards the VLAN A tagged packet to the router's physical interface. The router receives the tagged packet, recognizes the VLAN ID, and routes the packet to the appropriate sub interface for VLAN B. The router then sends the packet back to the switch, but this time tagged for VLAN B. The switch receives the VLAN B tagged packet and forwards it to the destination device in VLAN B. Why it's used in the simulation (if applicable):

While the diagram shows "Multilayer Switches" that can perform Layer 3 routing themselves (inter-VLAN routing without a router), Router-on-a-Stick might still be implemented for a few reasons in such a simulation:

Cost-Effectiveness (in real-world scenarios): In smaller networks or labs, if you have a Layer 2 switch and a router, RoaS is a very cost-effective way to achieve inter-VLAN routing without needing to purchase an expensive Layer 3 switch.

Centralized Control/Security: Sometimes, network designers prefer to centralize all routing and security policies on a dedicated router, even if Layer 3 switches are present. A router provides more advanced routing protocols, firewall capabilities, and deeper packet inspection than most Layer 3 switches.

Learning and Demonstration: In a Cisco Packet Tracer simulation, Router-on-a-Stick is a fundamental concept for CCNA and other networking certifications. It's often included to demonstrate inter-VLAN routing principles. Specific Routing Requirements: If there are specific routing features or protocols needed that are only available on the dedicated routers (Router0, Router1, Router2) and not fully

supported by the multilayer switches, then RoaS would be necessary for those VLANs to communicate through the router. Given that the diagram explicitly labels "Multilayer Switches" which can do inter-VLAN routing, the presence of a "Router-on-a-Stick" setup would specifically imply that the routers (Router0, Router1, Router2) are handling the routing between VLANs that are connected to the respective multilayer switches, rather than the multilayer switches themselves performing all of the inter-VLAN routing locally. This would typically be achieved by having the multilayer switch's port connected to the router configured as a trunk, and the router having sub interfaces for each VLAN.

➢ DNS important in the university network

DNS (Domain Name System) is absolutely critical and important in a university network for several key reasons Human-Friendly Naming vs. Machine Addresses People remember names (like google.com, bing.com, moodle.university.edu, library.university.edu, etc.) much more easily than IP addresses (like 172.16.1.2 or 174.16.2.2).DNS translates these human-readable domain names into the numerical IP addresses that computers need to locate and connect to resources on the network and the internet. Access to External Web Services:

The diagram explicitly shows Server-PT bing.com DNS and Server-PT google.com http. For users within the university network (students, faculty, staff) to access external websites like Google, Bing, YouTube, social media, research databases, etc., DNS resolution is essential. When a user types google.com into their browser, the network's DNS server is queried to find Google's IP address. Access to Internal University Services:

University networks host numerous internal services:

Learning Management Systems (LMS): Moodle, Canvas, Blackboard

Student Portals: Registration, grades, financial aid

Faculty/Staff Portals: HR, payroll, internal communication

Library Resources: Online journals, databases

Email Servers: For university-provided email accounts

Departmental Servers: For specific research groups or departments Print Servers, File Servers, etc.

All these services typically have domain names (e.g., lms.university.edu, portal.university.edu). DNS allows users to access these services by their names rather than requiring them to memorize complex internal IP addresses. Network Resilience and Flexibility:

IP addresses can change (e.g., a server is moved, re-IPed, or replaced). With DNS, only the DNS record needs to be updated; users can continue to use the same domain name without interruption.

DNS can also be used for load balancing (e.g., directing traffic to different servers based on their load) and disaster recovery (e.g., directing traffic to a backup server if the primary fails).Security and Trust

DNS is fundamental to many security protocols. For example, SSL/TLS certificates (used for HTTPS, which encrypts web traffic) are issued to domain names. DNS ensures that when you connect to bank.com, you are indeed connecting to the server that has the certificate for bank.com.

DNSSEC (DNS Security Extensions) can add a layer of security to prevent DNS spoofing and other attacks. Centralized Management:

Having dedicated DNS servers (like Server-PT bing.com dns and Server-PT dns-2 in the diagram, though the bing.com DNS server might be a public DNS server cached locally or a DNS server primarily serving that domain) allows the IT department to centralize the management of all network resources and their corresponding names. This simplifies administration and troubleshooting. Support for Other Network Services Many other network services, such as email (MX records), directory services (SRV records for Active Directory/LDAP), and even some VoIP systems, rely heavily on DNS for proper functioning and discovery.

➢ expand this network to multiple campuses

If I were to expand this network to multiple campuses based on the provided diagram, my focus would shift towards scalability, redundancy, centralized management, and enhanced security across geographically dispersed locations. Here's a breakdown of the key changes I would implement:

1. Core Network Infrastructure (Inter-Campus Connectivity)

Dedicated WAN Links: Instead of potentially simple connections between routers shown, I would implement dedicated, robust Wide Area Network (WAN) links (e.g., MPLS, dedicated fiber, VPN over redundant internet connections) between the main campus (likely Site 1 or Site 2, depending on which is designated as HQ) and each new campus. These links would be high-bandwidth and low-latency.

Redundant WAN Links: Crucially, implement redundant WAN links to each campus to prevent single points of failure. This could involve different service providers or different physical paths.

Border Routers/Firewalls: Each campus would have its own border router(s) to connect to the WAN and the internet. These routers would ideally be integrated with or have dedicated Next-Generation Firewalls (NGFWs) to enforce security policies between campuses and the internet.

Routing Protocols: Implement dynamic routing protocols (e.g., OSPF, EIGRP, or BGP if connecting to diverse external networks/ISPs) across all campus routers to ensure efficient and redundant path selection. For inter-campus routing, a robust IGP like OSPF or EIGRP would be suitable, with BGP if there are multiple ISPs or peering arrangements.

2. Campus Network Architecture (Within Each New Campus)

Standardized Design: Replicate the successful elements of the existing sites (e.g., a core/distribution layer with multilayer switches and an access layer with Layer 2 switches). This ensures consistency and simplifies management. Campus Core/Distribution Layer: Each new campus would have its own set of redundant (e.g., HSRP/VRRP) multilayer switches at the core/distribution layer, providing inter-VLAN routing and acting as aggregation points for access layer switches.

Access Layer Redundancy: Where critical, implement redundant links from access layer switches to the distribution layer using technologies like Ether Channel (LACP) and Spanning Tree Protocol (STP) enhancements (Rapid PVST+, MSTP).Wireless Infrastructure: Implement a robust, scalable wireless network across all new campuses. This would involve Wireless LAN Controllers (WLCs) for centralized management of Access Points (APs) across all campuses, ensuring consistent SSIDs, security policies, and roaming capabilities. Physical Security for Networking Equipment: Ensure all network closets and data centers in new campuses are secure, climate-controlled, and have redundant power.

3. IP Addressing and VLANs

Hierarchical IP Addressing Scheme: Develop a comprehensive, hierarchical IP addressing plan that can accommodate future growth and clearly delineates address spaces for each campus, building, and VLAN. This helps with routing summarization and troubleshooting.

Consistent VLAN Naming/Numbering: Establish a consistent VLAN numbering and naming scheme across all campuses for specific functions (e.g., VLAN 10 for Students, VLAN 20 for Faculty, VLAN 30 for Servers, VLAN 40 for IP Phones). This simplifies policy application and troubleshooting.

Unique Subnets per Campus/VLAN: Ensure each VLAN subnet is unique per campus to avoid IP address conflicts when routing traffic between campuses.

4. Centralized Services and Management:

Centralized Data Center/Cloud Services: Consolidate critical services (e.g., main DNS servers, DHCP servers, Active Directory/LDAP, email servers, ERP systems, core applications) into a central data center (which could be at the main campus or a dedicated facility) or migrate them to cloud-based solutions. This allows all campuses to access the same resources. Dedicated DNS Servers: Maintain primary and secondary DNS servers, likely centrally located, to serve all campuses. The Server-PT bing.com DNS and Server-PT dns-2 would become part of a more robust, possibly redundant, internal DNS infrastructure. Centralized Network Management System (NMS): Implement a robust NMS (e.g., Cisco Prime Infrastructure, Solar Winds, PRTG) to monitor, manage, and troubleshoot all network devices across all campuses from a single pane of glass. This is crucial for large-scale operations.

Authentication, Authorization, and Accounting (AAA): Implement a centralized AAA server (e.g., Cisco ISE, Free RADIUS) for network access control, ensuring consistent authentication policies for users connecting from any campus.

5. Security Enhancements

Campus-Specific Firewalls/Security Zones: While a central firewall is good, each campus might benefit from local firewalls or security zones to control traffic within that campus and to segment different departments or sensitive areas. Intrusion Prevention/Detection Systems (IPS/IDS): Deploy IPS/IDS at key points (especially at WAN ingress/egress and within the data center) to detect and prevent malicious activities.

Network Access Control (NAC): Implement NAC solutions to control device access based on identity, compliance, and posture, especially important in a university environment with diverse user devices.

VPN for Remote Access: Enhance VPN capabilities for secure remote access for students, faculty, and staff, allowing them to connect to campus resources from off-campus.Regular Security Audits and Penetration Testing: Conduct these routinely across the entire expanded network.

6. Quality of Service (QoS)

QoS Implementation: Implement QoS policies end-to-end across all campuses and WAN links to prioritize critical applications like VoIP, video conferencing, and research data, ensuring a good user experience for all applications.

➢ The limitations of this simulation

Limited Device Count (Scalability for Enterprise):

While the diagram shows a decent number of PCs (especially in Site 1), a real-world university with "multiple campuses" would involve thousands, even tens of thousands, of end devices (PCs, laptops, tablets, smartphones, IoT devices, IP phones). Packet Tracer has practical limits on the number of devices it can simulate without becoming extremely slow or unstable. Adding hundreds of switches and thousands of end devices across multiple campuses would likely exceed Packet Tracer's performance capabilities.

Simplified WAN Representation The "red lines" connecting the routers likely represent basic serial or Fast Ethernet links configured as WAN connections. In a real multi-campus network, WAN connections are complex, involving various technologies like MPLS, dedicated fiber, dark fiber, SD-WAN, and redundant internet circuits with BGP peering.

Packet Tracer can simulate basic WAN links but lacks the ability to realistically model ISP networks, complex BGP routing policies, Quality of Service (QoS) across a real WAN, or the intricacies of provider-managed services like MPLS VPNs.

Absence of Wireless Infrastructure:

The diagram shows only wired connections. A modern university network relies heavily on Wi-Fi for students, faculty, and staff. The simulation currently lacks Wireless Access Points (APs)

Wireless LAN Controllers (WLCs) for centralized management of APs

Guest Wi-Fi networks and associated authentication/authorization.

No Dedicated Security Devices:

There are no dedicated firewalls (e.g., ASA, FTD), Intrusion Prevention/Detection Systems (IPS/IDS), or Network Access Control (NAC) devices shown. In a real university environment, these are critical for protecting sensitive data, segmenting networks, and controlling who/what can connect . While routers can provide basic access control lists (ACLs), they are not a substitute for robust security appliances.

Limited Server Types and Services:

Only a few generic servers are depicted (bing.com dns, google.com http, dns-2). A real university would have a vast array of servers running various applications:

Email servers (Exchange, Postfix)

Learning Management Systems (LMS - Moodle, Canvas)

Database servers

Active Directory/LDAP for centralized authentication

VoIP/Unified Communications servers

File servers

ERP systems (e.g., SAP, Oracle)

Packet Tracer's generic server emulation is very basic; it doesn't simulate the underlying operating systems or complex application layer protocols realistically.

Basic Network Management & Monitoring:

The simulation doesn't show any Network Management System (NMS) or monitoring tools (e.g., SNMP, Net Flow collectors, Syslog servers). In a production environment, these are essential for monitoring network health, performance, security events, and troubleshooting. No Redundancy for Core Devices (Explicitly Shown):While Layer 3 switches can provide redundancy (e.g., HSRP/VRRP), the diagram doesn't explicitly show redundant routers or multilayer switches at the core of each site. In a production university network, critical devices would be redundant to prevent single points of failure. There's no explicit depiction of redundant links between switches and routers, or between core/distribution layers.

Limited Realistic Traffic Simulation:

Packet Tracer can generate some basic traffic (ping, HTTP, DNS), but it cannot realistically simulate the complex and varied traffic patterns of a large university (e.g., high-bandwidth video streaming, large file transfers for research, Voice over IP (VoIP) calls, P2P traffic, etc.).It doesn't truly model network congestion or advanced QoS behavior under heavy load.

No Cloud Integration:

Many modern universities utilize cloud services (SaaS, IaaS, PaaS). The diagram is entirely on-premise, lacking any representation of cloud connectivity or hybrid network architectures.

- ## security measures would you implement to protect the servers and network

here are the key security measures I would implement to protect the servers and the overall network, moving beyond what's visually represented in a basic Packet Tracer simulation:

I. Network Segmentation & Access Control

VLANs for Security Segmentation:

Purpose: The diagram already shows VLANs, which is a great start. I would fully leverage VLANs to separate different types of traffic and user groups. Implementation:

Server VLANs Create dedicated VLANs for different server functions (e.g., DNS servers, Web servers, Database servers). This isolates them from general user traffic. Admin/Management VLAN: A separate, highly restricted VLAN for network administrators to access devices (routers, switches, servers).User VLANs: Separate VLANs for students, faculty, staff, and guests, each with distinct access policies. VoIP/ IoT VLANs: If present, segment voice and Internet of Things (IoT) devices into their own VLANs.

Benefit Limits the blast radius of a security breach. If one segment is compromised, the attacker's lateral movement to other segments is restricted.

Access Control Lists (ACLs) on Routers and Multilayer Switches:

Purpose To filter traffic based on IP addresses, ports, and protocols.

Implementation:

Inter-VLAN ACLs: Configure ACLs on the multilayer switches (which perform inter-VLAN routing) to control what traffic is allowed between different VLANs (e.g., allow web servers to communicate with databases but restrict general user access to sensitive servers).Router ACLs: Implement ACLs on Router0, Router1, and Router2 to control traffic flowing in and out of each site, and to the internet. Management Plane ACLs: Restrict access to device management interfaces (Telnet, SSH, SNMP, HTTP) to only specific management VLANs/IPs.

Benefit Granular control over network traffic, preventing unauthorized access to sensitive resources.

II. Perimeter Security

Next-Generation Firewalls (NGFWs):

Purpose: To inspect and control all traffic entering and leaving the network segments, especially at the internet edge and between campuses.

Implementation:

Deploy dedicated NGFWs (not just router ACLs) at the internet ingress/egress point(s) of each campus (e.g., logically in front of Router0, Router1, Router2, if they serve as internet gateways).Configure Stateful Packet Inspection, Application Control, Intrusion Prevention System (IPS), URL Filtering, and Anti-Malware features.

Implement VPN services on the firewall for secure remote access.

Benefit: Comprehensive threat protection, deep packet inspection, and robust policy enforcement.

Intrusion Prevention/Detection Systems (IPS/IDS):

Purpose: To detect and prevent known attack patterns and suspicious activities.

Implementation:

Integrate IPS functionality within the NGFW or deploy standalone IPS sensors at critical points (e.g., mirroring traffic from core switches or WAN links).

Benefit: Proactive threat mitigation.

III. Server-Specific Security:

Host-Based Firewalls:

Purpose: An additional layer of defense on the servers themselves.

Implementation: Enable and configure firewalls on all servers (e.g., Windows Firewall, ip tables on Linux) to allow only necessary inbound and outbound connections for their specific services.

Benefit: Protects the server even if network-level controls are bypassed or misconfigured Principle of Least Privilege Purpose: Limit access rights for users and applications to only what is absolutely necessary.

Implementation:

Strict user accounts with minimal permissions on servers.

Limit services running on servers to only those required for their function.

Benefit: Reduces the attack surface and impact of a compromised account.

Regular Patching and Updates:

Purpose: Address known vulnerabilities in operating systems and applications.

Implementation: Implement a robust patch management system for all servers and network devices.

Benefit: Prevents exploitation of common vulnerabilities.

IV. Authentication, Authorization, and Accounting (AAA)

Centralized AAA (e.g., Cisco ISE, RADIUS/TACACS+):

Purpose: To control access to network devices and resources based on user identity.

Implementation: Configure routers, switches, and potentially servers to authenticate users against a central AAA server.

Benefit: Strong authentication, granular authorization, and logging (accounting) of all administrative actions. Strong Password Policies:

Purpose: Prevent brute-force and dictionary attacks.

Implementation: Enforce complex passwords, regular rotations, and lockout policies for failed attempts.

V. Monitoring & Auditing

Network Management System (NMS) with Security Information and Event Management (SIEM):

Purpose: Collect and analyze logs from all network devices and servers for security events.

Implementation:

Configure all devices to send Syslog messages to a central Syslog server.

Implement a SIEM solution to correlate events, detect anomalies, and generate alerts.

Benefit: Early detection of security incidents, forensic analysis.

Regular Security Audits & Vulnerability Assessments:

Purpose: Identify weaknesses before attackers can exploit them.

Implementation: Periodically scan the network for vulnerabilities and conduct penetration tests.

VI. Data Protection

Data Backup and Recovery:

Purpose: Ensure business continuity in case of data loss due to attack, failure, or disaster.

Implementation: Implement regular, redundant backups of all critical server data and network device configurations, stored securely off-site.

Data Encryption:

Purpose: Protect data confidentiality, both in transit and at rest.

Implementation:

HTTPS/TLS: Ensure all web services use HTTPS.

VPNs: Encrypt traffic for remote access and between campuses (if dedicated WAN is not fully encrypted).Disk Encryption: Consider encrypting sensitive data on server hard drives.

VII. Physical Security

Restricted Access: Ensure network closets, server rooms, and data centers at all sites (Site 1, Site 2, Site 3) have controlled physical access (e.g., card readers, biometric scanners, surveillance

Conclusion:

Gondar University Network infrastructure Analysis

"In conclusion, the analysis of the provided network topology, conceptualized as a vital component of **Gondar University's infrastructure**, reveals a well-structured and strategically designed campus network. The implementation of **VLANs** is fundamental to this design, effectively segmenting the network into logical broadcast domains for enhanced security, improved performance, and streamlined management across diverse university departments and services.

The meticulous **assignment of IP addresses and default gateways** to each segment, primarily through Switched Virtual Interfaces (SVIs) on Multilayer Switches, ensures efficient inter-VLAN communication and precise traffic flow. Furthermore, the strategic choice of **Dynamic Routing** protocols (such as EIGRP or OSPF) between the main routers, complemented by **Default Routing** for external connectivity, provides the necessary scalability, fault tolerance, and automated route management essential for a dynamic university environment.

Finally, the deployment of critical **servers** – including dedicated DNS and Web servers – forms the backbone of the university's digital services, providing essential resources for students, faculty, and administration. This comprehensive network architecture, therefore, lays a robust foundation for Gondar University's current and future digital needs, ensuring a resilient, secure, and highly available communication platform vital for academic excellence and administrative efficiency."

Referrence

https://uog.edu.et/bachler-science-information-technology-bsc/

https://uog.edu.et/ict-policy/3-access-to-ict-infrastructure-and-services-policy/

https://uog.edu.et/ict-policy/3-access-to-ict-infrastructure-and-services-policy/

https://doi.org/10.1186/1472-6947-13-31