

**PROJECT TITTLE:**

**DESIGN AND IMPLEMENTATION OF A CAMPUS NETWORK DESIGN**

**TEAM NAME: CYBER BOTS**

**Presented by:**

**JYOSHNA.MEDURI HARSHITHA.PATI**

**226W1A4397 226W1A0438**

**ROUTHU.MOULIKA**

**226W1A0445**

***ISTS CAMPUS NETWORK DESIGN***



**TASK:**

Plan, Design and Implement the network topology for ISTS Campus Network using Cisco Packet Tracer.

**TABLE OF CONTENTS:**

|  |  |  |
| --- | --- | --- |
| S.NO | TITLE | PAGE NO |
| 1.  2.  3.  4.  5.  6.  7.  8.  9.  10.  11. | Abstract  Project scope  Project Requirements  Tools used  Topologies   * Basic structure of Campus Network Design   Network Segmentation  Subnetting and IP Addressing Scheme  Routers  Switches  Summary of Design & Future Considerations  Appendices  Device Specifications  Cable OR Connection specifications | 3  4  5  5  6 – 39  40  41 – 42  43- 44  45- 46  47-48  49-50 |

1. **ABSTRACT:**

The design and implementation of a campus network play a crucial role in ensuring seamless communication, efficient data transfer, and secure connectivity within an educational institution. This project focuses on creating a scalable, reliable, and high-performance network that meets the diverse needs of students, faculty, and administrative staff.

The proposed network architecture follows a hierarchical design model, including core, distribution, and access layers, to optimize traffic flow and enhance manageability. Key components such as VLANs, IP subnetting, and wireless access points are incorporated to provide flexibility, security, and adequate bandwidth for both wired and wireless users.

This project aims to provide a robust and future-ready campus network that facilitates collaboration, e-learning, and administrative efficiency.

1. **Project Scope:**
2. Network Assessment and Requirements Gathering
   * Identify user requirements (students, staff, and visitors).
   * Assess the number of devices, data traffic, and application usage.
   * Consider future scalability and emerging technologies.
3. Designing the Network Architecture
   * Core, distribution, and access layer design.
   * Selection of routing and switching protocols.
   * Integration of wired and wireless networks.
   * VLAN design for segmentation and security.
4. Infrastructure Planning
   * Location and placement of network devices (routers, switches, access points).
   * Structured cabling plan for buildings.
   * Power backup and redundancy requirements.
5. Network Security
   * Firewall and intrusion detection/prevention system (IDS/IPS).
   * Access control mechanisms (802.1X authentication, MAC filtering).
   * Secure guest access network.
6. Connectivity and Internet Access
   * ISP selection and bandwidth management.
   * Redundant internet links for fault tolerance.
7. Performance Optimization
   * Load balancing and traffic prioritization (QoS).
   * Monitoring tools for real-time network performance.
8. Implementation Plan
   * Phased deployment strategy.
   * Testing and validation of network components.
9. Documentation and Training
   * Detailed network diagrams and configurations.
   * User and IT staff training on maintenance and troubleshooting
10. **Project Requirements:**

ISTS Institution is a large campus which has two campus situated 20 miles apart. The Institution’s students and staff are distributed in 4 faculties; these include the faculties of Health and Sciences; Business; Engineering/Computing and Art /Design. Each member of staff has a PC and Students have access to PCs in the labs.

1. Create a network topology with the main components to support the following:

**Main Campus:**

* **Block A:** Administrative staff in the departments of management (ADMIN), HR and Finance. The admin staff PC’s are distributed in the Block offices and it is expected that they will share some networking equipment (HINT: use of VLANs is expected here). The Faculty of Business is also situated in this Block.
* **Block B:** Faculty of Engineering and Computing and Faculty of Art and Designs.
* **Block C :** Student’s labs and IT department. The IT department hosts the university web server and other servers.
* There is also an email server hosted externally on the Cloud.

**Smaller Campus:**

* Faculty of Health and Sciences (staff and students labs are situated on separate floors).
* You will be expected to configure the core devices and few end devices to provide end-to-end connectivity and access to the internal servers and the external server.
* Each department/faculty is expected to be on its own separate IP network.
* The switches should be configured with appropriate VLANs and security settings.
* RIPv2 will be used to provide routing for the routers in the internal network and static routing for the external server.
* The devices in Block A will be expected to acquire Dynamic IP addresses from a router-based DHCP server.

1. **Tools used:**

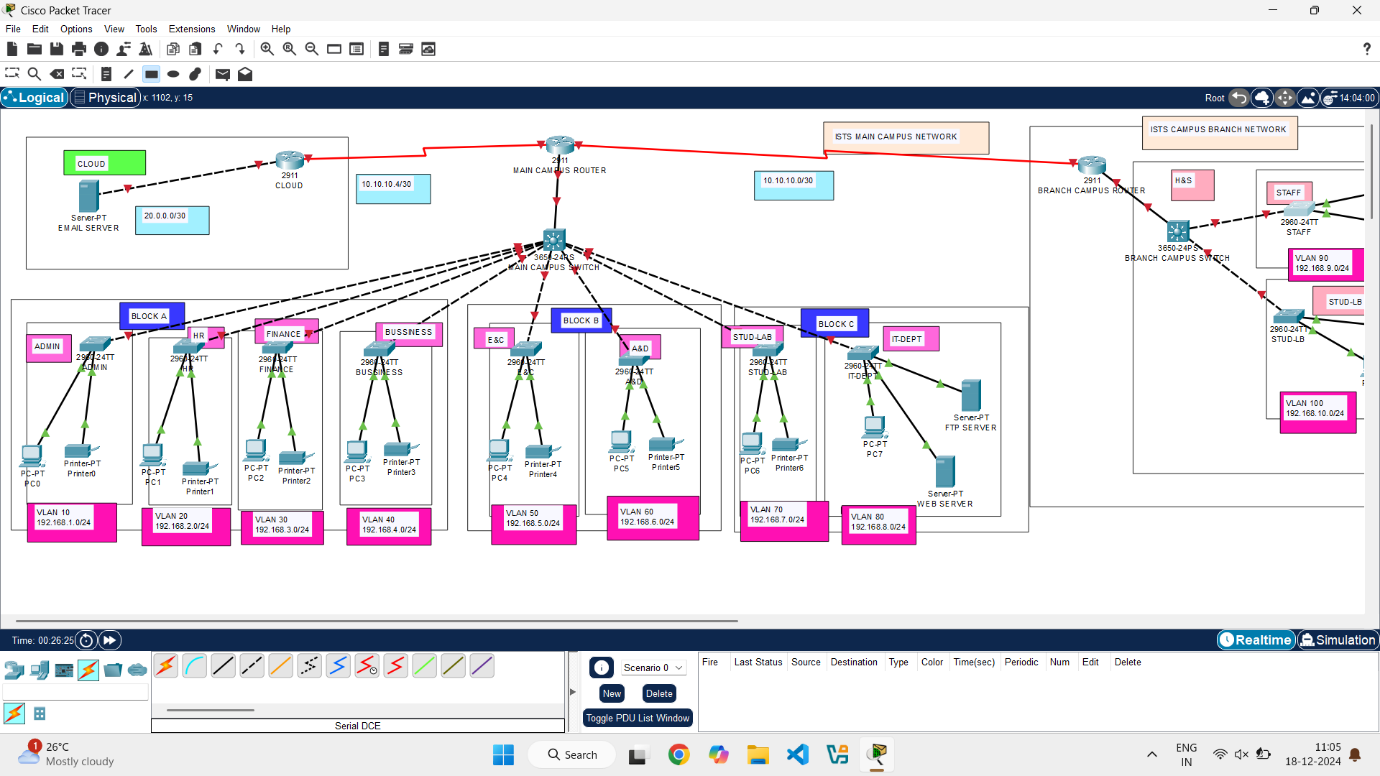
* Cisco Packet Tracer

**TOPOLOGIES:**

We are using ROUTING INFORMATION PROTOCOL (RIP) protocol in this network topology. the main working principle of RIP protocol is that it can connect beyond 15 routers not more than that.

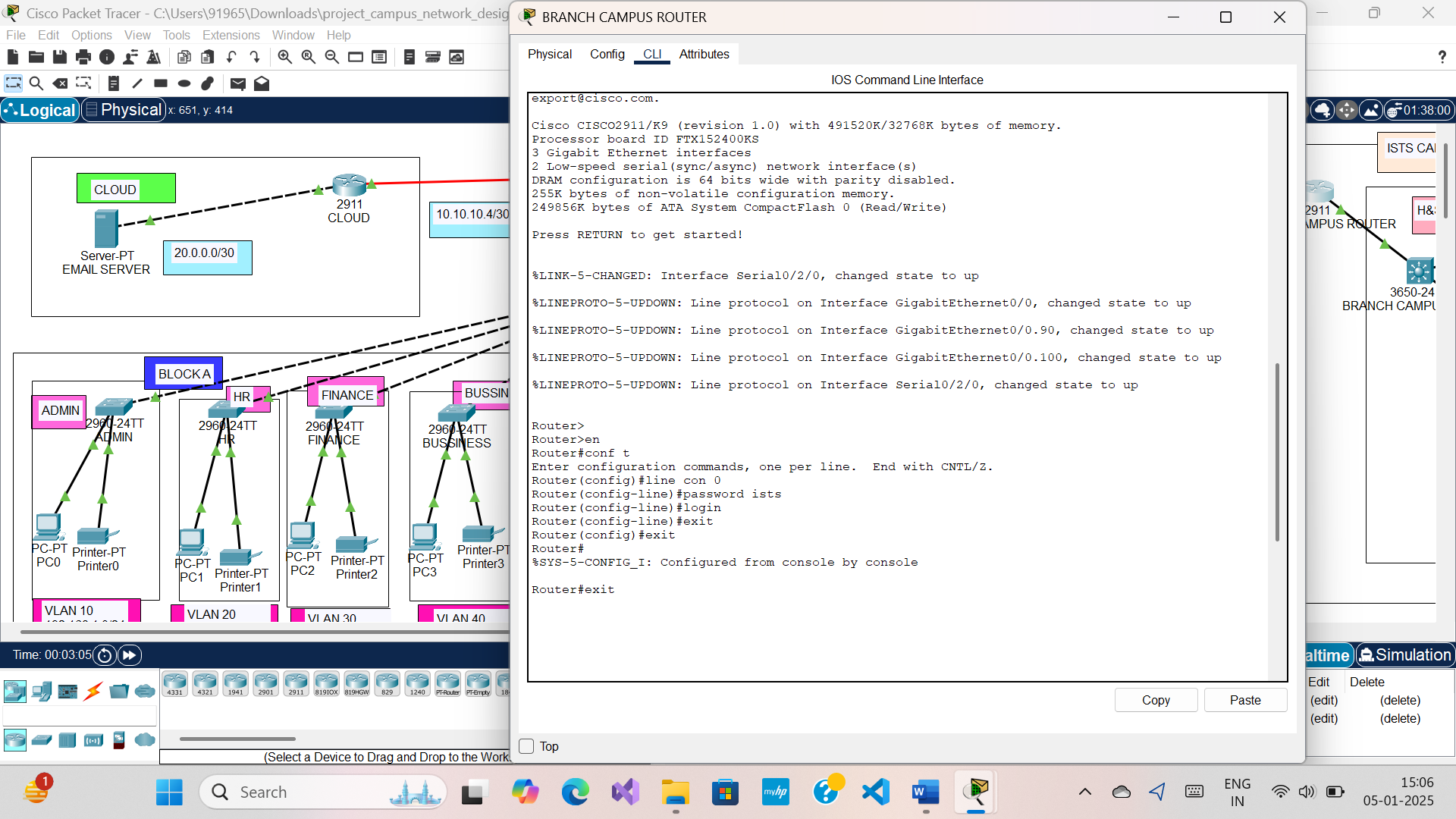
**Basic structure of Campus Network design:**

* The below figure shows that the basic structure of the ISTS MAIN CAMPUS AND BRANCHCAMPUS Network design



* The above ISTS campus network design and implementation of the figure is the combination of various routers (2911), servers (server-PT), switches (2960-24TT), pc’s (PC-PT), switches (3650-24PS), printer (printer-PT).
* The above router’s layer is called as CORE LAYER.

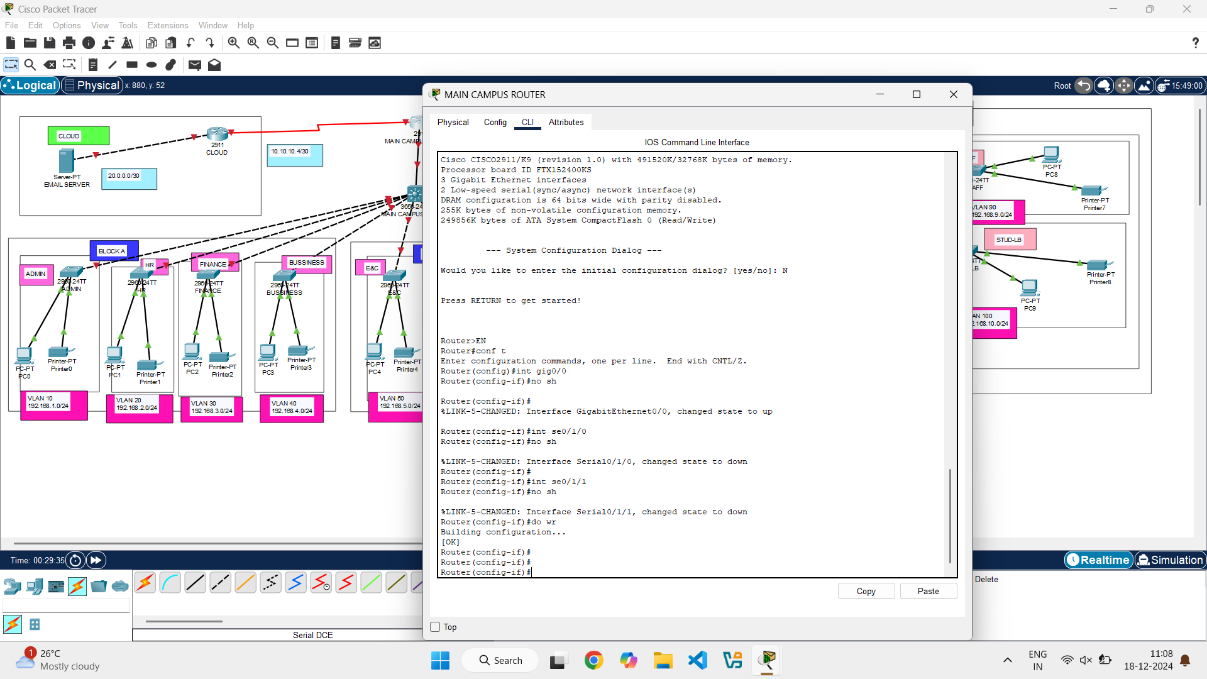
**ENCRYPTION KEY CONFIGURATION:**



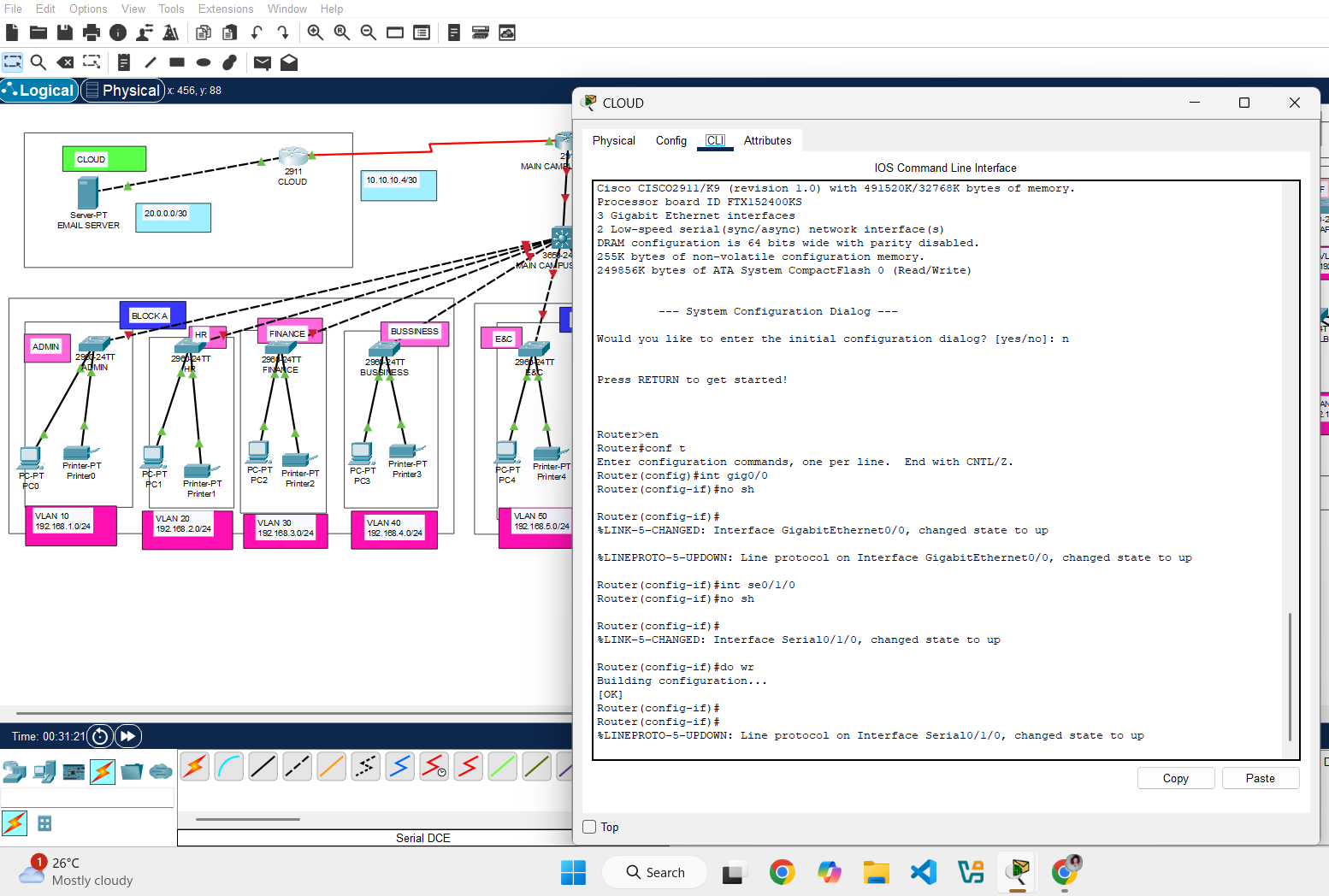
CONFIGURATION PART:

* Go to the Main campus router and click on the IOS Command line Interface.
* configure commands as shown in below figure to access all the PCs from Main campus router.

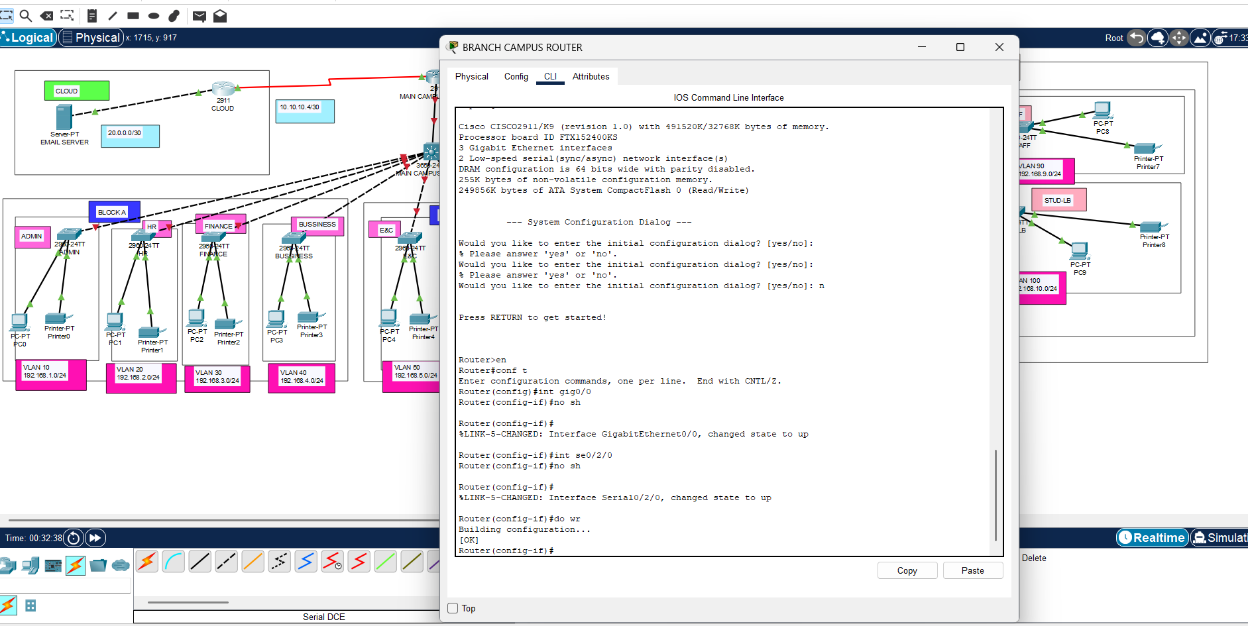
**Establishing a basic RIP routing configuration**



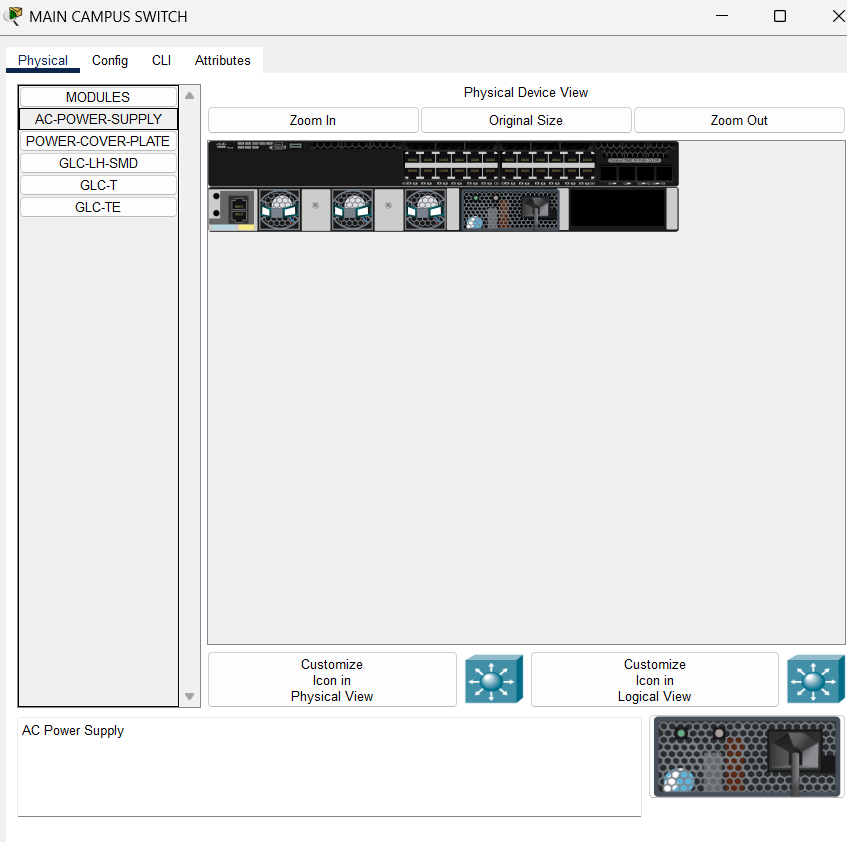
* Go to the Cloud router and do the same i.e. click on the IOS command line interface.
* Write the commands as shown below to make connections between the Cloud and main campus router



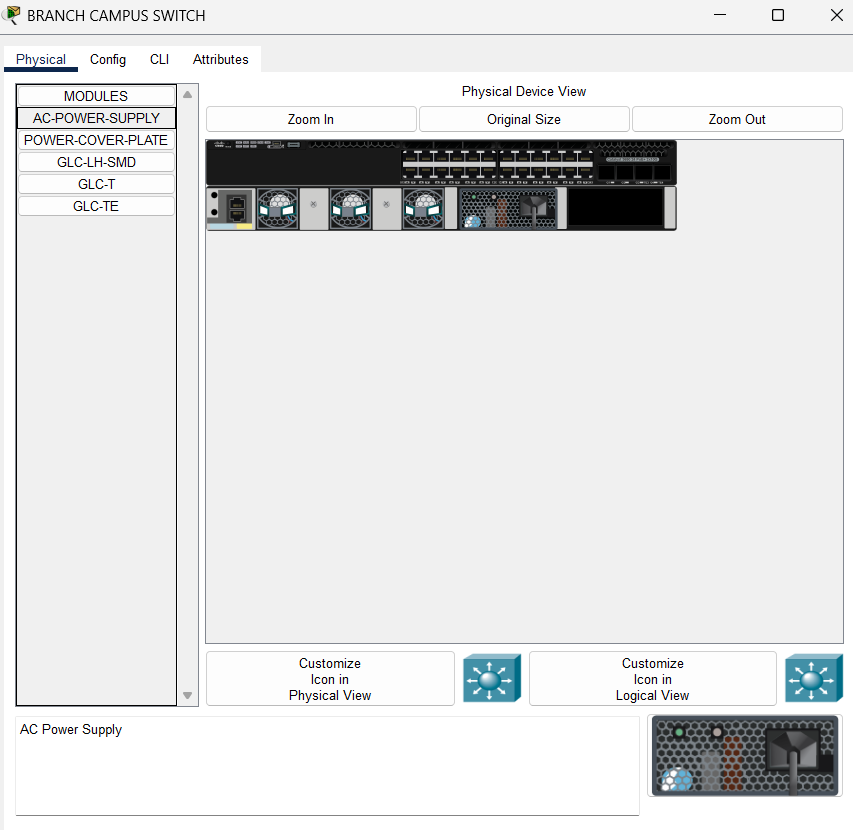
* Go the Branch campus router and click on the IOS command line interface.
* Write the commands as shown below to connect with the main campus router and also communicate with that campus PCs and switches



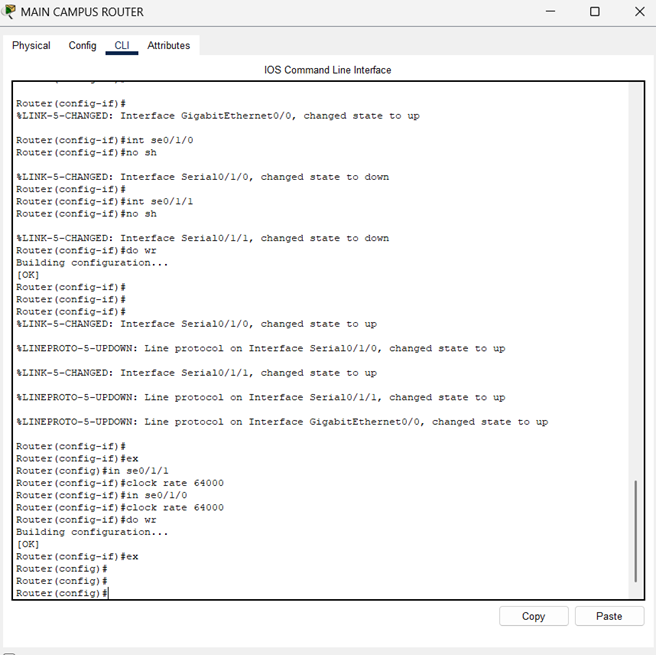
* Now, move to main campus switch (layer 3 switch) it is in default power supply turned OFF
* To make it turn ON, click on the AC – Power Supply and drag it to set in an empty slot.



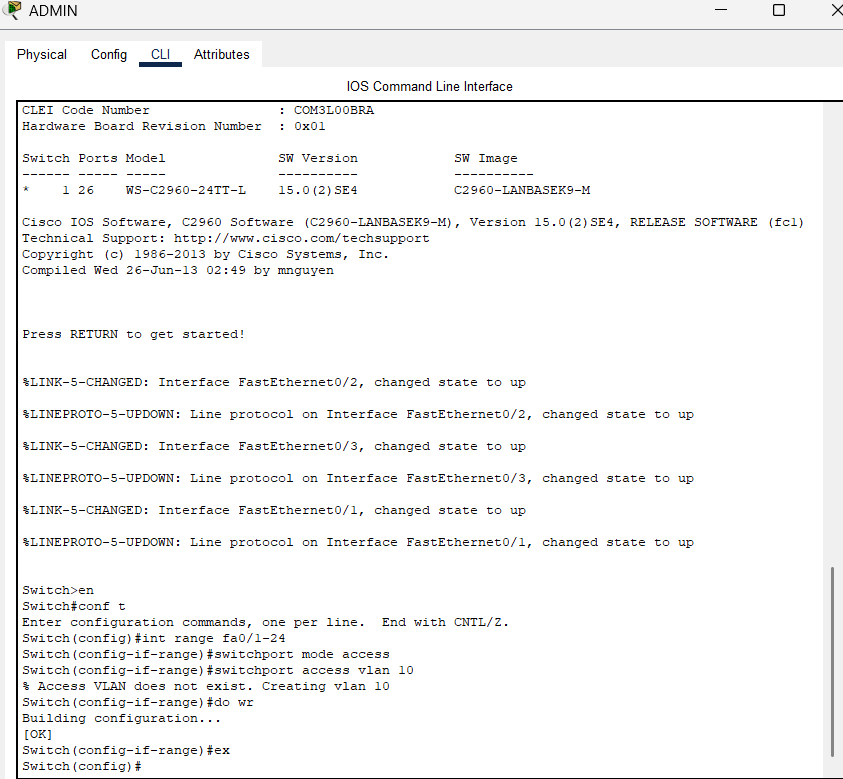
* Now, move to branch campus switch (layer 3 switch) it is in default power supply turned OFF
* To make it turn ON, click on the AC – Power Supply and drag it to set in an empty slot.



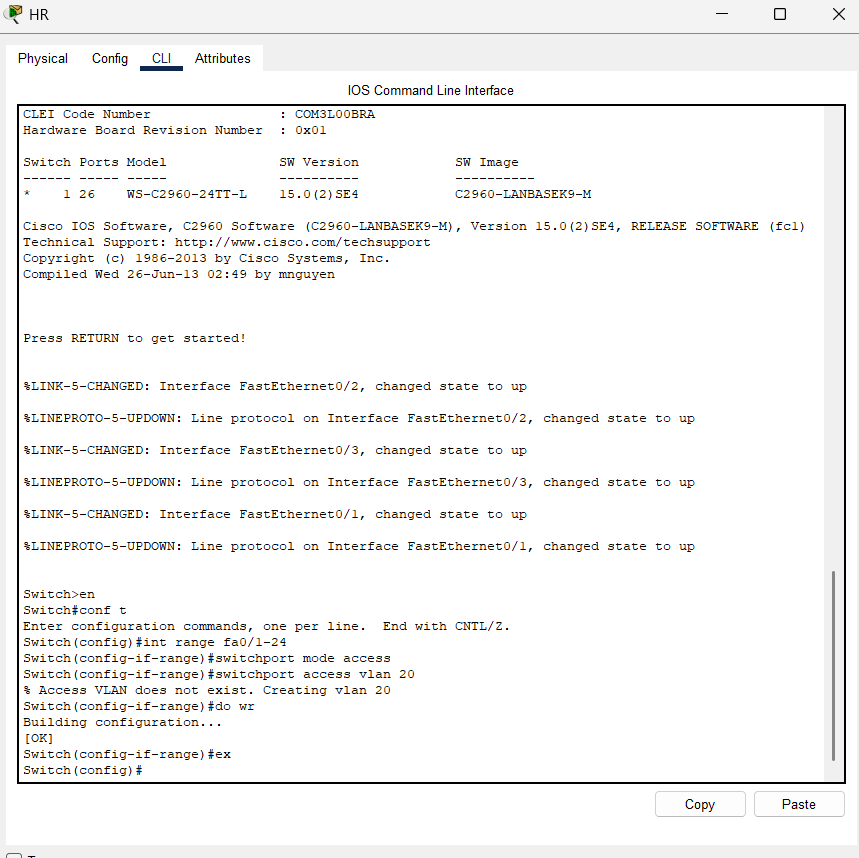
* Here we are using the SERIAL DCE cable to connect with the routers main campus and branch campus and cloud routers.
* One part of the SERIAL DCE cable has to configure with clock rate to enable traffic to flow through the cable.
* Write the commands as shown below to configure the clock rate one part of the SERIAL DC cable to enable the traffic flow through the cable/ interfaces.
* Now all the terminals of the network turn to GREEN that means the connection between them are successfully established.



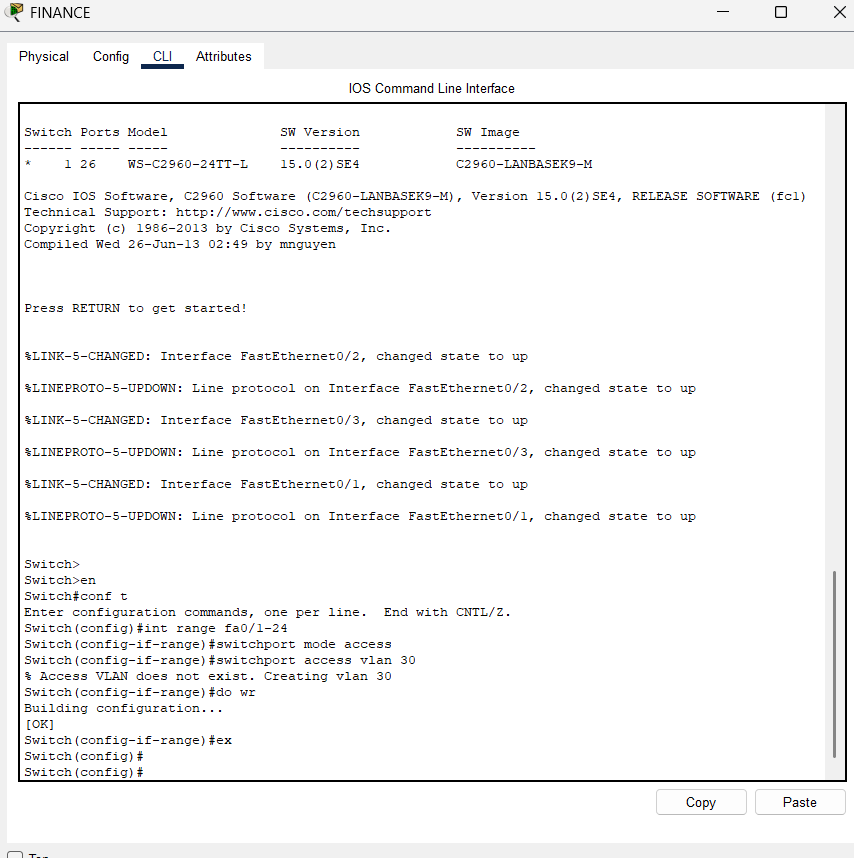
* Now the configuration begins in the access layer (layer two switches to layer three switch to the rounds).
* Now we will begin with the VLANs configuration on access layer switches
* ADMIN is in the VLAN 10
* Click on the ADMIN switch come to the IOS command line interface and write the commands as shown in the figure below.



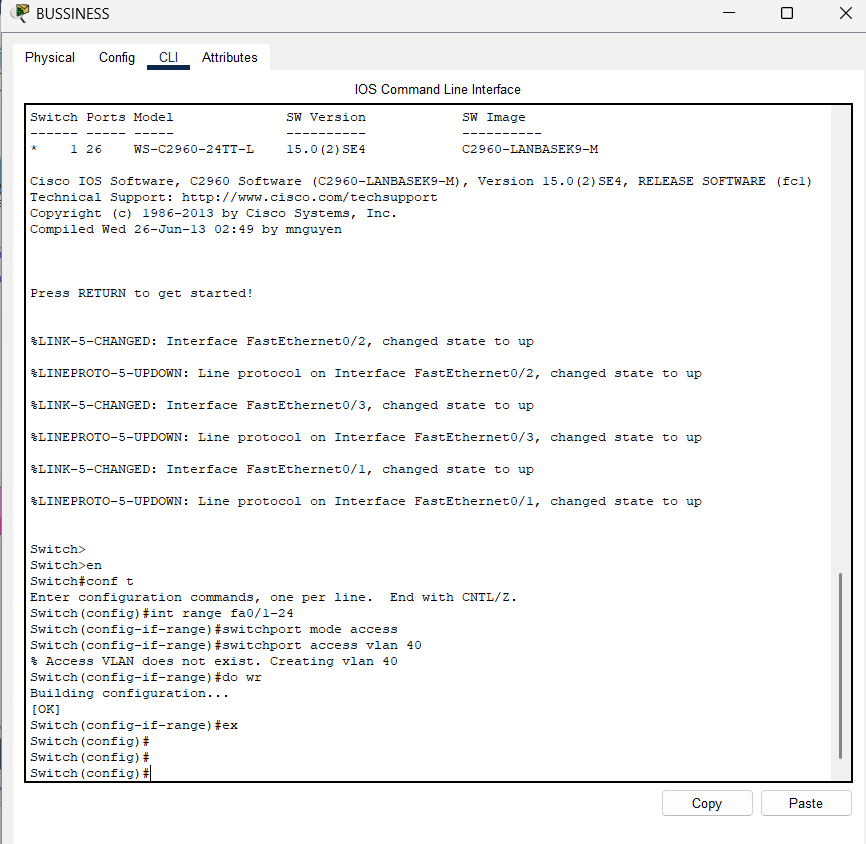
* HR is in the VLAN 20
* Click on the HR switch come to the IOS command line interface and write the commands as shown in the figure below.

****

* FINANCE is in the VLAN 30
* Click on the FINANCE switch come to the IOS command line interface and write the commands as shown in the figure below.



* BUSINESS is in the VLAN 40
* Click on the BUSINESS switch come to the IOS command line interface and write the commands as shown in the figure below.

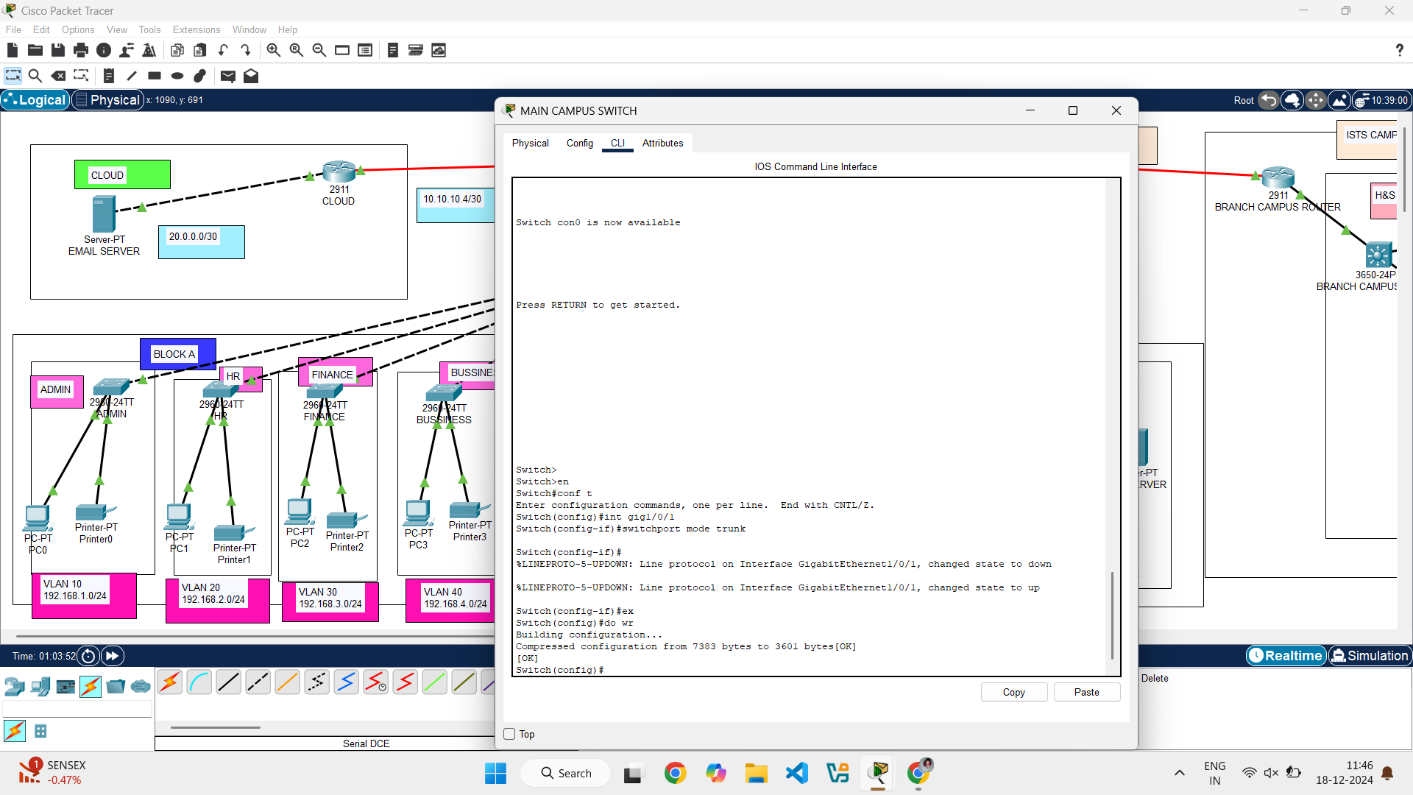


Simultaneously do for E&C, A&D, Student lab, IT dept

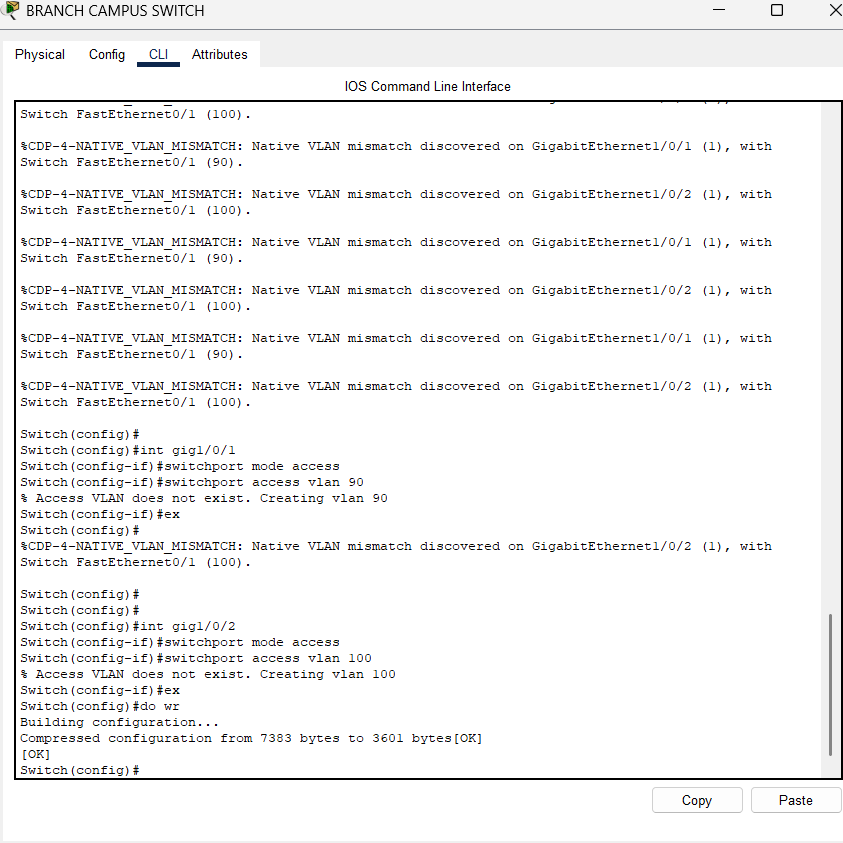
* E&C, A&D, Student lab, IT dept is in the VLAN 50,60,70,80 respectively.
* Click on the switch E&C, A&D, Student lab, IT dept come to the IOS command line interface and write the commands as shown in the figure below.

We made all the ports in the access layer switches to be in the access mode and we assigned those ports to with various VLANs.

* To access the ports in all the VLANs from the access layers with the main switch we should move to the main campus switch and click on the IOS command line interface write the commands as shown the below figure to communicate all the ports with the main switch.

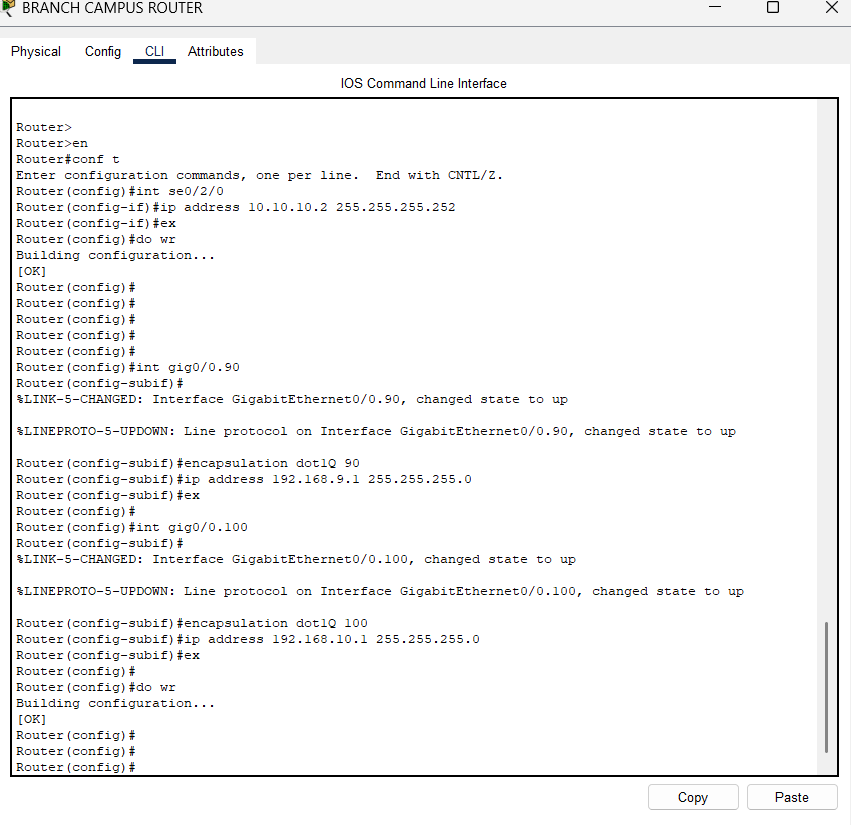


* Go to the Branch campus switch and click on the command line interface write the commands to communicate the switch with staff and stud lab in the VLANs of 90 and 100 respectively shown below.

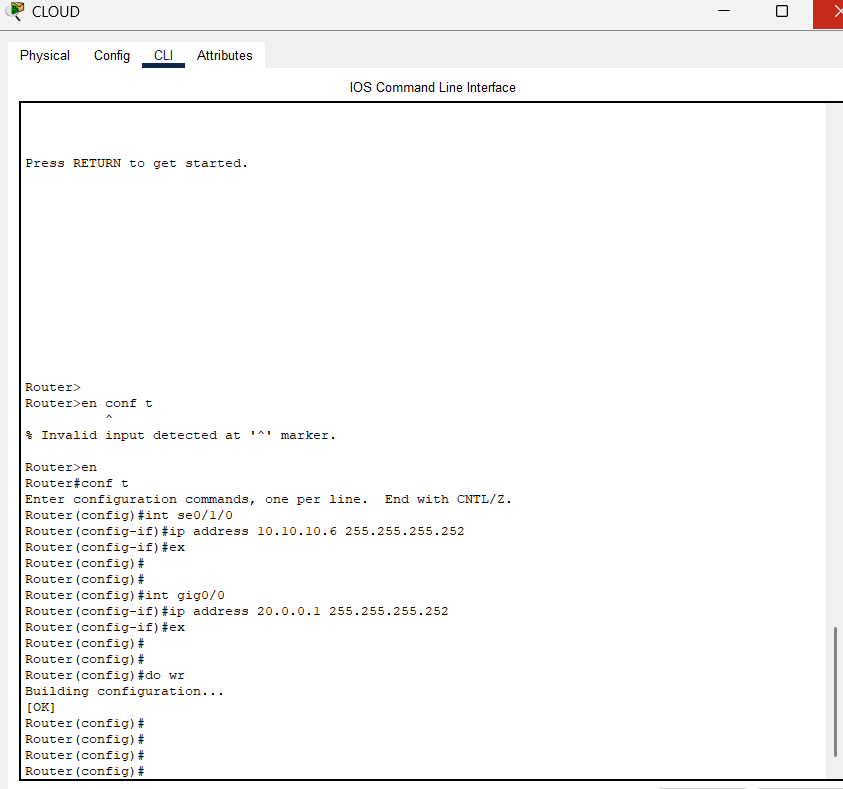


Connection between the main campus router and branch campus router. If this connection is disabled all the switches under the branch campus router doesn’t work.

So, the connection should be proper.



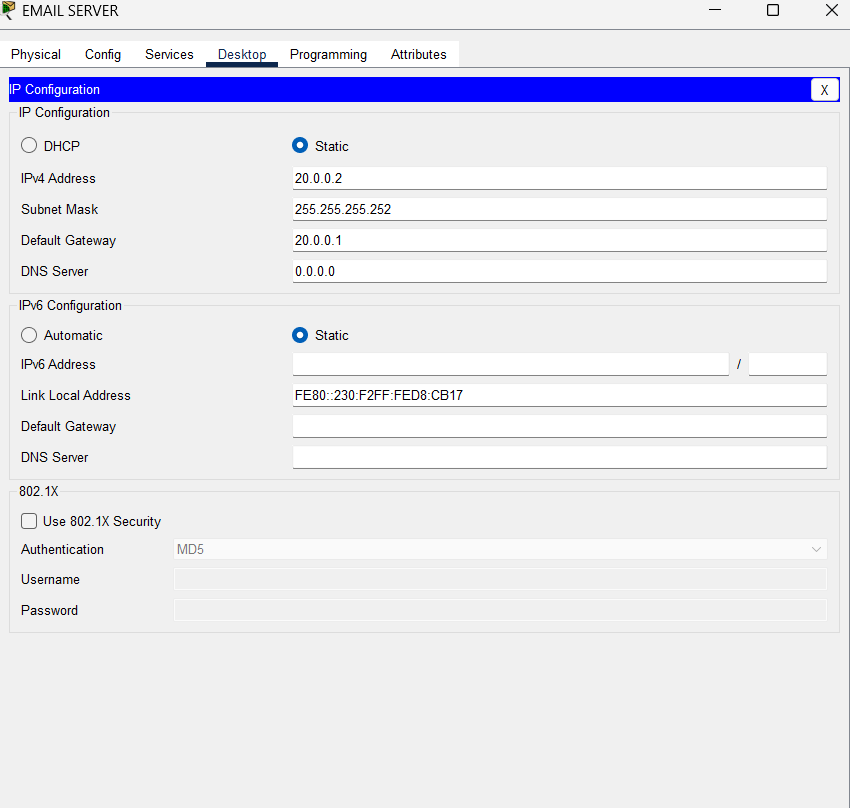
* The image shows a configuration session on a router using the Cisco IOS Command Line Interface (CLI).
* Users need to be in the correct mode to execute commands.
* **Interface Configuration**: Assigning IP addresses to interfaces is crucial for enabling communication.



The image shows the IP configuration settings for an **Email Server** in a simulation environment, likely from Cisco Packet Tracer.

**IPv4 Configuration:**

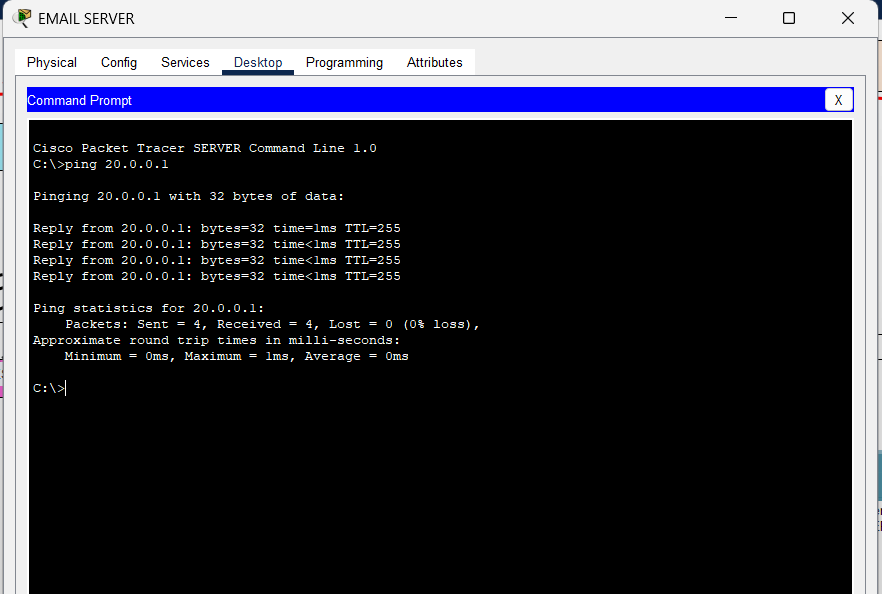
* **Mode**: Static
  + The server is using a static IP address, meaning the address is manually assigned and does not change dynamically.
* **IPv4 Address**: 20.0.0.2
  + This is the unique IP address of the email server on the network.
* **Subnet Mask**: 255.255.255.252
  + This defines the network segment, allowing only two usable host addresses (20.0.0.1 and 20.0.0.2) in this small subnet.
* **Default Gateway**: 20.0.0.1
  + The gateway through which the email server communicates with devices outside its subnet.
* **DNS Server**: 0.0.0.0
  + Indicates no DNS server is configured. DNS is typically used for resolving domain names to IP addresses.



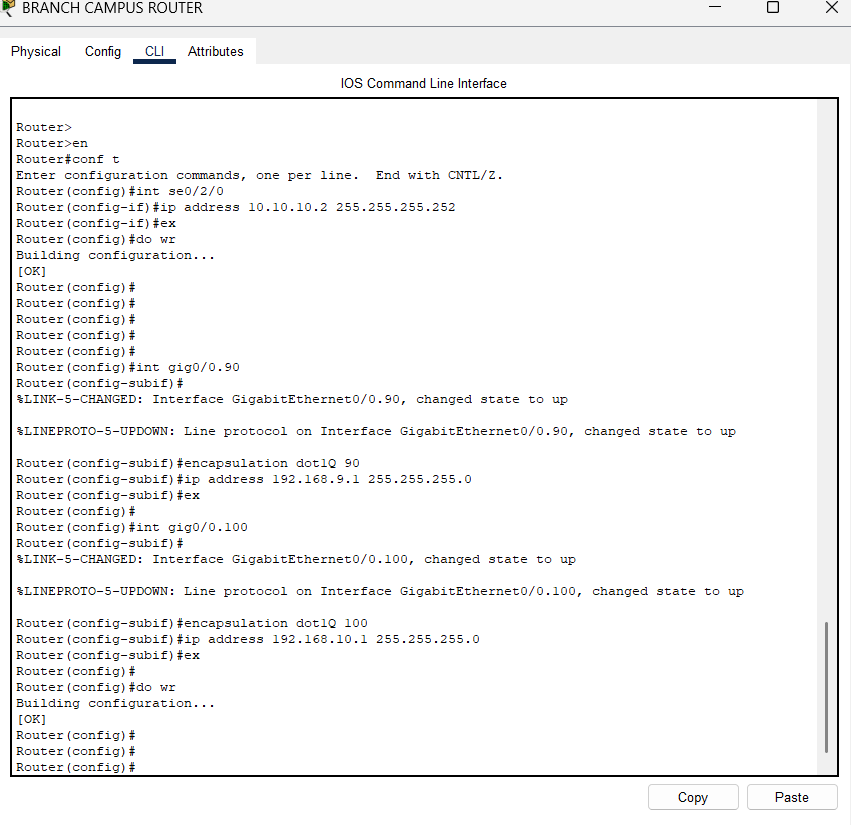
The image shows the **Command Prompt** on an **Email Server** in a simulation environment (likely Cisco Packet Tracer), performing a **ping test** to the IP address 20.0.0.1

* The user runs the command ping 20.0.0.1.
* The ping command is used to test the connectivity between the email server (source) and the device with the IP address 20.0.0.1 (destination).
* PacketsSent: 4
* PacketsReceived: 4

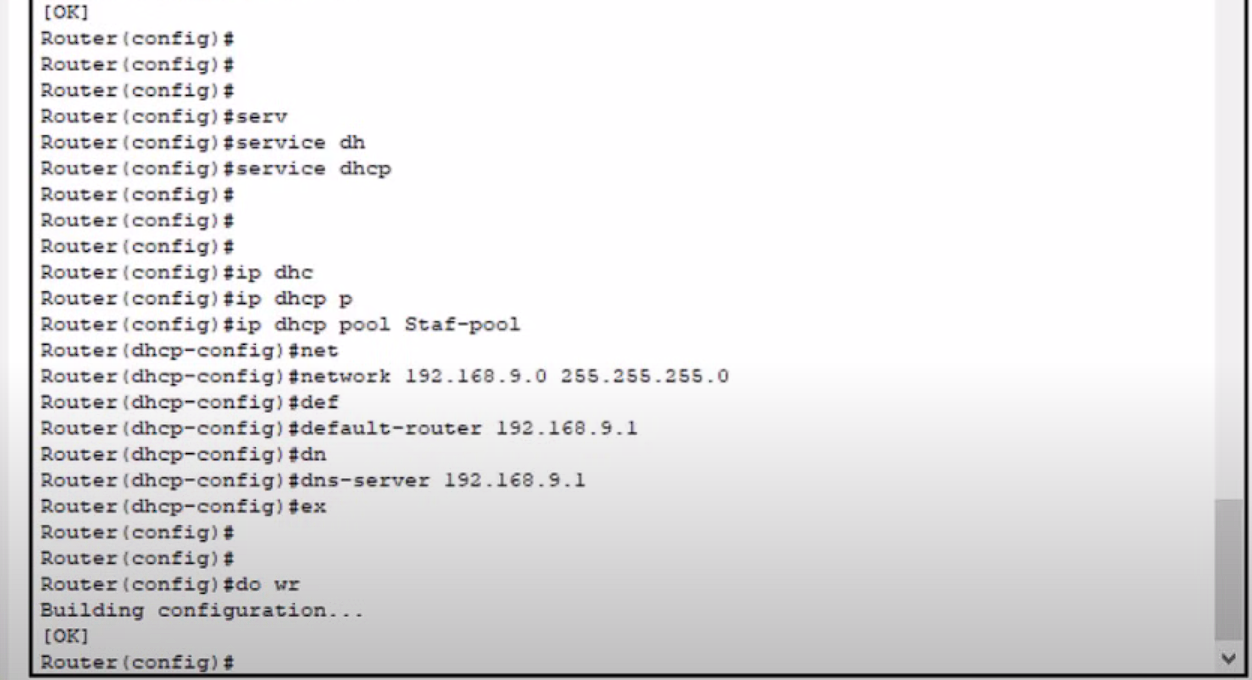
The email server (20.0.0.2) is successfully connected to the gateway or router (20.0.0.1), as verified by the replies.



* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to establish network connectivity.
* The router is being configured with multiple interfaces and sub interfaces. The Serial interface is likely used for a point-to-point connection, while the Gigabit Ethernet interface is used for multiple VLANs, each with its own IP address and subnet mask. This configuration allows the router to connect and route traffic between different network segments.



* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to act as a DHCP server.
* The router is being set up as a DHCP server to provide IP addresses, default gateway, and DNS server information to clients on the 192.168.9.0/24 network. This configuration automates the process of assigning IP addresses to clients, simplifying network administration.



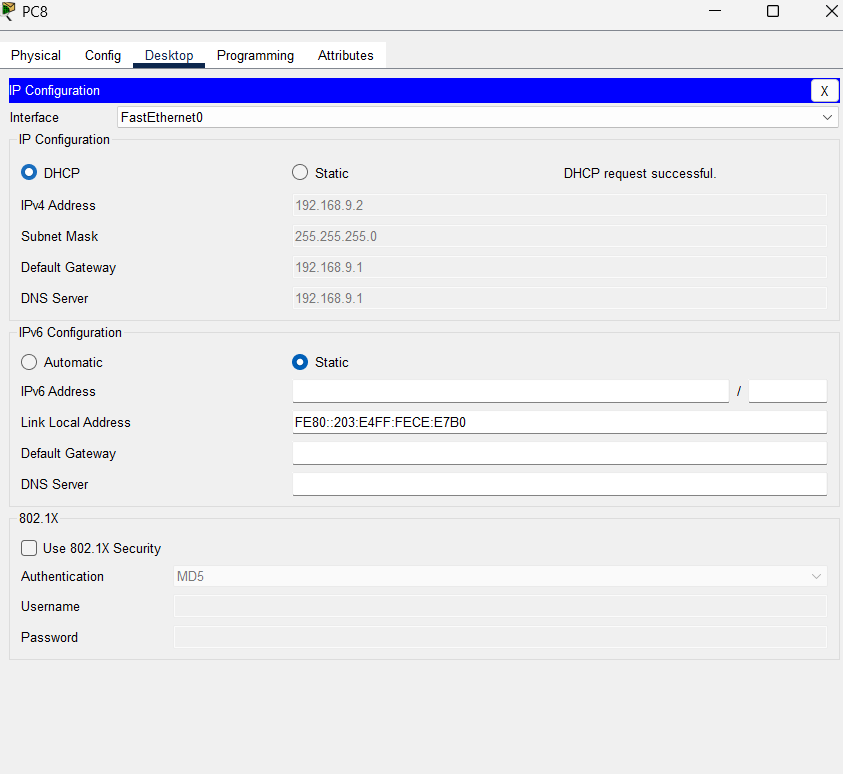
The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.

 **Interface:** FastEthernet0 - This indicates the specific network interface being configured.

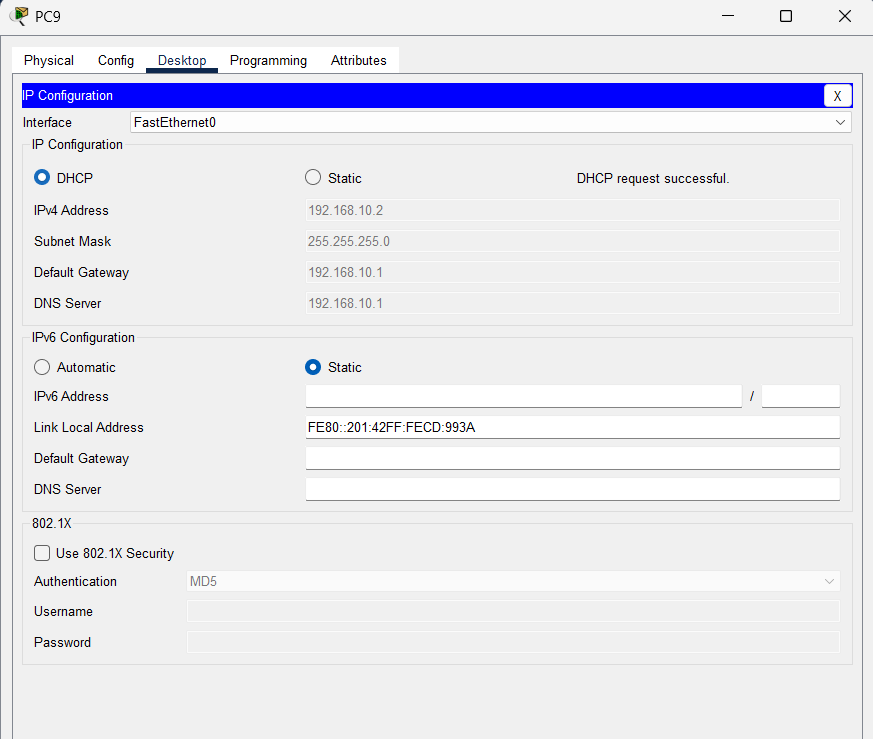
 **IP Configuration:**

* **DHCP:** The radio button for DHCP is selected, meaning the device is configured to obtain its IP address and other network settings dynamically via the DHCP protocol from a DHCP server.
* **Static:** This option is not selected, indicating that the device is not configured with static IP settings.
* **DHCP request successful:** This message confirms that the device has successfully requested and received its IP address and other network settings from the DHCP server.

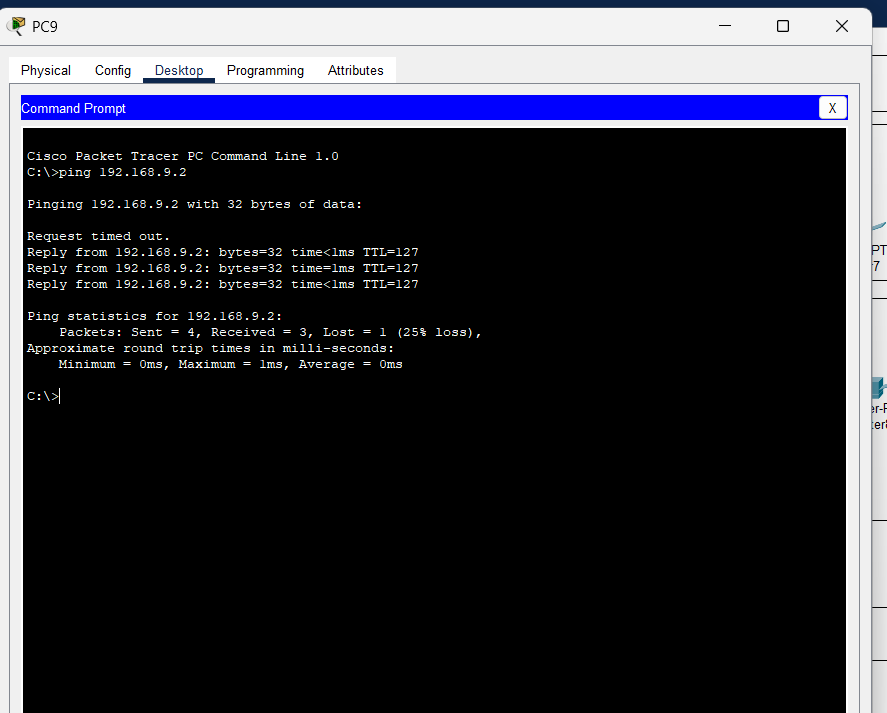
The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



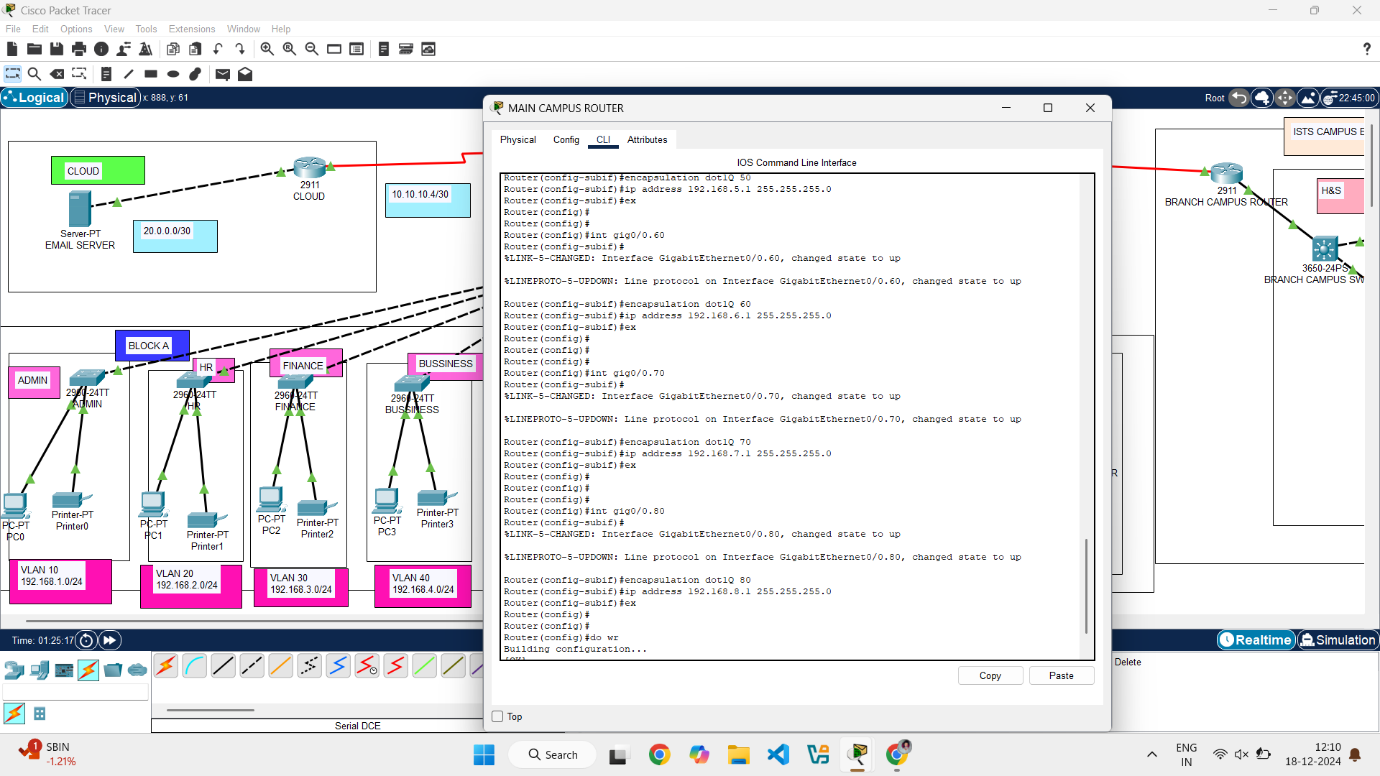
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



* The image shows a command prompt window in a Cisco Packet Tracer simulation.
* ping 192.168.9.2
* This command is used to test the connectivity between the device running the command prompt (likely PC9) and the device with the IP address 192.168.9.2.
* Overall, the ping test shows that PC9 can successfully communicate with the device at 192.168.9.2 with a low latency (1ms), but there was one packet loss.



* The image shows a Cisco IOS Command Line Interface (CLI) session on a router, specifically the Main Campus Router. The router is being configured to establish network connectivity.
* The router is being configured with multiple sub interfaces on Gigabit Ethernet interface 0/0. Each sub interface is assigned a specific VLAN (10,20,30,40,50, 60, 70, 80) and a corresponding IP address and subnet mask. This configuration enables the router to handle traffic for different VLANs, allowing for network segmentation and improved security.



The image you provided shows a network topology diagram, likely created using Cisco Packet Tracer.

**Overall Network Structure:**

* **Two Main Components:** It appears to be a network divided into two main sections:
  + **Main Campus:** This section has a central router (likely the "Main Campus Router") connected to multiple switches. These switches then connect to various devices like PCs, printers, and servers.
  + **Branch Campus:** This section has a separate router (likely the "Branch Campus Router") connected to switches and devices similar to the main campus.
* **Interconnection:** The main campus and branch campus are connected via a serial link.

**Key Devices:**

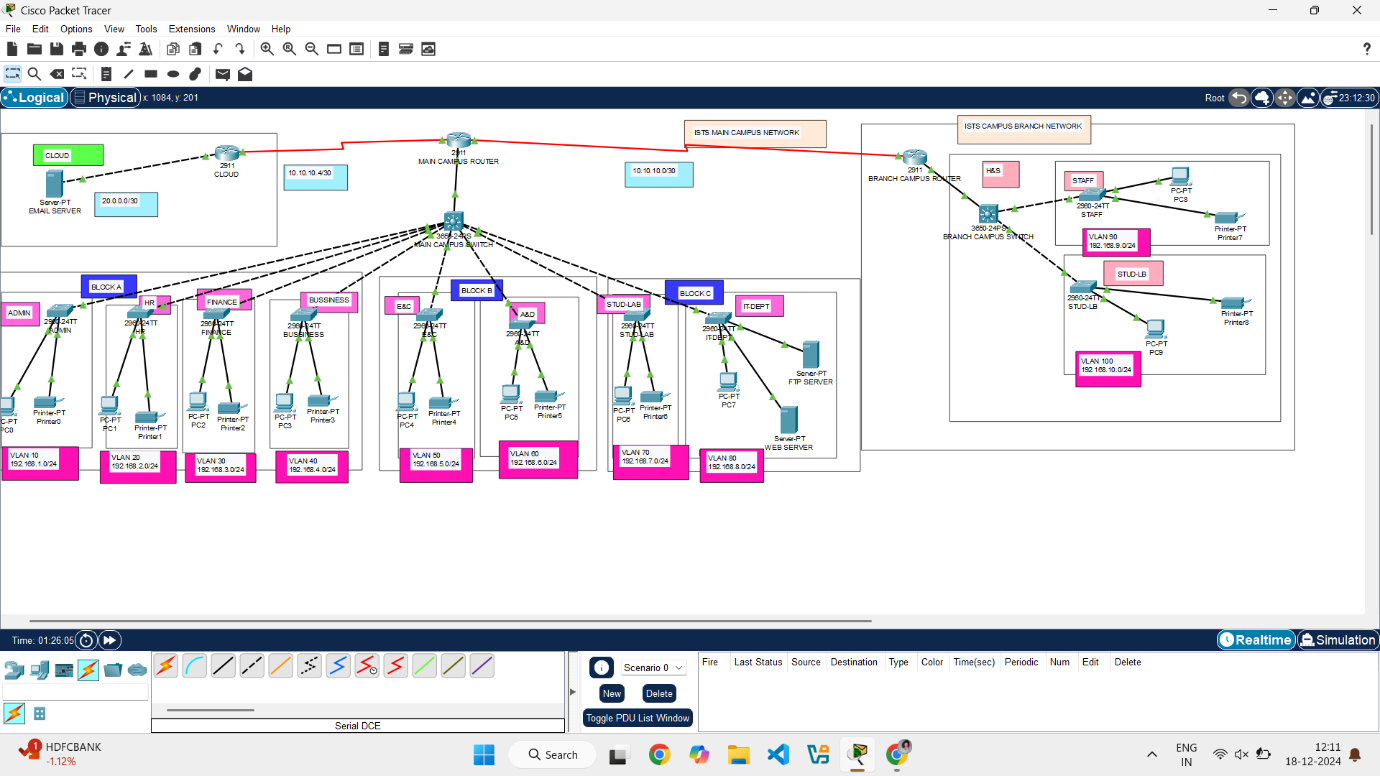
* **Routers:**
  + **Main Campus Router:** This is the central point for routing traffic within the main campus and connecting to the branch campus.
  + **Branch Campus Router:** This router handles traffic within the branch campus and connects back to the main campus.
* **Switches:** These devices connect multiple devices within a specific network segment (e.g., VLANs) and facilitate communication within that segment.
* **End Devices:** These include PCs, printers, servers, and other devices that use the network.

**VLANs (Virtual Local Area Networks):**

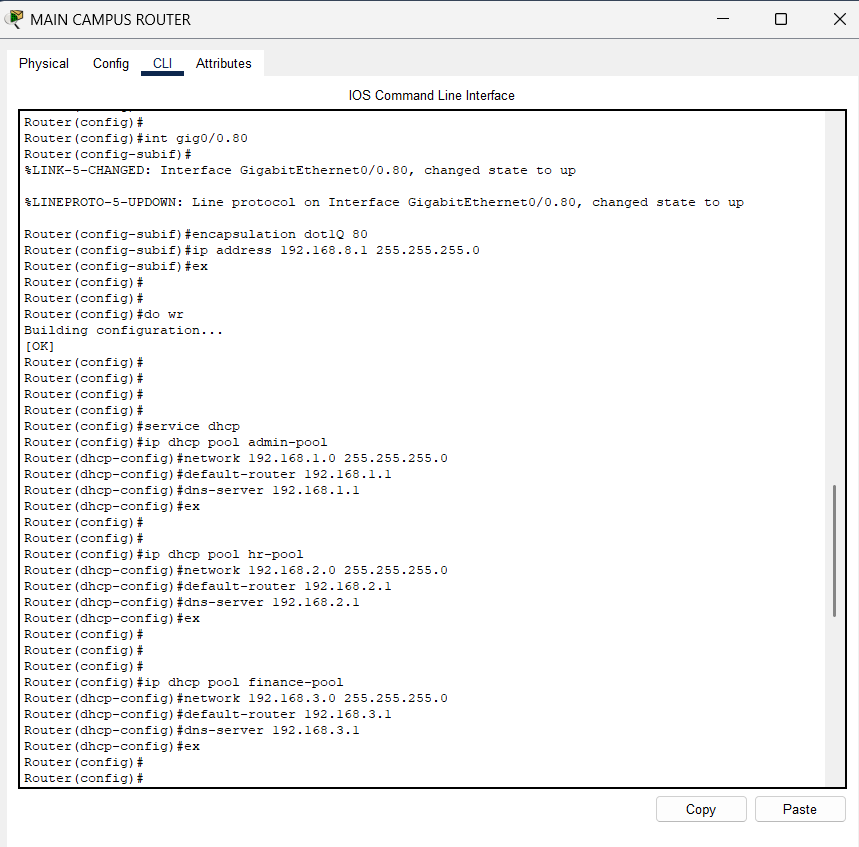
* **Color-Coded:** The different colored lines connecting devices to switches likely represent different VLANs.
* **Segmentation:** VLANs are used to logically segment the network, improving security and traffic management.

**Possible Observations:**

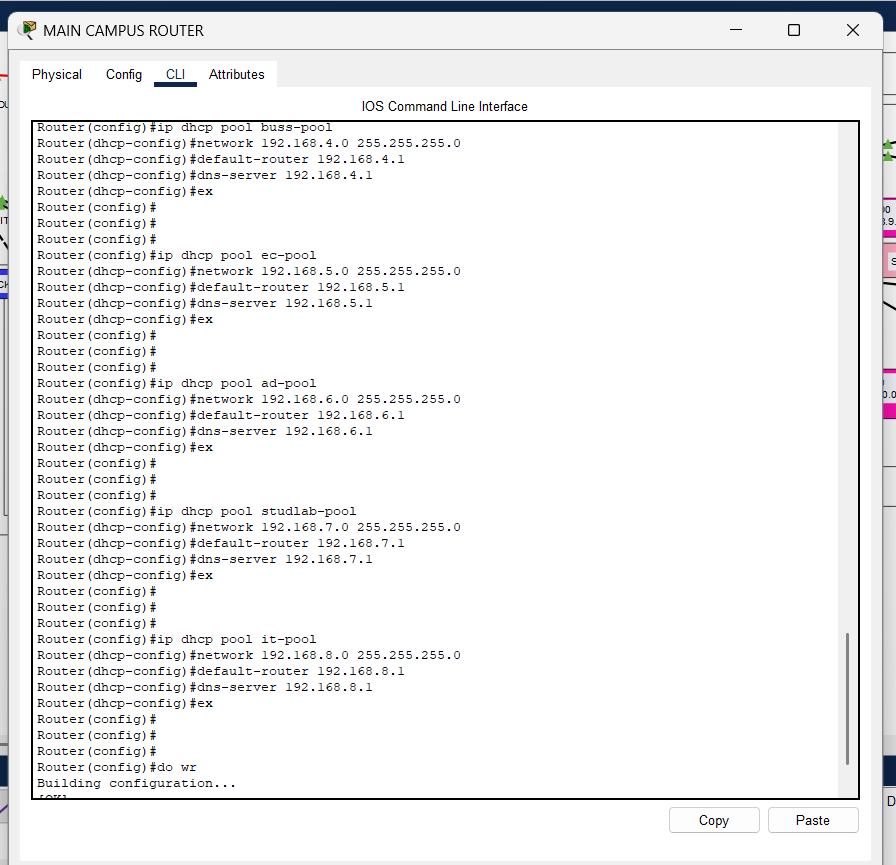
* **Network Size:** The network appears to be of a moderate size, suitable for a small to medium-sized organization.
* **Topology:** The hierarchical structure with a central router provides a good foundation for scalability and manageability.
* **Security:** VLANs and potentially firewalls (not explicitly shown) would be essential for network security.



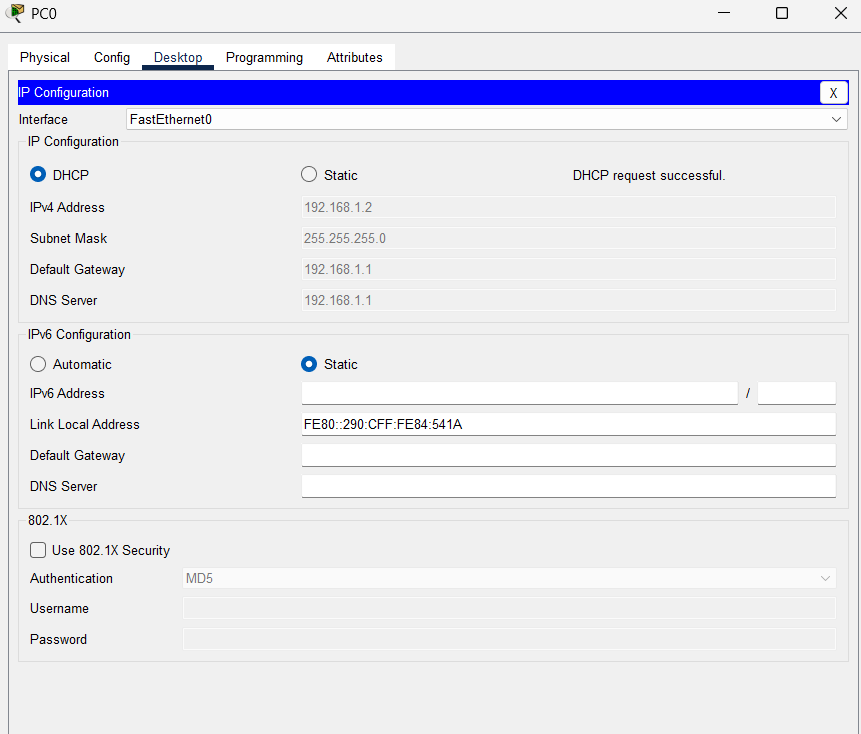
* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to act as a DHCP server.
* The router is being set up as a DHCP server to provide IP addresses, default gateway, and DNS server information to clients on three different networks (192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24). Each network has its own DHCP pool with specific settings. This configuration automates the process of assigning IP addresses to clients, simplifying network administration



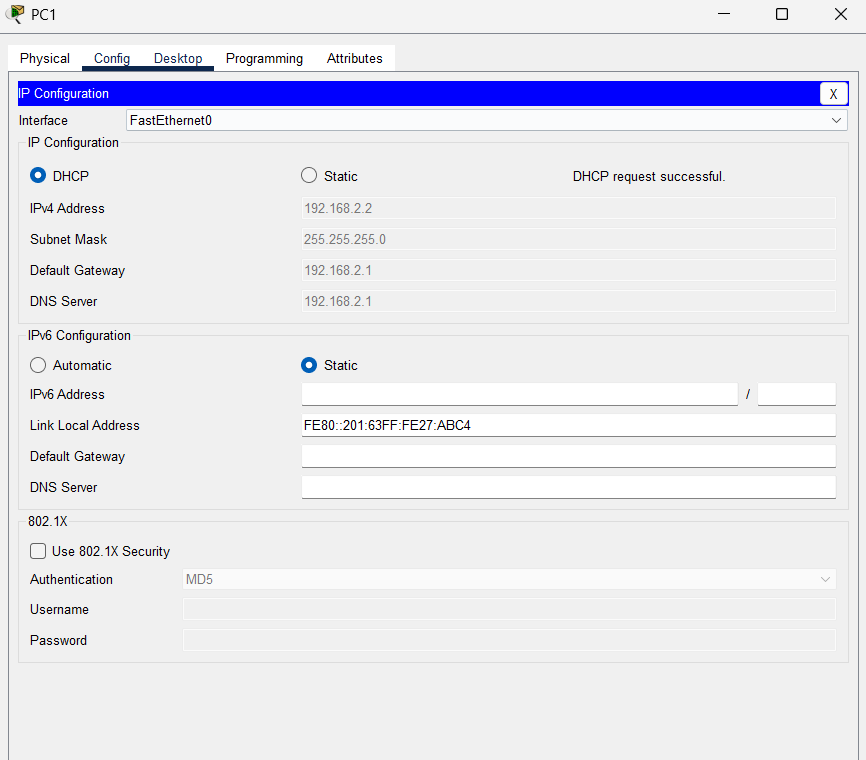
* The image shows a Cisco IOS Command Line Interface (CLI) session on a router, specifically the Main Campus Router. The router is being configured to act as a DHCP server.
* The router is being set up as a DHCP server to provide IP addresses, default gateway, and DNS server information to clients on five different networks (192.168.4.0/24, 192.168.5.0/24, 192.168.6.0/24, 192.168.7.0/24, and 192.168.8.0/24). Each network has its own DHCP pool with specific settings. This configuration automates the process of assigning IP addresses to clients, simplifying network administration.



* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



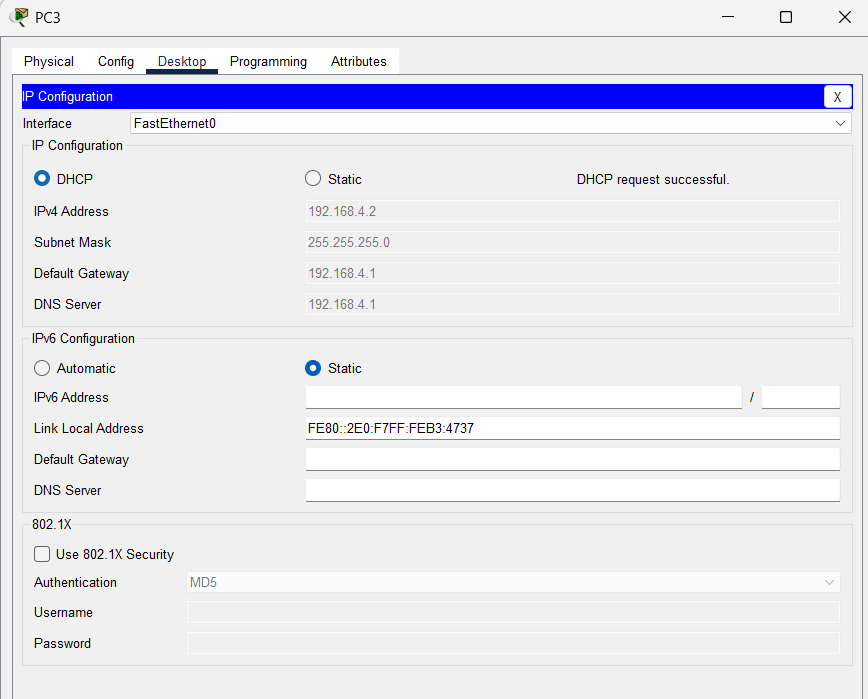
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled



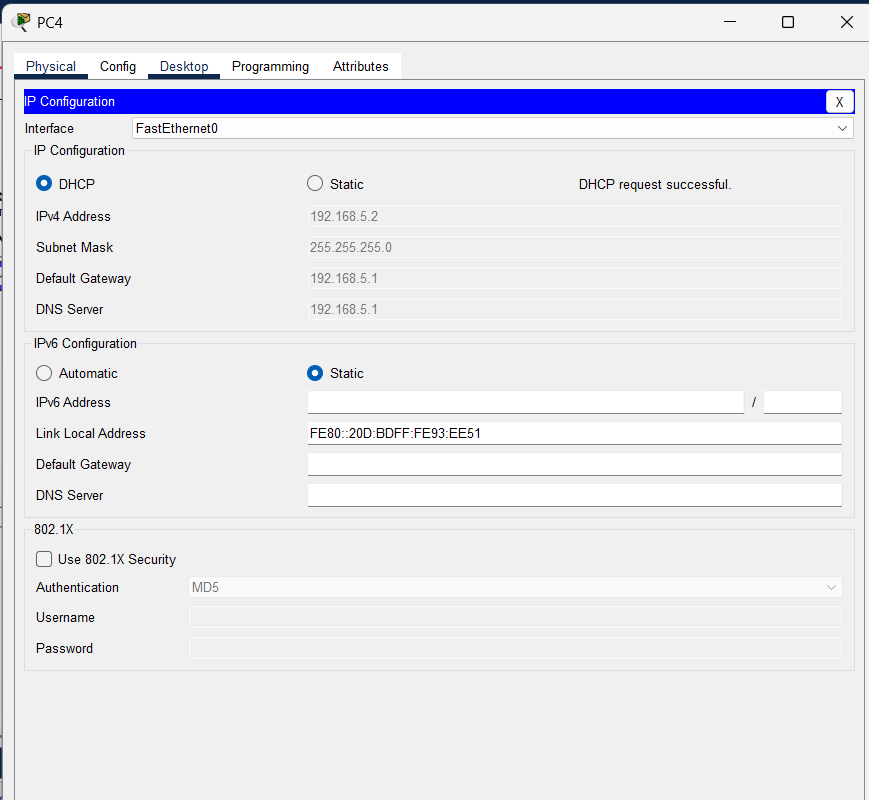
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



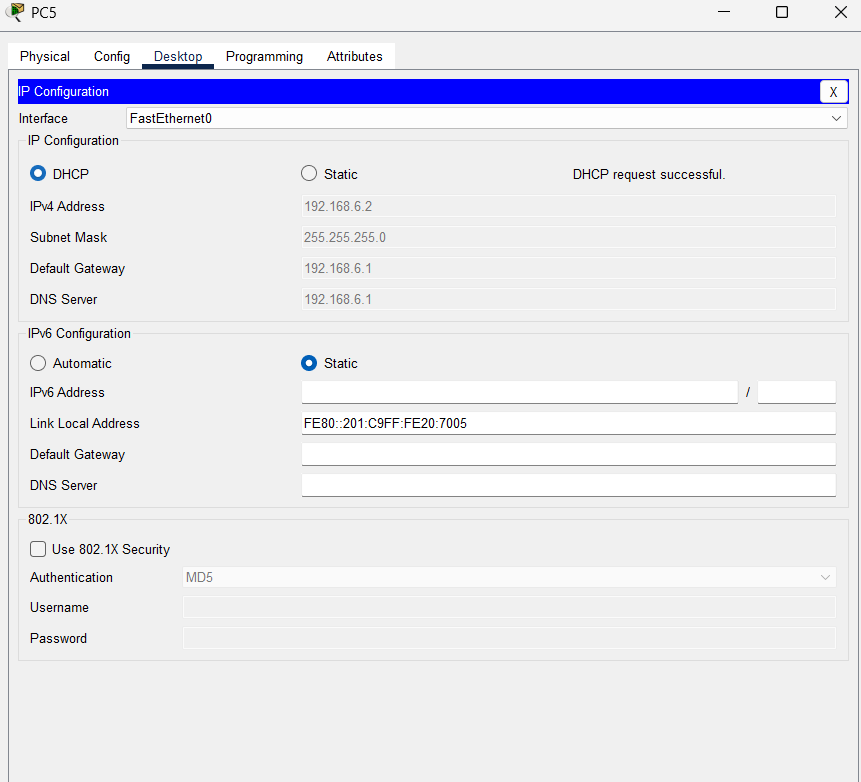
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



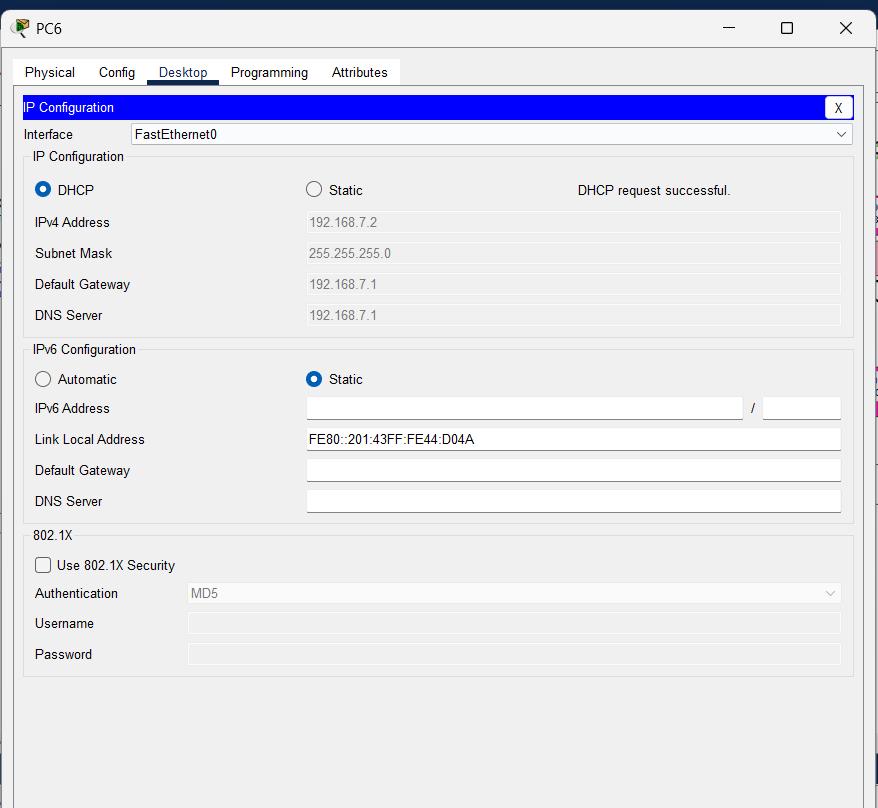
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



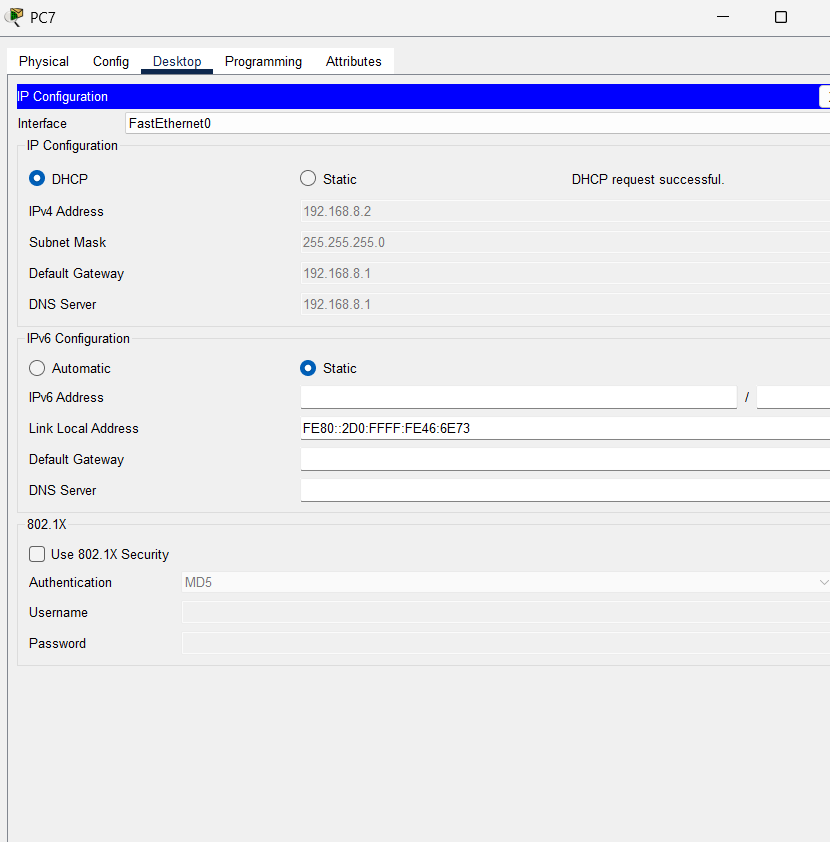
* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.

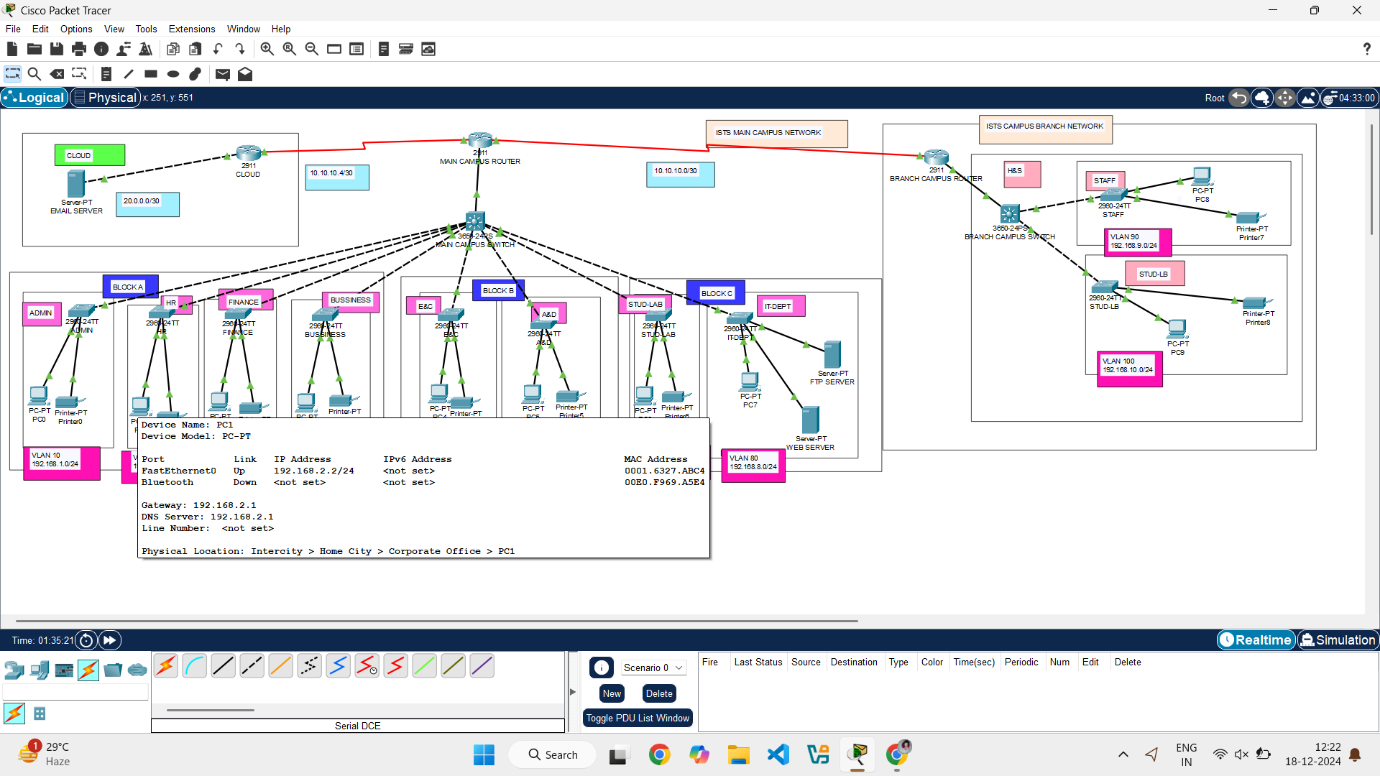


* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



* The image depicts the IP Configuration section of a network interface card (NIC) in a device, likely a computer or a virtual machine.
* The image shows that the network interface is configured to use DHCP for IPv4 settings and has a statically configured IPv6 address. It also indicates that 802.1X network access control is not enabled.



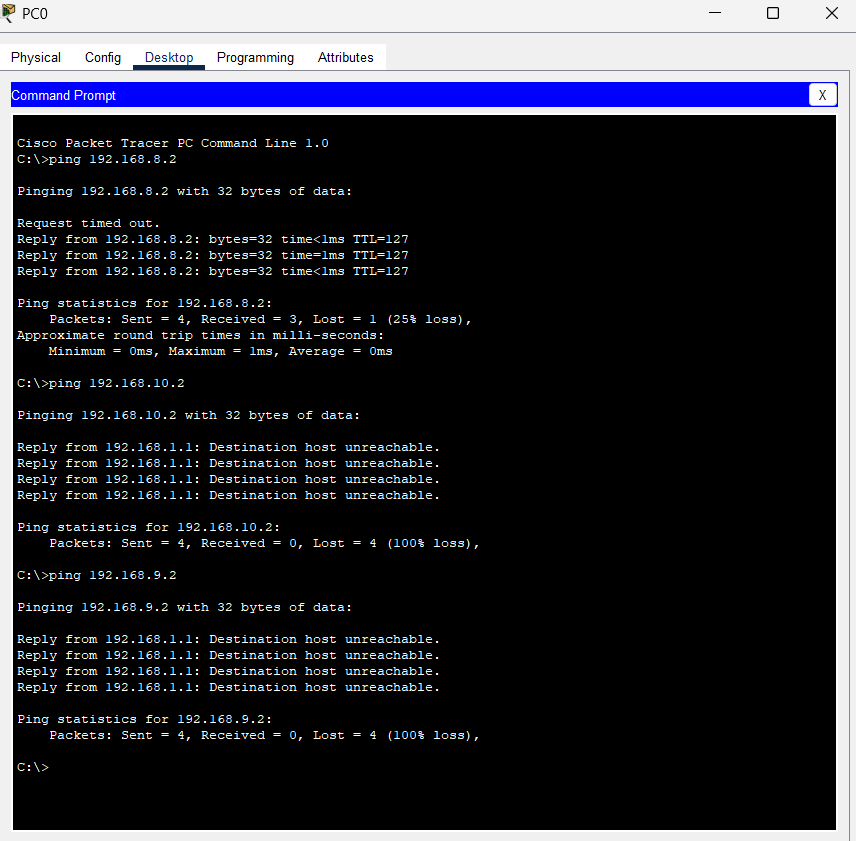


The image displays a Cisco Packet Tracer simulation with a command prompt window. It shows a series of ping commands being executed and their corresponding results.

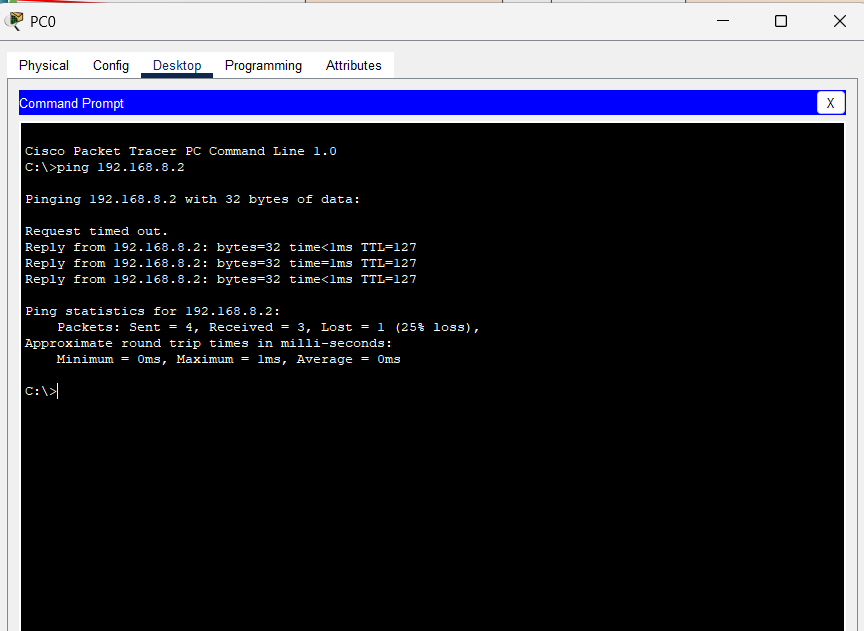
To troubleshoot the unreachable destinations, you would need to investigate the following:

* **Verify IP Addresses:** Double-check the correctness of the destination IP addresses.
* **Check Routing Tables:** Examine the routing tables on the routers involved to ensure they are correctly configured.
* **Review Firewall/ACL Rules:** Inspect any firewalls or ACLs that might be affecting traffic flow.
* **Check Device Status:** Verify that the destination devices are powered on and reachable.

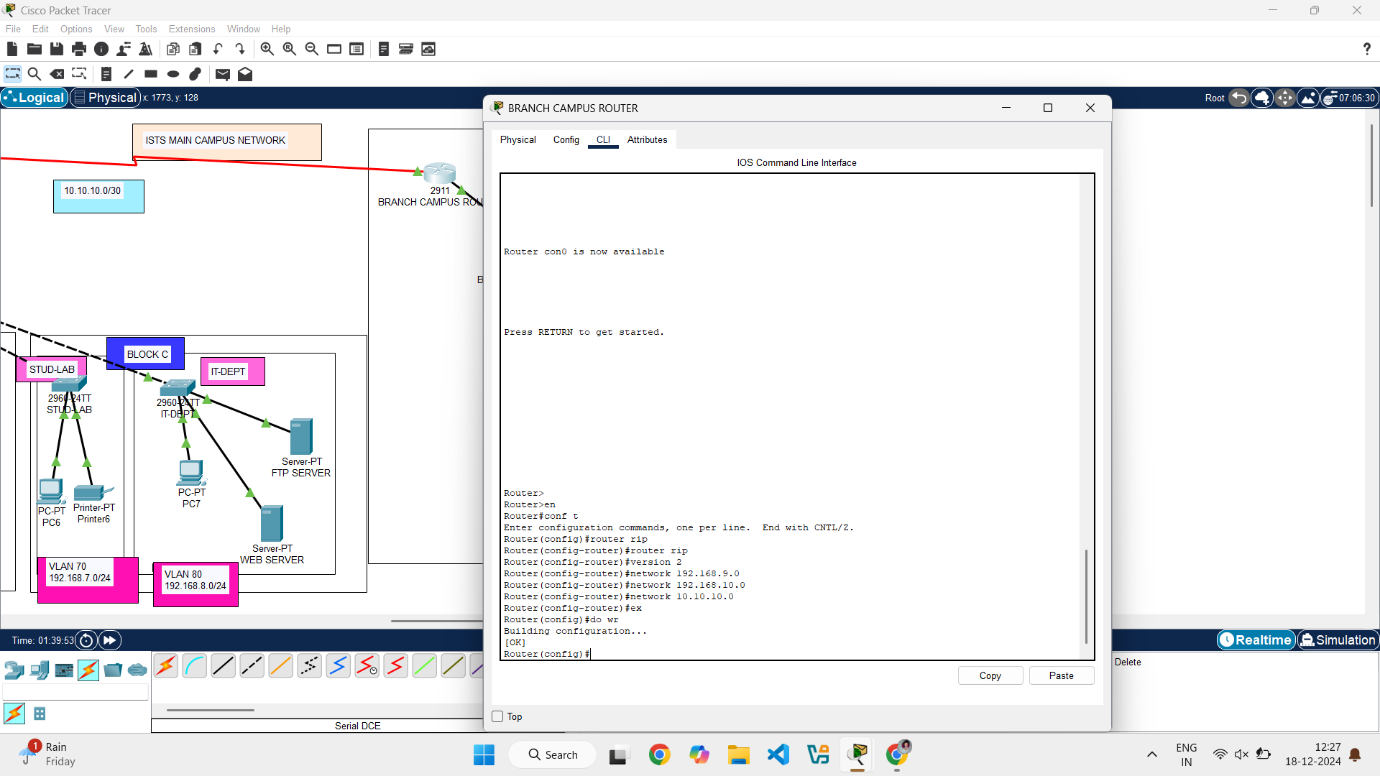
By systematically investigating these areas, you can pinpoint the cause of the "Destination host unreachable" errors and restore network connectivity.



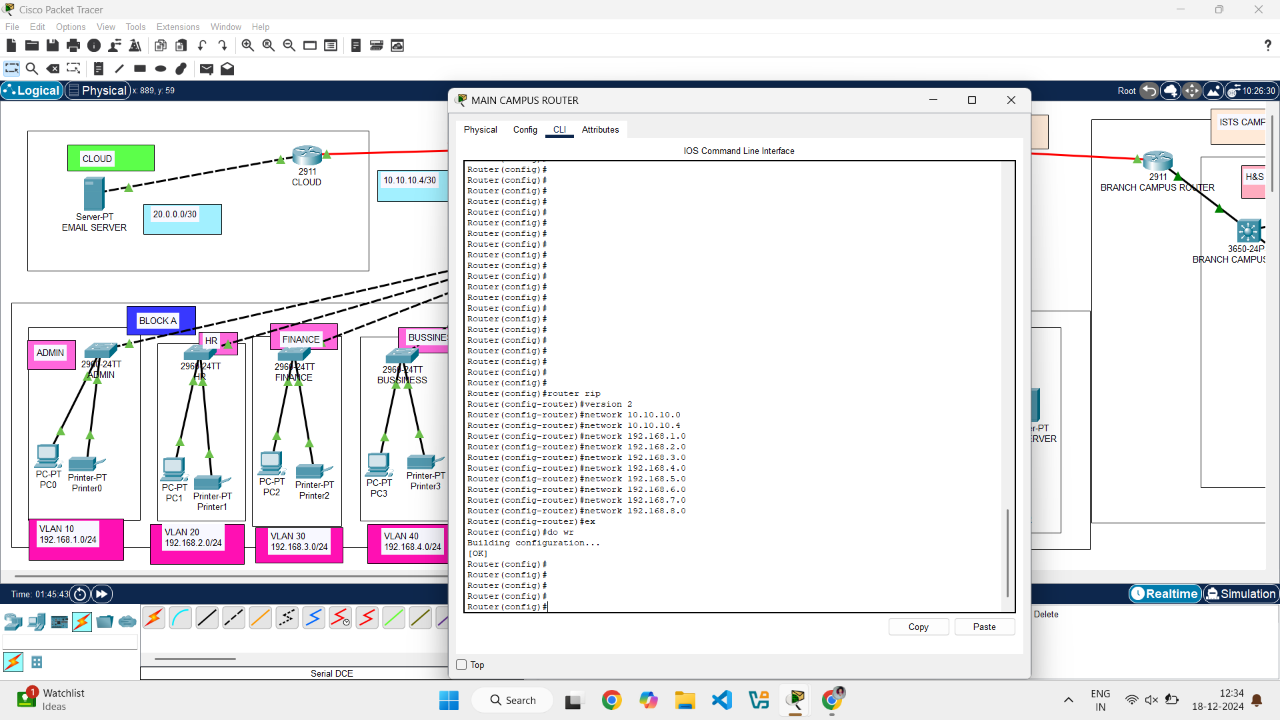
The image displays a Cisco Packet Tracer simulation with a command prompt window. It shows a series of ping commands being executed and their corresponding results.



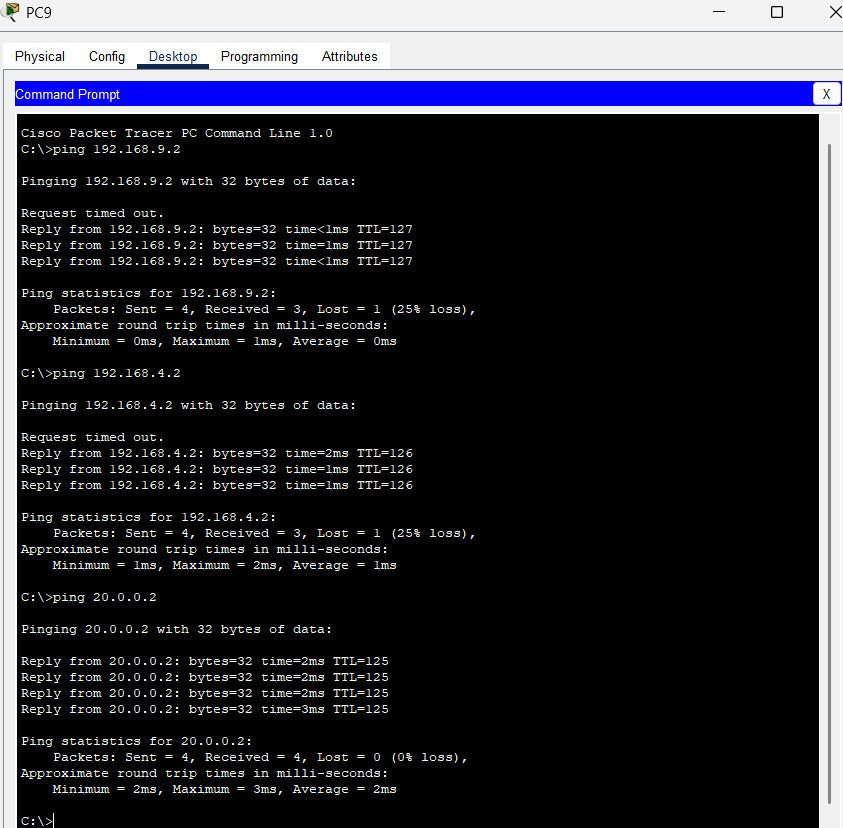
* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to run the **Routing Information Protocol (RIP)**, a distance-vector routing protocol.
* This configuration enables the router to participate in a RIP routing domain. It will advertise the reachability of networks 192.168.9.0, 192.168.10.0, and 10.10.10.0 to other RIP-enabled routers, allowing them to build routing tables and forward traffic accordingly.
* **Note:** RIP is a relatively simple routing protocol and has some limitations, such as a limited hop count (maximum of 15 hops) and potential for routing loops. In larger networks, more advanced routing protocols like OSPF or EIGRP are often preferred.

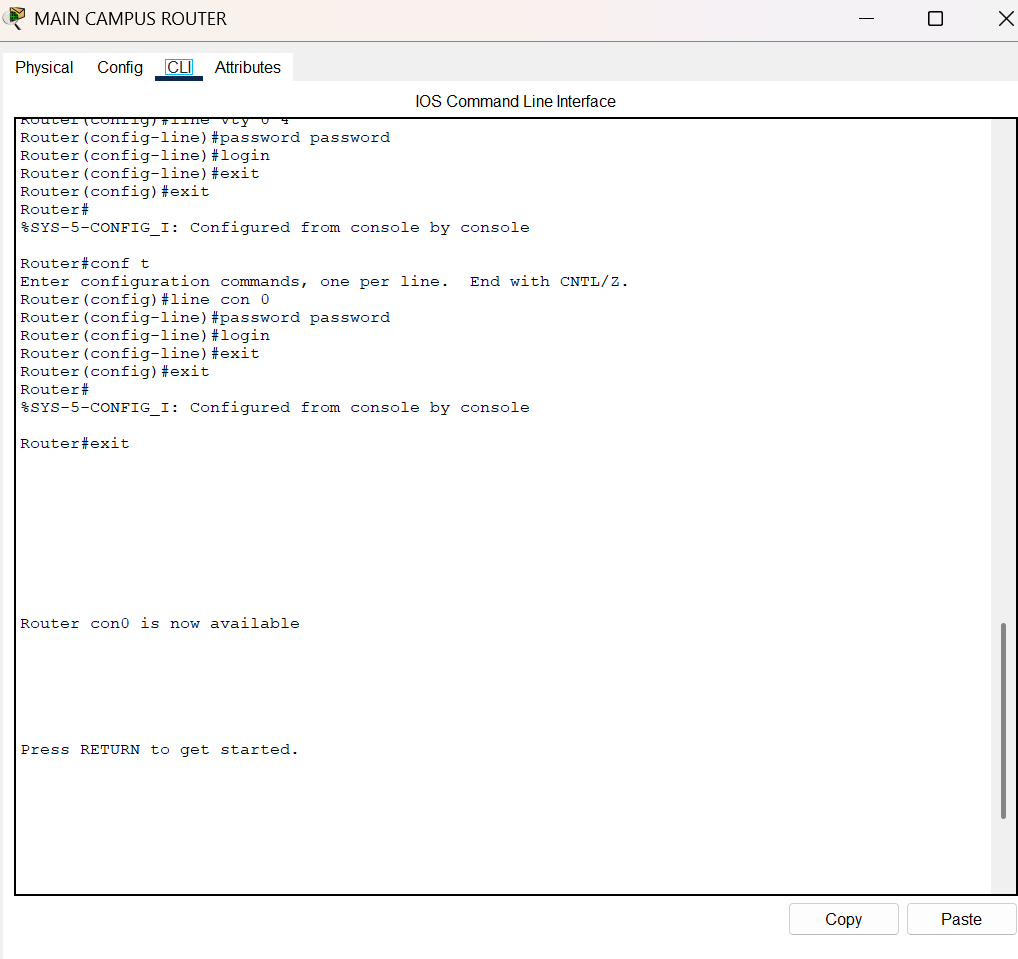


* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to run the **Routing Information Protocol (RIP)**, a distance-vector routing protocol.
* This configuration enables the router to participate in a RIP routing domain. It will advertise the reachability of multiple network segments (10.10.10.0/24, 10.10.10.4/32, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24, 192.168.6.0/24, 192.168.7.0/24, 192.168.8.0/24) to other RIP-enabled routers, allowing them to build routing tables and forward traffic accordingly.



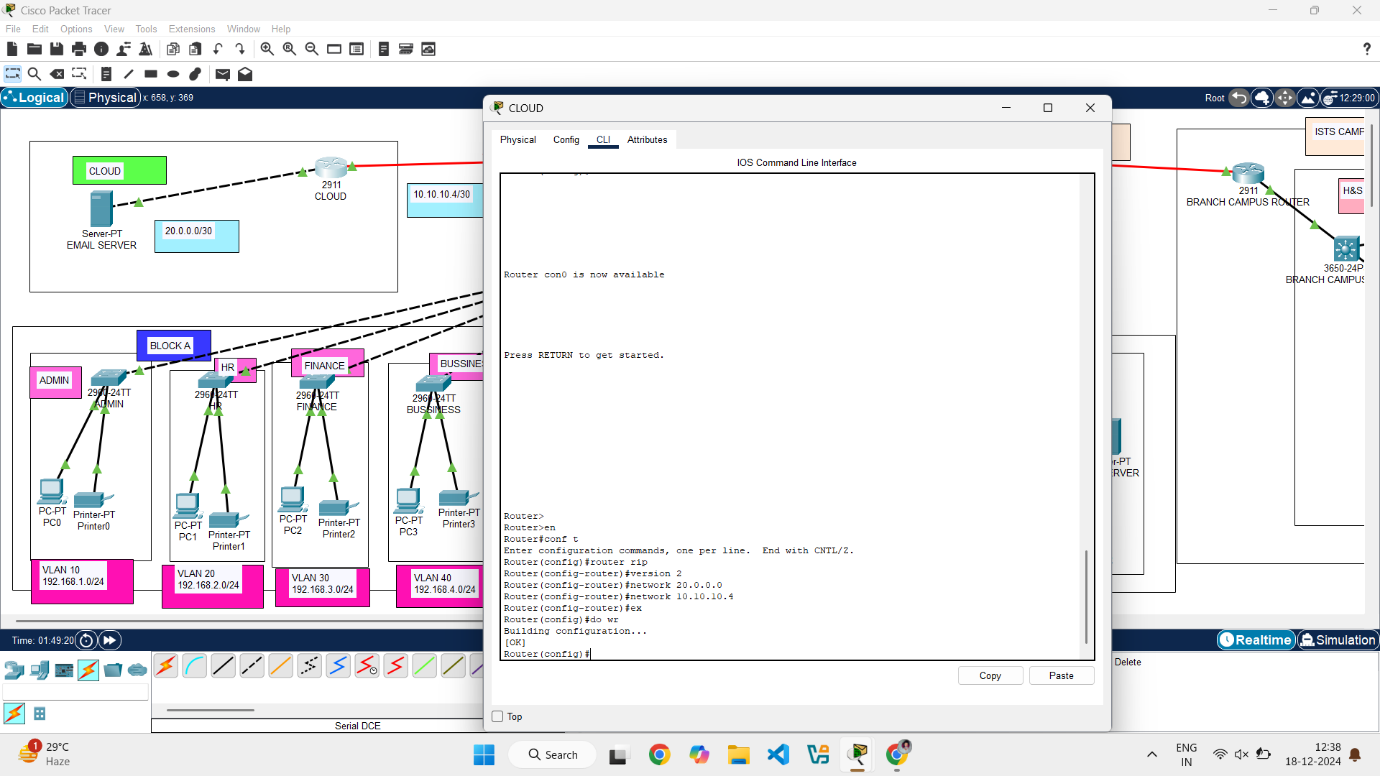
* The image displays a Cisco Packet Tracer simulation with a command prompt window. It shows a series of ping commands being executed and their corresponding results.
* The ping tests show that the device running the command prompt can successfully communicate with 20.0.0.2 and has partial connectivity to 192.168.9.2 and 192.168.4.2. The packet losses observed might be due to transient network issues or congestion.





**The above image shows the Password establishing for the router**

* The image shows a Cisco IOS Command Line Interface (CLI) session on a router. The router is being configured to run the **Routing Information Protocol (RIP)**, a distance-vector routing protocol.
* This configuration enables the router to participate in a RIP routing domain. It will advertise the reachability of two network segments (20.0.0.0 and 10.10.10.4) to other RIP-enabled routers, allowing them to build routing tables and forward traffic accordingly.



**NETWORK SEGMENTATION**

Network segmentation is like dividing your house into separate rooms with lockable doors. In a computer network, it's the practice of dividing a network into smaller, isolated sections called segments or subnetworks. Each segment acts as its own mini-network, with its own set of rules and security policies.

**How it works:**

Network segmentation is achieved using various techniques, including:

* \*\*VLANs (Virtual Local Area Networks): VLANs logically separate devices on a network, even if they are connected to the same physical switch. This allows you to group devices based on department, function, or security level.
* **Firewalls:** Firewalls act as gatekeepers between network segments, controlling traffic flow based on predefined rules. They can block unauthorized access and prevent malicious traffic from spreading.
* **Routers:** Routers connect different network segments and direct traffic between them. They can also be used to implement access control and enforce security policies.

**Benefits of Network Segmentation:**

* **Improved Security:** By isolating network segments, you limit the impact of security breaches. If one segment is compromised, the attacker's access is restricted, preventing them from easily moving to other parts of the network (lateral movement).
* **Enhanced Performance:** Segmenting the network reduces congestion and improves overall performance. This is because traffic is contained within specific segments, reducing the load on network devices.
* **Simplified Management:** Dividing the network into smaller, manageable units makes it easier to monitor, troubleshoot, and maintain.
* **Increased Compliance:** Network segmentation helps organizations meet regulatory requirements, such as PCI DSS for payment card data security and HIPAA for healthcare information.

**SUBNETTING AND IP ADDRESSING SCHEMES**

Subnetting and IP addressing schemes are fundamental concepts in network design, working together to efficiently manage and organize network traffic. Let's break them down:

**IP Addressing Scheme**

An IP address is a unique numerical identifier assigned to each device on a network. It's like a street address for your computer, allowing it to communicate with other devices. There are two main versions of IP addresses:

* **IPv4:** Uses 32-bit addresses, typically written in dotted decimal notation (e.g., 192.168.1.1).
* **IPv6:** Uses 128-bit addresses, written in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

An IP address has two parts:

* **Network ID:** Identifies the network to which the device belongs.
* **Host ID:** Identifies the specific device within that network.

**Subnetting**

Subnetting is the process of dividing a larger network into smaller subnetworks (subnets). This is done by borrowing bits from the host ID portion of the IP address and using them to create subnet IDs.

**Why Subnet?**

* **Efficient use of IP addresses:** Subnetting prevents wasting IP addresses by creating smaller networks tailored to the actual number of devices.
* **Improved network performance:** Dividing a large network into smaller subnets reduces network congestion and improves overall performance.
* **Enhanced security:** Subnets can be used to isolate different parts of a network, improving security by limiting the impact of security breaches.
* **Simplified network management:** Smaller, more manageable networks are easier to monitor, troubleshoot, and maintain.

**How Subnetting Works**

Subnetting involves using a **subnet mask**, which is a 32-bit number that separates the network ID from the host ID in an IP address. The subnet mask is also written in dotted decimal notation (e.g., 255.255.255.0).

* **1s in the subnet mask represent the network ID.**
* **0s in the subnet mask represent the host ID.**

By changing the subnet mask, you can create different numbers of subnets with different numbers of usable host addresses.

**Example**

Let's say you have a Class C network with the IP address 192.168.1.0 and a default subnet mask of 255.255.255.0. This gives you 254 usable host addresses (192.168.1.1 to 192.168.1.254).

If you want to create two subnets, you can borrow one bit from the host ID portion of the IP address. This changes the subnet mask to 255.255.255.128.

* **Subnet 1:** 192.168.1.0 - 192.168.1.127 (usable hosts: 192.168.1.1 to 192.168.1.126)
* **Subnet 2:** 192.168.1.128 - 192.168.1.255 (usable hosts: 192.168.1.129 to 192.168.1.254)

Now you have two subnets with 126 usable host addresses each.

**Key Considerations**

* **Number of subnets needed:** Determine how many subnets you need based on your network design.
* **Number of hosts per subnet:** Determine how many hosts will be in each subnet.
* **Subnet mask:** Choose an appropriate subnet mask that provides the required number of subnets and hosts per subnet.

Subnetting and IP addressing schemes are essential for efficient network management and security.

**ROUTERS**

Routers are essential networking devices that act as traffic directors for your network. They connect multiple networks together, forwarding data packets between them based on their destination IP addresses. Think of them as the postal service of the internet, ensuring that your data reaches the correct destination.

Key Functions of Routers

* Connecting Networks: Routers connect different networks, such as your home network to the internet, or different departments within a large organization.
* Packet Forwarding: Routers examine the destination IP address of each data packet and determine the best path to send it along.
* Routing Tables: Routers maintain routing tables, which are lists of network destinations and the best paths to reach them. These tables are used to make forwarding decisions.
* Network Address Translation (NAT): Routers often perform NAT, which allows multiple devices on a private network to share a single public IP address when accessing the internet.
* Firewall Functionality: Many routers include basic firewall functionality to protect the network from unauthorized access.

Types of Routers

* Home Routers: These are typically small, all-in-one devices that provide Wi-Fi, wired Ethernet connections, and basic routing functionality for home networks.
* Small Office/Home Office (SOHO) Routers: These offer more advanced features than home routers, such as VPN support, Quality of Service (QoS), and more robust firewall capabilities.
* Enterprise Routers: These are high-performance routers designed for large organizations with complex network requirements. They offer advanced features like advanced routing protocols, high availability, and extensive security features.
* Core Routers: These are high-capacity routers that form the backbone of large networks, such as internet service provider (ISP) networks.

How Routers Make Forwarding Decisions

1. Packet Arrival: A data packet arrives at the router's interface.
2. Destination IP Address Lookup: The router examines the destination IP address in the packet header.
3. Routing Table Lookup: The router consults its routing table to find the best path to reach the destination network.
4. Packet Forwarding: The router forwards the packet to the next hop along the chosen path. This process is repeated by other routers along the way until the packet reaches its final destination.

Routing Protocols

Routers use routing protocols to dynamically learn about network topology and update their routing tables. Some common routing protocols include:

* RIP (Routing Information Protocol): A simple routing protocol that uses hop count as a metric.
* OSPF (Open Shortest Path First): A more advanced routing protocol that uses link state information to determine the best paths.
* BGP (Border Gateway Protocol): A routing protocol used between different autonomous systems (AS), such as different ISPs.

**In this project we used 2911 router:**

The Cisco 2911 is a popular Integrated Services Router (ISR) from Cisco Systems. It's designed to provide a wide range of services for branch offices and small to medium-sized businesses. Here's a breakdown of its key features and capabilities:

**Key Features and Capabilities**

* **Integrated Services:** The "Integrated Services" in its name means it's more than just a router. It combines routing, switching, security, and voice services into a single platform.
* **Performance:** It offers good performance for its class, suitable for handling the demands of modern business applications and network traffic.
* **Modular Design:** The 2911 has a modular design with various slots for interface cards, allowing you to customize it to meet specific needs. This includes:
  + **Enhanced High-Speed WAN Interface Card (EHWIC) slots:** For connecting to different WAN technologies like T1/E1, DSL, and cable.
  + **Service Module slots:** For adding advanced services like firewall, intrusion prevention, and VPN.
  + **Internal Service Module slot:** For specialized modules.
  + **Onboard digital signal processor (DSP) slots:** For voice applications.
* **Security:** It offers a comprehensive suite of security features, including:
  + **Firewall:** To protect the network from unauthorized access.
  + **Intrusion Prevention System (IPS):** To detect and block malicious traffic.
  + **VPN:** To create secure connections over the internet.
* **Voice Support:** With the appropriate modules and licensing, the 2911 can function as a voice gateway, supporting IP telephony and unified communications.
* **Energy Efficiency:** It's designed with energy efficiency in mind, helping to reduce power consumption and operating costs.

**Important Notes**

* The Cisco 2911 is an older model, part of the Cisco ISR G2 (Integrated Services Routers Generation 2) series. While still functional, it might not offer the latest features and performance of newer Cisco routers.
* Licensing plays a crucial role in determining the features available on the 2911. Different licenses unlock different functionalities, such as advanced security features or voice support.

**SWITCHES**

Switches are fundamental components of computer networks, especially in Local Area Networks (LANs). They connect multiple devices, such as computers, printers, and servers, within the same network, enabling them to communicate with each other efficiently.

Here's a breakdown of what switches are and how they work:

**Key Functions of Switches**

* **Connecting Devices:** Switches provide multiple Ethernet ports to which devices can be connected via cables. This creates a network where devices can share resources and communicate.
* **Data Forwarding:** Unlike hubs that broadcast data to all connected devices, switches learn the MAC addresses (unique hardware identifiers) of connected devices and forward data only to the intended recipient. This significantly improves network efficiency and reduces collisions.
* **MAC Address Table:** Switches maintain a MAC address table that maps MAC addresses to specific ports. When a data packet arrives, the switch checks the destination MAC address in the table and forwards the packet only to the corresponding port.
* **VLANs (Virtual LANs):** Many switches support VLANs, which allow you to logically segment a physical network into multiple virtual networks. This enhances security, improves performance, and simplifies network management.

**Types of Switches**

* **Unmanaged Switches:** These are simple plug-and-play devices with no configuration options. They are suitable for small home or office networks.
* **Managed Switches:** These offer advanced features like VLANs, QoS (Quality of Service), port mirroring, and network monitoring. They are used in larger networks where more control and management are required.
* **PoE Switches:** These provide Power over Ethernet (PoE), which allows devices like IP phones and wireless access points to receive power through the Ethernet cable.

**How Switches Work**

1. **Device Connection:** Devices are connected to the switch's ports using Ethernet cables.
2. **MAC Address Learning:** When a device sends data, the switch learns its MAC address and associates it with the port it's connected to. This information is stored in the MAC address table.
3. **Data Forwarding:** When the switch receives a data packet, it examines the destination MAC address.
   * If the destination MAC address is in the MAC address table, the switch forwards the packet only to the corresponding port.
   * If the destination MAC address is not in the table, the switch floods the packet to all ports (except the one it received the packet on) in a process called "unknown unicast flooding." Once the destination device responds, the switch learns its MAC address and adds it to the table.

**Key Benefits of Using Switches**

* **Improved Performance:** Switches significantly improve network performance compared to hubs by reducing collisions and forwarding data only to the intended recipient.
* **Enhanced Security:** VLANs and other features in managed switches enhance network security by isolating traffic and controlling access.
* **Increased Bandwidth:** Switches provide dedicated bandwidth to each connected device, improving overall network capacity.

**We used 3650 and 2960 switches:**

**2960 switch:**

* **Focus:** Primarily Layer 2 access switches, designed for basic connectivity at the network edge (connecting end-user devices like computers and printers).
* **Key Features:**
  + Basic Layer 2 switching (VLANs, Spanning Tree Protocol).
  + Fixed configuration (no modularity for adding features).
  + PoE (Power over Ethernet) options available.
  + Relatively lower cost.

**3650 Switch:**

* **Focus:** Layer 2 and Layer 3 capable switches, designed for more demanding access and distribution layer deployments.
* **Key Features:**
  + Advanced Layer 2 switching features.
  + Layer 3 routing capabilities (static and dynamic routing protocols).
  + Higher performance and port density.
  + Stacking capabilities (allows multiple switches to operate as a single unit).
  + More advanced security features.
  + QoS (Quality of Service) for prioritizing network traffic.
  + Support for advanced features like NetFlow and Flexible NetFlow for network monitoring and analysis.

**SUMMARY OF DESIGN AND FUTURE CONSIDERATION**

A campus network design aims to provide robust, scalable, and secure network connectivity for a large, geographically localized area, such as a university campus, corporate headquarters, or large industrial complex. Here's a summary of key aspects and future considerations:

**Key Components of a Campus Network Design:**

* **Hierarchical Structure:** Typically follows a three-tier model:
  + **Core Layer:** High-speed backbone connecting different parts of the campus. Focuses on fast switching and redundancy.
  + **Distribution Layer:** Connects the core layer to the access layer. Handles routing, access control, and policy enforcement.
  + **Access Layer:** Connects end-user devices (computers, printers, phones) to the network. Focuses on port density and connectivity options (Ethernet, Wi-Fi).
* **Redundancy and High Availability:** Implemented at all layers to prevent single points of failure. Techniques include redundant links, redundant devices, and failover mechanisms.
* **Security:** Multi-layered approach using firewalls, intrusion detection/prevention systems (IDS/IPS), access control lists (ACLs), and network segmentation.
* **Wireless Network:** Integrated Wi-Fi coverage across the campus, supporting various standards (e.g., Wi-Fi 6/6E) and security protocols (e.g., WPA3).
* **Network Management:** Centralized management system for monitoring, configuring, and troubleshooting network devices.
* **IP Addressing and Subnetting:** Efficient IP addressing scheme and subnetting strategy to manage network traffic and allocate IP addresses.
* **Quality of Service (QoS):** Prioritizing critical network traffic, such as voice and video, to ensure optimal performance.

**Future Considerations for Campus Network Design:**

* **Increased Bandwidth Demand:** Growing use of bandwidth-intensive applications (e.g., video conferencing, streaming, cloud services) requires higher bandwidth capacity and faster network technologies (e.g., 10GbE, 40GbE, 100GbE).
* **Internet of Things (IoT):** The proliferation of IoT devices on campus networks presents new challenges for security, scalability, and management. Network designs need to accommodate the diverse requirements of these devices.
* **Software-Defined Networking (SDN):** SDN offers greater flexibility and control over network infrastructure by separating the control plane from the data plane. It can simplify network management, automate tasks, and improve network agility.
* **Network Automation:** Automating network tasks, such as configuration, provisioning, and troubleshooting, can improve efficiency and reduce operational costs. Tools like Ansible, Python scripting, and network automation platforms are becoming increasingly important.
* **Cloud Integration:** Integrating campus networks with cloud services (e.g., cloud storage, cloud applications) requires careful planning and secure connectivity.
* **Zero Trust Security:** Shifting towards a Zero Trust security model, where no user or device is trusted by default, requires strong authentication, micro-segmentation, and continuous monitoring.
* **Edge Computing:** Processing data closer to the source (at the network edge) can reduce latency and improve performance for certain applications. Campus networks need to be designed to support edge computing deployments.
* **IPv6 Adoption:** Transitioning to IPv6 is essential to address the limitations of IPv4 and accommodate the growing number of network devices.
* **Sustainability:** Designing energy-efficient networks by using power-efficient devices and optimizing network traffic flow is becoming increasingly important.

***APPENDICES***

**DEVICE SPECIFICATIONS:**

**1. 2911 ROUTER SPECIFICATIONS: (TYPICAL)**

* **General**: Integrated Services Router (ISR), 2U Rack-mountable
* **Interfaces**: 3x 10/100/1000 Ethernet
* **Expansion**: 4x EHWIC, 1x SM, 1x ISM, 2x DSP
* **Memory**: 512MB RAM (exp. to 2GB), 256MB Flash (exp. to 8GB)
* **Other:** USB 2.0, Compact Flash slots
* **Features:** Firewall, IPS, VPN, NAT, QoS, NetFlow, Voice (with licensing)

**2. 2960 SWITCH:(TYPICAL)**

* **Layer**: Layer 2
* **Ports**: 8-48 Fast Ethernet or Gigabit Ethernet
* **PoE**: Available on some models
* **Uplinks**: Typically, Gigabit Ethernet
* **Management**: Unmanaged or Managed (Web UI, CLI)
* **Stacking:** Limited or None
* **Use Case**: Basic access layer connectivity

**3. 3650 SWITCH:(TYPICAL)**

* **Layer:** Layer 2 and Layer 3
* **Ports:**24-48 Gigabit Ethernet, 10 Gigabit Ethernet uplinks available
* **PoE**: Available
* **Stacking**: StackWise-160 (up to 9 switches)
* **Management**: Managed (Web UI, CLI, Cisco DNA Centre)
* **Features:** Advanced Layer 2/3, QoS, NetFlow, advanced security
* **Use Case**: Access and distribution layer, converged networks

**4. SERVER PT (TYPICAL):**

* **Interface:** PCI Express (PCIe) x4
* **Ports:** Dual-port (2 x RJ-45) or Quad-port (4 x RJ-45) options available
* **Speed:** 10/100/1000 Mbps Gigabit Ethernet
* **Controller:** Intel 82571EB or 82571GB Gigabit Ethernet Controller
* **Cabling:** Copper (Category-5 or better)

**CABLE OR CONNECTION SPECIFICATIONS:**

1. STRAIGHT CABLE:

* **Type:** Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP)
* **Connectors:** RJ-45 (8P8C) on both ends
* **Wiring Standard**: T568A or T568B (both ends use the same standard)
* **Use Case:** Connecting dissimilar devices (e.g., PC to switch, router to switch)

2. SERIAL DCE CABLE:

* **Purpose:** Connects a Data Communication Equipment (DCE) device (typically a modem or CSU/DSU) to a Data Terminal Equipment (DTE) device (typically a router or computer).
* **Connectors**: Usually DB-25 or DB-9 on the DCE end and DB-25 or DB-9 on the DTE end. May also use other connectors like V.35 or Smart Serial.
* **Signals:** Transmits serial data using various standards like RS-232, V.35, RS-449, etc.
* **Clocking:** Provides clocking signals to the DTE device.
* **Pinout:** Specific pinouts vary depending on the standard used (e.g., RS-232, V.35). Requires correct pin configuration for proper communication.

**REAL TIME APPLICATIONS:**