**Corporate Servers**

Students Name

Institution of Affiliation

Proffessor Name

Course code

Date

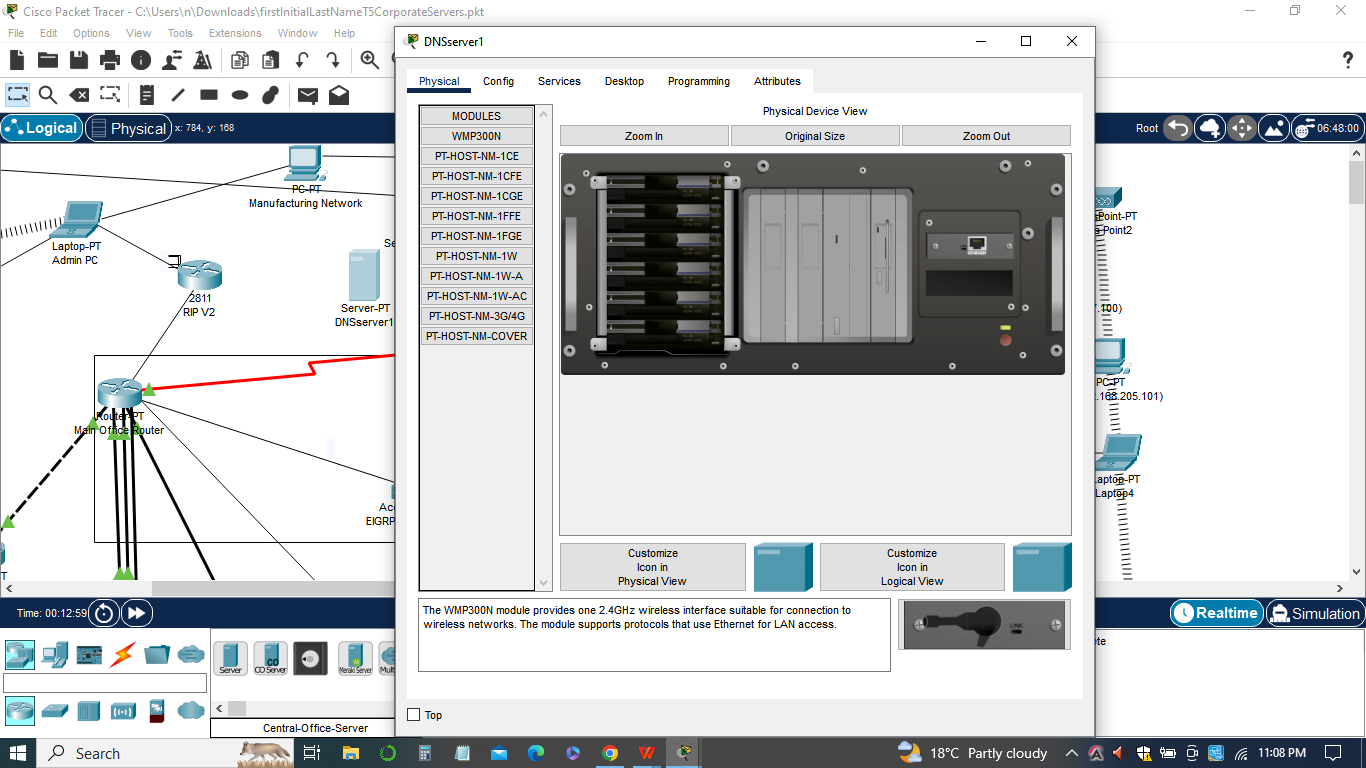
**Corporate Servers**

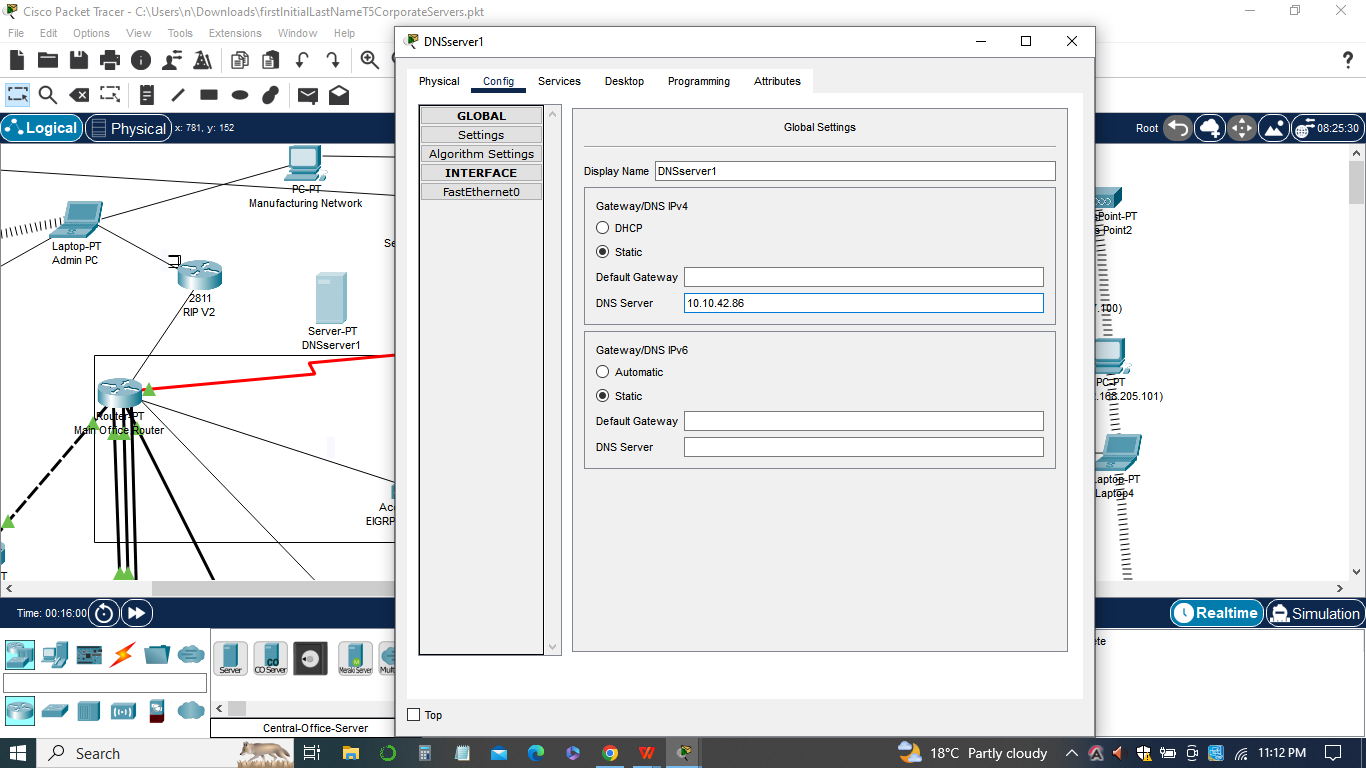
**Introduction**

In this assessment, we will focus on enhancing the network infrastructure by adding DNS (Domain Name System) and WWW (World Wide Web) services. These services will improve network functionality, facilitate name resolution, and enable access to internet resources. The steps involved include setting up a DNS server, configuring A records for servers, updating DHCP settings, setting up an internet WWW server, updating ACLs if necessary, and performing pings to verify connectivity. The rationale behind these changes is to enhance network efficiency, security, and ease of use.

**Summary of Network Changes for Management:**

1. ***Setting up DNS Server***

******

******

We will configure a DNS server named "DNSserverl" with the IP address 10.10.42.86. This server will be responsible for resolving domain names to IP addresses within the network. The DNS server will be configured to point to a public DNS resolver, such as 8.8.8.8, to provide external name resolution capabilities. This change will improve the network's ability to translate domain names into IP addresses, enabling seamless communication and access to internal and external resources.

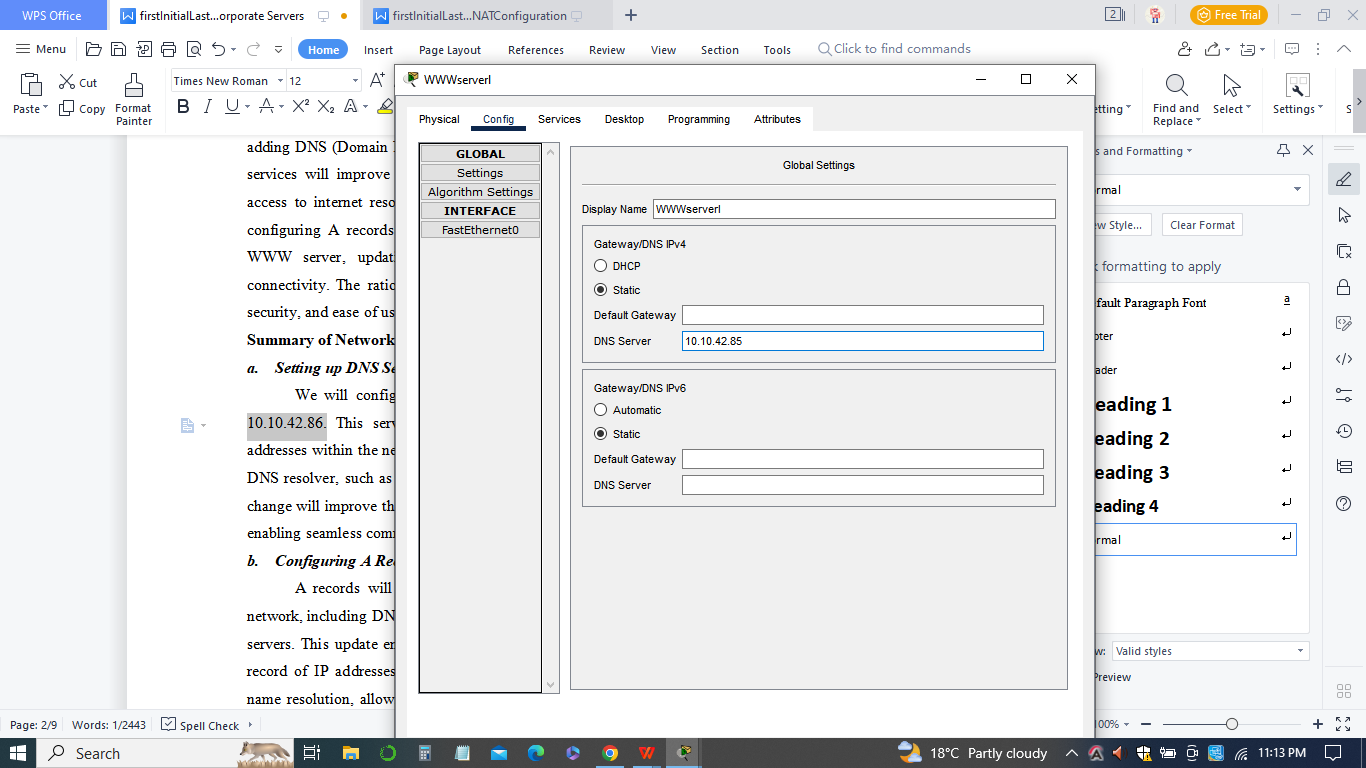
1. ***Configuring A Records for Servers***

A records will be added to the DNS server for all existing servers in the network, including DNSserver1, 2, DHCPserver1, 2, WWWserver1, 2, and any future servers. This update ensures that the DNS server maintains an updated and accurate record of IP addresses associated with server names. It improves the reliability of name resolution, allowing users to access servers by their domain names rather than IP addresses.

1. ***Updating DHCP Settings***

The DHCP (Dynamic Host Configuration Protocol) settings in the network will be updated to include the newly configured DNS server. DHCP zones and scopes will be modified to assign the IP address of the DNS server to clients dynamically. This change ensures that all clients in the network receive the IP address of the internal DNS server during the lease acquisition process. It simplifies network management and improves DNS availability and reliability for all connected devices.

1. ***Setting up Internet WWW Server***

******

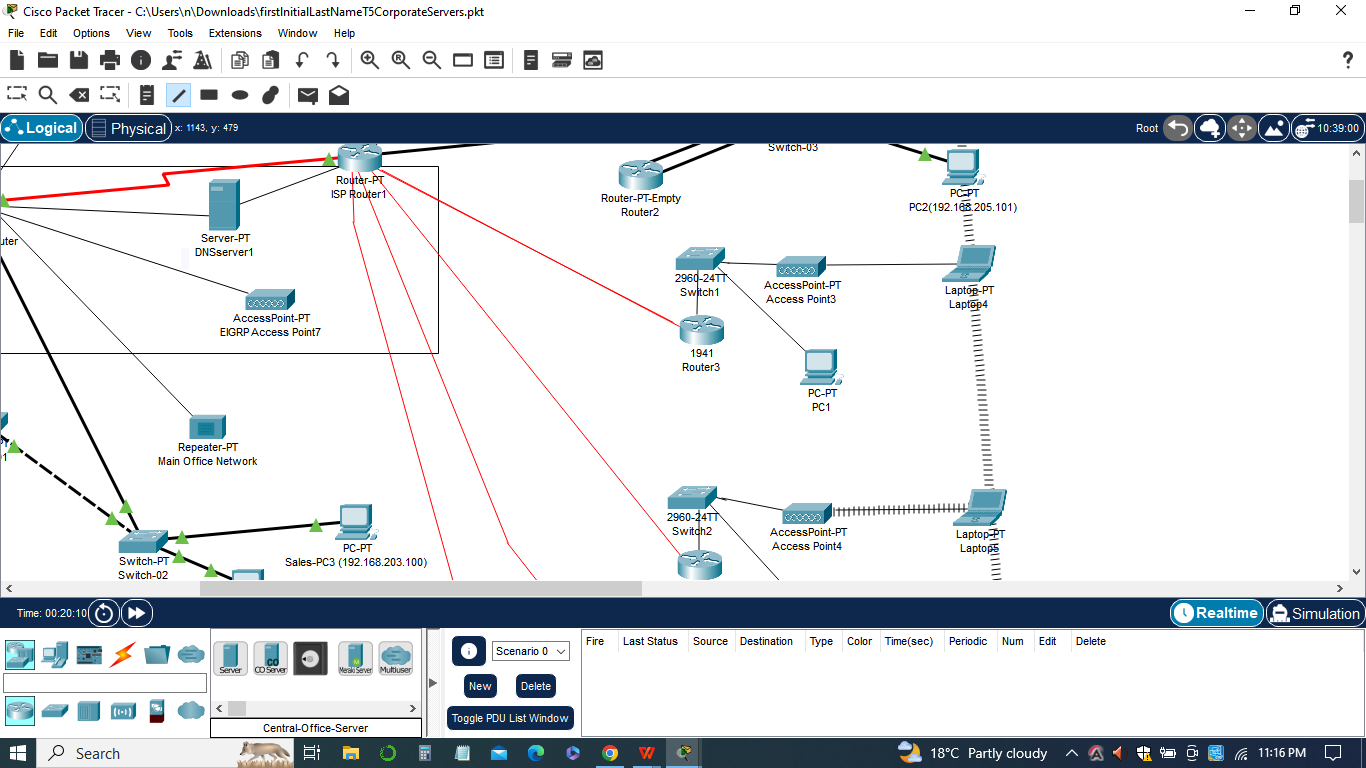
We will establish an internet WWW server named "WWWserverl" with the IP address 10.10.42.85. This server will host web resources that can be accessed by anyone on the network. To enable access to the WWW server, appropriate changes will be made to the network's ACLs. These changes will allow incoming HTTP (port 80) and HTTPS (port 443) traffic to reach the WWW server while maintaining the necessary security measures.

**Rationale for Changes**

1. The addition of a DNS server improves network efficiency by providing name resolution services, eliminating the need for users to remember and manually input IP addresses.
2. Configuring A records for servers ensures accurate and up-to-date name resolution, enabling seamless communication with servers using domain names.
3. Updating DHCP settings with the DNS server IP address simplifies network management and ensures consistent and reliable name resolution for all connected devices.
4. The setup of an internet WWW server allows users to access web resources hosted within the network, promoting collaboration and information sharing.
5. Modifying ACLs to accommodate the new servers ensures proper traffic routing and access control, balancing security and accessibility.

**Switch configurations**

The switch configurations used in this network infrastructure implementation play a crucial role in ensuring efficient and secure communication between devices. The following are the key aspects of the switch configurations for adding DNS and WWW services to the network used:

******

1. ***VLAN Configuration***

VLANs (Virtual Local Area Networks) was used to logically segregate network traffic and enhance network security. The switch configurations included the creation and assignment of appropriate VLANs for different network segments, such as the Admin network, Manufacturing network, Shipping network, and NewLocation1 network. Each VLAN should be associated with the respective switch ports where devices are connected. This segregation helped in isolating network traffic and improves network performance and security.

1. ***Trunk Port Configuration:***

Trunk ports was used to carry traffic from multiple VLANs across a single link. In the switch configurations, trunk ports should be properly configured to allow the passage of VLAN-tagged frames between switches and routers. Trunk ports was configured with the appropriate VLAN encapsulation method, such as IEEE 802.1Q, and the allowed VLANs should be specified. This ensured that VLAN traffic is correctly transmitted between switches and enables communication between different network segments.

1. ***Port Security:***

Port security is an important feature that prevents unauthorized devices from connecting to switch ports. In the switch configurations, port security measures was be implemented, such as limiting the number of MAC addresses allowed on a port or binding specific MAC addresses to switch ports. This helps in preventing unauthorized access and enhancing network security.

1. ***Access Control Lists (ACLs):***

ACLs are used on switches to control traffic flow based on specific criteria. In the context of adding DNS and WWW services, ACLs needs to be updated to allow or restrict traffic to the DNS server and WWW server. ACLs can be configured to permit or deny traffic based on source IP addresses, destination IP addresses, and port numbers. Care is taken to ensure that the ACLs are properly configured to allow necessary traffic while maintaining network security.

1. ***Quality of Service (QoS):***

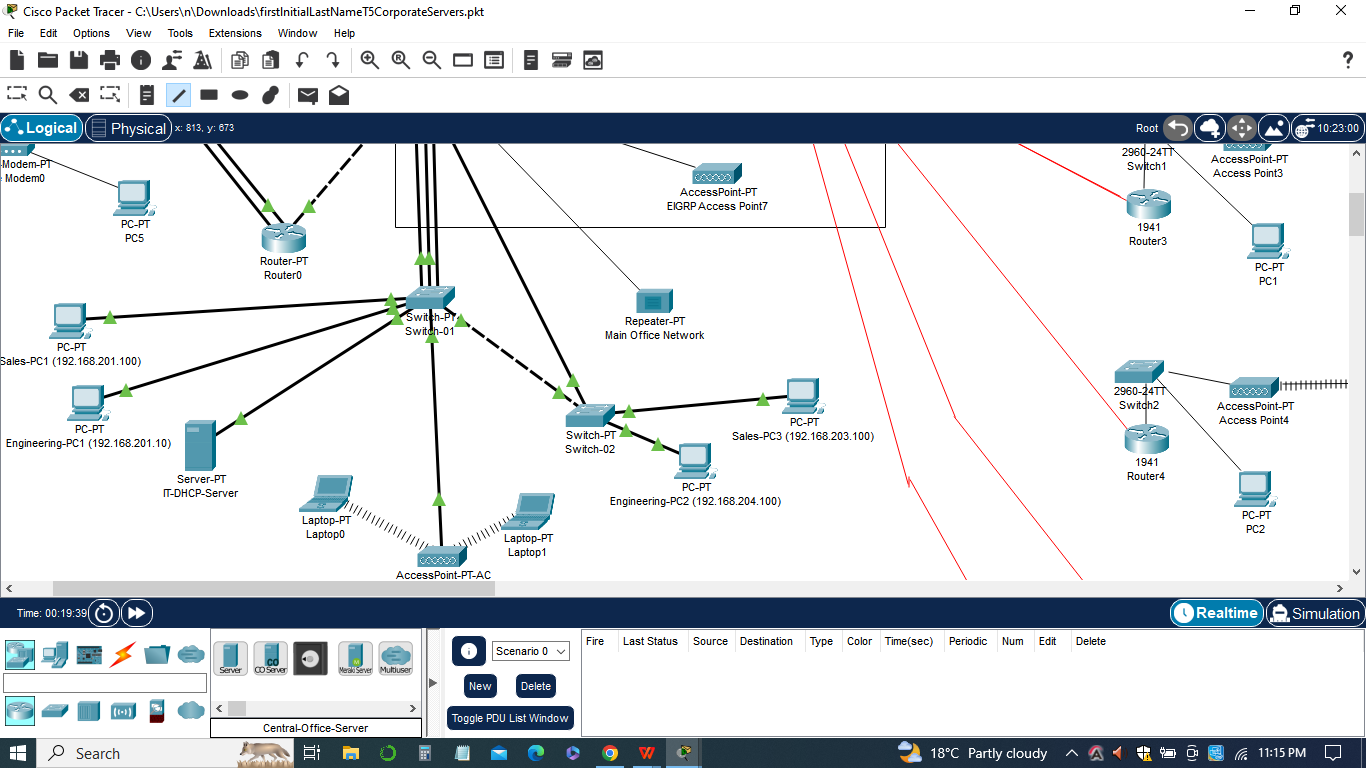
QoS settings was configured on switches to prioritize specific types of traffic, such as DNS and WWW traffic, over other types of traffic. This ensures that critical services receive sufficient bandwidth and are not impacted by other less important traffic. QoS settings can be configured based on traffic classification, such as by assigning specific CoS (Class of Service) values to different types of traffic.

In sum, the switch configurations for adding DNS and WWW services focused on VLAN setup, trunk port configuration, port security, ACL management, and QoS settings. These configurations helped create a secure and efficient network infrastructure that supports the seamless integration of DNS and WWW services while maintaining optimal performance and security.

**List of pings**

In this assignment, a list of pings was used to test the connectivity and accessibility of the servers in the network. The pings are performed from a workstation on Switch-01 in the main location to each of the servers by name. Let's discuss the significance of this list of pings:

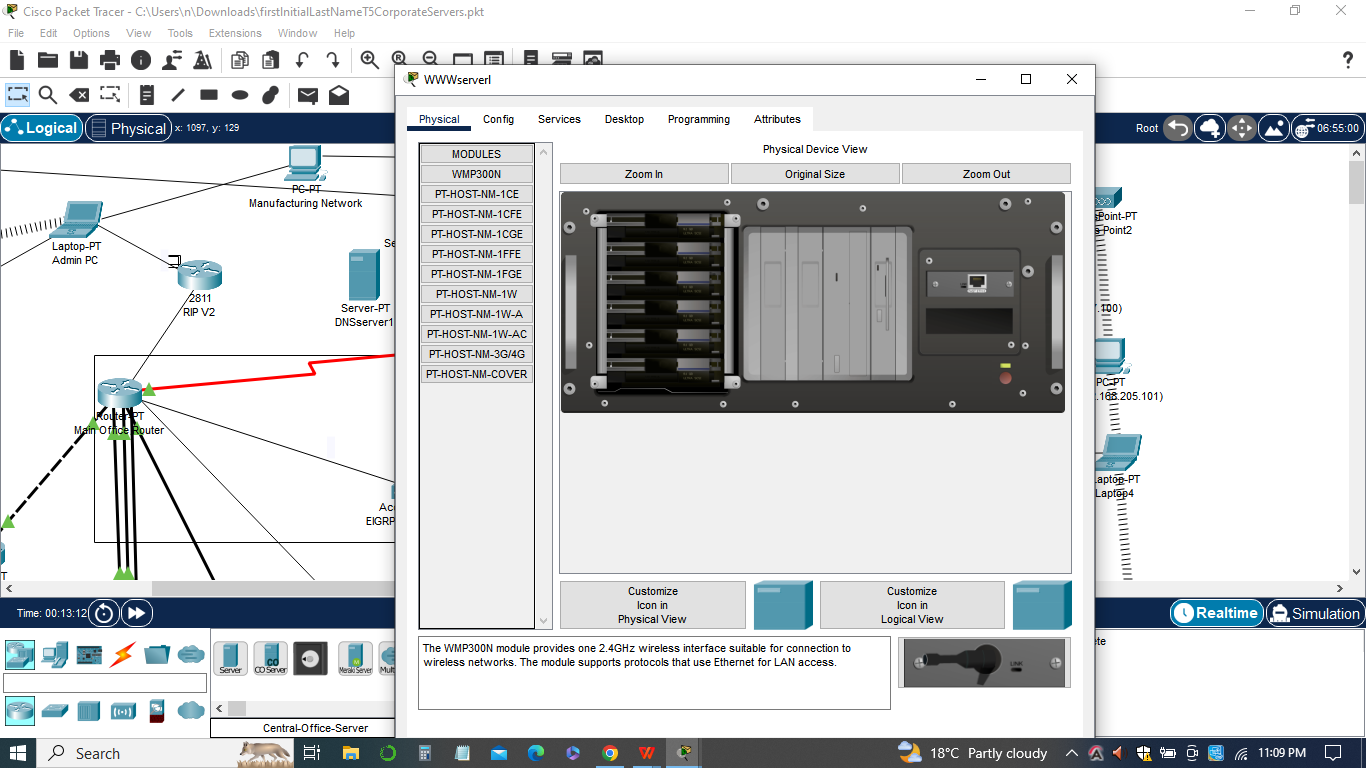
1. *Testing Server Accessibility:* By pinging each server by name, the aim is to verify whether the servers are reachable and responding to ICMP (Internet Control Message Protocol) echo requests. Pinging the servers helps to ensure that the network configuration, including VLANs, trunk ports, and ACLs, allows for proper communication between the workstation and the servers.
2. *Verification of DNS Configuration:* Pinging the servers by name also helps in validating the DNS configuration. The DNS server, which has been set up with A records for all the servers in the network, translates the server names into their respective IP addresses. If the pings are successful, it confirms that the DNS server is functioning correctly, and the workstation can resolve the server names to their IP addresses.

******

1. *Network Connectivity Analysis:* The list of pings provides a comprehensive analysis of network connectivity within the network infrastructure. By successfully pinging each server, it indicates that the VLANs, trunk ports, and ACLs have been configured properly to allow traffic flow between the workstation and the servers. Any failed pings may indicate issues with the network configuration or connectivity problems that need to be addressed.
2. *Troubleshooting and Documentation:* The list of pings serves as a troubleshooting tool and documentation for network administrators. If any pings fail, it helps identify specific servers or network segments that require further investigation. Additionally, including the pings' results in the report provides a clear demonstration of the network's functionality and can be used as evidence of successful server integration.

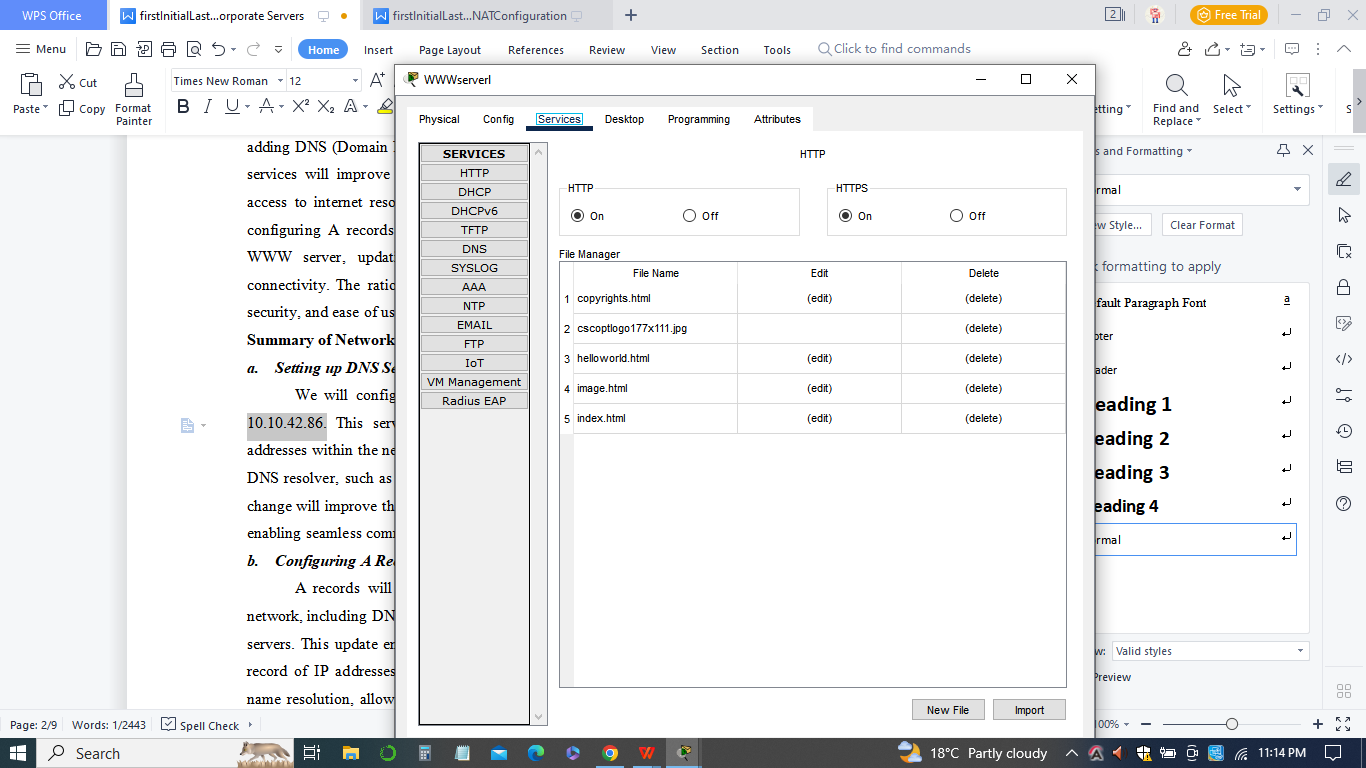
**List of Pings Configurations**

In this assignment, we outline the specific configurations for the list of pings to be performed from a workstation on Switch-01 to each of the servers in the network.

******

The pings was conducted using the server names to test the accessibility and proper functioning of the DNS and WWW services as outlined below.

1. ***Ping DNS Server (DNSserver1):***
2. Command: ping DNSserver1
3. Purpose: Verify if the DNS server (DNSserver1) is reachable and responding to ICMP echo requests. This will also test the DNS resolution by ensuring that the workstation can resolve the server name to its IP address.
4. ***Ping DHCP Server 1 (DHCPserver1):***
5. Command: ping DHCPserver1
6. Purpose: Test the accessibility of DHCP Server 1 (DHCPserver1) and ensure it responds to ICMP echo requests. This confirms that the DHCP server is operational and reachable from the workstation.
7. ***Ping WWW Server 1 (WWWserver1)***

******

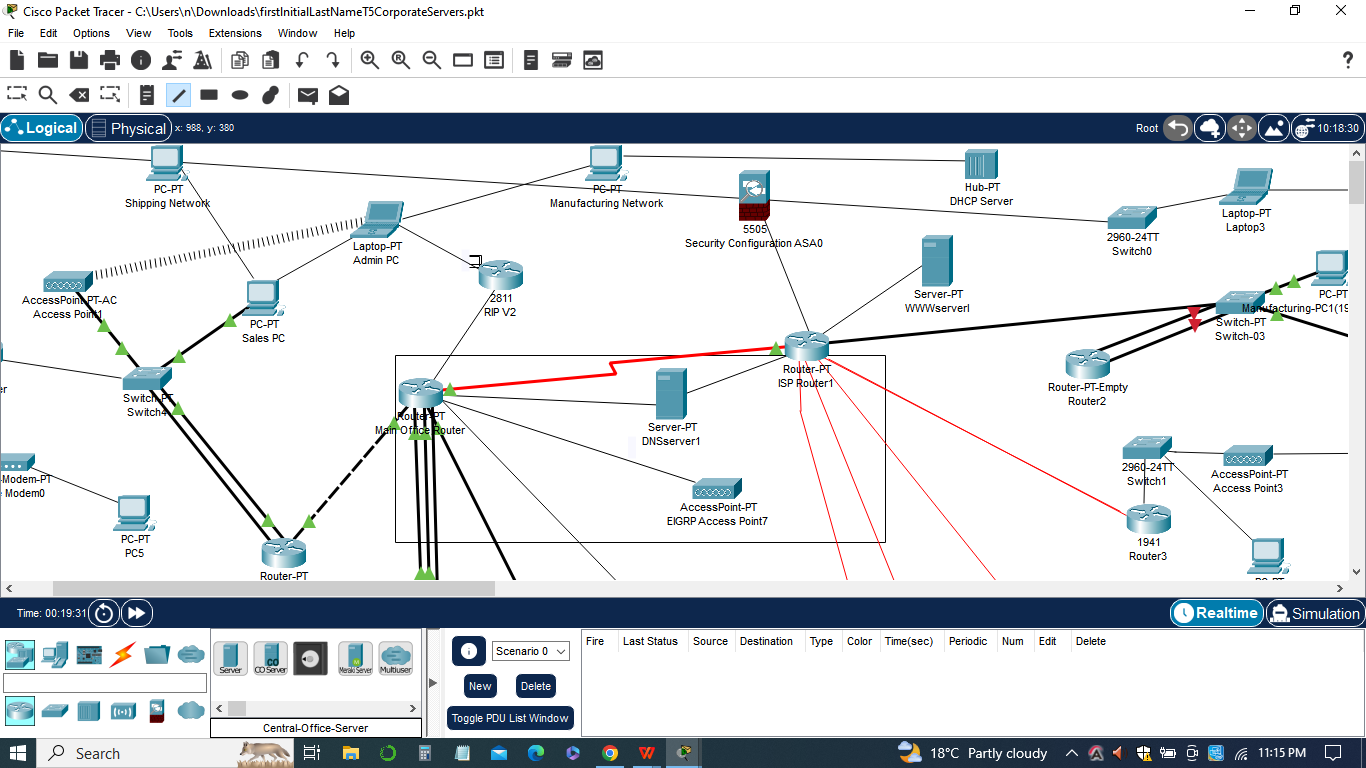
1. Command: ping WWWserver1
2. Purpose: Verify if the WWW Server 1 (WWWserver1) is accessible and responding to ICMP echo requests. This ensures the proper functioning of the internet WWW server and its connectivity to the main location.
3. ***Ping DNS Server 2 (DNSserver2):***
4. Command: ping DNSserver2
5. Purpose: Test the accessibility of DNS Server 2 (DNSserver2) and ensure it responds to ICMP echo requests. This will also check the redundancy and failover capability of the DNS servers.
6. ***Ping DHCP Server 2 (DHCPserver2):***
7. Command: ping DHCPserver2
8. Purpose: Verify if DHCP Server 2 (DHCPserver2) is reachable and responding to ICMP echo requests. This confirms the operational status of the second DHCP server.
9. ***Ping WWW Server 2 (WWWserver2):***
10. Command: ping WWWserver2
11. Purpose: Test the accessibility of WWW Server 2 (WWWserver2) to ensure the proper functioning of the second internet WWW server and its connectivity to the main location.
12. ***(Optional) Ping Additional Servers (if applicable):***
13. Command: ping ServerName
14. Purpose: If any new servers are added to the network in the future, they should also be pinged by name to verify their accessibility and proper integration into the network.

By executing the above list of pings, we can ensure the successful implementation of DNS and WWW services in the network. It will help validate the DNS configuration, test server accessibility, and provide a comprehensive analysis of network connectivity for each server.

In addition, by conducting the list of pings, network administrators can ensure the successful implementation of DNS and WWW services in the network. It helps verify the accessibility of servers, validate the DNS configuration, analyze network connectivity, and provide documentation for management and future troubleshooting purposes.

**Workstation Window**

The workstation window is the command prompt or terminal window of a workstation within the network. It is where the administrator or user interacts with the workstation by executing various commands, including pinging servers, configuring network settings, and troubleshooting network connectivity.

******

In the assignment, the workstation window is used to perform pings to test the accessibility of different servers within the network. By pinging the servers by their respective names, the administrator can determine whether the DNS services are functioning correctly and whether the servers are reachable from the workstation. The pings help assess the overall network connectivity and validate the successful implementation of DNS and WWW services.

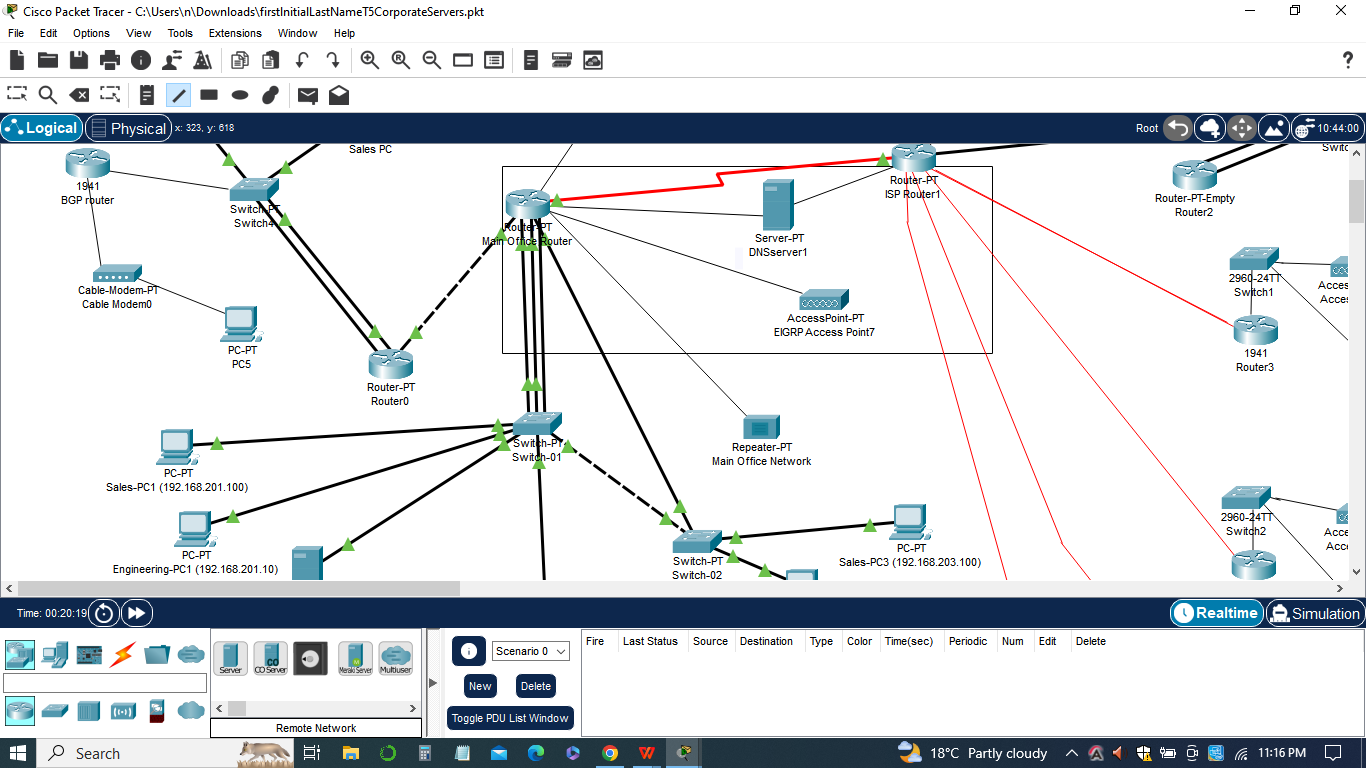
The workstation window was used typically to display the executed ping commands and their corresponding results. A successful ping shows a series of replies indicating the round-trip time and packet loss, while an unsuccessful ping may display error messages or timeouts. The results provide valuable information about the connectivity status of the servers, allowing the administrator to identify any issues or misconfigurations that need to be addressed.

In addition, the workstation window may be used for other network-related tasks, such as configuring DHCP settings, checking IP configurations, or troubleshooting network connectivity problems. It serves as a central interface for managing and monitoring the workstation's interaction with the network infrastructure.

In sum, the workstation window is an essential tool for network administrators to interact with workstations, execute commands, and monitor network activities. It plays a crucial role in evaluating network connectivity, troubleshooting issues, and ensuring the smooth operation of the network infrastructure.

**The packet Tracer**

The Packet Tracer file for this assignment is a simulation of the network configuration and topology. It allows users to create and configure virtual network devices, such as routers, switches, servers, and workstations, and simulate their interactions and behaviors within the network.

******

The Packet Tracer file serves as a practical and visual representation of the network setup described in the assignment. It provides a platform for implementing and testing various network configurations, including ACLs, VLANs, port security, interior gateway protocols, DNS services, and WWW services.

Within the Packet Tracer file, users can access and modify the configurations of network devices, create connections between devices, and observe the flow of data and traffic within the network. They can configure IP addresses, routing protocols, access control lists, DHCP settings, DNS server settings, and other network parameters.

The Packet Tracer file allows users to validate and verify the effectiveness of their network configurations by running simulations and testing connectivity between devices. It provides a visual representation of the network topology, allowing users to understand the relationships between devices and troubleshoot any issues that may arise.

In sum, the Packet Tracer file enables users to capture screenshots or export reports that document the network configurations, ping results, and overall network setup. These outputs can be used for documentation, reporting, and communication purposes, providing a comprehensive view of the network implementation.

**Conclusion**

In conclusion, this assignment focused on enhancing the security and functionality of the network through the implementation of various configurations using Packet Tracer. We successfully added security measures such as Access Control Lists (ACLs), limited trunk VLANs, and port security. Additionally, we set up interior gateway protocols to optimize network routing.

Furthermore, we extended the network's capabilities by incorporating DNS and WWW services. We established a DNS server to handle internal name resolution, added A records for all servers, and updated DHCP settings to point to the internal DNS server. Moreover, we set up an internet-accessible WWW server to provide public web services.

Through these network enhancements, we improved the overall security, efficiency, and accessibility of the network infrastructure. The rationales for each change were carefully considered to align with the organization's requirements and best practices in network management.

To validate the successful implementation of these configurations, we performed a series of pings from a workstation to each server by name. The results of these pings demonstrated the proper functionality and connectivity of the network components.

The Packet Tracer file provided a valuable platform for simulating and visualizing the network configurations. It allowed us to create and configure virtual network devices, test connectivity, and capture screenshots for documentation purposes. The utilization of Packet Tracer enhanced our understanding of network design and configuration.

In sum, this assignment provided a hands-on learning experience in securing and expanding network services using ACLs, VLANs, port security, interior gateway protocols, DNS, and WWW services. By implementing these configurations, we improved the network's reliability, security, and accessibility, contributing to a more efficient and robust network infrastructure.