Enterprise network

DEPI Graduation Project

Table of content:

Introduction:

This project aims to design and implement a scalable and secure network infrastructure capable of supporting various services and applications.

The primary focus will be on utilizing advanced networking technologies to ensure optimal performance, reliability, and flexibility. By incorporating best practices and industry standards, this endeavour seeks to create a robust and efficient network solution.

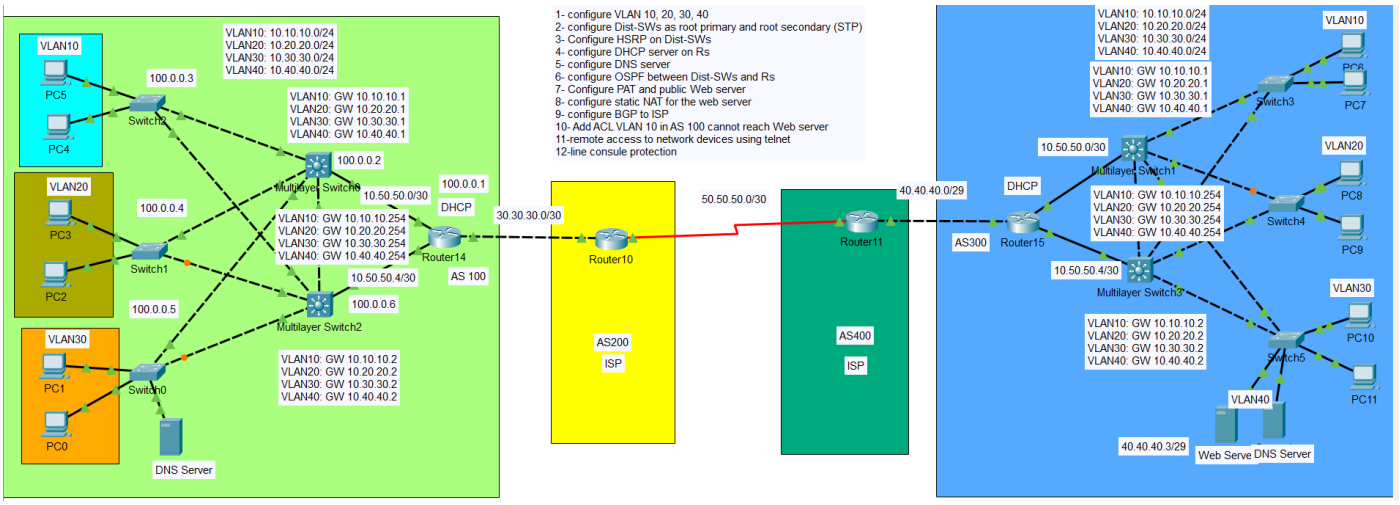
The network design will incorporate a hybrid topology, combining elements of hierarchical and flat architectures. This approach will provide a balance between scalability and manageability. The network will be segmented into multiple VLANs to enhance security and isolate different traffic flows.

The network will be implemented using a combination of routers, switches, and servers. High-performance routing protocols, such as OSPF and BGP, will be deployed to establish efficient inter-domain routing. VLANs will be configured on switches to create logical network segments. DHCP and DNS services will be provided to automate IP address assignment and name resolution.

The expected outcomes of this project include:

- A scalable and secure network infrastructure capable of supporting various services and applications.
- Optimized network performance through the use of advanced routing protocols and traffic management techniques.
- Enhanced network security through VLAN segmentation and access control mechanisms.
- Centralized management and monitoring capabilities for efficient network administration.

Topology:



Components:

- 4 Router model 2911Topology
- 4 Multilayer switch model 3560-24PS
- 6 Switch model 2960-24TT
- 2 DNS server
- 1 Public Web server
- 12 PC

Analysis:

Component Analysis

Routers (2911)

- **Role:** Provide inter-VLAN routing and connectivity between different network segments.
- **Configuration:**
    - OSPF configured for routing between Dist-SWs and Rs.
    - BGP configured for external connectivity to the ISP.
    - Static NAT configured for the web server.
- **Analysis:** The routers are effectively functioning as the core devices of the network, ensuring seamless communication between different VLANs and external networks. The OSPF and BGP configurations enable efficient routing and connectivity, while the static NAT allows for secure access to the web server.

Distribution Switches (3560-24PS)

- **Role:** Provide Layer 2 switching for VLANs and act as the primary and secondary root bridges for STP.
- **Configuration:**
    - VLANs 10, 20, 30, and 40 configured.
    - PVST+ enabled with priority settings to determine root bridge.
    - HSRP configured for redundancy.
- **Analysis:** The distribution switches are crucial for segmenting the network into VLANs, ensuring reliable communication within each VLAN, and providing redundancy through HSRP. The PVST+ configuration ensures efficient loop prevention and rapid convergence in case of failures.

Access Switches (2960-24TT)

- **Role:** Provide Layer 2 switching for end devices (PCs).
- **Configuration:**
    - VLANs 10, 20, 30, and 40 configured.
    - Interfaces assigned to appropriate VLANs.

- **Analysis:** The access switches are responsible for connecting end devices to the network and providing basic switching functions. The VLAN configuration allows for efficient management and isolation of different traffic flows.

DNS Servers

- **Role:** Resolve domain names to IP addresses.
- **Configuration:**
    - DNS zones and records created.
- **Analysis:** The DNS servers play a vital role in enabling users to access network resources by name rather than using IP addresses. The configuration ensures that domain names are correctly resolved to their corresponding IP addresses.

Public Web Server

- **Role:** Serve web content to external users.
- **Configuration:**
    - Web server software installed and configured.
    - Static NAT configured to map a public IP address to the web server.
- **Analysis:** The web server provides a platform for hosting and delivering web content to external users. The static NAT configuration allows for secure and controlled access to the web server from the internet.

PCs

- **Role:** End devices that access network resources.
- **Configuration:**
    - DHCP configured to obtain IP address and other network settings.
- **Analysis:** The PCs are the primary devices used by users to access network resources, such as the web server and other services. DHCP ensures automatic configuration and simplifies network management.

ACL

- **Role:** Restrict access to the web server from VLAN 10.
- **Configuration:**
    - ACL created to deny traffic from VLAN 10 to the web server.
- **Analysis:** The ACL effectively prevents users in VLAN 10 from accessing the web server, ensuring that only authorized users can access the service.

Routers configurations:

Notes:

For console username: amr, password: 2091

- ## Router “10”

```
Rs(AS200)#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       30.30.30.0/30 is directly connected, GigabitEthernet0/0
L       30.30.30.2/32 is directly connected, GigabitEthernet0/0
     40.0.0.0/29 is subnetted, 1 subnets
B       40.40.40.0/29 [20/0] via 50.50.50.2, 00:00:00
     50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       50.50.50.0/30 is directly connected, Serial0/3/0
L       50.50.50.1/32 is directly connected, Serial0/3/0
```

- ## Router “11”

```
Router>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     30.0.0.0/30 is subnetted, 1 subnets
B       30.30.30.0/30 [20/0] via 50.50.50.1, 00:00:00
     40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       40.40.40.0/29 is directly connected, GigabitEthernet0/2
L       40.40.40.2/32 is directly connected, GigabitEthernet0/2
     50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       50.50.50.0/30 is directly connected, Serial0/3/0
L       50.50.50.2/32 is directly connected, Serial0/3/0
```

- **Router "14"**

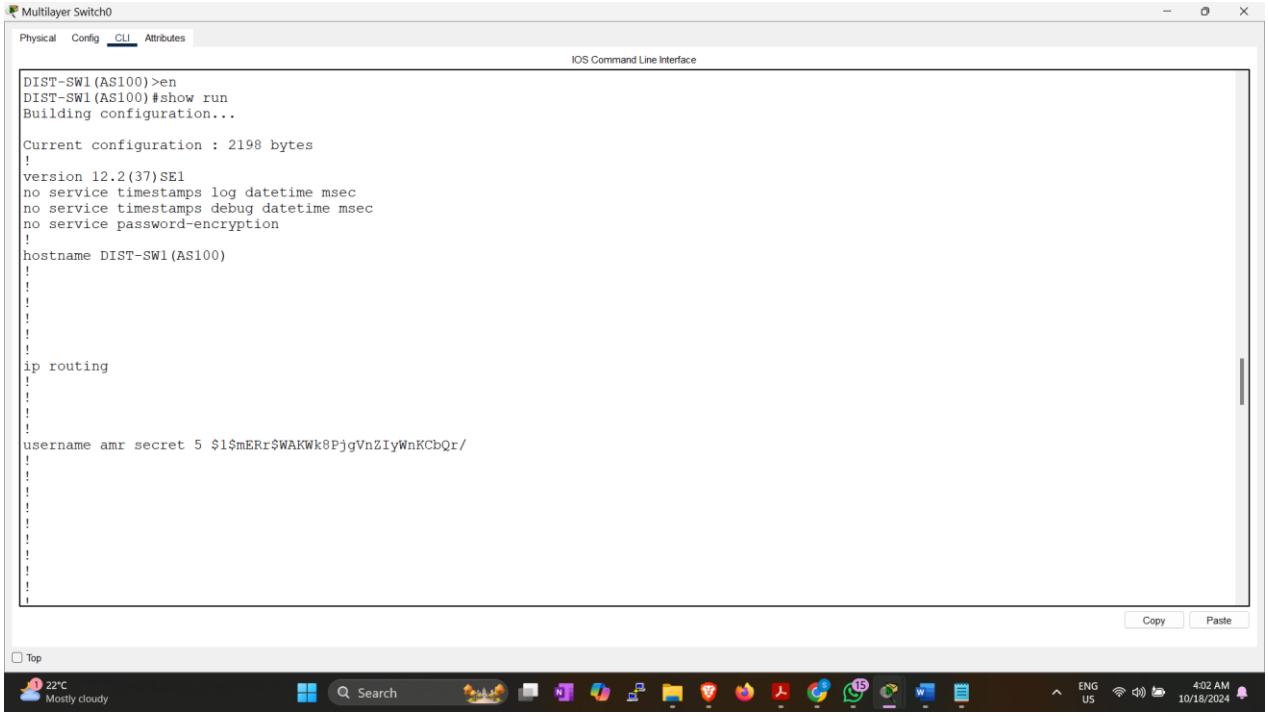
```
Rs(AS100)#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
O       10.10.10.0/24 [110/2] via 10.50.50.5, 00:42:15, GigabitEthernet0/0
                      [110/2] via 10.50.50.1, 00:42:15, GigabitEthernet0/1
O       10.20.20.0/24 [110/2] via 10.50.50.5, 00:42:15, GigabitEthernet0/0
                      [110/2] via 10.50.50.1, 00:42:15, GigabitEthernet0/1
O       10.30.30.0/24 [110/2] via 10.50.50.5, 00:42:15, GigabitEthernet0/0
                      [110/2] via 10.50.50.1, 00:42:15, GigabitEthernet0/1
O       10.40.40.0/24 [110/2] via 10.50.50.5, 00:42:15, GigabitEthernet0/0
                      [110/2] via 10.50.50.1, 00:42:15, GigabitEthernet0/1
C       10.50.50.0/30 is directly connected, GigabitEthernet0/1
L       10.50.50.2/32 is directly connected, GigabitEthernet0/1
C       10.50.50.4/30 is directly connected, GigabitEthernet0/0
L       10.50.50.6/32 is directly connected, GigabitEthernet0/0
     30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       30.30.30.0/30 is directly connected, GigabitEthernet0/2
L       30.30.30.1/32 is directly connected, GigabitEthernet0/2
     40.0.0.0/29 is subnetted, 1 subnets
B       40.40.40.0/29 [20/0] via 30.30.30.2, 00:00:00
     50.0.0.0/30 is subnetted, 1 subnets
B       50.50.50.0/30 [20/0] via 30.30.30.2, 00:00:00
O    100.0.0.0/8 [110/2] via 10.50.50.5, 00:42:15, GigabitEthernet0/0
                 [110/2] via 10.50.50.1, 00:42:15, GigabitEthernet0/1
```

Multilayer Switches configurations:

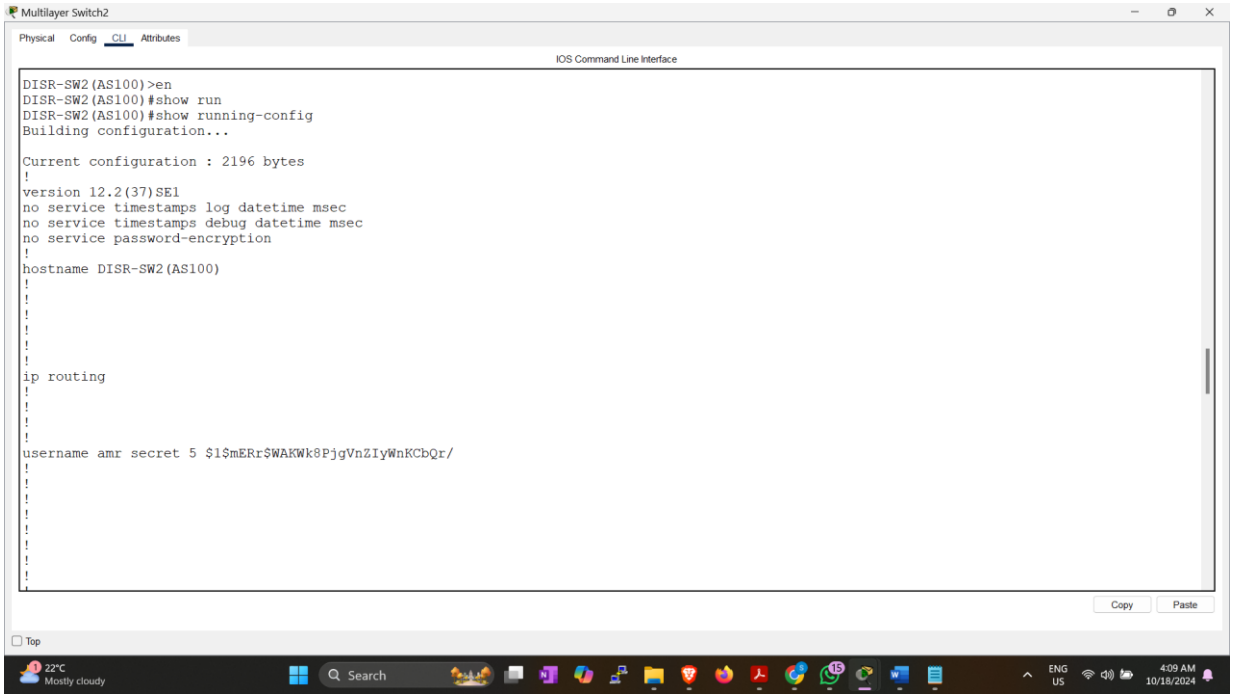
- **Multilayer Switch 0**




```
interface FastEthernet0/4
 no switchport
 ip address 10.50.50.1 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface Vlan1
 ip address 100.0.0.2 255.0.0.0
!
interface Vlan10
 mac-address 000b.be3e.6601
 ip address 10.10.10.1 255.255.255.0
 ip helper-address 10.50.50.2
 standby 1 ip 10.10.10.254
 standby 1 preempt
!
interface Vlan20
 mac-address 000b.be3e.6602
 ip address 10.20.20.1 255.255.255.0
 ip helper-address 10.50.50.2
 standby 2 ip 10.20.20.254
 standby 2 preempt
!
interface Vlan30
 mac-address 000b.be3e.6603
 ip address 10.30.30.1 255.255.255.0
 ip helper-address 10.50.50.2
 standby 3 ip 10.30.30.254
 standby 3 preempt
!
interface Vlan40
 mac-address 000b.be3e.6604
 ip address 10.40.40.1 255.255.255.0
 ip helper-address 10.40.40.254
 standby 4 ip 10.40.40.254
 standby 4 preempt
!
```

```
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
ip default-gateway 100.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.50.50.2
!
ip flow-export version 9
!
```

- # Multilayer Switch 1



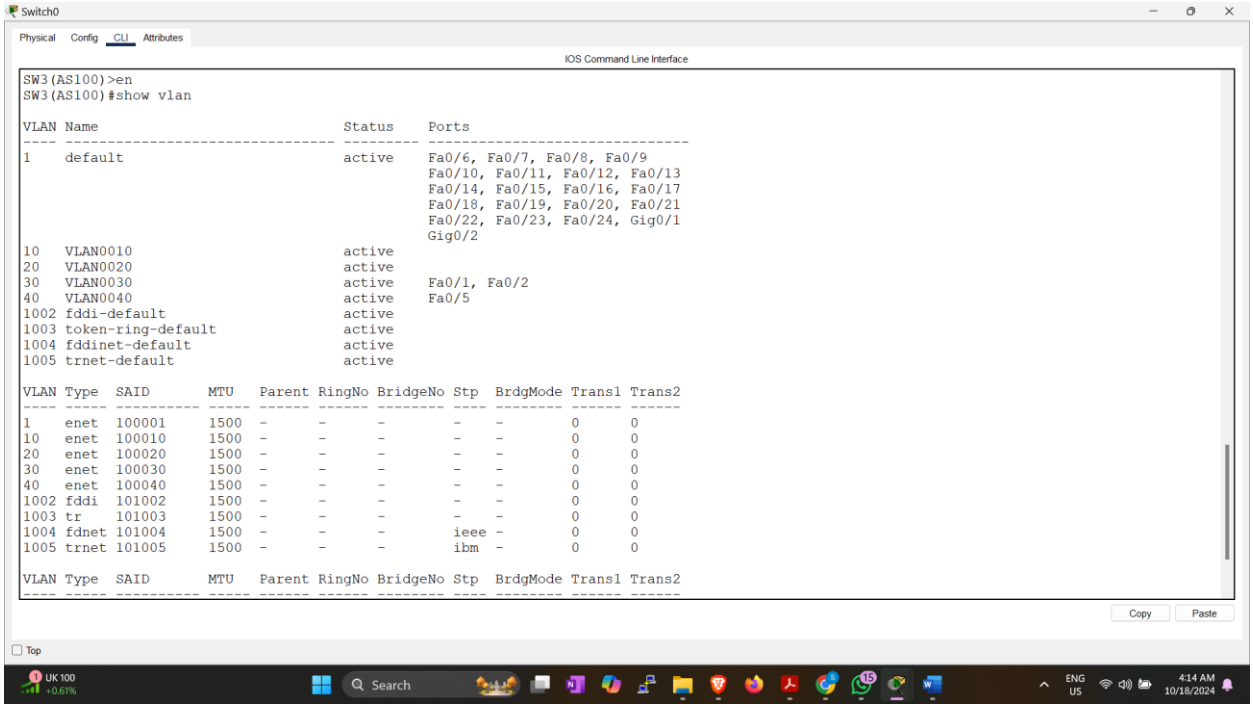

```
interface FastEthernet0/4
 switchport mode dynamic desirable
!
interface FastEthernet0/5
 no switchport
 ip address 10.50.50.5 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto

interface Vlan1
 ip address 100.0.0.6 255.0.0.0
!
interface Vlan10
 mac-address 00d0.bc4c.d101
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 10.50.50.6
 standby 1 ip 10.10.10.254
 standby 1 preempt
!
interface Vlan20
 mac-address 00d0.bc4c.d102
 ip address 10.20.20.2 255.255.255.0
 ip helper-address 10.50.50.6
 standby 2 ip 10.20.20.254
 standby 2 preempt
!
interface Vlan30
 mac-address 00d0.bc4c.d103
 ip address 10.30.30.2 255.255.255.0
 ip helper-address 10.50.50.6
 standby 3 ip 10.30.30.254
 standby 3 preempt
!
interface Vlan40
 mac-address 00d0.bc4c.d104
 ip address 10.40.40.2 255.255.255.0
 ip helper-address 10.50.50.6
 standby 4 ip 10.40.40.254
 standby 4 preempt
```

```
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
ip default-gateway 100.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.50.50.6
!
ip flow-export version 9
```

Switches configurations:

- **Switch 0,1,2**

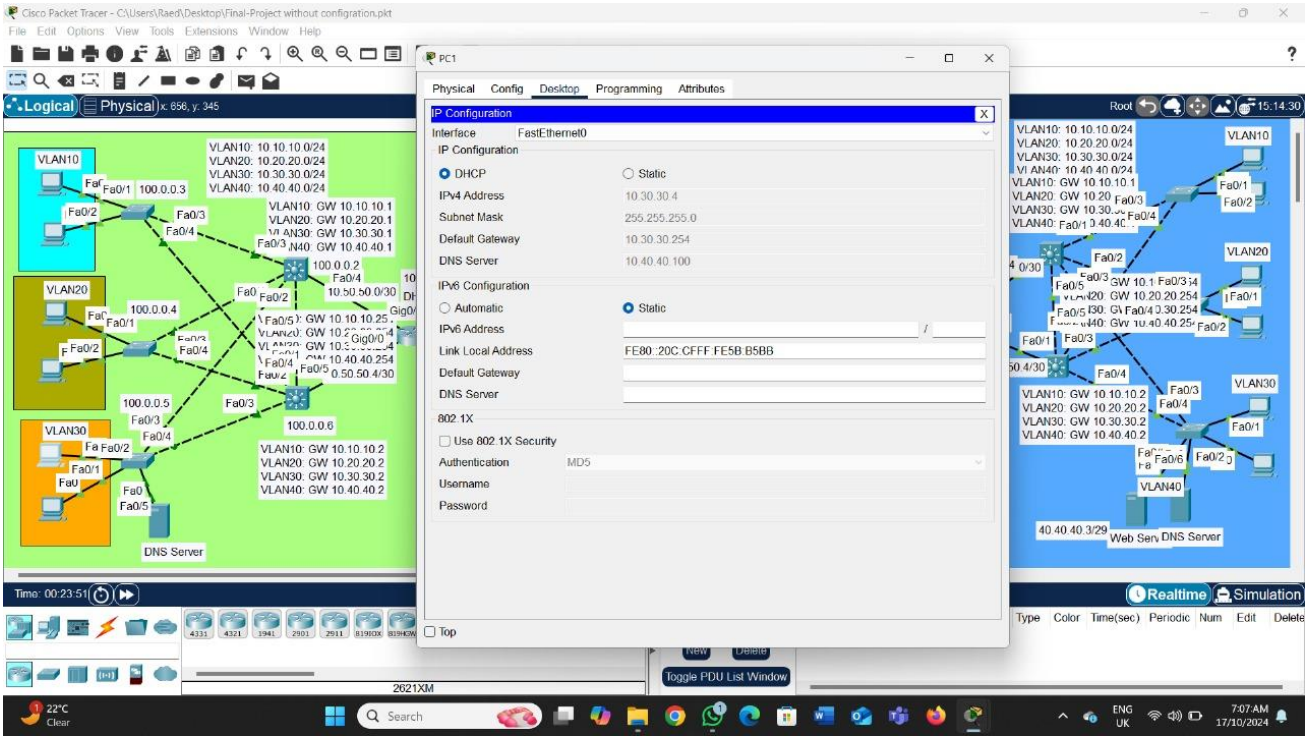


Notes: the other side of the topology has the same configurations

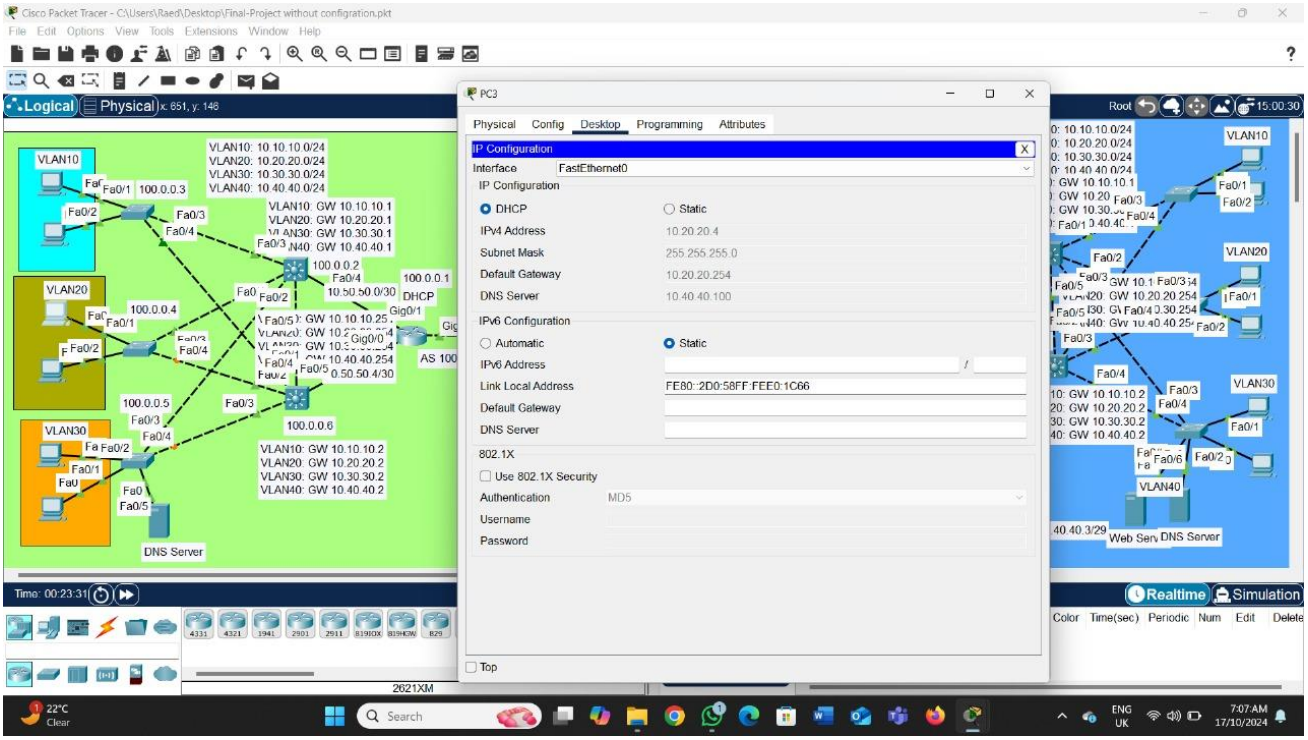
Reachability & troubleshooting:

DHCP

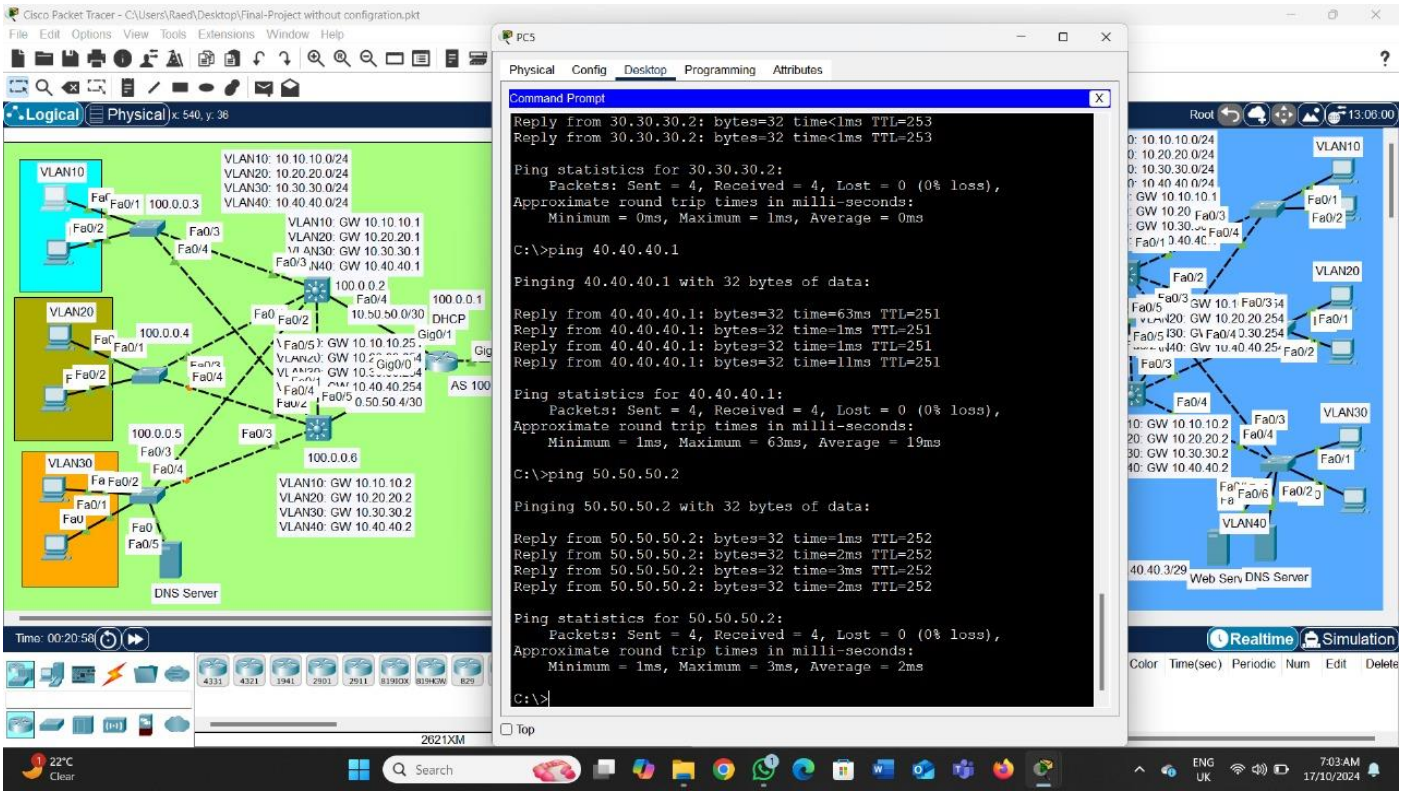
For PC1



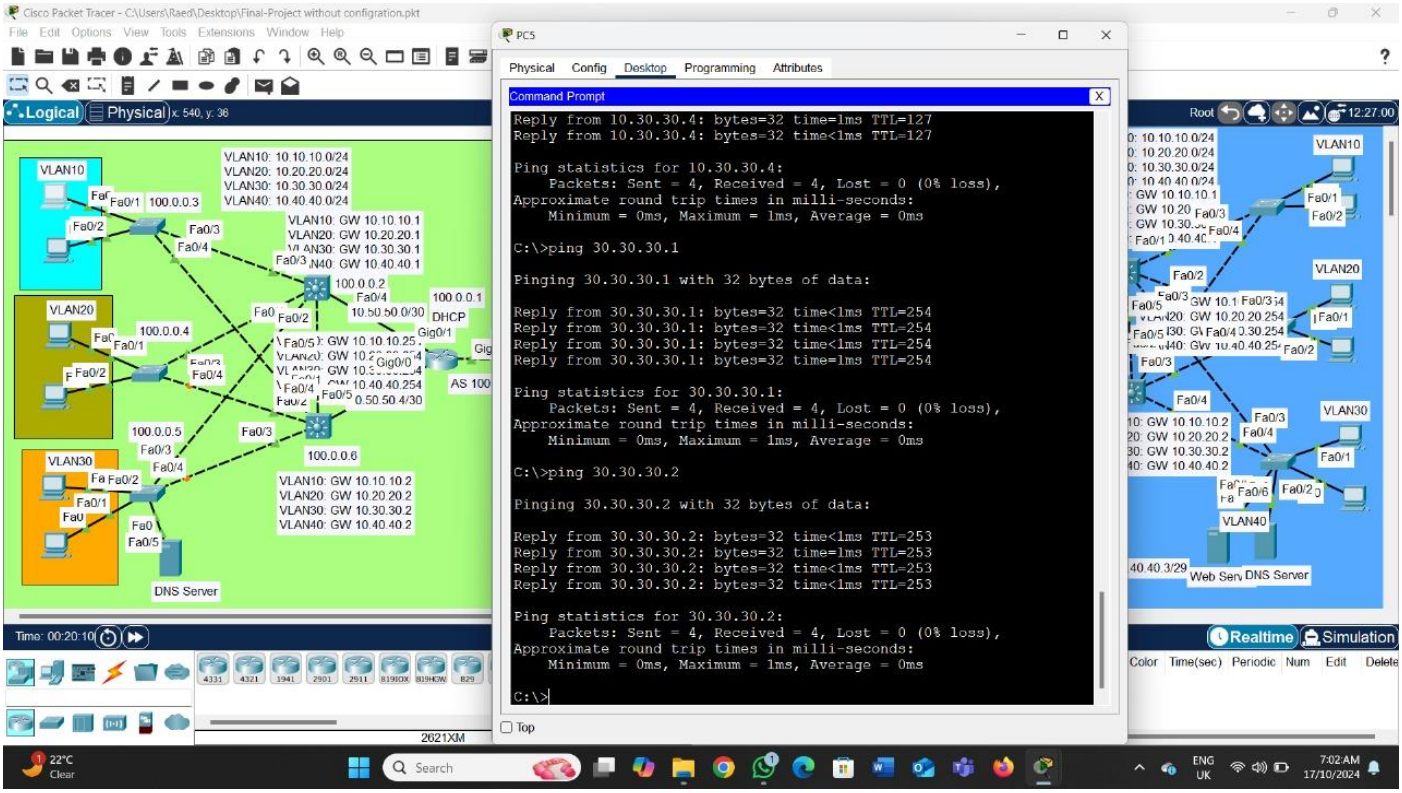
For PC3



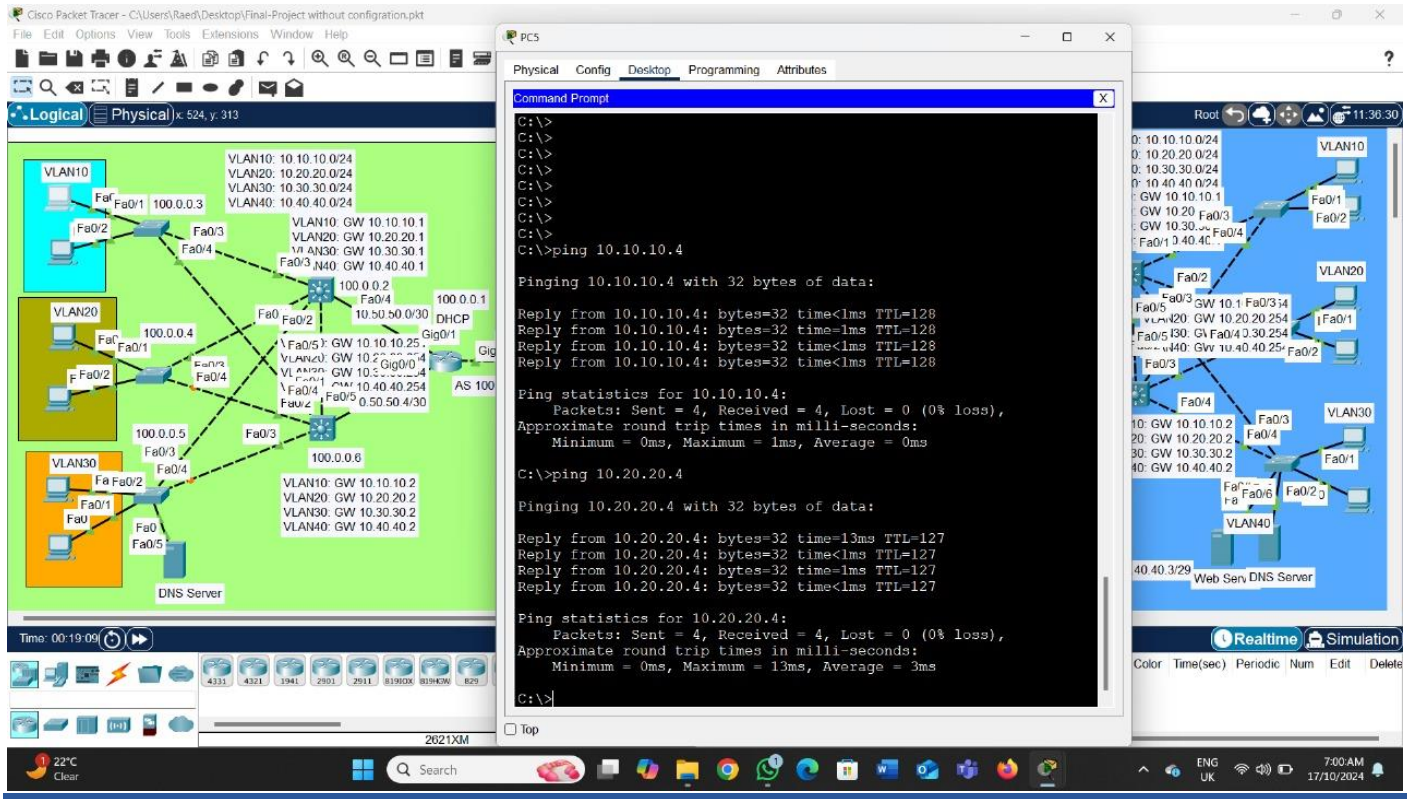
ping from pc5 to as 300 , as 400

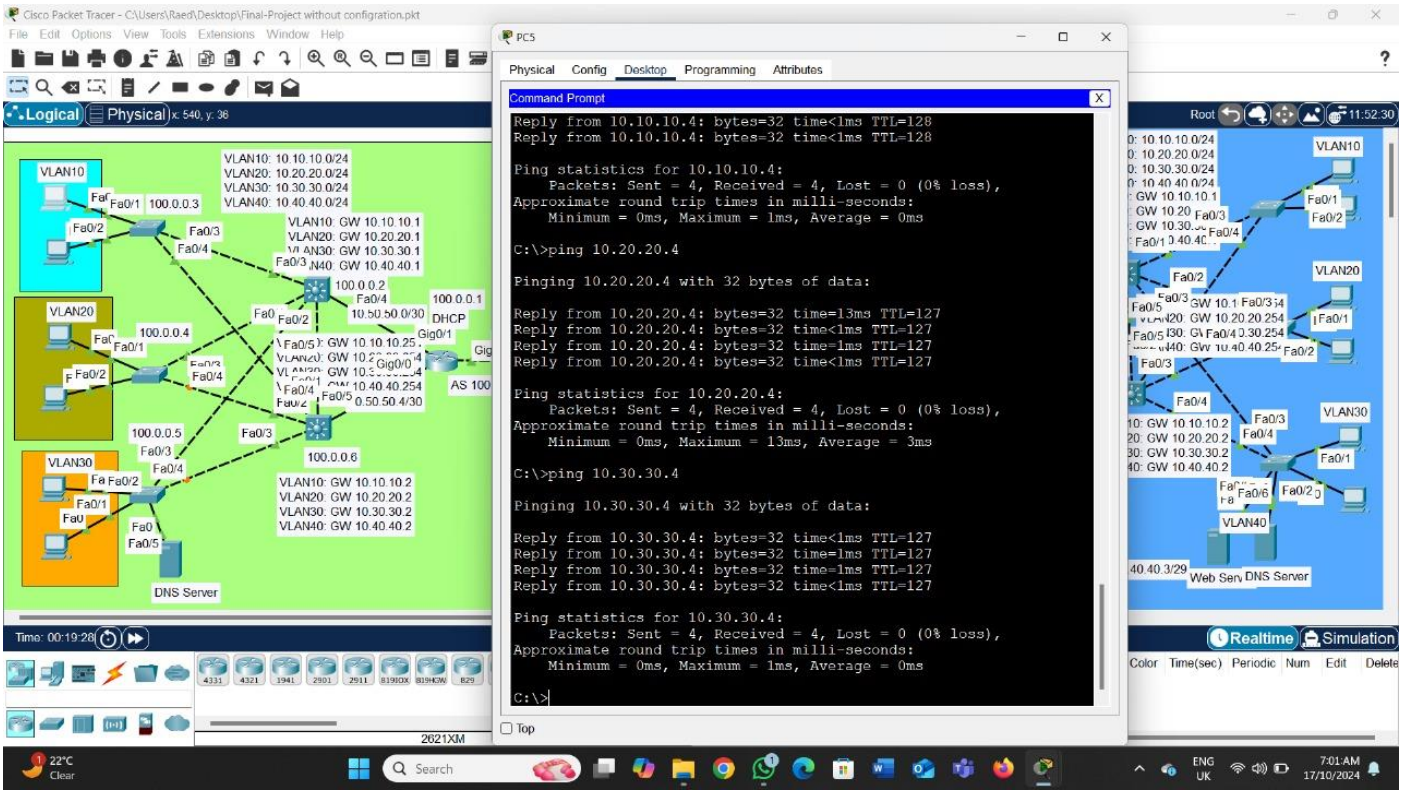


ping from pc5 to rs(as100) and rs(200)

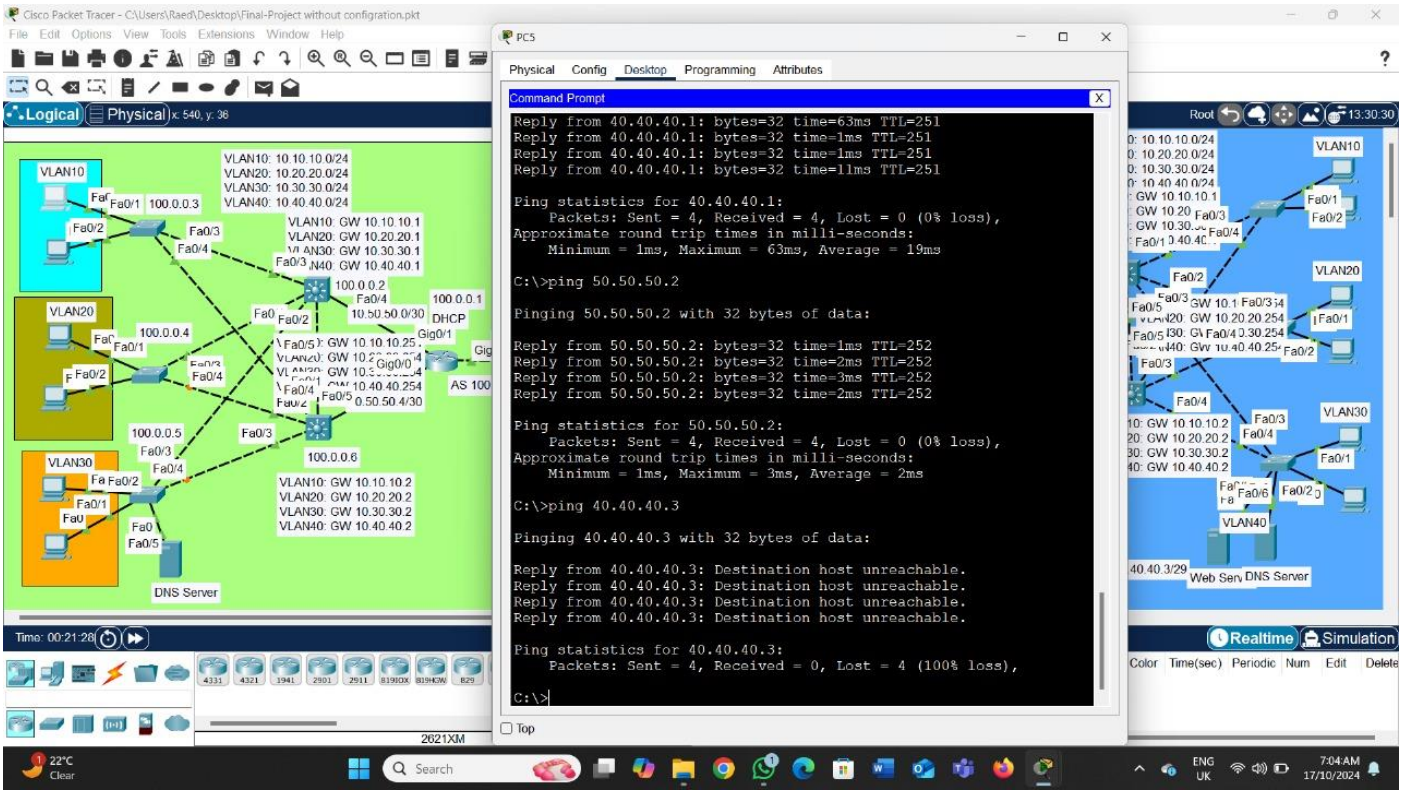


Ping from PC5 to PCs in deffirent Vlans

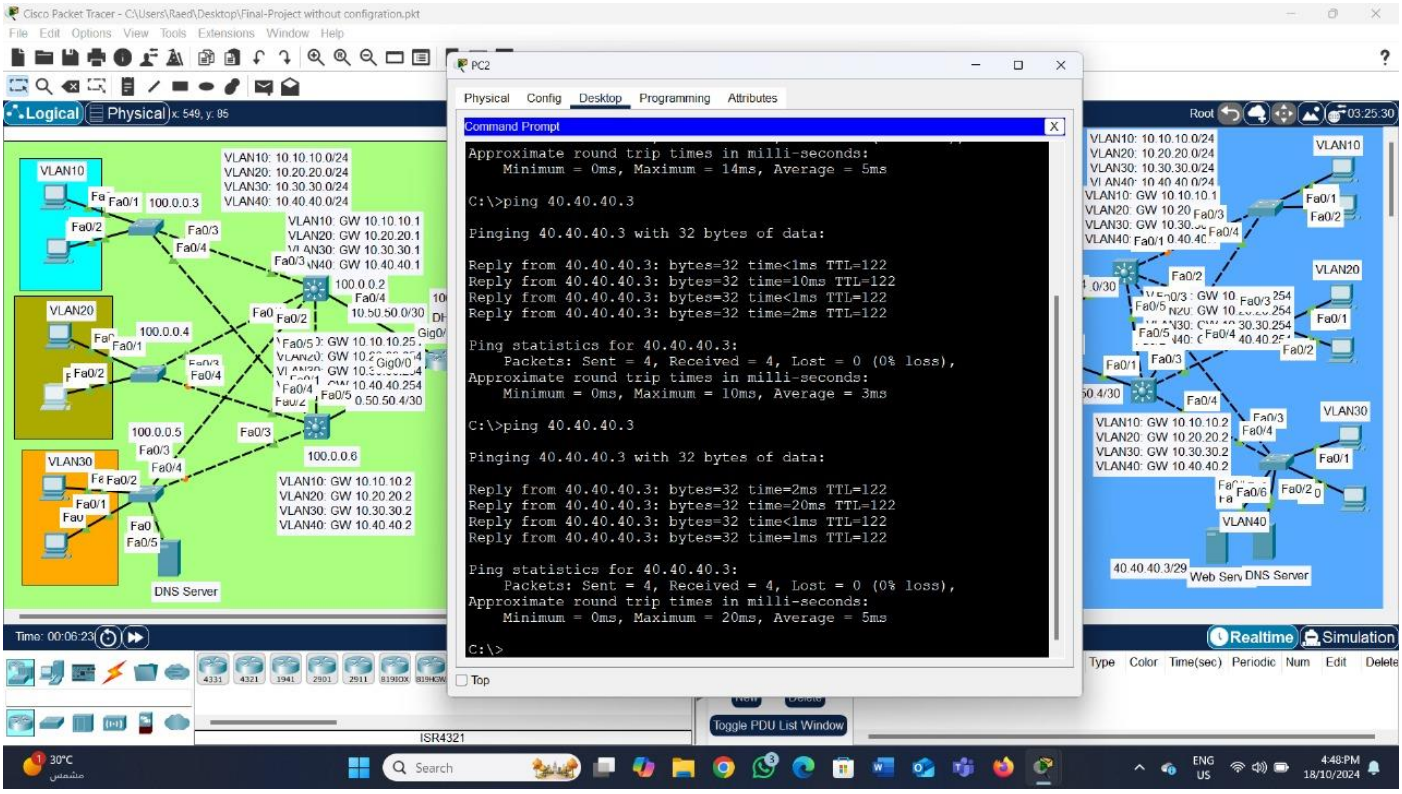




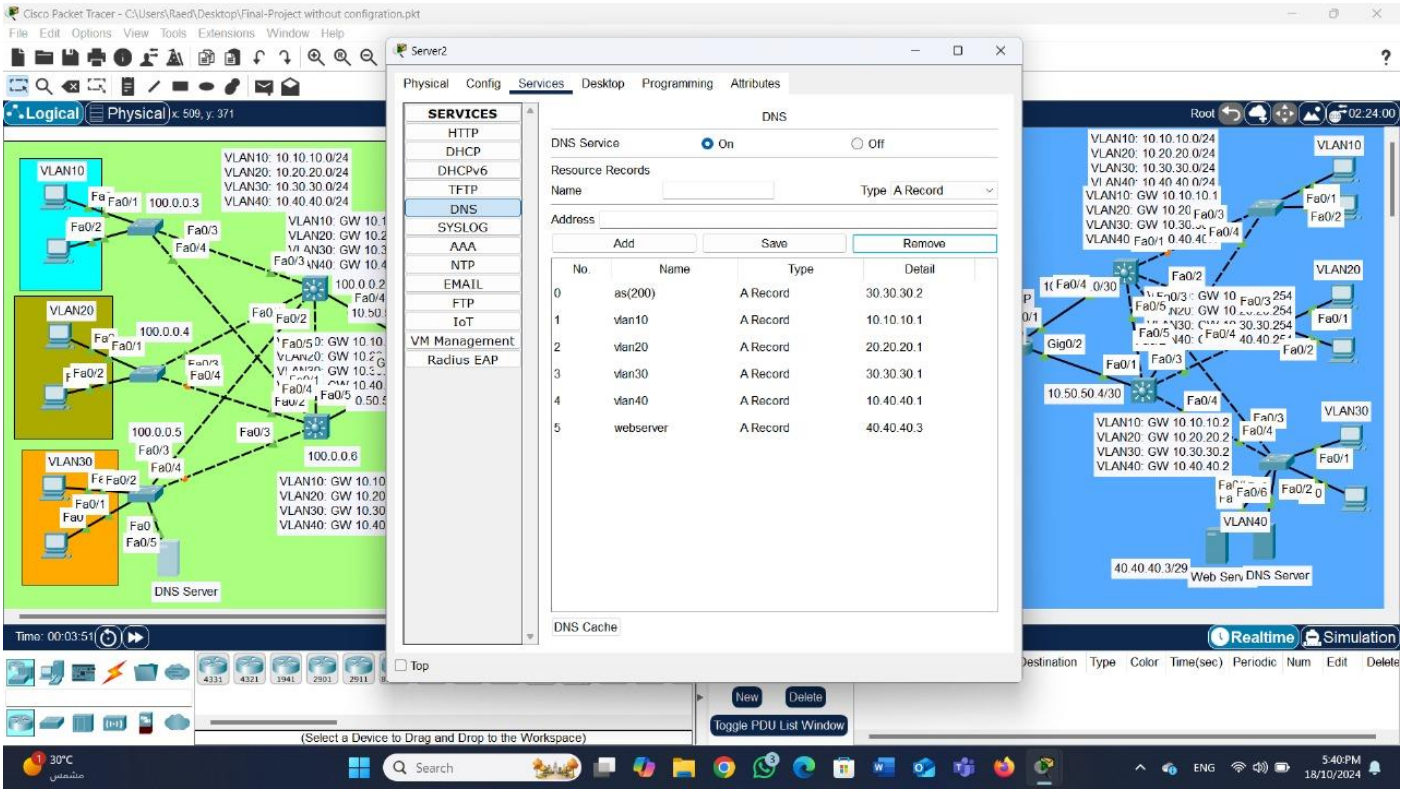
PC5 try to ping web server but ACL prevented that



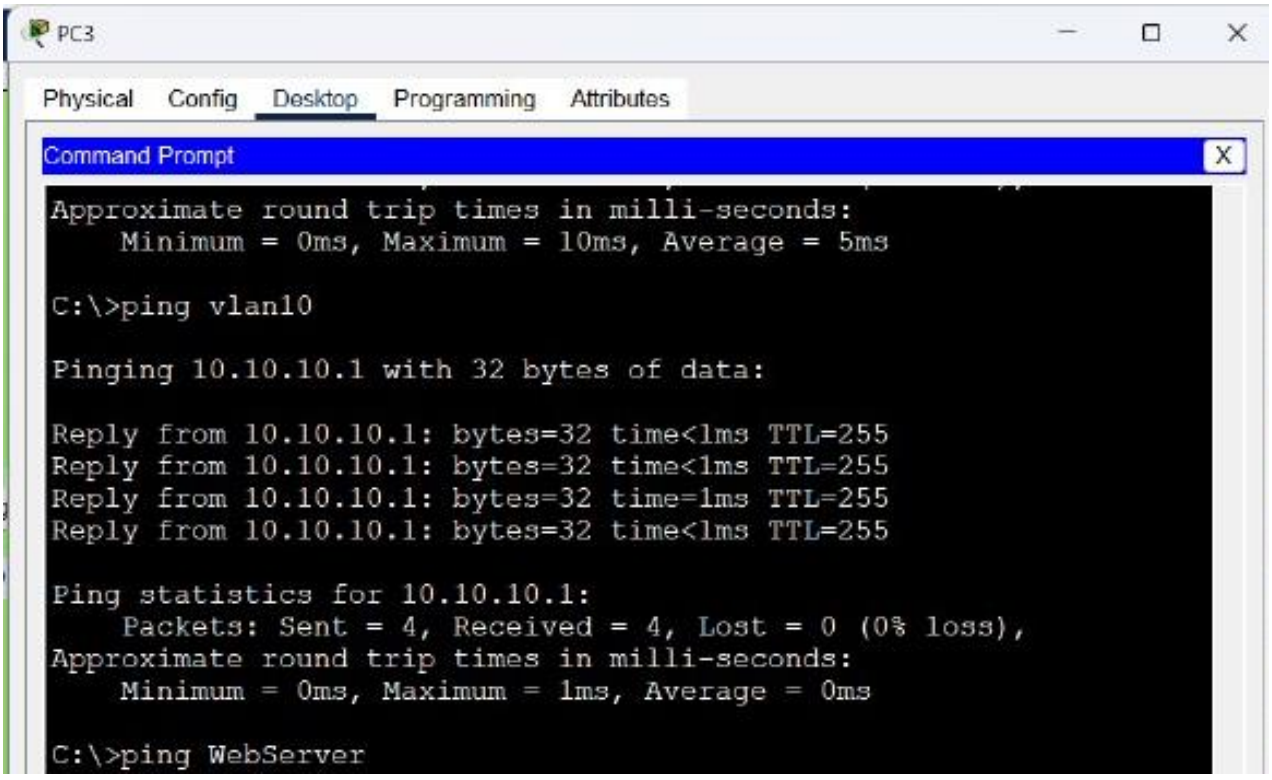
PC2 try to ping web server with PAT



DNS Configurations



DNS Test :



Team Rules:

Amr Raed Ali

- **Tasks:** Configure DHCP server, VLANs, Telnet, console security
- **Summary:** Amr successfully configured the DHCP on the routers to automatically assign IP addresses to devices on the network. Additionally, he created VLANs to segment the network into logical domains, improving security and traffic management.

Mohamed Yousry

- **Tasks:** Configure static NAT, HSRP
- **Summary:** Mohamed Yousry implemented static NAT to map specific private IP addresses to public IP addresses, enabling secure external access to the web server. Additionally, he configured HSRP for redundancy, ensuring high availability and minimizing downtime in case of failures.

Shymaa Saeed Elsyed

- **Tasks:** Configure PAT, DNS
- **Summary:** Shymaa configured PAT to translate multiple private IP addresses to a single public IP address, conserving public IP addresses. She also set up the DNS server to resolve domain names to IP addresses, facilitating easier access to network resources.

Eman Ragab Mohamed

- **Task:** Configure OSPF
- **Summary:** Eman configured OSPF to establish routing between the distribution switches and routers. This enables efficient communication and data transfer across the network.

Omar Alaa Saad

- **Task:** Configure BGP
- **Summary:** Omar configured BGP to establish a peering session with the ISP, allowing the network to connect to the internet and exchange routes with external networks.

Ahmed Mahmoud Ismail

- **Tasks:** Configure Dist-SWs as root primary and root secondary (STP), ACL
- **Summary:** Ahmed configured the distribution switches as the primary and secondary root bridges using STP, ensuring efficient loop prevention and rapid convergence. He also implemented an ACL to restrict access to the web server from VLAN 10, enhancing network security

Project Packet Tracer File : Here

Conclusion:

The implemented network infrastructure effectively addresses the project's objectives of providing a scalable, secure, and efficient network solution. The utilization of VLANs, routing protocols, and security measures ensures optimal performance, reliability, and protection.

The network topology, consisting of routers, switches, and servers, provides a robust foundation for supporting various services and applications. The configuration of VLANs, OSPF, BGP, DHCP, DNS, and NAT enables seamless communication, efficient routing, and secure access to network resources.

The implementation of security measures, such as ACLs, helps to protect the network from unauthorized access and potential threats. The network's scalability allows for future growth and expansion as the organization's needs evolve.

Overall, the project successfully demonstrates expertise in network design, implementation, and troubleshooting. The implemented network infrastructure is well-suited to meet the organization's current and future requirements.

Thanks.