Digital Egypt Pioneers Initiative

Final Project

Implementing a Secure Multi-Branch Office Network

Team Members

Ahmed Hossam Mohamed

Mohamed Abu-Bakr Saadi

Ziad Saad Abd-Elfattah

Omar Hamdy Qarni

Mohamed Ibrahim Mohamed

CONTENTS

01

Summary

Summary

This Presentation details the design and implementation of a robust and secure network infrastructure for a company, a fast-growing telecommunication one.

The network is designed to support the company's operations across its floors.

The network infrastructure will provide reliable connectivity, secure communication, and internet access.

The design prioritizes high performance, redundancy, scalability, and security, ensuring the confidentiality, integrity, and availability of data and communications.

Key network components include Cisco routers, switches, firewalls, a wireless LAN controller, and Servers for directory services and DHCP.

The network will implement network segmentation, robust security measures, and secure inter-office communication and protection against cyber threats.

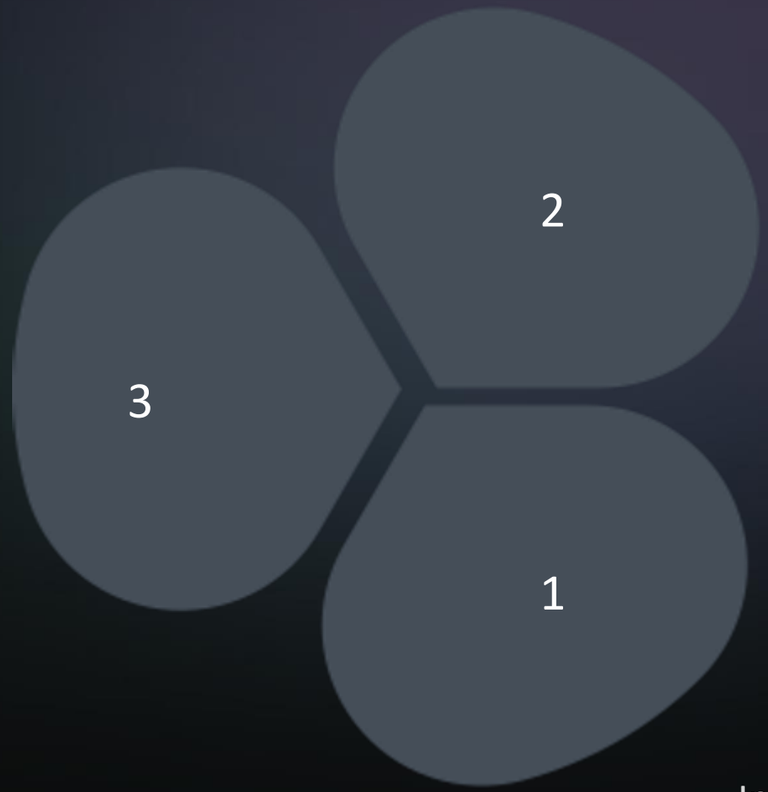
02

Company Profile

Company Profile

Key Infrastructure:

- ISP
- Cisco ASA 5525-X Firewall
- Cisco Catalyst 3850 48-Port Switch
- 3x Cisco Catalyst 2960 48-Port Switches
- 2x Cisco Catalyst 2960 24-Port Switches
- Cisco Voice Gateway (2811)
- Cisco Wireless LAN Controller (WLC)
- 6x Lightweight Access Points (LAPs)
- Windows Server 2022 (Active Directory, RADIUS, DNS, DHCP)
- Internally hosted ERP, Email, and File Servers
- Google Cloud Platform



Departments:

- 4th Floor:
- HR and Finance (40 users)
- Product Brand and Marketing (45 users)
- Admin and Corporate (35 users)
- 5th Floor:
- IT Network & Support (45 users)
- Software Engineering (36 users)
- Cloud Engineering (32 users)

Industry: Telecommunications and IT Solutions

03

Company Requirements

Company Requirements(1)

1. Provide reliable and high-performance network connectivity for all departments.
2. Ensure secure communication and access to internal resources.
3. Enable access to Google cloud resources for developers and cloud engineers.
4. Implement network segmentation to isolate LAN, WLAN, and VoIP traffic.
5. Protect the network from external threats using a firewall.
6. Support VoIP telephony services.

Company Requirements(2)

7 Provide centralized management for wireless access points.

8 Facilitate seamless business continuity.

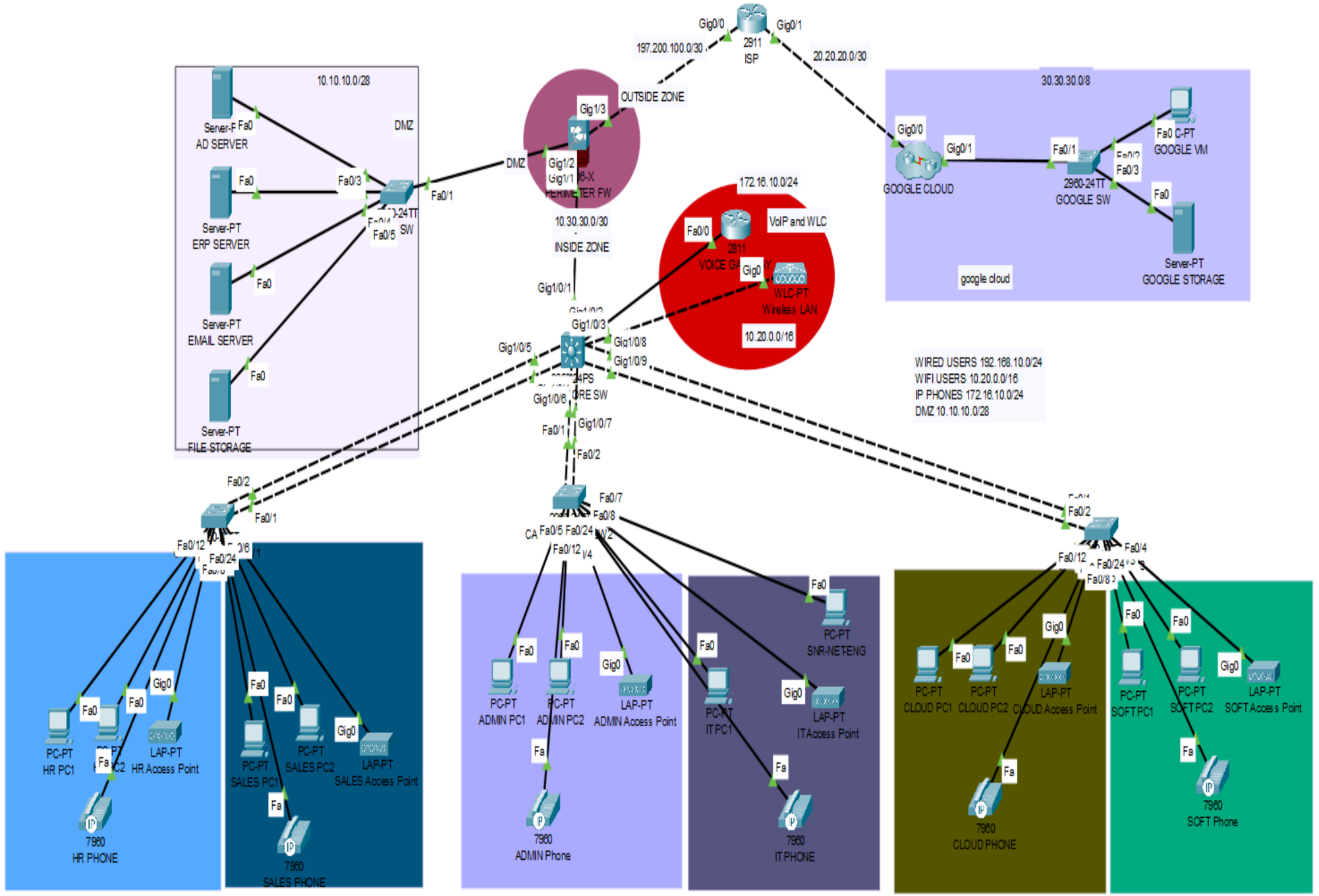
9 Adhere to the principles of Confidentiality, Integrity, and Availability (CIA).

04

Network Design

Network Design

The network is designed using a hierarchical model to provide scalability, redundancy, and ease of management.


Gig0/0
Gig0/1
2911
ISP
197.200.100.0/30
20.20.20.0/30
10.10.10.0/28
DMZ
Server-P
AD SERVER
Fa0
Server-PT
ERP SERVER
Server-PT
EMAIL SERVER
Server-PT
FILE STORAGE
Fa0/3
Fa0/1
Fa0/5
OUTSIDE ZONE
Gig1/3
Gig1/2
DMZ
10.30.30.0/30
INSIDE ZONE
172.16.10.0/24
Fa0/0
2811
VOICE GA
VoIP and WLC
Gig0
WLC-PT
Wireless LAN
10.20.0.0/16
Gig1/0/1
Gig1/0/3
Gig1/0/8
Gig1/0/9
Gig1/0/5
Gig1/0/6
Fa0/1
Gig1/0/7
Fa0/2
Fa0/7
Fa0/8
Fa0/5
Fa0/24
Fa0/12
30.30.30.0/8
Gig0/0
Gig0/1
GOOGLE CLOUD
Fa0/1
2960-24TT
GOOGLE SW
Fa0/3
Fa0 C-PT
GOOGLE VM
Server-PT
GOOGLE STORAGE
google cloud
WIRED USERS 192.168.10.0/24
WIFI USERS 10.20.0.0/16
IP PHONES 172.16.10.0/24
DMZ 10.10.10.0/28
PC-PT
HR PC1
LAP-PT
HR Access Point
7960
HR PHONE
PC-PT
SALES PC1
PC-PT
SALES PC2
LAP-PT
SALES Access Point
7960
SALES PHONE
PC-PT
ADMIN PC1
PC-PT
ADMIN PC2
LAP-PT
ADMIN Access Point
7960
ADMIN Phone
PC-PT
IT PC1
LAP-PT
ITAccess Point
7960
IT PHONE
PC-PT
SNR-NETENG
PC-PT
CLOUD PC1
PC-PT
CLOUD PC2
LAP-PT
CLOUD Access Point
7960
CLOUD PHONE
PC-PT
SOFT PC1
PC-PT
SOFT PC2
LAP-PT
SOFT Access Point
7960
SOFT Phone

Network Topology

Wireless Network: A Cisco Wireless LAN Controller (WLC) manages Lightweight Access Points (LAPs) distributed across both floors to provide wireless connectivity for employees and guests.

DMZ: A Demilitarized Zone (DMZ) is implemented to host the internal servers (ERP, Email, and File) and provide controlled access from the internal network and the internet.

Internet Connectivity: A connection to ISP is established through the Cisco ASA 5525-X Firewall.

A hierarchical topology is implemented, comprising the following layers:

•Core Layer: The Cisco Catalyst 3850 Multilayer switch acts as the core layer, providing high-speed switching and routing between different network segments.

•Distribution Layer: The Cisco Catalyst 2960 switches aggregate connections from access layer switches and provide redundancy.

•Access Layer: Cisco Catalyst 2960 switches provide connectivity for end-user devices (PCs, laptops, IP phones, and wireless access points).

IP Addressing Scheme

The following IP address ranges are used:

- WLAN: 10.20.0.0/16
- LAN: 192.168.10.0/24
- Voice: 172.16.10.0/24
- DMZ: 10.10.10.0/28
- Public Addresses: 197.200.100.0/24

Access Layer

The access layer grants end devices access to the network. In the WAN environment, it may provide teleworkers, or remote sites access to the corporate network across WAN connections.

Generally, incorporates Layer 2 switches and access points providing connectivity and serves several functions including:

- Layer 2 switching
- High availability
- Port security
- Address Resolution Protocol (ARP) inspection
- Basic setting (SSH - ACL for ssh)

configuration
All access switch

```
enable
configure terminal
hostname CAIRO-ACCESS-SWI
enable password cisco
banner motd *NO UNAUTHORISED ACCESS- THIS PUNISHABLE BY LAW*
username cisco password cisco
ip domain-name cisco_net
line console 0
password cisco
login
exit
no ip domain-lookup
service password-encryption
do wr
```

```
vlan 20
name LAN
vlan 30
exit
vlan 30
name WLAN
exit
vlan 50
name VoIP
exit
enable
configure terminal
interface rangeFastEthemet0/3- 0 - 4
exit
interface rangeFastEthemet0/3- 0 - 5
switchport mode access
switchport access vlan 20
switchport voice vlan 50
exit
```

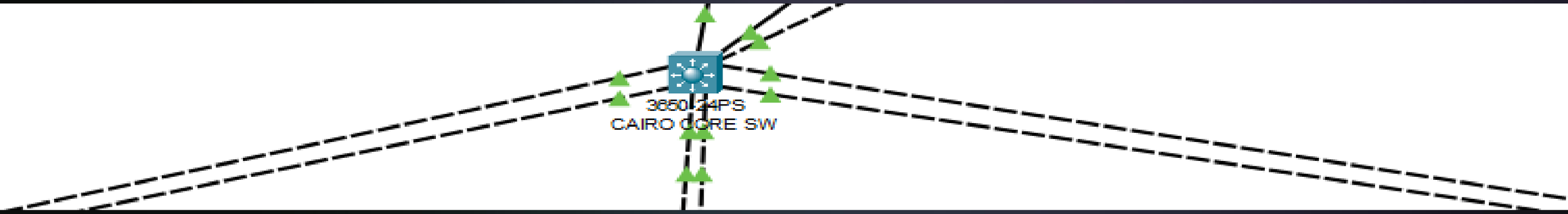
configuration

All access switch

```
enable
int
configure terminal
interface rangeFastEthernet0/1. 0 - 2
enable
configure terminal
interface rangeFastEthernet0/1- 0 - 2
channel-group 1 mode active
exit
interface Port-channel1
switchport mode trunk
exit
interface range
interface rangeFastEthernet0/3. 0 - 24
spanning-tree portfast
spanning-tree bpduguard enable
exit
```

```
int range fa0/3-8
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation protect
do wr
Exit
int range fa0/3-24
switchport nonegotiate
exit
int fa0/1
switchport mode trunk
switchport trunk native vlan 999
exit
int fa0/2
switchport mode trunk
switchport trunk native vlan 999
exit
```

Distribution Layer



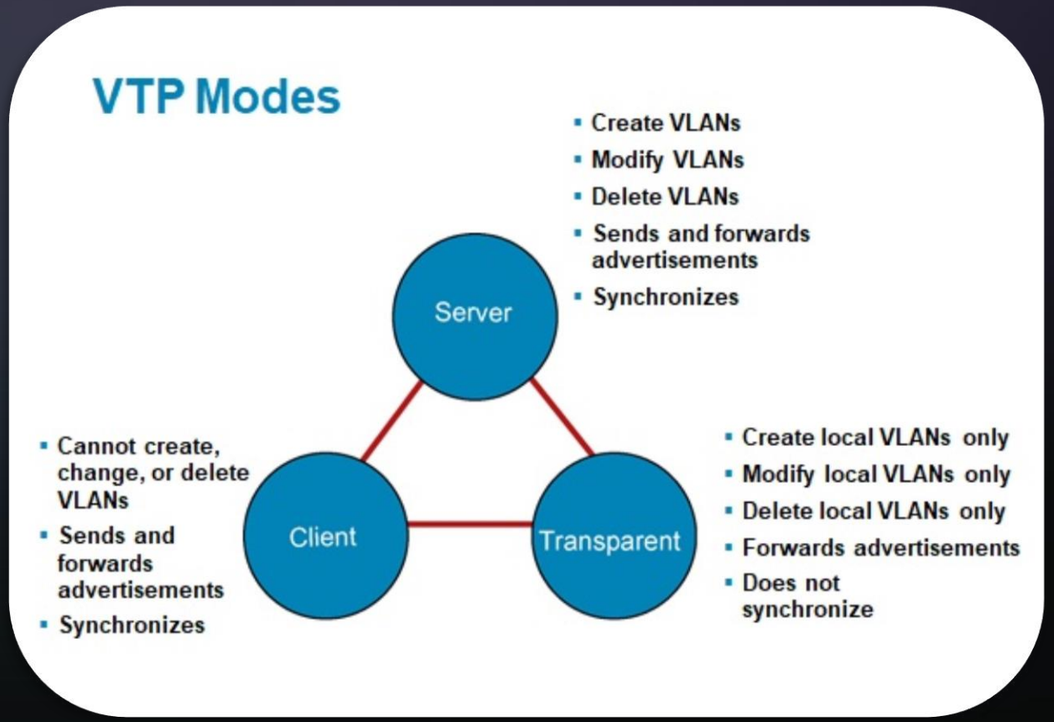
- The distribution layer is the boundary between the Layer 2 and the Layer 3 routed network.
- Layer 2 ether-channel.
- Routing services between LANs and VLANs and between routing domains.
- Redundancy.

Distribution Layer

VTP (VLAN Trunnking Protocol):

What’s VTP ?

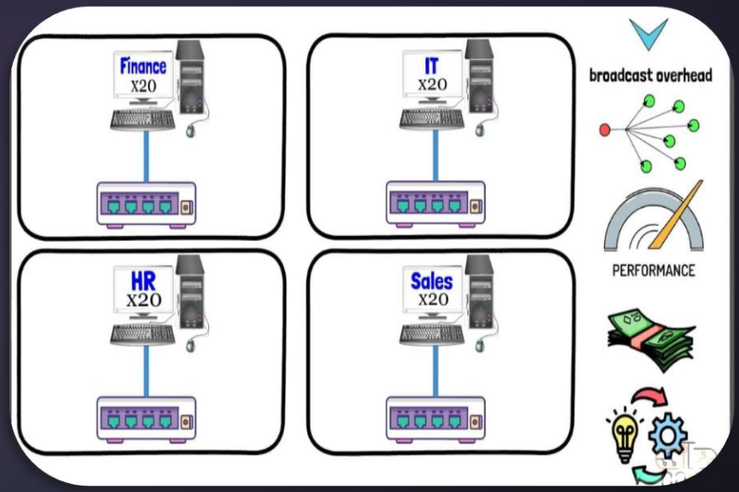
What’s VTP V3?

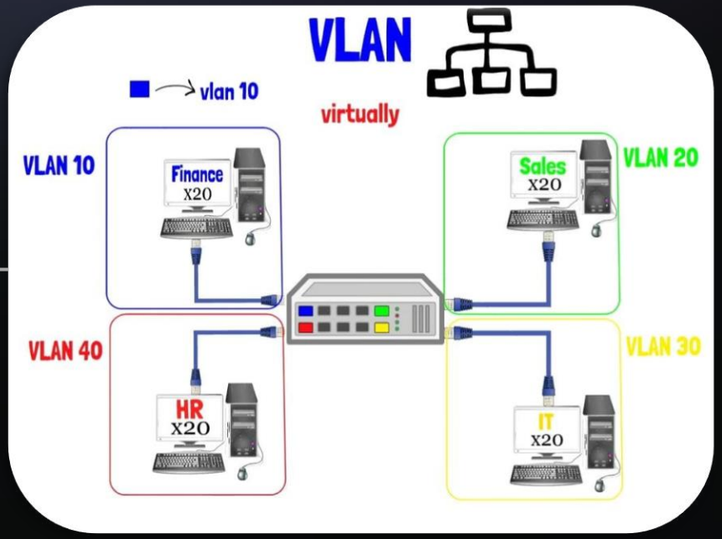


VLANs (Virtual Local Area Network):

What’s VLAN?

- **Advantages of a VLAN:**
  - **Separate broadcast domain.**
  - **Decrease broadcast domain.**
  - **Enhance network performance.**
  - **Scalable.**
  - **More security.**



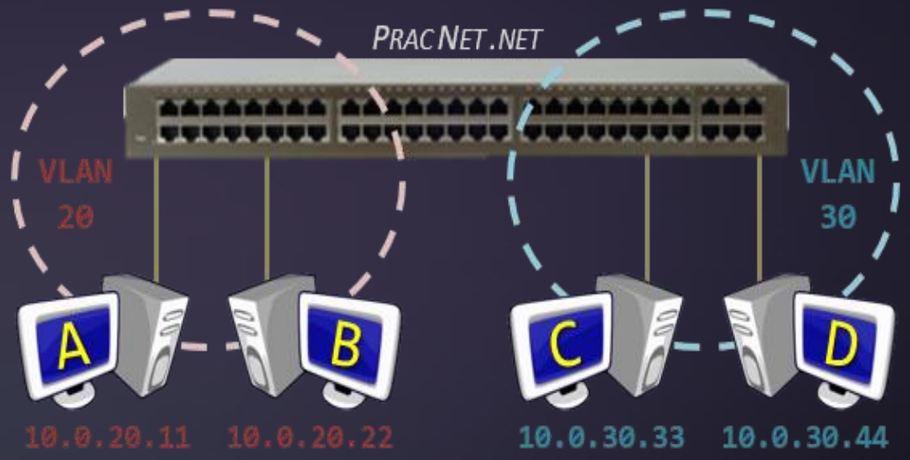


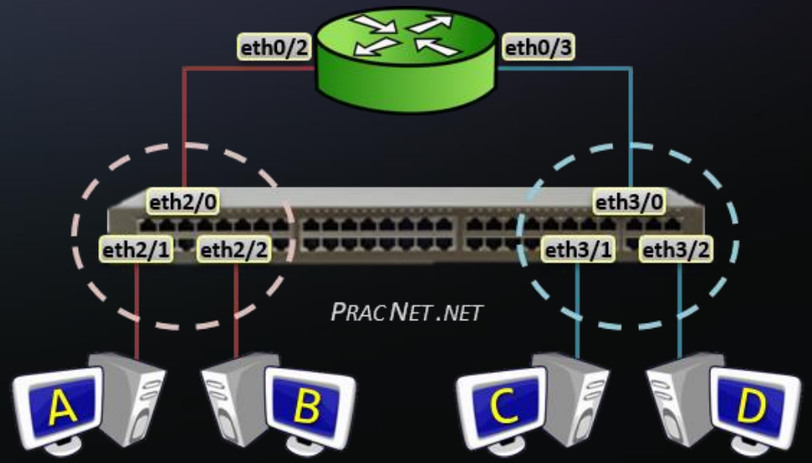
Routing Between VLANs

- **Why do we need Routing Between VLANs?**

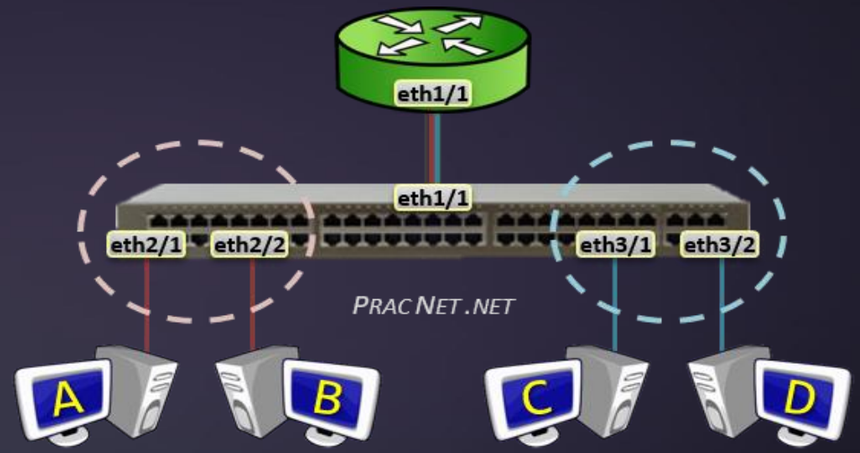
- **There are three options available to enable routing between the VLANs:**
  - ✓ **Router with a Separate Physical Interface in each VLAN**
  - ✓ **Router with a Sub-Interface in each VLAN**
  - ✓ **Using a Layer 3 Switch (Best method)**

- **Router with a Separate Physical Interface in each VLAN (Traditional Method)**





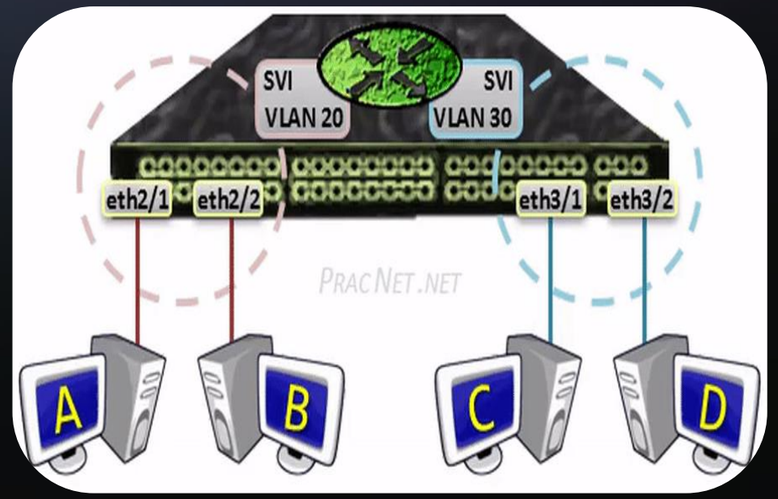
Router with a Sub-Interface in each VLAN (Router on a Stick)



- A Sub-Interface allows a single Physical interface to be split up into multiple virtual sub-interfaces, each of which terminate their own VLAN.

Layer 3 Switch (Best method)

- You have the option of configuring an IP address within what is known as an SVI (Switched Virtual Interface)
- The configuration for an SVI involves two parts. First, enabling IP Routing; and Second, applying an IP address to the VLAN.
- This IP will be the default gateway for the VLAN.



VLAN Design

VLANs are used to segment the network traffic for improved security, performance, and manageability.

- VLAN 20: LAN (for wired devices in each department)
- VLAN 30: WLAN (for wireless devices used by employees and guests)
- VLAN 50: VoIP (for IP phones)

configuration
Distribution switch

```
enable
configure terminal
interface rangeGigabitEthernet1/0/4 - 5
channel-group 1 mode active
exit
interface Port-channell
switchport mode trunk
exit
interface rangeGigabitEthernet1/0/6 - 7
channel-group 2 mode active
interface Port-channe12
switchport mode trunk
exit
interface rangeGigabitEthernet1/0/8 - 9
channel-group 3 mode active
interface Port-channe13
switchport mode trunk
exit
do wr
interface GigabitEthernet1/0/2
switchport mode trunk
exit
```

```
enable
configure terminal
interface GigabitEthernet1/0/1
no switchport
ip address 10.30.30.2 255.255.255.252
exit
do wr
```

```
enable
configure terminal
interface Vlan20
no shutdown
ip address 192.168.10.1 255.255.255.0
exit
interface Vlan30
no shutdown
ip address 10.20.0.1 255.255.0.0
exit
interface Vlan30
ip helper-address 10.10.10.5
exit
interface Vlan20
ip helper-address 10.10.10.5
exit
```

configuration

Distribution switch

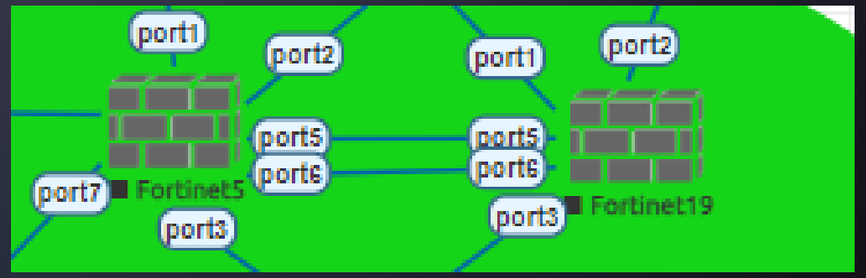
```
router ospf 1
network 10.30.30.0 0.0.0.3 area 0
exit
do wr
int g1/0/4
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
int g1/0/5
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
int g1/0/6
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
```

```
int g1/0/7
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
int g1/0/8
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
int g1/0/9
switchport nonegotiate
switchport mode trunk
switchport trunk native vlan 999
exit
```

Firewall

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules

- Its primary function is to establish a barrier between trusted internal networks and untrusted external networks, such as the internet, to prevent unauthorized access and potential threats.



Subnetting

Subnetting is employed to efficiently allocate IP addresses to each department and network segment. The specific subnetting scheme is as follows:

- LAN Subnetting (192.168.10.0/24):
- HR & Finance: [To be determined based on user count, e.g., 192.168.10.0/27]
- Product Brand & Marketing: [To be determined based on user count, e.g., 192.168.10.32/27]
- Admin & Corporate: [To be determined based on user count, e.g., 192.168.10.64/27]
- IT Network & Support: [To be determined based on user count, e.g., 192.168.10.96/27]
- Software Engineering: [To be determined based on user count, e.g., 192.168.10.128/27]
- Cloud Engineering: [To be determined based on user count, e.g., 192.168.10.160/27]
- WLAN Subnetting (10.20.0.0/16):
- Subnets will be created for each floor and/or department if needed for further segmentation.
- Voice Subnetting (172.16.10.0/24):
- The entire 172.16.10.0/24 subnet can be used for VoIP devices, or it can be further subnetted if required.
- DMZ Subnetting (10.10.10.0/28):
- The 10.10.10.0/28 subnet provides addresses for the servers in the DMZ.

Routing

OSPF (Open Shortest Path First) is used as the routing protocol for dynamic routing within the internal network. This includes routing between VLANs and to the core router.

Static routes and default routes are configured on the Cisco ASA Firewall to direct traffic to and from the internet and the internal network.

Inter-VLAN routing is configured on the Layer 3 switch (Catalyst 3850) to enable communication between devices in different VLANs.

High Availability and Redundancy

The hierarchical design provides redundancy.

Link aggregation (EtherChannel/LACP) is implemented to increase bandwidth and provide link redundancy between switches.

STP PortFast and BPDU Guard are configured to minimize downtime during topology changes and prevent spanning-tree loops.

Security Design

Security is a critical aspect of network design. The following measures are implemented:

- Firewall: A Cisco ASA 5525-X Firewall is deployed as the perimeter firewall to protect the network from external threats.
- Security zones are defined (e.g., Inside, Outside, DMZ).
- Security policies are configured to control traffic flow between zones.
- Network Address Translation (NAT) is used to translate private IP addresses to public IP addresses.
- Firewall inspection policies are implemented.
- Access Control:
- Standard ACLs are configured on the Cisco devices to restrict access to sensitive network resources. Specifically, an ACL is used to limit SSH access to authorized administrators.
- Device Hardening:
- Strong passwords are used for all network devices.
- Unused ports and services are disabled.
- IP domain lookup is disabled.
- All passwords are encrypted.

05

Implementation

Implementation

The network implementation involves the following steps:

- Device Configuration:
- Configure basic settings on all network devices (hostnames, console passwords, enable passwords, banner messages).
- Configure VLANs on the switches and assign ports to the appropriate VLANs.
- Configure IP addressing on all interfaces.
- Configure OSPF routing on the routers and Layer 3 switch.
- Configure EtherChannel (LACP) where required.
- Configure STP PortFast and BPDU Guard on access ports.
- Configure the Cisco ASA Firewall with security zones, policies, and NAT.
- Configure the Cisco WLC and Lightweight Access Points (LAPs) for wireless connectivity.
- Configure the Cisco Voice Gateway for VoIP services.
- Configure a Standard ACL for SSH access.

Implementation

- DHCP Configuration:
- Configure the Windows Server 2022 to provide DHCP services for LAN and WLAN clients.
- Configure the Cisco Voice Gateway (or a separate router) to provide DHCP services for IP phones.
- Server Configuration:
- Configure static IP addresses on the internal servers (ERP, Email, and File) within the DMZ.
- Cabling:
- Connect network devices using the appropriate cables (Ethernet).
- Testing and Verification:
- Test connectivity between all network devices and departments.
- Verify VLAN configuration and inter-VLAN routing.
- Test DHCP functionality.
- Verify OSPF routing.
- Test VoIP functionality.
- Test WLAN connectivity and security.
- Test firewall rules and security policies.
- Test SSH access with the configured ACL.
- Test access to internal servers from the LAN and the internet (if required).
- Verify access to Google cloud resources.

06

IP Address Allocation

IP Address Allocation(1)

Device/Location	Subnet	IP Address Range	Assigned IP Address(es)
ISP Router	197.200.100.0/24	197.200.100.1 - 197.200.100.254	197.200.100.1 (Example)
ASA Firewall (Outside)	197.200.100.0/30	197.200.100.1 - 197.200.100.254	197.200.100.2
ASA Firewall (Inside)	10.30.30.0/30	10.10.10.1 - 10.10.10.14	10.30.30.1
DMZ Server 1	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.5
DMZ Server 2	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.6

IP Address Allocation(2)

DMZ Server 3	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.7
DMZ Server 4	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.8
Core Switch (VLAN 20)	192.168.10.0/24	192.168.10.1 - 192.168.10.254	192.168.10.1
Core Switch (VLAN 30)	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.1
Core Switch (VLAN 50)	172.16.10.0/24	172.16.10.1 - 172.16.10.254	172.16.10.1
Windows Server 2022	192.168.10.0/24	192.168.10.1 - 192.168.10.254	192.168.10.2

IP Address Allocation(3)

Voice Gateway	172.16.10.0/24	172.16.10.1 - 172.16.10.254	172.16.10.254
Department 1 Switch	192.168.10.0/27	192.168.10.1 - 192.168.10.30	192.168.10.2
Department 1 PC 1	192.168.10.0/27	192.168.10.1 - 192.168.10.30	192.168.10.10
WLC	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.2
LAP 1	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.10

07

Device Configuration Standards

Device Configuration Standards

1 The following configuration standards are to be followed:

2 Hostnames: Use a consistent naming convention for all devices (e.g., Core-SW-01, Dist-SW-01, Access-SW-01, FW-01, Rtr-01, WLC-01).

3 Passwords:
- Strong, complex passwords must be used for all user and privilege levels.
- Console, VTY, and enable passwords must be configured.
- All passwords must be encrypted using service password-encryption.

4 Banner Message: A Message of the Day (MOTD) banner should be configured on all devices to provide a warning to unauthorized users.

5 IP Domain Lookup: Disable IP domain lookup using the no ip domain-lookup command to prevent unnecessary DNS queries.

6 SSH: SSH should be the only protocol allowed for remote management. Telnet should be disabled.

08

Technologies Implemented

Technologies Implemented

The following technologies are implemented in this network:	Hierarchical Network Design	VLANs (802.1Q)
Subnetting and IP Addressing (IPv4)	OSPF Routing Protocol	EtherChannel (LACP)

Technologies Implemented 2

Spanning Tree Protocol (STP) with PortFast and BPDU Guard	DHCP Server	SSH (Secure Shell)
Access Control Lists (ACLs)	VoIP (Voice over IP)	WLAN (Wireless LAN)

Technologies Implemented 3

Cisco ASA Firewall

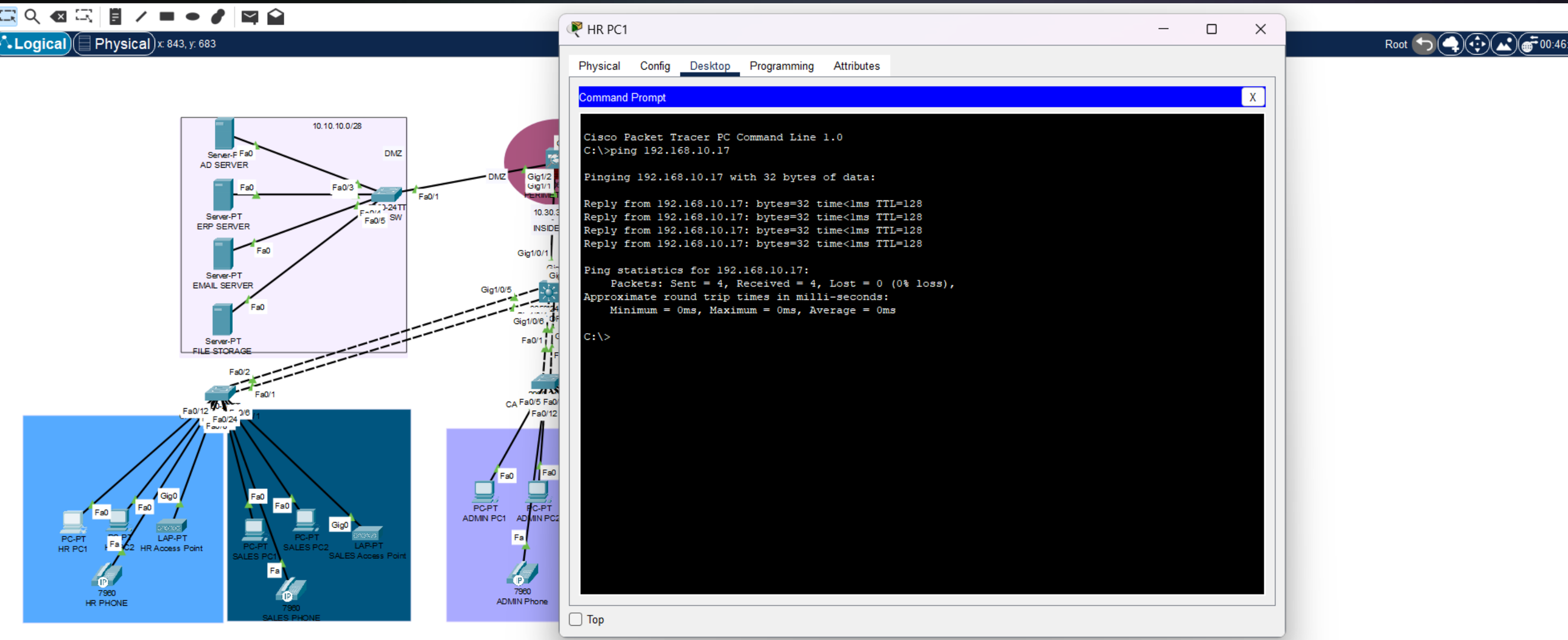
Network Address Translation (NAT)

09

Tests

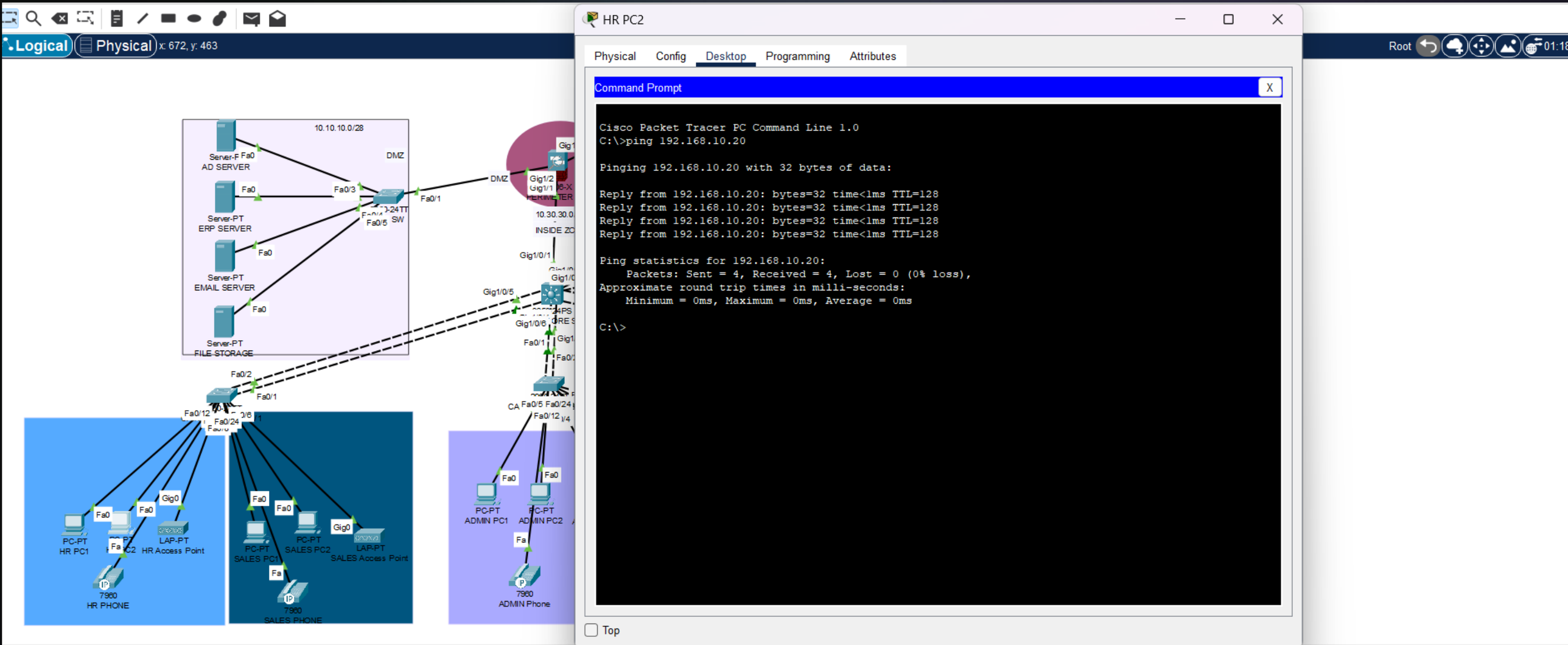
Tests

Test routing between vlan



Tests

Test routing between vlan



Thank You