

***RAW Office Building Communications
Network***

Computer Networks Project

by

Abizer Masavi E034

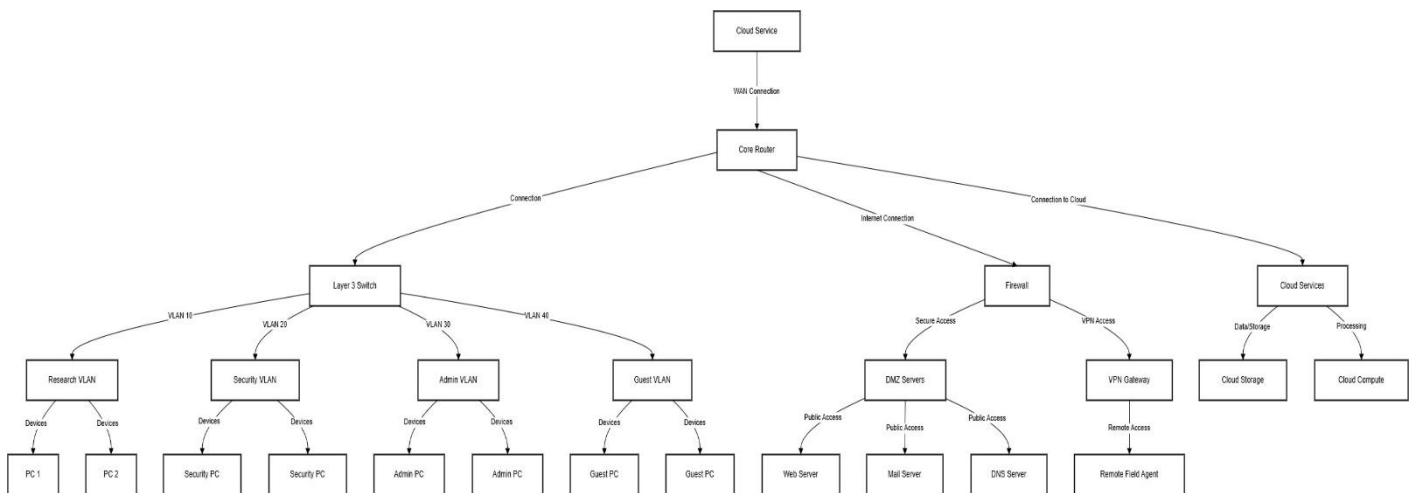
Subham Mohapatra E037

Arzaan Mulla E039

Introduction

The Research and Analysis Wing (RAW) network architecture is designed to provide a secure, scalable, and efficient infrastructure that supports the agency's critical intelligence operations. This network integrates advanced cloud-based services, VLAN segmentation, and robust security measures to safeguard sensitive data and ensure secure communication across departments and remote agents. The architecture includes firewalls, VPNs, and IDS/IPS systems to protect both internal and external communications, while enabling seamless access to resources for field agents. The network is designed for high availability and redundancy, ensuring that RAW can continue its operations without compromising security or performance.

The goal is to design a network system that supports efficient file sharing, communication tools, and access to shared resources, while considering factors like the physical layout, transmission medium, and network protocols. The proposed solutions will cover everything from network types and configurations to the choice of transmission media, IP addressing schemes, and security protocols.



Architecture for RAW office network

2. Requirements of the Case/Scenario

For the RAW office building, the following requirements are essential:

- **Departmental Communication:** Each department needs access to shared resources such as printers, files, and applications.
- **Internet Connectivity:** Employees must have access to the internet while maintaining a secure internal network.
- **Wireless Access:** The building must support wireless communication for mobile devices and laptops.
- **Server Access:** Critical services like DNS, DHCP, and file servers should be centralized to provide consistent and secure access.
- **VLAN Segmentation:** Different departments need to be separated using VLANs for network management, security, and performance optimization.
- **Scalability:** The network should be scalable to accommodate future growth, including adding more devices and departments without disrupting existing services.
- **High Availability:** Redundant paths for critical communications like servers and routers to ensure the network remains operational even if parts of it fail.

3. Types of Network Configuration Required

- **Client-Server Network Configuration:** This is the primary configuration for most of the office departments. Centralized servers will manage critical services such as file storage, printer access, DNS, and DHCP. End devices such as PCs, printers, and mobile devices will act as clients accessing these services.
- **Peer-to-Peer Configuration:** In specific areas such as smaller departments or isolated networks (e.g., IT team), peer-to-peer communication may be used for smaller-scale file sharing or direct device communication.
- **Hybrid Configuration:** In this case, the mix of client-server for departments needing centralized control (like HR, Finance, and IT) and peer-to-peer for smaller, independent groups (like the admin department) is ideal. The hybrid configuration ensures that departments with different communication needs have their appropriate setups, providing flexibility and scalability.

4. Types of Networks and Size of Networks

- **LAN (Local Area Network):** The office building fits within the LAN category, as all devices are confined within a single building or limited geographical area. The LAN will support a variety of communication protocols, high-speed data transfer, and offer centralized management.
- **VLAN Segmentation:** Since different departments (Sales, IT, Public Relations, Admin, etc.) require different network configurations, VLANs are used to segment traffic for security, performance, and ease of management. Each VLAN will have its own dedicated subnet.
- **IP Class:** The office network will use **Private IP Addressing (Class C - 192.168.x.x range)**, as the internal network does not need to be publicly routable. This ensures that there are enough IP addresses for all devices while also maintaining internal security.

Topologies with Justification

- **Star Topology for Office and Non-Critical Departments:** The star topology is ideal for RAW's general office network. In this setup, all devices, including PCs, workstations, and laptops, are connected to a central switch or router. This centralized approach simplifies network management and makes troubleshooting easier. Additionally, it allows for easy scalability as the network grows. If a single device or connection fails, it does not affect the rest of the network, which is crucial for maintaining operational continuity. Moreover, the centralized monitoring and security systems allow RAW's IT team to efficiently enforce security policies, track activity, and respond to threats in real-time.
- **Mesh Topology for Critical Systems:** A mesh topology is suitable for highly secure departments or critical network components within the RAW network, such as the server room and data storage systems. In a mesh network, each device has a direct connection to every other device, ensuring redundancy and reliable communication. This setup provides multiple paths for data to travel, reducing the risk of downtime and improving resilience. Mesh topology is particularly useful in high-traffic areas like the research network, where constant uptime is essential to process and store classified intelligence.
- **Hybrid Topology for Flexibility and Efficiency:** A hybrid topology is the most suitable for RAW, as it combines both star and mesh topologies to meet specific needs. For instance, critical departments like the security operations center or research and analysis rooms could use a mesh topology to ensure redundancy and fault tolerance. On the other hand, non-critical departments like administration or HR could implement a star topology for simplicity, cost-effectiveness, and easy management. This hybrid approach ensures that RAW's

network is both secure and efficient, meeting the requirements of both low and high-priority systems without unnecessary complexity.

6. Transmission Medium and Cost Considerations

- **Ethernet (Copper Cabling):** The most cost-effective and common solution for internal communications, using **Cat5e** or **Cat6** cables. These cables offer speeds up to 1 Gbps, which is sufficient for most office tasks such as file sharing, printing, and internet access. Ethernet also has lower installation costs and is easier to maintain.
- **Fiber Optic Cables:** Used for inter-floor or inter-building connections if high-speed communication is necessary between floors or areas with large data traffic. Although more expensive than copper, fibre optics provide significantly higher bandwidth and are more future-proof.
- **Wireless (Wi-Fi):** Wireless connectivity is used in areas like meeting rooms, employee lounges, and conference areas. Access points (APs) are strategically placed to ensure sufficient coverage. Wireless communication offers flexibility but may have limitations in terms of speed and range compared to wired connections.

7. Tentative Options for Types of Nodes Used

- **End Nodes:** These include:
 - **PCs:** Desktop computers for employees in different departments.
 - **Printers:** Network printers accessible by all departments.
 - **Smartphones and IP Phones:** Devices used by employees for communication (smartphones for mobile access and IP phones for voice communication).
- **Intermediate Nodes:** These include:
 - **Switches:** Switches serve as central nodes that manage local area traffic between devices within the same VLAN.
 - **Routers:** Routers connect different VLANs and handle inter-network traffic. They also provide routing between the office network and external networks such as the internet.
 - **Wireless Access Points (WAPs):** These devices extend the wireless network to mobile devices, allowing them to connect to the office network.

- **DMZ Servers:**

- **DNS Servers:** These servers resolve domain names to IP addresses, ensuring that employees can access websites using domain names. And helps in mail setup.
 1. **External DNS Server** - Hosted in the DMZ, these servers resolve public domain names and interact with external clients and the internet. The firewall between the DMZ and the internal network ensures that the internal DNS is protected from external threats.
 2. **Internal DNS Server** - These are hosted within RAW's internal network and are not accessible directly from the public internet. They resolve internal domain names for internal resources such as file servers, internal applications, and email servers.
- **DHCP Server:** Automatically assigns IP addresses to devices connecting to the network.
- **Email Servers:** Provide centralized access to shared files and printers across the building.
- **Web server :** Provides internal and safe email servers through mail.com on the DNS server.

8. Suggested IP Class Range with Justification

Private IP Range: 192.168.x.x:

- **VLAN 10 (Counterintelligence Division):** 192.168.10.0/24
- **VLAN 20 (Cyber Surveillance Unit):** 192.168.20.0/24
- **VLAN 30 (Strategic Operations):** 192.168.30.0/24
- **VLAN 40 (Cryptanalysis Division):** 192.168.40.0/24
- **VLAN 50 (IT and Communications):** 192.168.50.0/25
- **VLAN 60 (Server Room):** 192.168.60.0/27
- **VLAN 70 (Wireless Network):** 192.168.70.0/22

These subnets allow for up to **254 devices** in each major department, with a smaller subnet for the **Server Room** and **Wireless Network** based on their specific needs. The IP ranges ensure that the network remains private and isolated from public networks while providing sufficient address space for each department.

9. Suggested Protocol Model

- **TCP/IP Protocol Suite:** The **TCP/IP** model is the most commonly used protocol suite for office networks, offering support for reliable data transmission, routing, and internet connectivity. The **Internet Protocol (IP)** and **Transmission Control Protocol (TCP)** provide the necessary mechanisms for communication across the network, while **UDP** can be used for applications requiring faster transmission with less overhead.
- **OSI Model:** The **OSI model** helps in visualizing the network's layers, with focus on:
 - **Layer 3 (Network Layer):** IP routing between VLANs.
 - **Layer 2 (Data Link Layer):** Ethernet switches managing data link frames and MAC addressing.
 - **Layer 7 (Application Layer):** Protocols such as HTTP, FTP, and DNS to facilitate application communication within the office network.
- **Routing Protocols:** The **OSPF (Open Shortest Path First)** protocol could be employed for routing between different VLANs and for redundancy purposes within the internal network.

10. Security Features for RAW Network

Given the sensitive nature of the work handled by the Research and Analysis Wing (RAW), security is the highest priority in the network design. The network must be secure, reliable, and able to handle classified data without compromising its confidentiality, integrity, or availability. The following security features are crucial for the RAW network:

10.1 Network Segmentation with VLANs

- **VLAN Segmentation:** The network should be segmented into Virtual Local Area Networks (VLANs), isolating different departments (e.g., research, security, admin, and guest networks) to prevent unauthorized access between them. Sensitive data should reside in its own VLAN, ensuring that only authorized users can access it.
- **Security Control:** Implementing Access Control Lists (ACLs) on switches and routers ensures that each VLAN has controlled access to specific resources, minimizing the attack surface by limiting traffic flow between departments.

10.2 Firewalls

- **Perimeter Firewalls:** RAW's network should be protected by next-generation firewalls (NGFWs) such as Cisco Firepower at the network perimeter. These firewalls will inspect both incoming and outgoing traffic, enforcing security policies and blocking unauthorized access.
- **Internal Firewalls:** For additional security, internal firewalls should be deployed between VLANs to ensure strict control over intra-network communication. These firewalls act as gatekeepers, preventing unauthorized access to sensitive internal resources.
- **Web Application Firewall (WAF):** A WAF should be implemented to protect web servers and applications from common threats such as SQL injection, cross-site scripting (XSS), and DDoS attacks.

10.3 Intrusion Detection and Prevention Systems (IDS/IPS)

- **IDS/IPS:** An effective Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are essential for detecting and blocking malicious activities within the network. Snort, Suricata, or Cisco Firepower can be used to monitor and analyze network traffic for suspicious patterns, including malware, exploits, and anomalous behavior.
- **Real-time Alerts:** The IDS/IPS will send real-time alerts to the security operations center (SOC) whenever an attack is detected, enabling rapid incident response.

10.4 Virtual Private Network (VPN) for Secure Remote Access

- **VPN Gateway:** Field agents and remote workers must securely connect to the network using a VPN (Virtual Private Network). A site-to-site VPN or client-based VPN (using IPsec or SSL/TLS) ensures that communications between remote devices and the internal network are encrypted and authenticated.
- **Multi-Factor Authentication (MFA):** To ensure secure access, MFA should be implemented for remote users, requiring more than just a password for access. This adds an additional layer of protection against unauthorized access.

10.5 Zero Trust Architecture (ZTA)

- **Zero Trust Model:** A Zero Trust Architecture (ZTA) must be implemented across the entire network. This means that no device, user, or system is inherently trusted, even if it is inside the network. Every request for access to network resources must be authenticated, authorized, and encrypted.
- **Identity and Access Management (IAM):** An effective IAM system should be used to verify the identity of users and devices before granting access to any resource. Roles and permissions should be tightly controlled, with least-privilege access enforced for all users.

10.6 Data Encryption

- **Data at Rest:** All sensitive data stored on the network, whether on servers, databases, or cloud storage, should be encrypted using strong algorithms such as AES-256. This ensures that even if unauthorized access occurs, the data remains unreadable.
- **Data in Transit:** To protect data being transmitted across the network, SSL/TLS encryption should be used for web applications, email, and other communications. The VPN connection for remote workers also ensures that data in transit is encrypted.
- **Disk Encryption:** Devices used by field agents and other employees, including laptops and mobile phones, should have full disk encryption (e.g., BitLocker or FileVault) to protect against data theft or loss.

10.7 Access Control and Monitoring

- **Role-Based Access Control (RBAC):** Users should be granted access based on their role within the organization. For example, administrative users may have broader access, while researchers may only have access to certain data sets. This ensures that sensitive information is only accessible by authorized personnel.
- **Physical Access Control:** Biometric authentication (e.g., fingerprint scanners or facial recognition) should be implemented for physical access to data centers, server rooms, and other secure areas. Badge-based entry systems can also be used to monitor and restrict physical access.
- **Continuous Monitoring and Logging:** Security Information and Event Management (SIEM) tools should be used to monitor all network activity and generate real-time alerts. Centralized logging of security events is essential for forensic analysis, incident response, and compliance with regulatory standards.

10.8 DNS Security and Protection

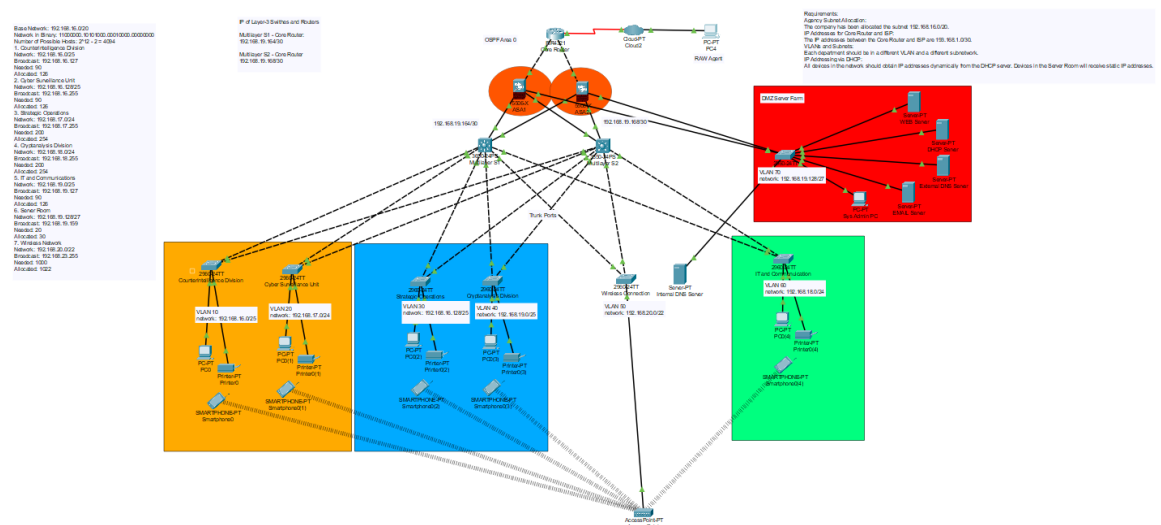
- **DNSSEC:** The use of DNS Security Extensions (DNSSEC) is crucial for protecting the network from DNS spoofing and cache poisoning attacks. By ensuring that DNS queries and responses are authentic and integrity-protected, RAW can prevent cybercriminals from redirecting users to malicious sites.
- **DNS Filtering:** Use DNS filtering to block access to known malicious websites and prevent users from accidentally visiting phishing sites or downloading malware.

10.9 Cloud Security and Compliance

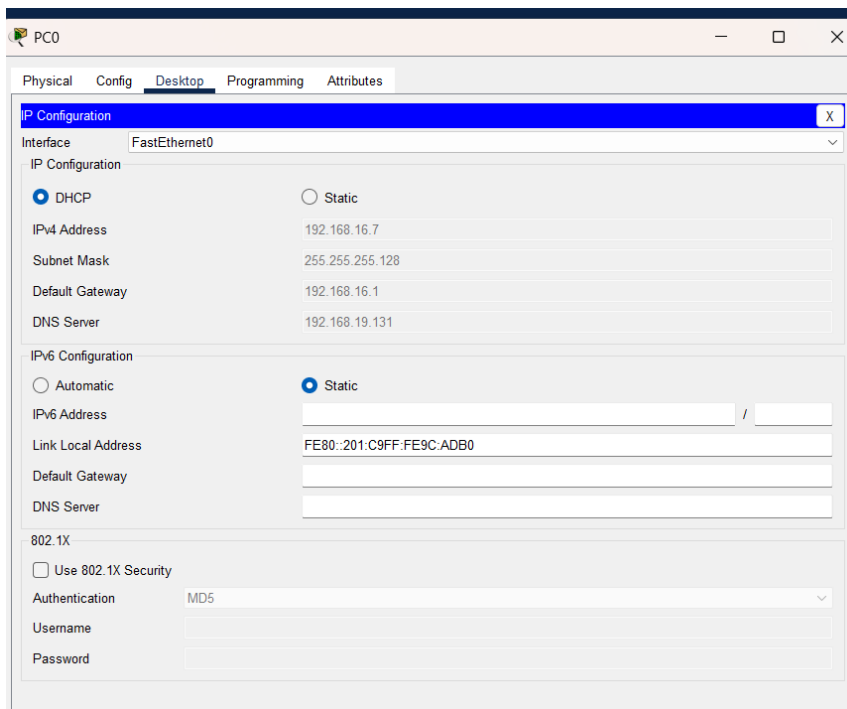
- **Cloud Access Security Broker (CASB):** RAW can use a CASB to monitor and enforce security policies for cloud-based services, ensuring that only authorized applications and services are used by employees. A CASB can also help with data loss prevention (DLP) and ensure compliance with security policies.
- **Cloud Data Encryption:** All cloud-based storage should be encrypted, and access should be controlled via IAM policies. Multi-factor authentication (MFA) should be required for accessing cloud resources to prevent unauthorized access.
- **Cloud Firewall:** Ensure that a cloud firewall is implemented to protect public-facing services in the DMZ and restrict access to critical resources within the internal network.

11. Screenshots and Visual Representation of the Network

1. **Screenshot 1:** Entire Network Map in Cisco Packet Tracer showing the connection between departments, switches, and routers.



2. Screenshot 2: PC0 IP configuration



The screenshot shows the 'PC0' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is highlighted in blue. The 'Interface' dropdown is set to 'FastEthernet0'. Under 'IP Configuration', the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The fields for IPv4 Address, Subnet Mask, Default Gateway, and DNS Server are populated with the values 192.168.16.7, 255.255.255.128, 192.168.16.1, and 192.168.19.131 respectively. Under 'IPv6 Configuration', the 'Automatic' radio button is unselected and the 'Static' radio button is selected. The fields for IPv6 Address, Link Local Address, Default Gateway, and DNS Server are empty. The 'Link Local Address' field contains the value FE80::201:C9FF:FE9C:ADB0. Under '802.1X', the 'Use 802.1X Security' checkbox is unselected. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.16.7

Subnet Mask 255.255.255.128

Default Gateway 192.168.16.1

DNS Server 192.168.19.131

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FE9C:ADB0

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

3. Screenshot 3: Router configurations for VLAN routing and DHCP server settings.

The screenshot displays the configuration interface for a Core Router. The interface is divided into several sections:

- Physical** (selected), **Config**, **CLI**, and **Attributes** tabs.
- GLOBAL** section: Includes **Settings**, **Algorithm Settings**, **ROUTING** (with **Static** and **RIP** sub-sections), **SWITCHING**, **VLAN Database**, and **INTERFACE**.
- INTERFACE** section: Lists **GigabitEthernet0/0/0**, **GigabitEthernet0/0/1**, **Serial0/1/0**, and **Serial0/1/1**.
- GigabitEthernet0/0/0** configuration details:
 - Port Status**: ☒ On
 - Bandwidth**: ☒ 1000 Mbps, ☐ 100 Mbps, ☐ 10 Mbps, ☒ Auto
 - Duplex**: ☐ Half Duplex, ☒ Full Duplex, ☒ Auto
 - MAC Address**: 0060.5C02.A401
 - IP Configuration**:
 - IPv4 Address**: 192.168.19.166
 - Subnet Mask**: 255.255.255.252
 - Tx Ring Limit**: 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

☐ Tnn

Core Router

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

SWITCHING

- VLAN Database

INTERFACE

- GigabitEthernet0/0/0
- GigabitEthernet0/0/1**
- Serial0/1/0
- Serial0/1/1

GigabitEthernet0/0/1

Port Status ☒ On

Bandwidth ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.5C02.A402

IP Configuration

IPv4 Address 192.168.19.170

Subnet Mask 255.255.255.252

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
```

☐ Top

Core Router

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

SWITCHING

- VLAN Database

INTERFACE

- GigabitEthernet0/0/0
- GigabitEthernet0/0/1
- Serial0/1/0**
- Serial0/1/1

Serial0/1/0

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 64000

IP Configuration

IPv4 Address 193.168.1.1

Subnet Mask 255.255.255.252

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
```

☐ Top

DHCP Server

Physical
Config
Services
Desktop
Programming
Attributes

SERVICES
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP

DHCP
Interface: FastEthernet0
Service: On
Pool Name: Counterintelligence Division Pool
Default Gateway: 192.168.16.1
DNS Server: 192.168.19.131
Start IP Address: 192.168.16.16
Subnet Mask: 255.255.255.128
Maximum Number of Users: 90
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0

Add
Save
Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Server Room Pool	192.168.19.129	192.168.19.131	192.168.19.135	255.255.255.224	20	0.0.0.0	0.0.0.0
IT and Communications Pool	192.168.16.129	192.168.19.131	192.168.16.134	255.255.255.128	90	0.0.0.0	0.0.0.0
Cryptanalysis Division Pool	192.168.18.1	192.168.19.131	192.168.18.6	255.255.255.0	200	0.0.0.0	0.0.0.0
Strategic Operations Pool	192.168.17.1	192.168.19.131	192.168.17.6	255.255.255.0	200	0.0.0.0	0.0.0.0
Counterintelligence Division Pool	192.168.16.1	192.168.19.131	192.168.16.6	255.255.255.128	90	0.0.0.0	0.0.0.0
Cyber Surveillance UnitPool	192.168.19.1	192.168.19.131	192.168.19.6	255.255.255.128	90	0.0.0.0	0.0.0.0
wirelessPool	192.168.19.161	192.168.19.131	192.168.20.6	255.255.252.0	1000	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.19.128	255.255.255.224	31	0.0.0.0	0.0.0.0

Top

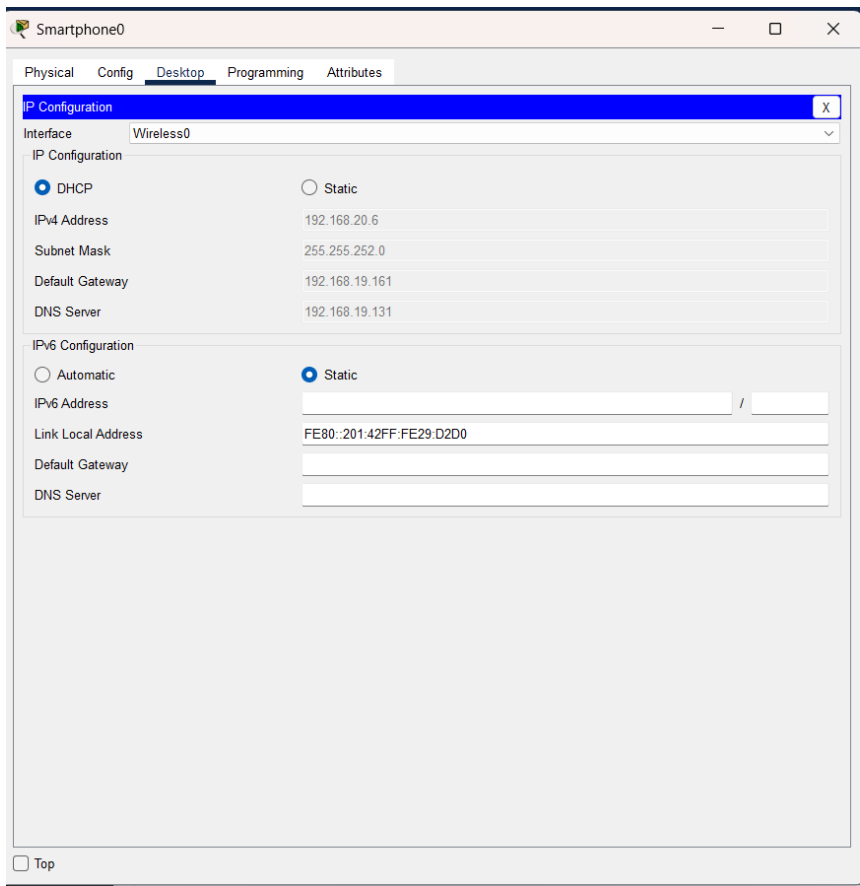
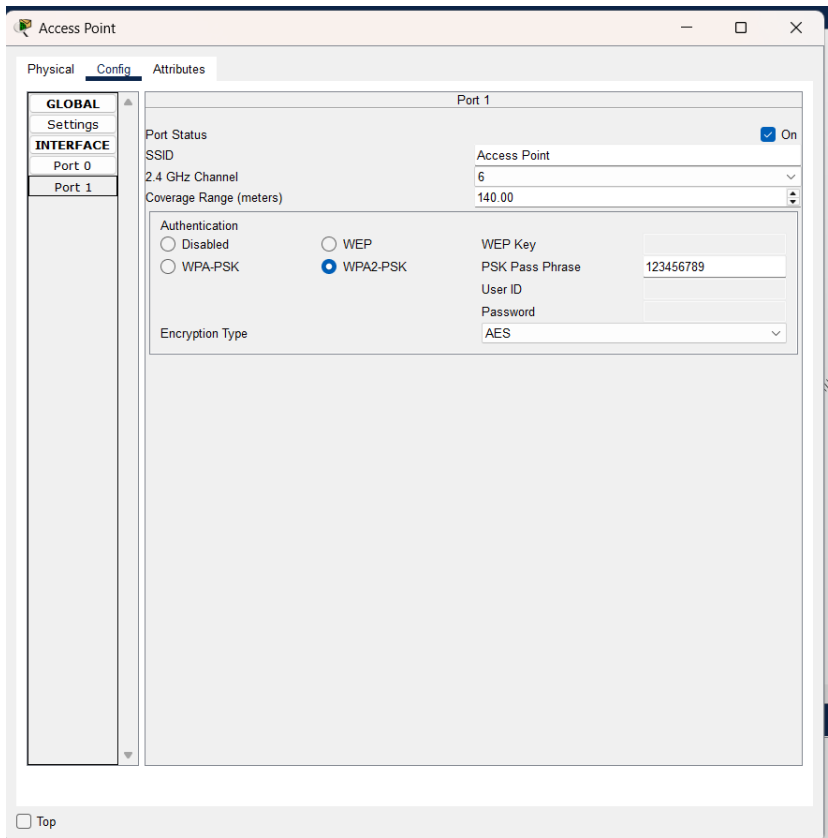
DHCP Server

Physical
Config
Services
Desktop
Programming
Attributes

IP Configuration

IP Configuration
DHCP
Static
IPv4 Address: 192.168.19.130
Subnet Mask: 255.255.255.224
Default Gateway: 192.168.19.129
DNS Server: 192.168.19.131
IPv6 Configuration
Automatic
Static
IPv6 Address:
Link Local Address: FE80::2E0:F7FF:FE2E:C309
Default Gateway:
DNS Server:
802.1X
Use 802.1X Security
Authentication: MD5
Username:
Password:

4. **Screenshot 4:** Wireless Access Points (WAPs) placement and configuration for mobile device access.



5. Screenshot 5: Message simulation inter department and intra department

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC0(1)	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0(1)	PC0(2)	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0(2)	PC0(3)	ICMP		0.000	N	2	(edit)	(delete)

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.083	--	Multilayer S1	STP
	0.083	--	Multilayer S1	STP
	0.084	--	Multilayer S1	STP
	0.084	--	Multilayer S1	STP
	0.084	--	Multilayer S1	STP
	0.084	--	Multilayer S1	STP
	0.084	--	Multilayer S1	STP
	0.084	Multilayer S1	Strategic Operations	STP
	0.084	Multilayer S1	Cyber Surveillance Unit	STP
	0.084	Multilayer S1	Counterintelligence Division	STP
	0.084	Multilayer S1	Wireless Connection	STP
	0.084	Multilayer S1	Server Room	STP
	0.084	Multilayer S1	Cryptanalysis Division	STP
	0.084	Multilayer S1	IT and Communication	STP
	0.084	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	--	Multilayer S1	STP
	0.085	Multilayer S1	Strategic Operations	STP
	0.085	Multilayer S1	Cyber Surveillance Unit	STP

Reset Simulation

☒ Constant Delay

Captured to: 0.086 s

Play Controls

Event List Filters - Visible Events

ACL Filter, Bluetooth, CAPWAP, CDP, DHCPv6, DNS, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPFv6, PaGP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RiPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters

Show All/None

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.085	Multilayer S1	Counterintelligence Division	STP
	0.085	Multilayer S1	Wireless Connection	STP
	0.085	Multilayer S1	Server Room	STP
	0.085	Multilayer S1	Cryptanalysis Division	STP
	0.085	Multilayer S1	IT and Communication	STP
	0.085	Counterintelligence Division	Multilayer S2	STP
	0.085	Counterintelligence Division	PC0	STP
	0.085	Counterintelligence Division	Printer0	STP
	0.085	--	Multilayer S1	STP
	0.086	--	Strategic Operations	STP
	0.086	--	Cyber Surveillance Unit	STP
	0.086	--	Counterintelligence Division	STP
	0.086	--	Server Room	STP
	0.086	Multilayer S1	Strategic Operations	STP
	0.086	Multilayer S1	Cyber Surveillance Unit	STP
	0.086	Multilayer S1	Counterintelligence Division	STP
	0.086	Multilayer S1	Wireless Connection	STP
	0.086	Multilayer S1	Server Room	STP
	0.086	Multilayer S1	Cryptanalysis Division	STP
	0.086	Multilayer S1	IT and Communication	STP
	0.086	Strategic Operations	Multilayer S2	STP
	0.086	Cyber Surveillance Unit	Multilayer S2	STP
	0.086	Counterintelligence Division	Multilayer S2	STP
	0.086	Server Room	Multilayer S2	STP

Reset Simulation

☒ Constant Delay

Captured to: 0.086 s

Play Controls

Event List Filters - Visible Events

ACL Filter, Bluetooth, CAPWAP, CDP, DHCPv6, DNS, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPFv6, PaGP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RiPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters

Show All/None

Simulation Panel

Event List

Vis	Time(sec)	Last Device	At Device	Type
	0.086	--	Strategic Operations	STP
	0.086	--	Cyber Surveillance Unit	STP
	0.086	--	Counterintelligence Division	STP
	0.086	--	Server Room	STP
	0.086	Multilayer S1	Strategic Operations	STP
	0.086	Multilayer S1	Cyber Surveillance Unit	STP
	0.086	Multilayer S1	Counterintelligence Division	STP
	0.086	Multilayer S1	Wireless Connection	STP
	0.086	Multilayer S1	Server Room	STP
	0.086	Multilayer S1	Cryptanalysis Division	STP
	0.086	Multilayer S1	IT and Communication	STP
	0.086	Strategic Operations	Multilayer S2	STP
	0.086	Cyber Surveillance Unit	Multilayer S2	STP
	0.086	Counterintelligence Division	Multilayer S2	STP
	0.086	Server Room	Multilayer S2	STP
	0.086	Cryptanalysis Division	Multilayer S2	STP
	0.086	Multilayer S2	Cyber Surveillance Unit	STP
	0.086	Multilayer S2	Strategic Operations	STP
	0.086	Multilayer S2	Cryptanalysis Division	STP
	0.086	Multilayer S2	IT and Communication	STP
	0.086	Multilayer S2	Server Room	STP
	0.086	Multilayer S2	Wireless Connection	STP
	0.086	--	Cryptanalysis Division	STP

Reset Simulation
☒ Constant Delay
Captured to: 0.086 s

Play Controls

Event List Filters - Visible Events

ACL Filter, Bluetooth, CAPWAP, CDP, DHCPv6, DNS, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RiPing, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters

Show All/None

6. Screenshot 6: Multilayer switches configurations.

```

Device Name: Multilayer Switch 1
Device Model: 3650-24PS
Hostname: Switch

Port                Link    VLAN    IP Address      IPv6 Address      MAC Address
GigabitEthernet1/0/1    Up      1       192.168.19.165/30 <not set>         0060.47C7.7901
GigabitEthernet1/0/2    Up      --      <not set>        <not set>         0060.47C7.7902
GigabitEthernet1/0/3    Up      --      <not set>        <not set>         0060.47C7.7903
GigabitEthernet1/0/4    Up      --      <not set>        <not set>         0060.47C7.7904
GigabitEthernet1/0/5    Up      --      <not set>        <not set>         0060.47C7.7905
GigabitEthernet1/0/6    Up      --      <not set>        <not set>         0060.47C7.7906
GigabitEthernet1/0/7    Up      --      <not set>        <not set>         0060.47C7.7907
GigabitEthernet1/0/8    Up      --      <not set>        <not set>         0060.47C7.7908
GigabitEthernet1/0/9    Down    --      <not set>        <not set>         0060.47C7.7909
GigabitEthernet1/0/10   Down    --      <not set>        <not set>         0060.47C7.790A
GigabitEthernet1/0/11   Down    --      <not set>        <not set>         0060.47C7.790B
GigabitEthernet1/0/12   Down    --      <not set>        <not set>         0060.47C7.790C
GigabitEthernet1/0/13   Down    --      <not set>        <not set>         0060.47C7.790D
GigabitEthernet1/0/14   Down    --      <not set>        <not set>         0060.47C7.790E
GigabitEthernet1/0/15   Down    --      <not set>        <not set>         0060.47C7.790F
GigabitEthernet1/0/16   Down    --      <not set>        <not set>         0060.47C7.7910
GigabitEthernet1/0/17   Down    --      <not set>        <not set>         0060.47C7.7911
GigabitEthernet1/0/18   Down    --      <not set>        <not set>         0060.47C7.7912
GigabitEthernet1/0/19   Down    --      <not set>        <not set>         0060.47C7.7913
GigabitEthernet1/0/20   Down    --      <not set>        <not set>         0060.47C7.7914
GigabitEthernet1/0/21   Down    --      <not set>        <not set>         0060.47C7.7915
GigabitEthernet1/0/22   Down    --      <not set>        <not set>         0060.47C7.7916
GigabitEthernet1/0/23   Down    --      <not set>        <not set>         0060.47C7.7917
GigabitEthernet1/0/24   Down    --      <not set>        <not set>         0060.47C7.7918
GigabitEthernet1/1/1    Down    1       <not set>        <not set>         0090.2BE3.C801
GigabitEthernet1/1/2    Down    1       <not set>        <not set>         0090.2BE3.C802
GigabitEthernet1/1/3    Down    1       <not set>        <not set>         0090.2BE3.C803
GigabitEthernet1/1/4    Down    1       <not set>        <not set>         0090.2BE3.C804
Vlan1                  Down    1       <not set>        <not set>         0001.9750.77DD
Vlan10                  Up      10      192.168.16.1/25   <not set>         0001.9750.7701
Vlan20                  Up      20      192.168.17.1/24   <not set>         0001.9750.7702
Vlan30                  Up      30      192.168.16.129/25 <not set>         0001.9750.7703
Vlan40                  Up      40      192.168.19.1/25   <not set>         0001.9750.7704
Vlan50                  Up      50      192.168.20.1/22   <not set>         0001.9750.7705
Vlan60                  Up      60      192.168.18.1/24   <not set>         0001.9750.7706
Vlan70                  Up      70      192.168.19.129/27 <not set>         0001.9750.7707

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Multilayer Switch 1

```

Device Name: Multilayer S2
Device Model: 3650-24PS
Hostname: Switch

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet1/0/1	Up	1	192.168.19.169/30	<not set>	000D.BDBA.8801
GigabitEthernet1/0/2	Up	--	<not set>	<not set>	000D.BDBA.8802
GigabitEthernet1/0/3	Up	--	<not set>	<not set>	000D.BDBA.8803
GigabitEthernet1/0/4	Up	--	<not set>	<not set>	000D.BDBA.8804
GigabitEthernet1/0/5	Up	--	<not set>	<not set>	000D.BDBA.8805
GigabitEthernet1/0/6	Up	--	<not set>	<not set>	000D.BDBA.8806
GigabitEthernet1/0/7	Up	--	<not set>	<not set>	000D.BDBA.8807
GigabitEthernet1/0/8	Up	--	<not set>	<not set>	000D.BDBA.8808
GigabitEthernet1/0/9	Down	--	<not set>	<not set>	000D.BDBA.8809
GigabitEthernet1/0/10	Down	--	<not set>	<not set>	000D.BDBA.880A
GigabitEthernet1/0/11	Down	--	<not set>	<not set>	000D.BDBA.880B
GigabitEthernet1/0/12	Down	--	<not set>	<not set>	000D.BDBA.880C
GigabitEthernet1/0/13	Down	--	<not set>	<not set>	000D.BDBA.880D
GigabitEthernet1/0/14	Down	--	<not set>	<not set>	000D.BDBA.880E
GigabitEthernet1/0/15	Down	--	<not set>	<not set>	000D.BDBA.880F
GigabitEthernet1/0/16	Down	--	<not set>	<not set>	000D.BDBA.8810
GigabitEthernet1/0/17	Down	--	<not set>	<not set>	000D.BDBA.8811
GigabitEthernet1/0/18	Down	--	<not set>	<not set>	000D.BDBA.8812
GigabitEthernet1/0/19	Down	--	<not set>	<not set>	000D.BDBA.8813
GigabitEthernet1/0/20	Down	--	<not set>	<not set>	000D.BDBA.8814
GigabitEthernet1/0/21	Down	--	<not set>	<not set>	000D.BDBA.8815
GigabitEthernet1/0/22	Down	--	<not set>	<not set>	000D.BDBA.8816
GigabitEthernet1/0/23	Down	--	<not set>	<not set>	000D.BDBA.8817
GigabitEthernet1/0/24	Down	--	<not set>	<not set>	000D.BDBA.8818
GigabitEthernet1/1/1	Down	1	<not set>	<not set>	0060.47DB.DA01
GigabitEthernet1/1/2	Down	1	<not set>	<not set>	0060.47DB.DA02
GigabitEthernet1/1/3	Down	1	<not set>	<not set>	0060.47DB.DA03
GigabitEthernet1/1/4	Down	1	<not set>	<not set>	0060.47DB.DA04
Vlan1	Down	1	<not set>	<not set>	0001.C929.C96E
Vlan10	Up	10	192.168.16.1/25	<not set>	0001.C929.C901
Vlan20	Up	20	192.168.17.1/24	<not set>	0001.C929.C902
Vlan30	Up	30	192.168.16.129/25	<not set>	0001.C929.C903
Vlan40	Up	40	192.168.19.1/25	<not set>	0001.C929.C904
Vlan50	Up	50	192.168.20.1/22	<not set>	0001.C929.C905
Vlan60	Up	60	192.168.18.1/24	<not set>	0001.C929.C906
Vlan70	Up	70	192.168.19.129/27	<not set>	0001.C929.C907

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Multilayer S2

7. DNS Server :

DNS Server

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type

Address

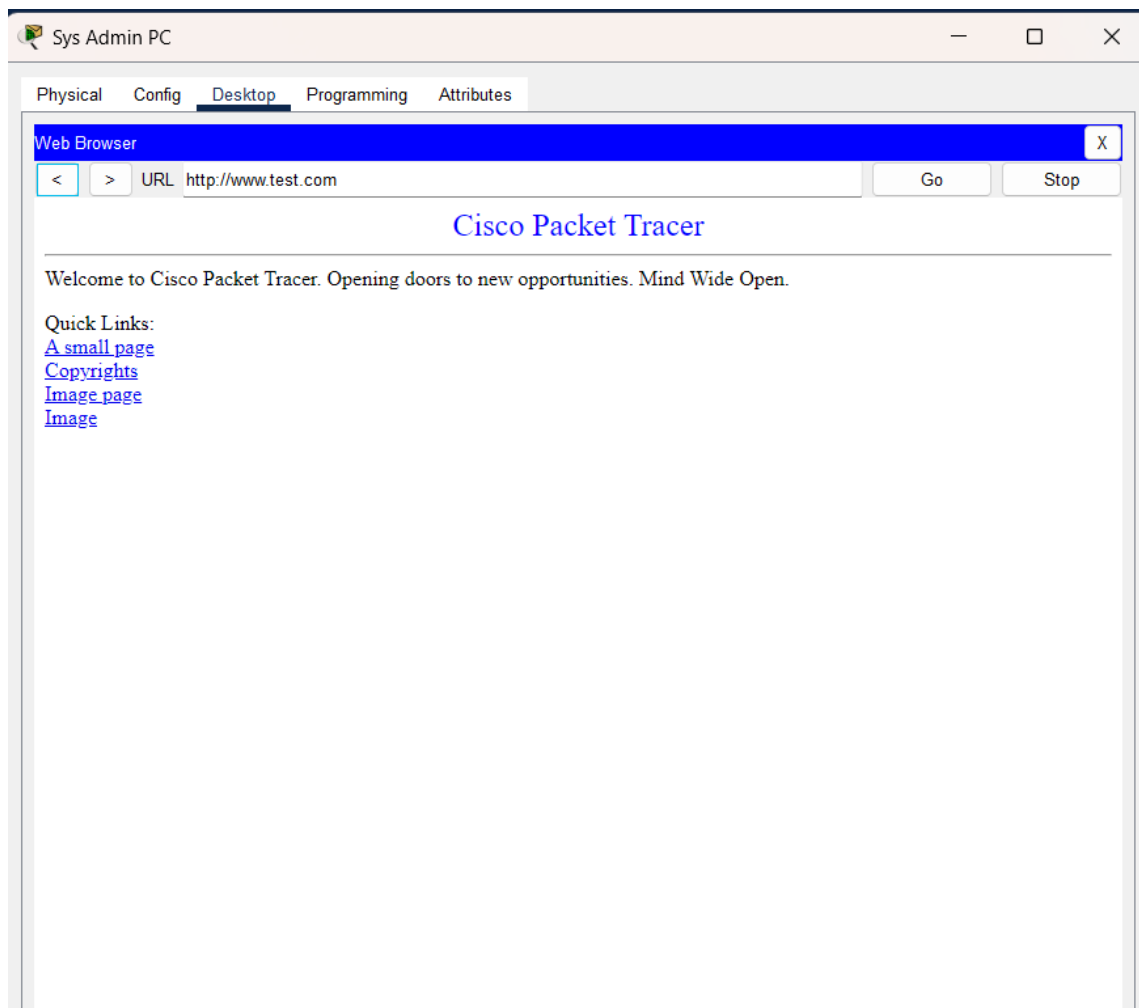
Add

Save

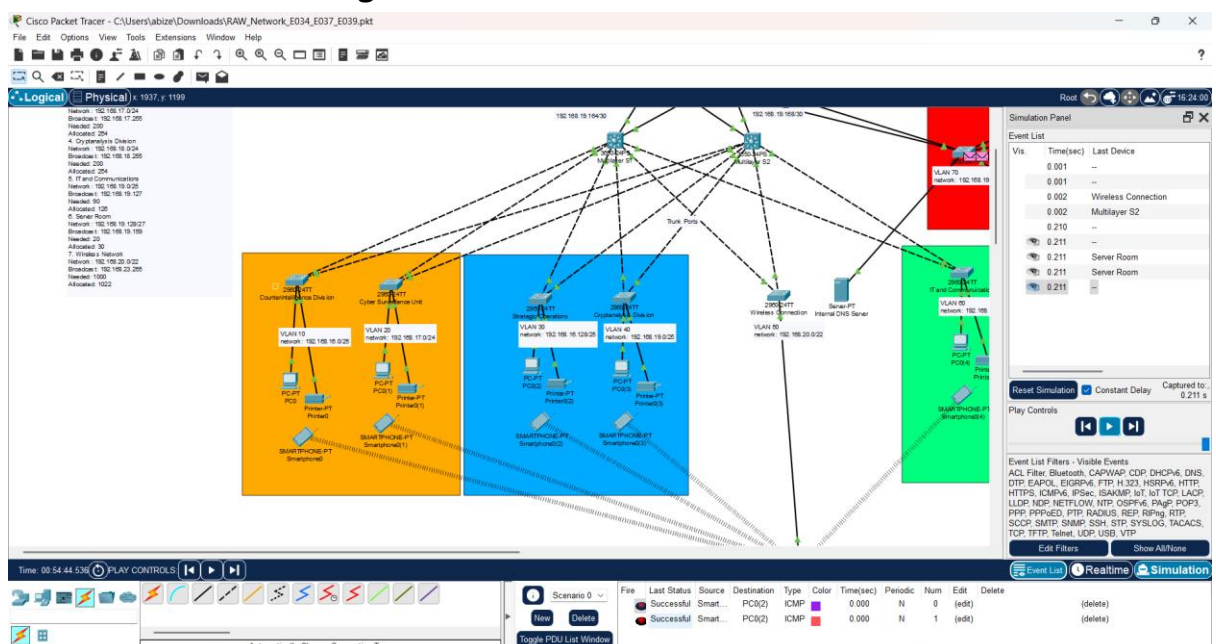
Remove

No.	Name	Type	Detail
0	www.test.com	A Record	192.168.19.131

DNS Cache



8. Wireless to wired Message



Cisco Packet Tracer - C:\Users\abize\Downloads\RAW_Network_E034_E037_E039.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1198, y: 230

Physical Config CLI Attributes

IOS Command Line Interface

```
PERIMETER-FW(config-if)#int g1/2
PERIMETER-FW(config-if)#ip address 192.168.19.169 255.255.255.252
PERIMETER-FW(config-if)#invalid password
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#interface GigabitEthernet1/1
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#interface GigabitEthernet1/2
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config-if)#
PERIMETER-FW(config)#interface GigabitEthernet1/3
PERIMETER-FW(config-if)#invalid password
PERIMETER-FW(config-if)#exit
PERIMETER-FW(config)#interface GigabitEthernet1/1
PERIMETER-FW(config-if)#ip address 192.168.19.165 255.255.255.252
PERIMETER-FW(config-if)#access denied.
PERIMETER-FW(config)#int g1/1
PERIMETER-FW(config-if)#nameif INSIDE
INFO: Security level for "INSIDE" set to 0 by default.
PERIMETER-FW(config-if)#security-level 100
PERIMETER-FW(config-if)#int g1/4
PERIMETER-FW(config-if)#access denied.
PERIMETER-FW(config)#
PERIMETER-FW(config)#interface GigabitEthernet1/4
PERIMETER-FW(config-if)#no shutdown
PERIMETER-FW(config-if)#access denied.
PERIMETER-FW(config-if)#int g1/4
PERIMETER-FW(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
PERIMETER-FW(config-if)#security-level 50
PERIMETER-FW(config-if)#int g1/3
ALINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/3, changed state to down
% Invalid input detected at '^' marker.
PERIMETER-FW(config-if)#int g1/3
PERIMETER-FW(config-if)#nameif Outside
INFO: Security level for "Outside" set to 0 by default.
PERIMETER-FW(config-if)#
```

Copy Paste

Automatically Choose Connection Type

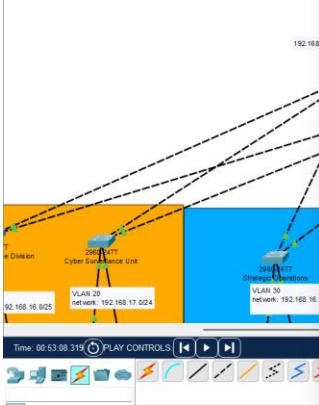
Time: 00:53:08.318 PLAY CONTROLS

Event List Realtime Simulation

Periodic Num Edit Delete (delete)

Root

Agency Subnet Allocation
The company has been allocated the subnet 192.168.16.0/20.
IP Addresses for Core Router and ISP
The IP addresses between the Core Router and ISP are 192.168.1.0
VLANs and Subnets.
Each department should be in a different VLAN and a different subnet
IP Addressing via DHCP.
All devices in the network should obtain IP addresses dynamically.



Cisco Packet Tracer - C:\Users\abize\Downloads\RAW_Network_E034_E037_E039.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1526, y: 191

Physical Config CLI Attributes

IOS Command Line Interface

```
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#ip address 192.168.19.16 255.255.255.252
ciscoasa(config-if)#ip address 192.168.19.169 255.255.255.252
ciscoasa(config-if)#ciscoasa#ciscoasa#
ciscoasa(config)#configure terminal
ciscoasa(config)#interface GigabitEthernet1/4
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#ciscoasa#
ciscoasa#int g1/1
% Invalid input detected at '^' marker.
ciscoasa#config t
ciscoasa(config)#int g1/2
ciscoasa(config-if)#nameif INSIDE1
INFO: Security level for "INSIDE1" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1/1
ciscoasa(config-if)#nameif INSIDE2
INFO: Security level for "INSIDE2" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1/4
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#int g1/3
ciscoasa(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#
```

Copy Paste

Automatically Choose Connection Type

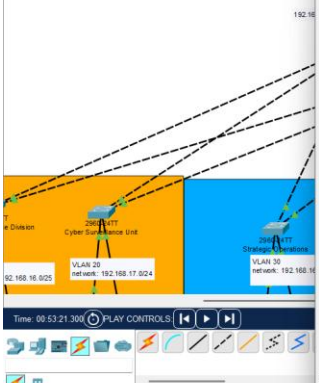
Time: 00:53:21.304 PLAY CONTROLS

Event List Realtime Simulation

Periodic Num Edit Delete (delete)

Root

Agency Subnet Allocation
The company has been allocated the subnet 192.168.16.0/20.
IP Addresses for Core Router and ISP
The IP addresses between the Core Router and ISP are 192.168.1.0
VLANs and Subnets.
Each department should be in a different VLAN and a different subnet
IP Addressing via DHCP.
All devices in the network should obtain IP addresses dynamically.



Cisco Packet Tracer - C:\Users\abize\Downloads\RAW_Network_E034_E037_E039.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x 696, y 78

Time: 00:53:21.300 [PLAY CONTROLS]

ASAS

Physical Config CLI Attributes

IOS Command Line Interface

```

ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#ip address 192.168.19.16 255.255.255.252
ciscoasa(config-if)#ip address 192.168.19.169 255.255.255.252
ciscoasa(config-if)#ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/4
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#ciscoasa#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/4, changed state to down
ciscoasa#int g1g1/1

% Invalid input detected at '''' marker.

ciscoasa#config t
ciscoasa(config)#int g1g1/2
ciscoasa(config-if)#nameif INSIDE1
INFO: Security level for "INSIDE1" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1g1/1
ciscoasa(config-if)#nameif INSIDE2
INFO: Security level for "INSIDE2" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1g1/4
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#int g1g1/3
ciscoasa(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#for mem
Building configuration...
Cryptochecksum: 06f6085 2175507b 1d691560 0311239a
1143 bytes copied in 2.087 secs (547 bytes/sec)
[OK]
ciscoasa(config-if)#

```

Copy Paste

Event List Realtime Simulation

Delete (delete)

Cisco Packet Tracer - C:\Users\abize\Downloads\RAW_Network_E034_E037_E039.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x 1054, y 580

Time: 00:53:21.300 [PLAY CONTROLS]

ASAS

Physical Config CLI Attributes

IOS Command Line Interface

```

ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1g1/1
ciscoasa(config-if)#nameif INSIDE1
INFO: Security level for "INSIDE1" set to 0 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#int g1g1/4
ciscoasa(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#int g1g1/3
ciscoasa(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)#for mem
Building configuration...
Cryptochecksum: 06f6085 2175507b 1d691560 0311239a
1143 bytes copied in 2.087 secs (547 bytes/sec)
[OK]
ciscoasa(config-if)#sh start
% Saved
% Written by enable_15 at 00:53:20 UTC Mar 1 1993
% Call-home enabled from prompt by enable_15 at 00:53:20 UTC Mar 1 1993
ASA Version 9.6(1)
!
hostname ciscoasa
names
!
interface GigabitEthernet1/1
nameif INSIDE2
security-level 100
ip address 192.168.19.165 255.255.255.252
!
interface GigabitEthernet1/2
nameif INSIDE1
security-level 100
ip address 192.168.19.169 255.255.255.252
!
interface GigabitEthernet1/3
nameif OUTSIDE
security-level 0
!
None

```

Copy Paste

Event List Realtime Simulation

Delete (delete)

Cisco Packet Tracer - C:\Users\yabize\Downloads\RAW_Network_E034_E037_E039.pkt

File Edit Options View Tools Extensions Window Help

Logical Physical x 200, y 100

ASA7

Physical Config CLI Attributes

IOS Command Line Interface

```
Invalid input detected at '^' marker.
PERIMETER-FW(config-if)#int gig1/3
PERIMETER-FW(config-if)#nameif Outside
INFO: Security level for "Outside" set to 0 by default.
PERIMETER-FW(config-if)#int gig1/2
PERIMETER-FW(config-if)#nameif INSIDE
ERROR: Name "INSIDE" has been assigned to interface GigabitEthernet1/1
PERIMETER-FW(config-if)#nameif INSIDE2
INFO: Security level for "INSIDE2" set to 0 by default.
PERIMETER-FW(config-if)#security-level 100
PERIMETER-FW(config-if)#we BEM
Building configuration...
Cryptochecksum: 5b1833ba 6606372 73d1078 24850794
1236 bytes copied in 3.472 secs (500 bytes/sec)
[OK]
PERIMETER-FW(config-if)#sh start
!
Written by enable_15 at 09:39:05 UTC Apr 16 2025
!
Call-home enabled from prompt by enable_15 at 09:39:05 UTC Apr 16 2025
!
ASA Version 9.6(1)
!
hostname PERIMETER-FW
enable password KFFa9ovs14ULc5GD encrypted
nameif
!
interface GigabitEthernet1/1
nameif INSIDE
security-level 100
ip address 192.168.19.169 255.255.255.252
!
interface GigabitEthernet1/2
nameif INSIDE2
security-level 100
ip address 192.168.19.169 255.255.255.252
!
interface GigabitEthernet1/3
nameif Outside
!
More
```

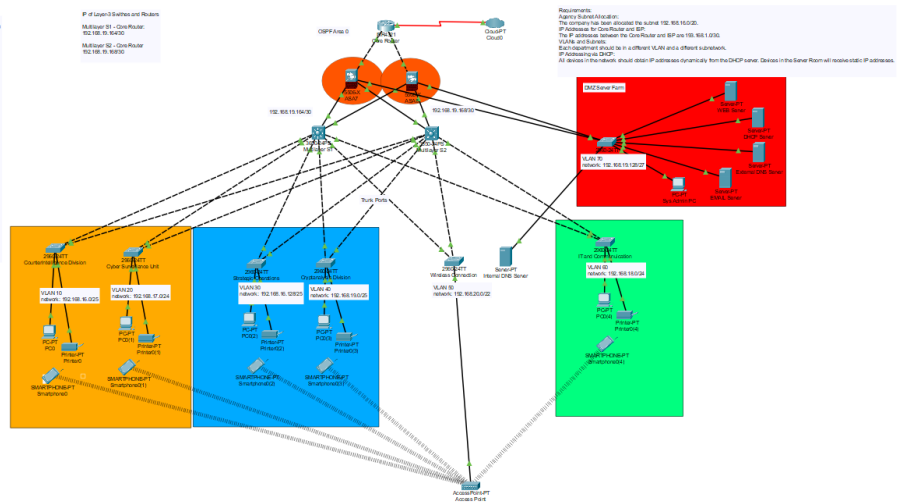
Time: 00:53:21.390 PLAY CONTROLS

Automatically Choose Connection Type

Root

Event List Realtime Simulation

Delete (delete)



10. Web server and Email server setup

WEB Server

Physical

Config

Services

Desktop

Programming

Attributes

IP Configuration

IP Configuration

☒ DHCP

☐ Static

IPv4 Address

192.168.19.129

Subnet Mask

255.255.255.224

Default Gateway

0.0.0.0

DNS Server

192.168.19.131

IPv6 Configuration

☒ Automatic

☐ Static

IPv6 Address

/

Link Local Address

FE80::2E0:8FFF:FE80:29B5

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

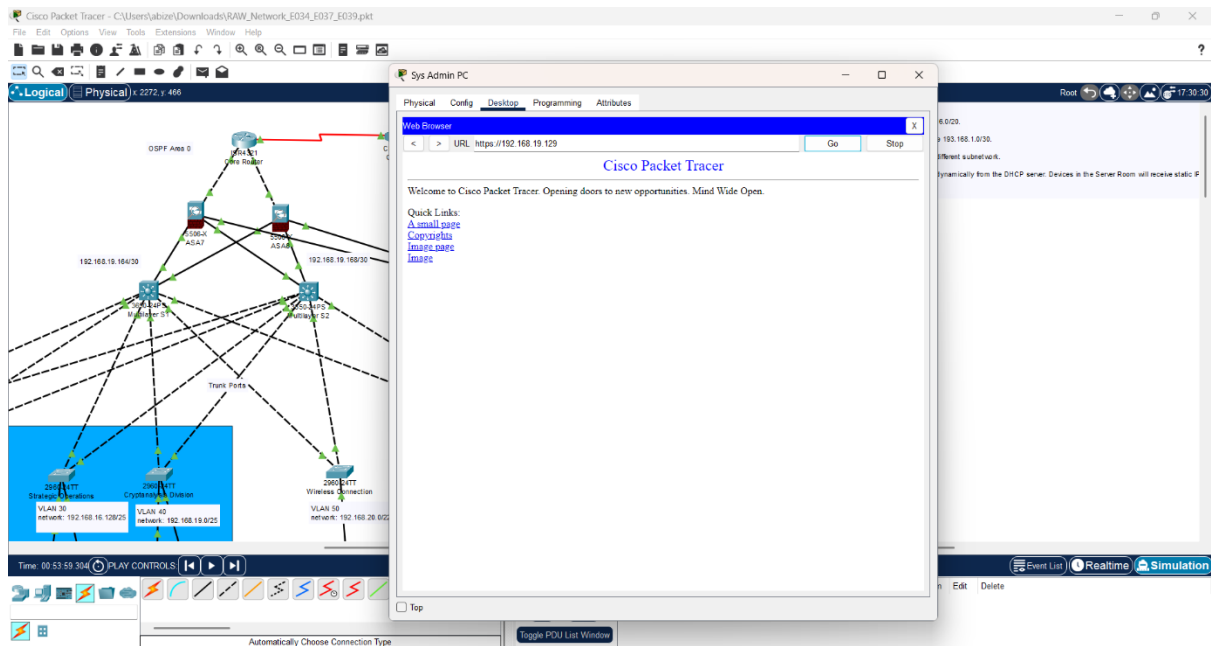
Authentication

MD5

Username

Password

☐ Top



EMAIL Server

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

EMAIL

SMTP Service

ON

OFF

POP3 Service

ON

OFF

Domain Name: mailcom

Set

User Setup

User

Password

client1

client2

+

-

Change

Password

Top

11. Firewall

In this network design, firewalls play a critical role in securing the internal network, the Demilitarized Zone (DMZ), and external sources like the internet. The configuration of the interfaces on the firewalls (ASA 5506-X devices) defines the trust levels for different network segments:

1. Internal Network (Gig1/1 and Gig1/2):

- **Gig1/1** is configured as an **internal trusted interface** with a **security level of 100**. This interface connects to the internal office network, providing access to internal systems like workstations, printers, and servers. Since the internal network is trusted, the firewall allows traffic to flow freely between this network and the DMZ, ensuring that no malicious traffic from the external network can affect it.
- **Gig1/2** is also configured as a **trusted interface** but assigned a **security level of 50**. This is the **DMZ network**, which contains services like web, email, and DNS servers that need to be accessible from both the internal network and the external internet. The DMZ is considered a semi-trusted zone because it needs to interact with external traffic but should still be separated from the core internal network for security reasons.

2. External Network (Gig1/4):

- **Gig1/4** is configured as an **external untrusted interface** with a **security level of 0**. This interface connects to the **internet** and is responsible for managing inbound and outbound traffic to/from external sources. The external network is not trusted, as it exposes the system to various threats and must be carefully controlled by the firewall.

Firewall Rules and Policies

• Access Control Lists (ACLs):

- ACLs should be applied to each interface to specify what kind of traffic is allowed to enter or exit from the network. For example, only HTTP/HTTPS traffic should be allowed to enter the DMZ servers from the external network (internet), while any traffic from the DMZ to the internal network should be restricted to the specific ports required for server management.

• NAT (Network Address Translation):

- The firewall should implement **NAT** to allow devices in the internal network and DMZ to share the public IP address for communication with external networks. This prevents internal IP addresses from being exposed to the outside world and adds an extra layer of security.

- **Inspection and Logging:**

- The firewall should inspect and log traffic passing through each interface. This includes looking for threats like port scanning, malware, and unauthorized access attempts. The logs should be regularly reviewed to identify and mitigate potential threats before they escalate.

How Real-World Companies Use Similar Firewalls at a Larger Scale

In larger organizations, the principles outlined in this setup are expanded into more complex configurations with multiple layers of security:

1. **Multiple Firewalls:**

- Large enterprises often use **multiple firewalls** placed in various strategic locations. For example, **Next-Generation Firewalls (NGFWs)** may be deployed at the perimeter, between internal segments, and even within individual departments for micro-segmentation.
- Firewalls in enterprise environments are not limited to protecting the perimeter but are also used to create isolated network zones like DMZs, dedicated user segments, and cloud environments.

2. **Distributed Denial of Service (DDoS) Protection:**

- Larger organizations typically integrate **DDoS protection** into their firewall systems. This involves automatically detecting and mitigating DDoS attacks before they can impact the services. For instance, companies like **Akamai** and **Cloudflare** provide DDoS mitigation services to ensure network traffic is not disrupted.

3. **Zero Trust Architecture:**

- Many modern enterprises now implement **Zero Trust Architecture (ZTA)**, where firewalls are part of a broader strategy to never trust any device or user inside or outside the network by default. Every access request is continuously validated using **identity-based security policies, multi-factor authentication, and micro-segmentation**. This approach is becoming critical as organizations adopt cloud and hybrid infrastructures.

4. **Example: Amazon Web Services (AWS)**

- In the cloud, organizations like **Amazon** use firewalls in the form of **AWS Security Groups** and **Network Access Control Lists (NACLs)** to create secure isolated environments for different services. They deploy multiple security layers around their cloud instances (VMs), databases, and storage to protect them from unauthorized access.

5. Example: Large Corporations (e.g., IBM, Cisco)

- Companies like **IBM** and **Cisco** often deploy **Firewalls in High Availability (HA) mode** to ensure continuous availability. They use **redundant** firewall configurations to prevent single points of failure, guaranteeing that if one firewall goes down, another automatically takes over.
- They also utilize **firewalls with Intrusion Prevention Systems (IPS)** to monitor network traffic for signs of suspicious activity and automatically block potentially harmful traffic.

By implementing multiple layers of security, firewalls not only prevent unauthorized access but also ensure that even if one security layer is bypassed, others will still protect critical infrastructure.

Conclusion

In conclusion, the network design for the RAW office building is engineered to meet the specific requirements of departmental communication, security, scalability, and high availability. By adopting a Client-Server network configuration for centralized control, alongside VLAN segmentation, we have successfully optimized the performance, security, and manageability of the network. The inclusion of Ethernet as the primary transmission medium, combined with fibre optics for high-bandwidth inter-floor connections, ensures efficient and cost-effective communication throughout the office.

The configuration of firewalls plays a pivotal role in securing both internal resources and external communications, with different security levels applied across various segments of the network, including the DMZ, internal network, and external interface. Network Address Translation (NAT) and Access Control Lists (ACLs) are implemented to prevent unauthorized access and manage traffic flow between different network zones.

The high availability design with redundant network paths and the strategic placement of firewalls ensures that the network remains resilient against failures and security threats, providing continuous service for all departments. The network is also designed with scalability in mind, allowing for seamless growth as new departments or devices are added without compromising performance or security.

In a larger enterprise context, similar strategies are applied but at a more complex scale. Companies implement multi-layered firewall solutions, integrating advanced features like Intrusion Prevention Systems (IPS), DDoS protection, and Zero Trust Architecture (ZTA) to ensure robust security across their networks. This multi-layered approach ensures that even if one security measure is bypassed, others provide continued protection. Furthermore, organizations such as Amazon and IBM deploy high availability firewall setups to ensure no downtime, with automated failovers to keep the network running smoothly.

Ultimately, this proposed network design for the RAW office building aligns with modern network requirements, balancing performance, security, and future scalability, while offering a flexible foundation that can be adapted to larger, more complex environments.

References

1. **Cisco Systems.** "Cisco ASA 5500-X Series Firewalls: Overview and Configuration." *Cisco Documentation*, 2022.
2. **Stallings, William.** *Data and Computer Communications*, 10th ed. Pearson Education, 2013.
3. **Tanenbaum, Andrew S., and David J. Wetherall.** *Computer Networks*, 5th ed. Pearson, 2011.
4. **Cisco Networking Academy.** "Introduction to Networks." *Cisco Networking Academy*, 2020.
5. **Amazon Web Services (AWS).** "Securing Cloud Networks with Firewalls and Security Groups." *AWS Documentation*, 2021.
6. **Gartner, Inc.** "Magic Quadrant for Network Firewalls." *Gartner Research*, 2021.
7. **FireEye, Inc.** "Advanced Threat Protection: A Guide to Modern Firewall Technologies." *FireEye Whitepapers*, 2020.
8. **Google Cloud.** "Designing Secure Networks with Google Cloud: Firewalls and Zero Trust Security." *Google Cloud Documentation*, 2021.