رواد مصر الرقمية

ALX1_ISS2_M1e

Names	IDs
Ahmed Salah AbdelMawgoud	21047208
Ahmed Gamal Mohamed	21050443
Diaa Mohamed	21013911
Moamen Rezika	21050279
Moataz Mohamed	21000793

Objectives:

The objective of this project is to design, implement, and secure a small office network by leveraging Cisco's security features. The project focuses on creating a secure, efficient, and scalable network environment by planning the network topology, implementing security protocols, and configuring advanced features. By the end of the project, the network will be equipped with VLANs, OSPF, and other advanced security mechanisms to ensure secure data flow and traffic segmentation. The primary goal is to create a robust, efficient, and scalable network infrastructure that protects sensitive data, ensures network integrity, and meets the specific needs of a small office environment.

Key Deliverables:

- **Network Topology Design:** Develop a comprehensive network diagram outlining the physical and logical layout, including devices (routers, switches, firewalls), connections, and VLANs.
- **Security Policy Implementation:** Define and implement a robust security policy that addresses access control, data confidentiality, and network integrity.
- **VLAN Configuration:** Create virtual LANs (VLANs) to segregate network traffic, enhance security, and improve performance.
- **OSPF Routing Protocol:** Implement the Open Shortest Path First (OSPF) routing protocol to enable efficient and scalable routing between network devices.

- **Advanced Security Features:** Configure advanced security features, such as intrusion prevention systems (IPS), VPNs, and encryption, to protect against various threats.
- **Documentation:** Create detailed documentation outlining the network design, implementation steps, and configuration settings for future reference and troubleshooting.

Expected Outcomes:

- A secure and reliable network infrastructure that meets the specific needs of the small office.
- Improved network performance and efficiency through the use of VLANs and OSPF.
- Protection against common network threats and vulnerabilities.
- Adherence to industry best practices for network security and compliance.

By addressing these aspects, the project will deliver a secure, efficient, and scalable small office network that meets the organization's goals and protects its valuable assets.

Timeline:

- **Week 1: Planning and Design**
  Define the network requirements based on the number of users, devices, and internet needs. The deliverable includes a network design document with topology diagrams, IP addressing schemes, and device lists.
- **Week 2: VLAN Implementation**
  Implement VLANs to enhance security and regulate traffic between network segments. The deliverable includes configuration files and a report documenting the implementation. AVLAN (Virtual Local Area Network) is a logical grouping of network devices that allows them to communicate as if they were on the same physical network, regardless of their actual physical location. VLANs are used to improve network performance, security, and manageability by separating network traffic into different broadcast domains. VLANs are a powerful tool for network administrators to segment networks, improve performance, enhance security, and simplify management. By understanding the concepts and benefits of VLANs, network professionals can design and implement efficient and secure network infrastructures.

A **VLAN (Virtual Local Area Network)** is a technology that allows network administrators to create separate, isolated networks within a single physical network infrastructure. Here are some key points about VLANs:

- **Segmentation**: VLANs divide a network into smaller, logical segments, which can improve performance and security by reducing broadcast traffic and isolating sensitive data.
- **Flexibility**: Devices in different physical locations can be grouped into the same VLAN, making network management more flexible and efficient.
- **Security**: By isolating network segments, VLANs can help prevent unauthorized access to sensitive information and resources.
- **Traffic Management**: VLANs can prioritize certain types of traffic, ensuring that critical applications receive the necessary bandwidth.

Benefits of AVLAN:

- **Increased Efficiency**: It eliminates the need for constant synchronization of devices on the network.
- **Cost-Effective**: Reduces the need for expensive network hardware since it relies more on logical segmentation rather than physical infrastructure.
- **Simplified Management**: Network admins can manage distributed devices more easily, without the hassle of physical constraints.
- **Geographic Independence**: Devices don’t need to be in the same building or country to communicate as if they’re on the same network.

How AVLAN Works

AVLAN extends the basic principles of VLANs but incorporates mechanisms to allow asynchronous communication between devices. Here's how it operates at a high level:

- **Logical Segmentation**: Like a regular VLAN, AVLAN groups devices logically rather than physically. However, with AVLAN, these logical connections don’t have to be synchronous, meaning that devices don't have to be directly connected at the same time to communicate.
- **Asynchronous Communication**: Unlike traditional networks where all devices must communicate synchronously (e.g., within the same session or time window), AVLAN enables devices to transmit and receive information at different times without losing network integrity.
- **Layer 2 and Layer 3**: Just like traditional VLANs, AVLAN operates across Layer 2 (data link layer) and Layer 3 (network layer) of the OSI

model. It may use **MAC addresses** and **IP addresses** to identify devices within the virtual LAN. However, what sets AVLAN apart is that it accommodates different time delays and geographical locations within the network setup.

- **Week 3: OSPF Configuration**

  Configure OSPF in a single area to enable efficient routing across the network. The deliverable consists of OSPF configuration files and a verification report.

  OSPF (Open Shortest Path First) is a routing protocol used in IP networks to determine the best path for data packets to travel between network devices. It's a distance-vector routing protocol, meaning it calculates routes based on the distance between routers. OSPF is a robust and efficient routing protocol that is widely used in IP networks. Its key features include link-state routing, hierarchical design, authentication, and rapid convergence. OSPF is well-suited for large and complex networks that require reliable and efficient routing.it is a dynamic routing protocol used in IP networks that enables routers to determine the best path for forwarding packets. It’s an interior gateway protocol (IGP) designed for large and complex networks, typically deployed in enterprise networks and ISPs.

  Open Shortest Path First (OSPF) is a widely used routing protocol for Internet Protocol (IP) networks. Here are some key points about OSPF:

  1. **Link-State Routing Protocol**: OSPF uses a link-state routing algorithm to determine the best path for data packets. It maintains a database of the network topology, which it updates regularly.
  2. **Interior Gateway Protocol (IGP)**: OSPF operates within a single autonomous system (AS), making it an interior gateway protocol. It’s commonly used in large enterprise networks.
  3. **Areas and Hierarchical Design**: OSPF divides the network into areas to optimize traffic and simplify management. The backbone area (Area 0) connects all other areas.
  4. **Fast Convergence**: OSPF quickly detects changes in the network topology, such as link failures, and recalculates the best paths, ensuring minimal disruption.
  5. **Support for IPv4 and IPv6**: OSPF supports both IPv4 and IPv6, making it versatile for modern network environments.

How OSPF Works:

1. **Neighbor Discovery**: OSPF routers discover neighbors on directly connected networks by sending **Hello packets**. Once a neighbor relationship is established, routers can begin exchanging routing information.
2. **LSA (Link-State Advertisement)**: Each router in the OSPF network sends LSAs to all of its neighbors, describing the state of its own links. These LSAs are flooded throughout the OSPF area, allowing all routers to have the same view of the network.
3. **LSDB (Link-State Database)**: Each OSPF router stores all the LSAs it receives in its Link-State Database. The LSDB represents a complete map of the network.
4. **SPF Calculation**: Once the LSDB is complete, each router independently runs the Shortest Path First (SPF) algorithm to calculate the best path to each destination. This results in the creation of the **OSPF routing table**.
5. **Route Propagation**: OSPF routers then propagate the best route information to their neighbors. If there are changes in the network (e.g., a link goes down), routers will update their LSAs and trigger recalculation.

Advantages of OSPF:

1. **Scalability**: OSPF is well-suited for large networks, thanks to its hierarchical area design.
2. **Efficiency**: It only sends routing updates when there are changes, rather than periodically broadcasting the entire routing table.
3. **Fast Convergence**: OSPF's use of LSAs and the SPF algorithm allows it to quickly react to network changes.
4. **Support for VLSM and CIDR**: OSPF is classless, meaning it supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR).

- **Week 4: Advanced Security Features and EtherChannel**
  Deploy advanced security measures such as port security and IP Source Guard. For **IP Source Guard**, the configuration will be enhanced by binding the MAC address to the switch port, allowing only one MAC address to access the port. This ensures that only the authorized device can send traffic through the port, strengthening the security of the network. Additionally, EtherChannel will be configured for link aggregation and redundancy.

EtherChannel is a technology that allows multiple physical network interfaces to be aggregated into a single logical interface, providing increased bandwidth and redundancy. This is particularly useful for high-bandwidth applications or environments where network reliability is critical. EtherChannel is a valuable technology for improving network bandwidth, redundancy, and performance. By understanding the concepts and benefits of EtherChannel, network administrators can effectively utilize this feature to enhance their network infrastructure.it is a Cisco technology that allows you to bundle multiple physical links between switches, servers, or routers into a single logical link, providing increased bandwidth and redundancy. This combined link appears as a single connection to Layer 2 protocols like Spanning Tree Protocol (STP) and Layer 3 routing protocols, helping prevent network loops and improve fault tolerance.

EtherChannel is a technology used primarily on Cisco switches to combine multiple physical Ethernet links into a single logical link. Here are some key points about EtherChannel:

1. **Link Aggregation**: EtherChannel aggregates several physical Ethernet links to create one logical link, providing increased bandwidth and redundancy.
2. **Fault Tolerance**: If one of the physical links fails, EtherChannel automatically redistributes the traffic across the remaining active links, ensuring continuous network availability[1].
3. **Load Balancing**: Traffic is distributed across the links based on various criteria such as source and destination MAC addresses, IP addresses, or TCP/UDP port numbers.
4. **Compatibility**: EtherChannel can be used with Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports. It supports up to 8 active links and additional standby links for failover.
5. **Protocols**: There are two main protocols for configuring EtherChannel:
    - **Port Aggregation Protocol (PAgP)**: A Cisco proprietary protocol.
    - **Link Aggregation Control Protocol (LACP)**: An IEEE 802.3ad standard that works with devices from different vendors.

Types of EtherChannel Protocols:

1. **Static EtherChannel**: A manual configuration where network administrators specify which links are aggregated. This type does not

require any negotiation protocol, but both ends of the EtherChannel must be manually configured to match.

2. **Dynamic EtherChannel**: This involves automatic negotiation between devices to form the EtherChannel using specific protocols:
    - **Port Aggregation Protocol (PAgP)**: A Cisco proprietary protocol that dynamically negotiates the creation of an EtherChannel. PAgP ensures that the configurations of both ends match before establishing the EtherChannel.
    - **Link Aggregation Control Protocol (LACP)**: An open standard protocol defined by IEEE (IEEE 802.3ad). Like PAgP, LACP negotiates the creation of EtherChannel dynamically, but it can be used between devices from different vendors.

Benefits of EtherChannel:

1. **Increased Bandwidth**: By aggregating multiple physical links, EtherChannel provides higher throughput, allowing more data to be transmitted simultaneously.
2. **Fault Tolerance**: If one of the physical links in the EtherChannel bundle fails, the remaining links continue to function, maintaining network connectivity without requiring protocol reconvergence.
3. **Load Balancing**: EtherChannel balances traffic across the available links using specific load-balancing algorithms, which can be based on factors like source and destination IP addresses, MAC addresses, or Layer 4 port numbers.
4. **Simplified Management**: Once multiple links are combined into a single logical interface, network administrators manage the EtherChannel as if it were one link, simplifying network configurations and reducing complexity.
5. **STP Efficiency**: EtherChannel reduces the number of interfaces seen by the Spanning Tree Protocol (STP), which prevents STP from treating the bundled links as separate interfaces. This enhances network performance by avoiding unnecessary blocking of redundant links.

Port security: is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator configure individual switch ports to allow only a specified number of sources MAC addresses on the port. is a feature on network switches that helps control and restrict access to a network by limiting and identifying the MAC addresses of devices allowed to connect to the switch ports. is a network security feature that restricts access to specific network ports based on the Media Access Control (MAC) address of devices connected to those ports. It's a crucial tool for preventing unauthorized access to a network and mitigating various security threats.

Here are some key points about port security:

1. **Purpose**: Port security is used to prevent unauthorized devices from connecting to the network, thereby enhancing security.
2. **Configuration and Best Practices:**

- **Configure Secure Defaults:** Set strict port security settings to minimize risks.
- **Regular Monitoring:** Monitor port security logs to detect and address any issues.
- **Use a Combination of Security Measures:** Implement port security in conjunction with other security measures like firewalls, intrusion detection systems, and access control lists.
- **Consider Dynamic Port Security:** In environments with frequent device changes, dynamic port security can simplify management.

To configure port security on a Cisco switch, you typically:

   - Define the interface as an access interface.
   - Enable port security on the interface.
   - Specify the allowed MAC addresses, either manually or dynamically using the “sticky” option.

3. **Violation Actions**: When an unauthorized device attempts to connect, the switch can take actions such as:
   - **Protect**: Discards traffic from unauthorized devices without logging.
   - **Restrict**: Discards traffic and logs the violation.
   - **Shutdown**: Discards traffic, logs the violation, and shuts down the port.

4. Key Benefits of Port Security

- **Prevents Unauthorized Access:** Restricts access to network ports, making it difficult for unauthorized devices to connect.
- **Mitigates MAC Spoofing Attacks:** Prevents attackers from using forged MAC addresses to gain access.
- **Enhances Network Security:** Provides a layer of protection against various security threats.
- **Improves Network Performance:** Can reduce network congestion by limiting the number of devices that can connect to a port.

Port security helps in mitigating risks such as MAC address spoofing and unauthorized access, ensuring that only trusted devices can communicate on the network.

5.How Does Port Security Work?

1. **MAC Address Binding:** The network administrator configures a port to allow only specific MAC addresses to connect.
2. **MAC Address Checking:** When a device connects to the port, its MAC address is compared against the allowed list.
3. **Access Control:** If the MAC address matches, the device is granted access. If it doesn't, access is denied.

6.Types of Port Security

- **Static Port Security:** The administrator manually configures the allowed MAC addresses.
- **Dynamic Port Security:** The switch automatically learns the MAC addresses of devices connected to the port and adds them to the allowed list.

7.Common Use Cases

- **Data Centers:** Protecting critical infrastructure and preventing unauthorized access to servers.
- **Small Offices and Home Networks:** Securing network resources and preventing unauthorized use.
- **Public Wi-Fi Networks:** Limiting access to specific devices to prevent unauthorized access and misuse.

By effectively implementing port security, organizations can significantly enhance their network security posture and protect their valuable assets from unauthorized access.

Work flow:

 Moamen Rezika will take the lead in finalizing the overall network design, ensuring that it supports the configurations needed for VLANs, and security features. This includes making sure the IP addressing scheme is compatible with VLAN segmentation and OSPF routing, as well as accounting for security measures like port security and IP Source Guard. They will also ensure that the network topology and design are flexible enough to support the advanced security features that will be implemented in later stages.

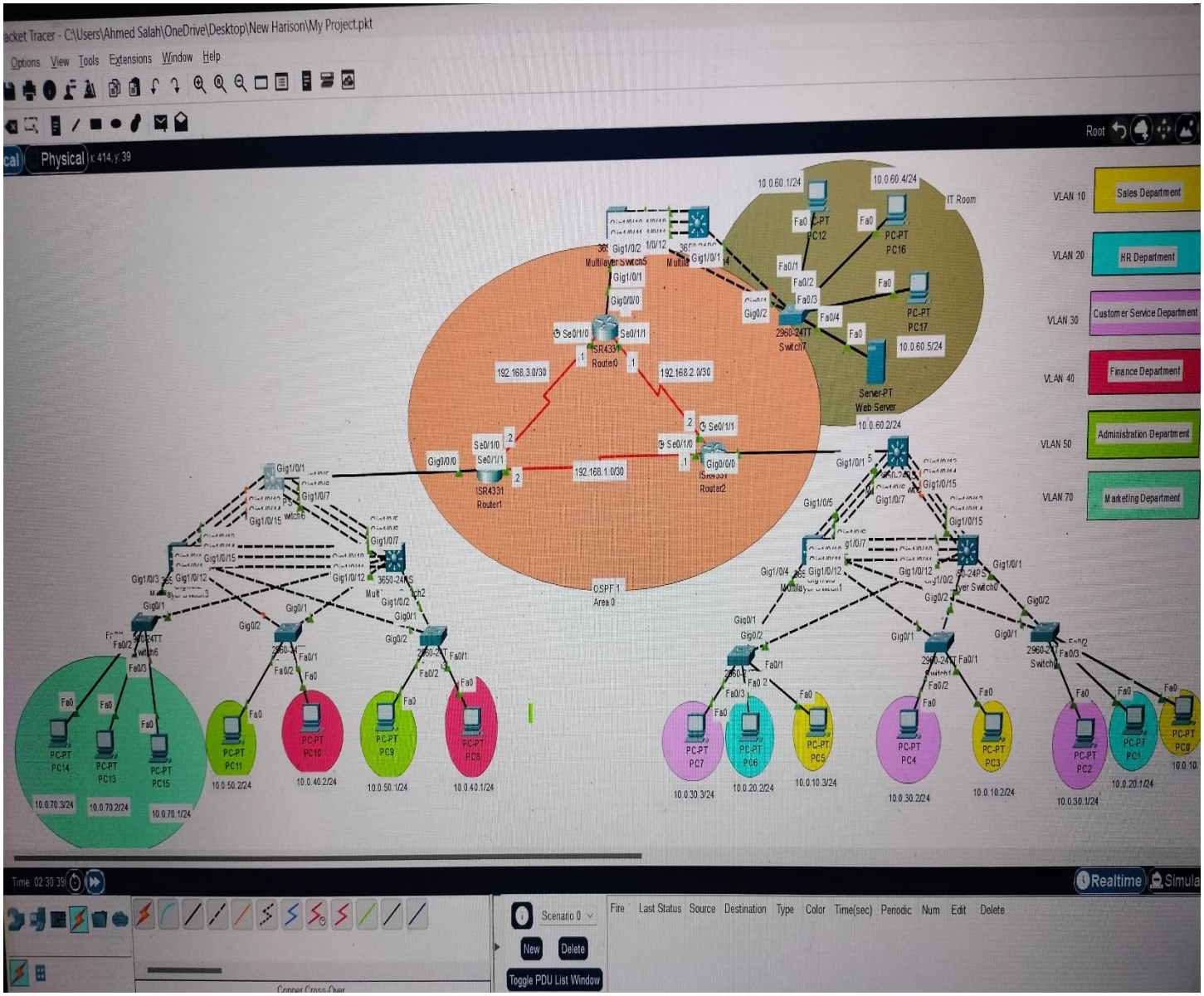
 Ahmed Gamal and Ahmed Salah will work to ensure smooth integration between VLANs and OSPF routing. **Ahmed Gamal** will focus on setting up VLANs to segment network traffic, while **Ahmed Salah** will configure OSPF to handle dynamic routing within the network. Both members need to ensure that the VLAN configuration is properly supported by OSPF, meaning that OSPF can route traffic across VLANs and maintain network performance and security. They will communicate regularly to verify that VLANs are properly advertised in OSPF and that the routing protocol works across all network segments.

 Diaa Mohamed &**Moataz Mohamed** will handle advanced security features, including configure IP Source Guard to bind specific MAC addresses to switch ports, and implement EtherChannel for redundancy and increased bandwidth.

Conclusion

By the end of this project, the small office network will be fully designed, implemented, and secured using Cisco’s advanced security features. The network will provide secure and efficient communication between devices, with VLANs ensuring proper traffic segmentation. OSPF will be configured for dynamic routing, maintaining seamless data flow across the network. With the implementation of advanced security measures such as IP Source Guard, and port security, the network will be fortified against unauthorized access. EtherChannel will also enhance network performance by providing redundancy and link aggregation.

Diagram:


Physical
Root
IT Room
VLAN 10
Sales Department
VLAN 20
HR Department
VLAN 30
Customer Service Department
VLAN 40
Finance Department
VLAN 50
Administration Department
VLAN 70
Marketing Department
192.168.3.0/30
192.168.2.0/30
192.168.1.0/30
OSPF 1
Area 0
ISR4331
Router0
ISR4331
Router1
ISR4331
Router2
2960-24TT
Switch7
Server-PT
Web Server
10.0.60.2/24
10.0.60.5/24
10.0.50.2/24
10.0.40.2/24
10.0.50.1/24
10.0.40.1/24
10.0.70.3/24
10.0.70.2/24
10.0.70.1/24
10.0.30.3/24
10.0.20.2/24
10.0.10.3/24
10.0.30.2/24
10.0.10.2/24
10.0.30.1/24
10.0.20.1/24
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete