**Building and Securing a Small Network**

**Team Members:**

* Mohamed Abdullah Mohamed
* Mohamed Fathy Abdel Hameed Mohamed
* Mohanad Ashraf Ahmed
* Joseph Wagih Gerges Wanis
* Tarek Yahia Atef
* Kerollos Sabry Nazim Nazmy

**Project Overview**

**Scope:**

The goal of this project was to design, configure, and secure a small network using Cisco routers and switches. The network was segmented using VLANs to isolate traffic and secured through access control lists (ACLs), port security, and firewall configurations.

**Objectives:**

* Isolate network segments using VLANs while enabling secure communication.
* Protect the network from unauthorized access and vulnerabilities.

**Step 1: Network Design and Topology**

**Network Design:**

The network was designed with a hierarchical IP addressing scheme for scalability. Departments were segmented into VLANs to provide logical separation. A small number of Cisco routers and switches were used to create a flexible and scalable topology.

* **VLANs for Segmentation:** VLANs were assigned to different departments such as Sales, IT, and Management.
* **IP Addressing Scheme:** A structured IP plan was created to ensure future scalability, assigning different subnets to each VLAN.

**Network Topology:**

* **Core Devices:** Cisco routers and switches were used to connect all segments.
* **Layer 2 Switches:** Used to connect end devices to VLANs.
* A screenshot of a computer

  Description automatically generated**Router-on-a-Stick:** A single router interface was used to handle inter-VLAN routing by creating multiple sub interfaces
* **IP Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **Router0** | **G0/0** | **11.0.0.2** | **255.255.255.0** | **N/A** |
| **Router0** | **G0/1** | **192.168.1.1** | **255.255.255.0** | **N/A** |
| **Router1** | **G0/0** | **11.0.0.3** | **255.255.255.0** | **N/A** |
| **Router1** | **G0/1** | **12.0.0.2** | **255.255.255.0** | **N/A** |
| **Router1** | **G0/2** | **192.168.2.1** | **255.255.255.0** | **N/A** |
| **Router2** | **G0/0** | **12.0.0.3** | **255.255.255.0** | **N/A** |
| **Router2** | **G0/1** | **13.0.0.2** | **255.255.255.0** | **N/A** |
| **Router2** | **G0/2** | **192.168.3.1** | **255.255.255.0** | **N/A** |
| **Router3** | **G0/0** | **13.0.0.3** | **255.255.255.0** | **N/A** |
| **Router3** | **G0/1** | **192.168.4.1** | **255.255.255.0** | **N/A** |
| **Switch0** | **VLAN 1** | **192.168.1.2** | **255.255.255.0** | **192.168.1.1** |
| **Switch1** | **VLAN 1** | **192.168.2.2** | **255.255.255.0** | **192.168.2.1** |
| **Switch2** | **VLAN 1** | **192.168.3.2** | **255.255.255.0** | **192.168.3.1** |
| **Switch3** | **VLAN 1** | **192.168.4.2** | **255.255.255.0** | **192.168.4.1** |
| **PC0** | **NIC** | **192.168.1.2** | **255.255.255.0** | **192.168.1.1** |
| **PC1** | **NIC** | **192.168.1.3** | **255.255.255.0** | **192.168.1.1** |
| **PC2** | **NIC** | **192.168.2.2** | **255.255.255.0** | **192.168.2.1** |
| **PC3** | **NIC** | **192.168.2.3** | **255.255.255.0** | **192.168.2.1** |
| **PC4** | **NIC** | **192.168.3.2** | **255.255.255.0** | **192.168.3.1** |
| **PC5** | **NIC** | **192.168.3.3** | **255.255.255.0** | **192.168.3.1** |
| **PC6** | **NIC** | **192.168.4.2** | **255.255.255.0** | **192.168.4.1** |
| **PC7** | **NIC** | **192.168.4.3** | **255.255.255.0** | **192.168.4.1** |

**Step 2: VLAN Configuration and Trunking**

**VLAN Implementation:**

VLANs were implemented to segment the network and isolate traffic based on department. Each VLAN was given a unique ID, and the corresponding IP subnet was assigned to the devices within that VLAN.

* **VLAN Creation:** On the switches, VLANs were created and assigned to specific ports where end devices were connected.
* **VLAN Trunking:** To allow communication between multiple VLANs across switches, VLAN trunks were configured using 802.1Q tagging. This allowed VLAN traffic to travel between the switches while maintaining the separation of different network segments.

**Inter-VLAN Routing:**

A single router interface (Router-on-a-Stick) was configured to handle inter-VLAN routing. Multiple subinterfaces were created on the router, each corresponding to a VLAN.

* **Subinterface Configuration:** Each subinterface was assigned a unique IP address from its respective VLAN’s subnet. These subinterfaces enabled routing between VLANs, allowing devices in different VLANs to communicate securely.
* **Routing Protocol:** Static routes were set up for simple routing, but dynamic routing protocols like OSPF or EIGRP could be added for scalability.

**Deliverables:**

* **VLAN Configuration Scripts:** Detailed commands for VLAN creation and port assignment.
* **Trunking and Subinterface Configuration:** Scripts showing the trunking configuration on switches and Router-on-a-Stick setup on the router.
* **Documentation of Inter-VLAN Communication:** Explanation of how devices in different VLANs communicate through the router.

A screenshot of a computer

Description automatically generated

**Step 3: Security Implementation**

**Port Security:**

To prevent unauthorized devices from connecting to the network, port security was implemented on the switches.

* **MAC Address Limiting:** Configured to limit the number of MAC addresses that could be learned on a switch port, restricting access to only known devices.
* **Violation Modes:** Ports were configured to shut down if a violation occurred, further ensuring the security of the network.

**Access Control Lists (ACLs):**

ACLs were configured on the routers to control traffic flow and provide an additional layer of security. This prevented unauthorized traffic from entering or leaving the network.

* **Standard ACLs:** Configured to restrict access to specific network resources based on source IP addresses.
* **Extended ACLs:** Used to filter traffic based on source, destination, and protocol, providing more granular control.

**Basic Firewall Rules:**

Basic firewall rules were implemented to protect the network from external threats. The firewall was configured to block incoming traffic from untrusted sources while allowing legitimate traffic.

* **Inbound/Outbound Rules:** Configured to allow essential services such as HTTP and deny access to unauthorized ports or services.
* **Firewall Testing:** Simulated external threats were tested against the firewall to ensure that it could block malicious attempts.

**Deliverables:**

* **Security Configuration Scripts:** Port security, ACLs, and firewall configuration scripts.
* **Security Policy Document:** Comprehensive documentation outlining the security policies and justifications for each configuration.
* **Security Assessment Report:** A report on the effectiveness of the security measures, including the results of tests performed to verify network protection.

**Step 4: Network Testing and Troubleshooting**

**Testing Network Functionality:**

After configuration, the network was thoroughly tested to ensure functionality and performance.

* **Connectivity Testing:** Ping and traceroute tests were performed between devices in different VLANs to verify inter-VLAN routing and connectivity.
* **Performance Testing:** The network was monitored for latency, packet loss, and bandwidth utilization to ensure optimal performance.

**Security Testing:**

The security measures were tested by simulating various scenarios such as unauthorized access attempts, port scanning, and denial-of-service (DoS) attacks.

* **Port Security Testing:** Tested with unauthorized devices to verify that the configured port security shut down the compromised port.
* **ACL Effectiveness:** Attempted to access restricted resources to ensure ACLs were functioning as intended.

**Troubleshooting:**

Any issues encountered during testing were identified and resolved. This included misconfigurations in VLANs or trunking, incorrect ACL rules, or firewall misconfigurations.

**Deliverables:**

* **Test Results Summary:** Detailed documentation of all test results, including the network's performance metrics and security effectiveness.
* **Troubleshooting Report:** A record of issues encountered and their solutions, ensuring the network operates smoothly.

A screenshot of a computer program

Description automatically generated

**Conclusion and Recommendations**

**Conclusion:**

The project successfully demonstrated the design and implementation of a small, segmented, and secure network. All objectives were met, including VLAN segmentation, inter-VLAN routing, and the application of security measures. The network performed as expected, with all tests passing.