Project Report: Building and Securing a Small Network

Prepared by

Walid Ghanem

Kyrillos Gabra Mahrous Youssef

Mohamed mohamed Elsayed

Mina Atef

Ahmed Ibrahim

Ahmed Hamoda

Overview

- This report Outlines the stages of networking design, deployment and management of a small network based on Cisco platforms. The project is structured in **Four main Parts**: network conceptualization and building, configuration and routing of inter-VLANs, integration of network security measures into the system, and evaluation of the system's performance and drafting the report. The main object of this project is the construction of operational and secure network which provides multiple VLANs, inter-VLAN communication, and security controls.

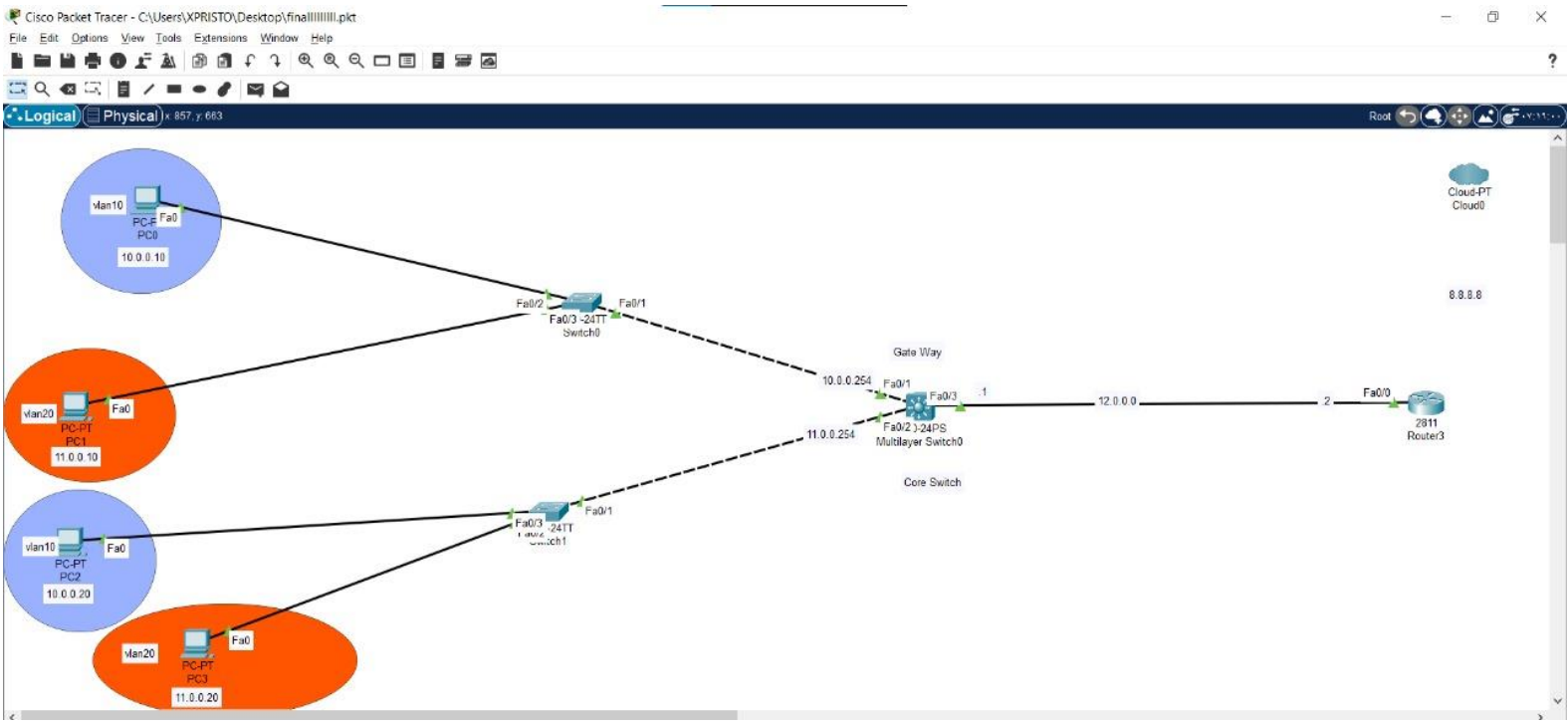
Part 1: Network Design and Configuration

- **Objective:**
  Create small scale network for testing using Cisco devices, define the network Topology, allocate IP addresses, and configure network systems.

- **Network Design:**
  The network is segmented using Virtual Local Area Networks (VLANs) which are interlinked via multilayer switches and routers. Such an arrangement makes it possible to promote data traffic between the segments of the network while at the same time ensuring that traffic from other segments is blocked. The Chief structure of the network is:

  - PCs organized into two VLANs:
    - VLAN 10: 10.0.0.0/24 network.
    - VLAN 20: 192.168.1.0/24 network

  - Multilayer switches are used to manage routing between VLANs.
  - Cisco ISR Router provides additional Routing functionality and external Network connectivity.



- **IP Addressing Scheme:**

- VLAN 10:10.0.0.0/24 is used by the user devices (e.g., PC0, PC2).
- VLAN 20: 11.0.0.0/24 has been assigned users devices that include (e.g.,PC1, PC3).
- Each VLAN is within a specific subnet to relieve congestion and manage the infrastructure.

- **Device Configuration :**

1. VLAN Setup on Cisco switches:
   - Two VLANs (VLAN 10 and VLAN 20) are configured for Network traffic separation.
   - IP addresses are statically assigned within each VLAN subnet.

2. Through Multilayer switches, which are used to perform Routing of VLANs traffic this is the Interconnection achieved

- **Deliverables:**

  - Network Design Diagram: Represents the network which forms the switches and routers and the connected end devices.
  - IP Addressing Table:
    - VLAN 10: 10.0.0.0/24
    - VLAN 20:11.0.0.0/24
  - Initial Configuration:
    - VLANs, IP addressing, and basic Device configurations have been Established.

Part 2: VLANs and Inter-VLAN Routing

- **Objective:**

To allow communication between segments of the network by implementing VLANs, configuring VLAN trunks and enabling inter-VLAN routing.

- **Implementation of VLANs:**

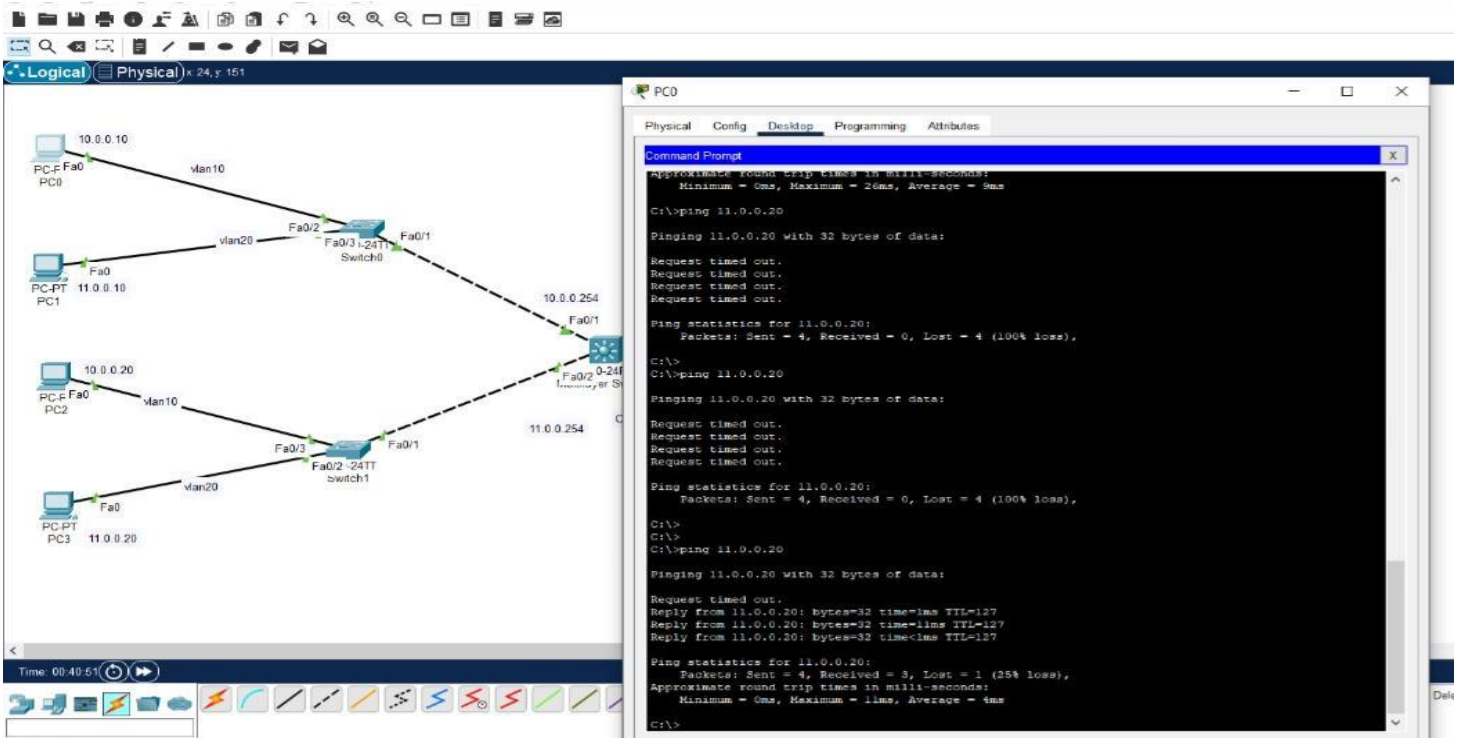
  - Implementation of VLANs was performed on the switches to reduce the size of the subnet to two subdivisions.

  - VLAN Trunks were configured between the switches for the purpose of inter-VLAN communication.

- **Inter VLAN Routing:**

  - Inter VLAN routing was done to allow intercommunication between VLANs 10 and 20 using a Router-on-a-stick or layer three switch routing.

  - The multilayer switches were configured to perform inter-VLAN routing and were assigned as the default gateway for their corresponding VLAN.
  - routing setup on the switch:



- **Deliverables:**

    - VLAN Configuration:
        1. VLAN 10 and 20 were created.
        2. Enabled trunk ports on the switches to allow inter VLAN communication.

    - Inter VLAN Routing Setup:
        1. Multilayer switches were used to interconnect the VLANs through routing.

    - Troubleshooting Report:
        1. Tests on connectivity were done using the ICMP pings measuring how devices from two different VLANs communicate with each other.

Part 3: Network Security Implementation

- **Objective:**

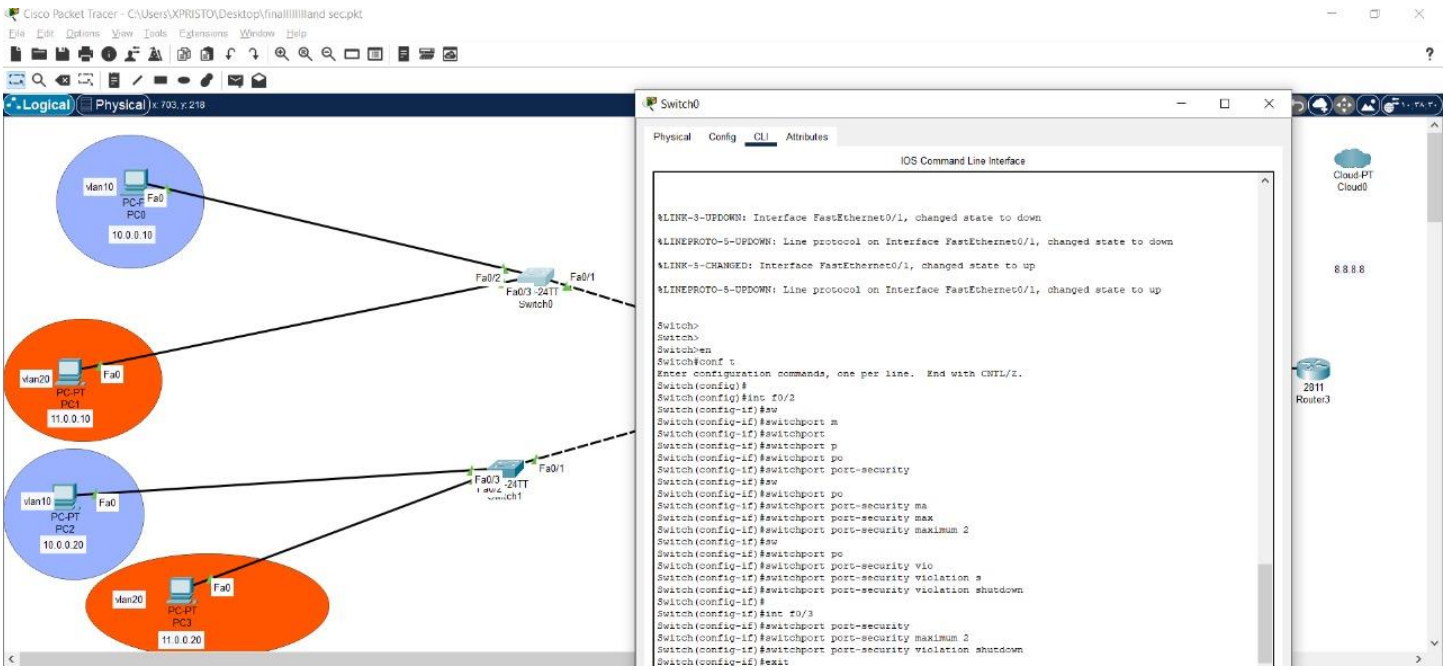
To carry out protective measures that prevent unauthorized access and malicious activity on the network. This will be done by configuring port security, access control lists (ACLs), and also some basic firewall rules.

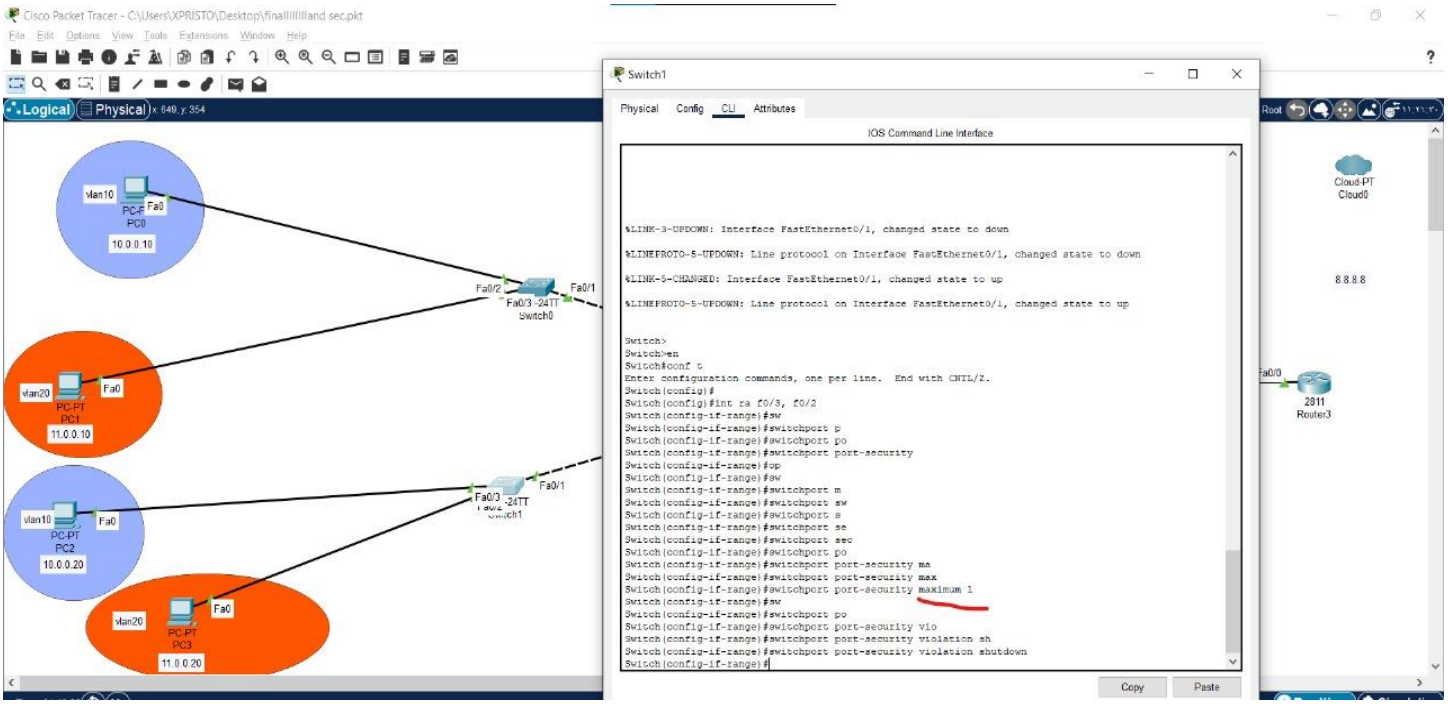
- **Security Features Implemented:**

  - Port Security Policy:

    - Port security was put in place as a means of limiting the number of devices connected to an individual port on a switch.
    - This guarantees that rogue devices cannot breach the network simply by being plugged into an available port.

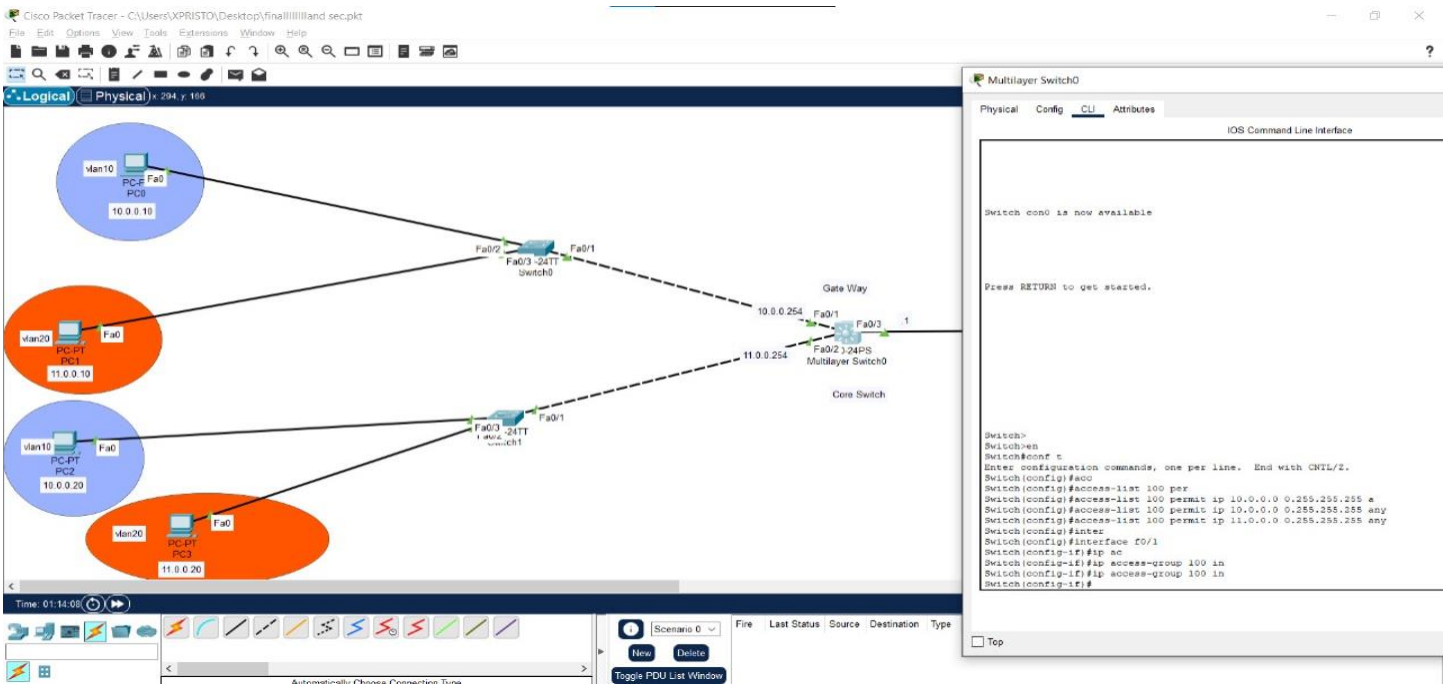
As understood, this security feature restricts the number of devices that can be accessed by the network security devices port security policy in the following way:





- **Access Control Lists (ACLs):**
  - ACLs were set up to manage the traffic between different VLANs and specified devices were provided authorization to communicate with other specific devices. The authorized communication between specific devices facilitated the ACLs, which helped to communicate with only one VLAN.

For instance, the ACL that restricts access between VLANs is 100 wherein:



- **Firewall Rules:**
  - The basic firewall rules were implemented on the router to prevent the breach of external access to the site and control the movement of information to various connections within the network.
  - Configure simple firewall rules if needed. Packet Tracer does not fully support advanced firewall settings, but basic ACLs can simulate some firewall behavior.

- **Deliverables:**

  - Security Procedures Guide/Scripts: Focused on the configurations of ports, ACLs and fire wall rule for port security active security.
  - Security policy already prepared at the organization and ready to be acted upon by the authority.

Week 4: Completing The Tests and Compiling Reports

- **Objective:**

  - To check not only the functionality of the system bet to test its' security and performance so that when various systems are integrated, they operate as they are intended to operate. A network design, implementation, and evaluation is presented in the last report and presentation.

- **Testing Conducted:**

1. **Functional Testing:**

Through the use of ICMP pings, connectivity tests verifying the communication of devices located on different VLANs were carried out. All users managed to realize the objectives of the tests, as the communication was successful, http routing inter vlan was working well.

2. **Security Testing:**
    - Testing of network ports was done by connecting amplifiers that were not authorized and attempting to access the network devices. As planned the blocked devices managed to be interdicted.
    - Testing the ACLs was also done to verify if unauthorized traffic was allowed to flow through the VLANs.

3. **Performance Testing:**
    - Optimal performance was to be able to measure the parameters of bandwidth, latency and packet lost. The network was good and reasonably stable and showed a good level of latency.

- **Deliverables:**

- Final Report: This will be a very important document as it will present the information on system security, and the implementation of the design and all the testing sessions that were carried out.
- Test Results: Network Implementation success is contextualized through the three networks tests' detailed results; connectivity, security and performance tests.

Conclusion

In this project, we managed to create and Configure a small network utilizing Cisco Equipment.

VLANs were employed to isolate Certain traffic and increase security. Inter-VLAN routing was established allowing devices from various VLANs to converse.

Measures were also taken against The unauthorized access by applying security such As place blockage and Access Control Lists.

There were however some devices Failing to communicate at the beginning but these were worked on during network. In general, the network is now working, it is secure as intended, and it communicates effectively in accordance with the expectations as formulated in the objectives of the project.