**Diverse Network Security Measures with Cisco Devices**

Name: Karim Hussam Al-Din El-Sayed Mohamed

ID: 21001442

National ID: 30109030202259

**Objective of the Lab**

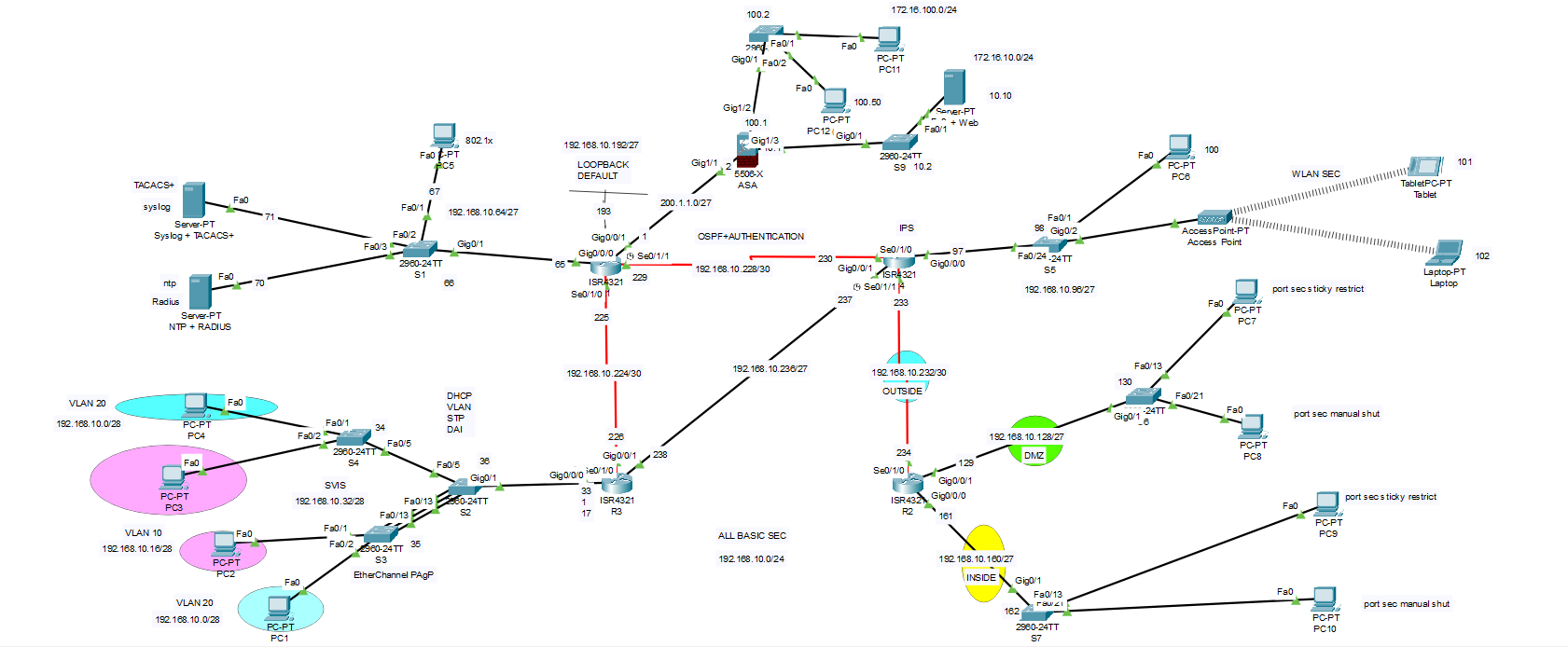
The objective of this lab is to design and implement a secure network topology by integrating a variety of network security measures and configurations. The lab focuses on ensuring robust protection against potential threats, enhancing network performance, and securing communication.

The key security measures applied include:

1. **IPSec**: Secure communication over untrusted networks by encrypting IP traffic between endpoints.
2. **VLANs**: Logical segmentation of the network to enhance security and reduce broadcast domains.
3. **No CDP**: Disabling Cisco Discovery Protocol on non-essential interfaces to mitigate potential information disclosure risks.
4. **IP Source Guard**: Preventing IP address spoofing attacks at the Layer 2 level.
5. **STP Security**: Protecting the spanning tree topology from malicious attacks.
   * **BPDU Guard**: Preventing unauthorized switches from affecting the STP topology.
6. **ASA Firewall**: Implementing perimeter security using Cisco Adaptive Security Appliance to filter and inspect traffic.
7. **Zone-Based Firewall (ZPF)**: Defining zones and policies for granular traffic control and protection.
8. **802.1X**: Implementing port-based network access control to ensure only authenticated devices can connect.
9. **TACACS+ and RADIUS**: Configuring AAA (Authentication, Authorization, and Accounting) for centralized user access management.
10. **WLAN Security**: Securing wireless networks with encryption and authentication mechanisms to prevent unauthorized access.
11. **EtherChannel**: Enhancing link reliability and bandwidth by aggregating multiple physical links into a single logical link.

By applying these measures, the lab demonstrates the implementation of a comprehensive, layered approach to securing both wired and wireless network components while maintaining operational efficiency.

**Topology**



**Updated Devices Used in the Lab**

1. **Cisco Routers: Cisco ISR 4321**
   * Provides inter-VLAN routing, IPSec VPN, and WAN connectivity.
2. **Cisco Switches: Catalyst 2960**
   * Layer 2 devices for VLANs, STP security, IP Source Guard, EtherChannel, 802.1X, and BPDU Guard.
3. **Cisco ASA 5506-X**
   * Acts as a firewall for perimeter security, providing advanced filtering and VPN functionality.
4. **PC-PT Devices (End Hosts)**
   * Simulate standard client devices for connectivity, testing AAA configurations, and accessing services like HTTP and DNS.
5. **TACACS+ Server**
   * A centralized authentication server for managing network device access through AAA.
6. **RADIUS Server**
   * Handles AAA for wireless clients, integrated with access points for 802.1X and WLAN security.
7. **Mail/HTTP/DNS Servers**
   * Provide essential network services:
     + **Mail Server**: To test email connectivity in a secure environment.
     + **HTTP Server**: For testing secure web access over the network.
     + **DNS Server**: Handles name resolution within the network.
8. **Access Points**
   * Provide wireless connectivity for mobile devices, configured with WPA2/WPA3 security, integrated with RADIUS for 802.1X authentication.
9. **Tablets and Laptops**
   * Simulate mobile clients connecting wirelessly to test WLAN security and seamless authentication via RADIUS.

This expanded setup offers a robust and comprehensive testbed for implementing and validating wired and wireless network security features.

**Steps of the lab and basic configurations**

Note: The exact commands are in the **.pkt** file uploaded on GitHub.

Here’s a step-by-step guide for configuring each of the mentioned security measures. Let’s break it down by category.

**1. VLAN Configuration (Switches)**

**Goal:** Segment traffic to improve security and performance.

**Steps:**

1. Configure VLANs:
2. Switch(config)# vlan 10
3. Switch(config-vlan)# name HR
4. Switch(config-vlan)# vlan 20
5. Switch(config-vlan)# name IT
6. Assign interfaces to VLANs:
7. Switch(config)# interface range fa0/1-10
8. Switch(config-if-range)# switchport mode access
9. Switch(config-if-range)# switchport access vlan 10
10. Configure the trunk port for inter-VLAN communication:
11. Switch(config)# interface fa0/24
12. Switch(config-if)# switchport mode trunk

**2. IPSec VPN (Router)**

**Goal:** Secure communication between two networks using encryption.

**Steps:**

1. Define ISAKMP policy:
2. Router(config)# crypto isakmp policy 10
3. Router(config-isakmp)# encryption aes
4. Router(config-isakmp)# hash sha256
5. Router(config-isakmp)# authentication pre-share
6. Router(config-isakmp)# group 14
7. Router(config-isakmp)# lifetime 86400
8. Set the pre-shared key:
9. Router(config)# crypto isakmp key VPN\_KEY address 192.168.1.1
10. Create an IPSec transform set:
11. Router(config)# crypto ipsec transform-set TRANS\_SET esp-aes esp-sha-hmac
12. Define the crypto map:
13. Router(config)# crypto map VPN\_MAP 10 ipsec-isakmp
14. Router(config-crypto-map)# set transform-set TRANS\_SET
15. Router(config-crypto-map)# match address VPN\_TRAFFIC
16. Apply the crypto map to the interface:
17. Router(config)# interface g0/0
18. Router(config-if)# crypto map VPN\_MAP

**3. Disable CDP (Switches)**

**Goal:** Prevent information disclosure.

**Steps:**

1. Disable globally:
2. Switch(config)# no cdp run
3. Disable on specific interfaces:
4. Switch(config)# interface fa0/1
5. Switch(config-if)# no cdp enable

**4. IP Source Guard (Switches)**

**Goal:** Mitigate spoofing attacks.

**Steps:**

1. Enable DHCP snooping:
2. Switch(config)# ip dhcp snooping
3. Switch(config)# ip dhcp snooping vlan 10
4. Enable source guard on interfaces:
5. Switch(config)# interface fa0/1
6. Switch(config-if)# ip verify source

**5. STP Security and BPDU Guard (Switches)**

**Goal:** Protect spanning tree topology from malicious or misconfigured devices.

**Steps:**

1. Enable BPDU Guard:
2. Switch(config)# interface fa0/1
3. Switch(config-if)# spanning-tree bpduguard enable
4. Configure root guard (if necessary):
5. Switch(config)# interface fa0/2
6. Switch(config-if)# spanning-tree guard root

**6. ASA Firewall Configuration**

**Goal:** Implement advanced filtering and VPN capabilities.

**Steps:**

1. Configure basic settings:
2. ASA(config)# interface g0/0
3. ASA(config-if)# nameif outside
4. ASA(config-if)# ip address 203.0.113.1 255.255.255.0
5. ASA(config-if)# no shutdown
6. Create access control policies:
7. ASA(config)# access-list OUTSIDE\_IN extended permit tcp any any eq 80
8. ASA(config)# access-group OUTSIDE\_IN in interface outside

**7. Zone-Based Firewall (Router)**

**Goal:** Define zones and secure inter-zone traffic.

**Steps:**

1. Define zones:
2. Router(config)# zone security INSIDE
3. Router(config)# zone security OUTSIDE
4. Assign interfaces to zones:
5. Router(config)# interface g0/0
6. Router(config-if)# zone-member security INSIDE
7. Create a zone pair and policies:
8. Router(config)# zone-pair security IN-OUT source INSIDE destination OUTSIDE
9. Router(config-sec-zone-pair)# service-policy type inspect OUT\_POLICY

**8. 802.1X Authentication**

**Goal:** Secure port-based network access.

**Steps:**

1. Enable 802.1X globally:
2. Switch(config)# dot1x system-auth-control
3. Configure interfaces:
4. Switch(config)# interface fa0/1
5. Switch(config-if)# dot1x port-control auto
6. Integrate with RADIUS:
7. Switch(config)# radius-server host 192.168.1.100 auth-port 1812 acct-port 1813 key RADIUS\_KEY

**9. TACACS+/RADIUS AAA**

**Goal:** Centralized authentication for device access and WLAN.

**Steps:**

1. Enable AAA:
2. Router(config)# aaa new-model
3. Define TACACS+ server:
4. Router(config)# tacacs-server host 192.168.1.100 key TACACS\_KEY
5. Define RADIUS server:
6. Router(config)# radius-server host 192.168.1.101 auth-port 1812 acct-port 1813 key RADIUS\_KEY
7. Apply authentication:
8. Router(config)# aaa authentication login default group tacacs+ local

**10. WLAN Security (Access Points)**

**Goal:** Secure wireless connectivity.

**Steps:**

1. Configure WPA2/WPA3:
2. AP(config)# ssid Secure\_WLAN
3. AP(config-ssid)# authentication open
4. AP(config-ssid)# authentication key-management wpa version 2
5. AP(config-ssid)# wpa-psk ascii WPA\_KEY

**11. EtherChannel (Switches)**

**Goal:** Aggregate links for redundancy and increased bandwidth.

**Steps:**

1. Create EtherChannel:
2. Switch(config)# interface range fa0/1-2
3. Switch(config-if-range)# channel-group 1 mode active
4. Verify configuration:
5. Switch# show etherchannel summary

A diagram of a computer network

Description automatically generated

A diagram of a computer network

Description automatically generatedA computer network diagram with words and numbers

Description automatically generated

A computer network diagram with a few computers connected to each other

Description automatically generated with medium confidence

A diagram of a computer network

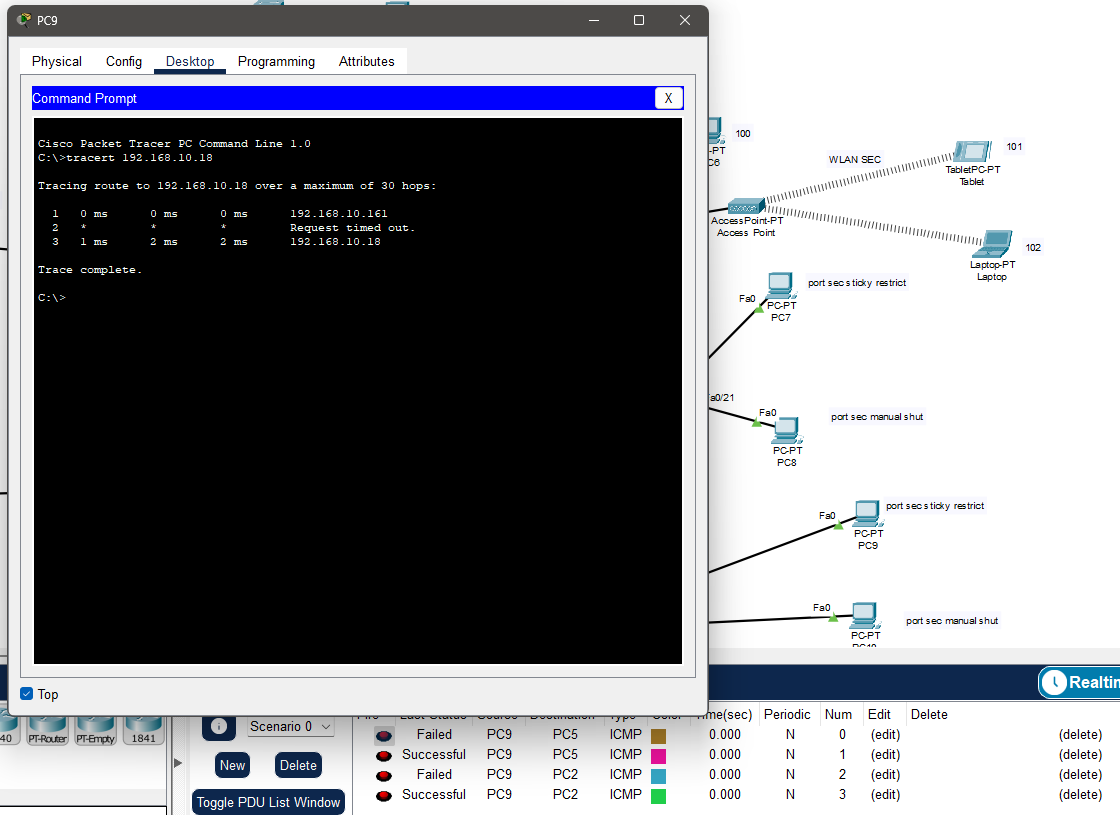
Description automatically generated

A diagram of a network

Description automatically generated

**Testing**

VPN IPsec testing

****

For the rest of the configuration, they have to be monitored by using **ICMP** or the configurations themselves and they will be provided in the **.pkt** file itself.

**(Same for the results)**.

For the exact commands of the configurations for each device .. they can be extracted from the devices themselves from the packet tracer file into a .txt file