Packet Tracer Lab Procedure

This document outlines the procedure for creating and configuring a network in Cisco Packet Tracer. The network will include devices such as routers, switches, PCs, and servers. We will focus on implementing security features such as ACLs, NAT, ZBF, and AAA. This lab will also involve setting up DHCP, RADIUS, Syslog servers, and monitoring network traffic.

# Table of Contents

1. Setting up Devices and Connections  
2. Configuring IP Addresses  
3. Setting up Network Services (DHCP, RADIUS, Syslog)  
4. Configuring ACLs  
5. Implementing NAT  
6. Configuring Zone-Based Firewall (ZBF)  
7. Testing the Configuration  
8. Saving the Configuration

# 1. Set up Devices and Connections

In this step, we will place all the required devices in Packet Tracer and establish the connections between them.  
  
Devices to be added:  
- Routers: 2911 Router (Router 2), ISR4331 Router (Router 3)  
- Switches: 2960-24TT Switch (Switch 1), 2950-24TT Switch (Switch 2), 2950-24TT Switch (Switch 5)  
- PCs: PC-PT (PC\_SSH), PC-PT (PC\_VLAN10), PC-PT (PC\_VLAN20), PC-PT (PC\_ACL\_IN), PC-PT (PC\_ACL\_OUT), PC-PT (PC\_ZBF\_IN), PC-PT (PC\_ZBF\_OUT)  
- Servers: DHCP Server, RADIUS Server, SYSLOG Server  
  
Connections:  
- Use \*\*Copper Straight-Through\*\* cables to connect PCs to switches and switches to routers.  
- Use \*\*GigabitEthernet\*\* or \*\*FastEthernet\*\* cables to connect routers to switches.

# 2. Configuring IP Addresses

Now, configure the devices with IP addresses as per the addressing table. Follow the steps for each device.  
  
1. \*\*Router 2 (2911)\*\*:   
 - G0/0/0: `192.168.1.1 255.255.255.0`  
 - G0/0/1: `192.168.2.1 255.255.255.0`  
  
2. \*\*Router 3 (ISR4331)\*\*:  
 - G0/0/0: `192.168.10.1 255.255.255.0`  
 - G0/0/1: `192.168.20.1 255.255.255.0`  
  
3. \*\*Switches\*\*:  
 - Assign the appropriate IP addresses to VLAN interfaces. For example:  
 - Switch 1: `192.168.30.1 255.255.255.0`  
 - Switch 2: `192.168.40.1 255.255.255.0`  
 - Switch 5: `192.168.50.1 255.255.255.0`  
  
4. \*\*PCs\*\*:  
 - Use the \*\*Desktop > IP Configuration\*\* settings to assign IP addresses, subnet masks, and default gateways.  
  
5. \*\*Servers\*\*:  
 - DHCP Server: `192.168.10.20 255.255.255.0`  
 - RADIUS Server: `192.168.30.20 255.255.255.0`  
 - SYSLOG Server: `192.168.40.20 255.255.255.0`

# 3. Setting up Network Services (DHCP, RADIUS, Syslog)

In this step, configure the network services:  
  
1. \*\*DHCP Server\*\*:  
 - Configure the DHCP server on the Server for the subnet `192.168.10.0/24`.  
 - Set the IP address pool range for the subnet and set the default gateway as `192.168.10.1`.  
  
2. \*\*RADIUS Server\*\*:  
 - Set up the RADIUS server with authentication details (username/password).  
 - Ensure the routers and switches are configured to authenticate using RADIUS.  
  
3. \*\*SYSLOG Server\*\*:  
 - Set up the SYSLOG server to collect logs from network devices.  
 - Configure all routers and switches to send logs to the SYSLOG server.

# 4. Configuring ACLs

1. \*\*Create Standard ACLs\*\*:  
 - Configure a standard ACL on Router 2 to block traffic from `192.168.10.0/24` subnet.  
 Example:  
 ```  
 Router(config)# access-list 1 deny 192.168.10.0 0.0.0.255  
 Router(config)# access-list 1 permit any  
 ```  
 - Apply the ACL to the appropriate interface:  
 ```  
 Router(config-if)# ip access-group 1 in  
 ```  
  
2. \*\*Create Extended ACLs\*\*:  
 - Configure extended ACLs to filter traffic based on source/destination IP, protocol, and port.  
 Example:  
 ```  
 Router(config)# access-list 101 deny tcp any any eq 80  
 Router(config)# access-list 101 permit ip any any  
 ```  
 - Apply the extended ACL to an interface:  
 ```  
 Router(config-if)# ip access-group 101 in  
 ```

# 5. Implementing NAT

1. \*\*Configure NAT Inside and Outside\*\*:  
 - Configure `ip nat inside` on internal-facing interfaces:  
 ```  
 Router(config-if)# interface GigabitEthernet0/0/1  
 Router(config-if)# ip nat inside  
 ```  
 - Configure `ip nat outside` on external-facing interfaces:  
 ```  
 Router(config-if)# interface GigabitEthernet0/0/0  
 Router(config-if)# ip nat outside  
 ```  
 - Configure NAT to allow internal networks to access external resources:  
 ```  
 Router(config)# ip nat inside source list 1 interface GigabitEthernet0/0/0 overload  
 ```

# 6. Configuring Zone-Based Firewall (ZBF)

1. \*\*Enable ZBF\*\* for traffic filtering between internal and external zones:  
 ```  
 Router(config)# zone security inside  
 Router(config)# zone security outside  
 Router(config-if)# interface GigabitEthernet0/0/1  
 Router(config-if)# zone-member security inside  
 Router(config-if)# interface GigabitEthernet0/0/0  
 Router(config-if)# zone-member security outside  
 ```  
  
2. \*\*Create ZBF Policies\*\*:  
 - Define ZBF policies to allow or deny traffic between zones based on security level.  
 ```  
 Router(config)# zone-pair security inside-to-outside source inside destination outside  
 Router(config-sec-zone-pair)# service-policy type inspect INSIDE-OUTSIDE  
 ```

# 7. Testing the Configuration

1. \*\*Test Connectivity\*\*:  
 - Use the `ping` command to verify that devices can communicate across the network.  
 - Test SSH access to the routers and switches.  
  
2. \*\*Test DHCP\*\*:  
 - Verify that PCs are receiving IP addresses from the DHCP server.  
  
3. \*\*Verify ACLs\*\*:  
 - Check that the ACLs are correctly filtering traffic.  
  
4. \*\*Monitor Logs\*\*:  
 - Use the Syslog server to verify that logs are being collected from network devices.

# 8. Saving the Configuration

1. \*\*Save the Configuration\*\*:  
 - Save the running configuration to the startup configuration on each device:  
 ```  
 Router# copy running-config startup-config  
 ```  
  
2. \*\*Save the Packet Tracer File\*\*:  
 - Save the Packet Tracer file as a \*\*.pka\*\* file for future practice and analysis.