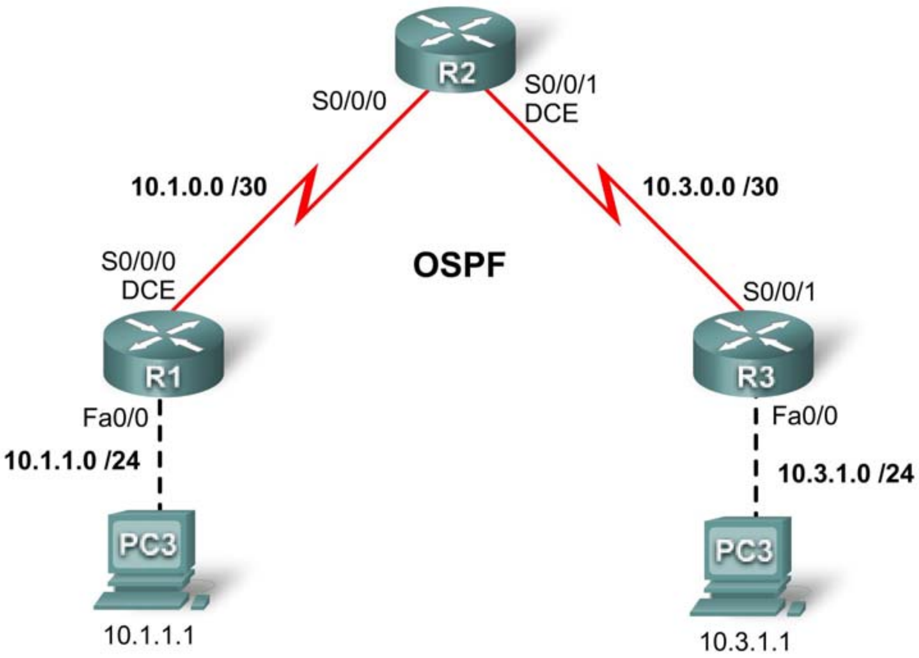
PT Activity 5.5.2: Challenge Access Control Lists

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**S0/0/0**	10.1.0.1	255.255.255.252	N/A
	Fa0/0	10.1.1.254	255.255.255.0	N/A
R2	**S0/0/0**	10.1.0.2	255.255.255.252	N/A
	S0/0/1	10.3.0.1	255.255.255.252	N/A
R3	**S0/0/1**	10.3.0.2	255.255.255.252	N/A
	Fa0/0	10.3.1.254	255.255.255.0	N/A
PC1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC2	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

- Perform basic router configurations
- Configuring standard ACLs
- Configuring extended ACLs
- Verifying ACLs

Introduction

In this activity, you will design, apply, test and troubleshoot access list configurations.

Task 1: Perform Basic Router Configurations

Configure all devices according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode secret of **class**.
- Configure a **message-of-the-day** banner
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure IP addresses and masks on all devices. Clock rate is **64000**.
- Enable OSPF with process ID 1 on all routers for all networks.
- Verify full IP connectivity using the **ping** command.

Task 2: Configuring Standard ACLs

Configure standard named ACLs on the R1 and R3 vty lines, permitting hosts connected directly to their Fast Ethernet subnets to gain Telnet access. Deny all other connection attempts. Name these standard ACLs **VTY-Local** and apply to all telnet lines. Document your ACL configuration.

____

____

____

____

____

____

____

Task 3: Configuring Extended ACLs

Using extended ACLs on R2, complete the following requirements:

- Name the ACL block
- Prohibit traffic originating from the R1 connected subnets from reaching the R3 connected subnets.
- Prohibit traffic originating from the R3 connected subnets from reaching the R1 connected subnets.
- Permit all other traffic.

Document your ACL configuration

Task 4: Verifying ACLs

Step 1. Test telnet.

- PC1 should be able to telnet into R1
- PC3 should be able to telnet into R3
- R2 should be denied telnet access to R1 and R3

Step 2. Test traffic.

Pings between PC1 and PC3 should fail.