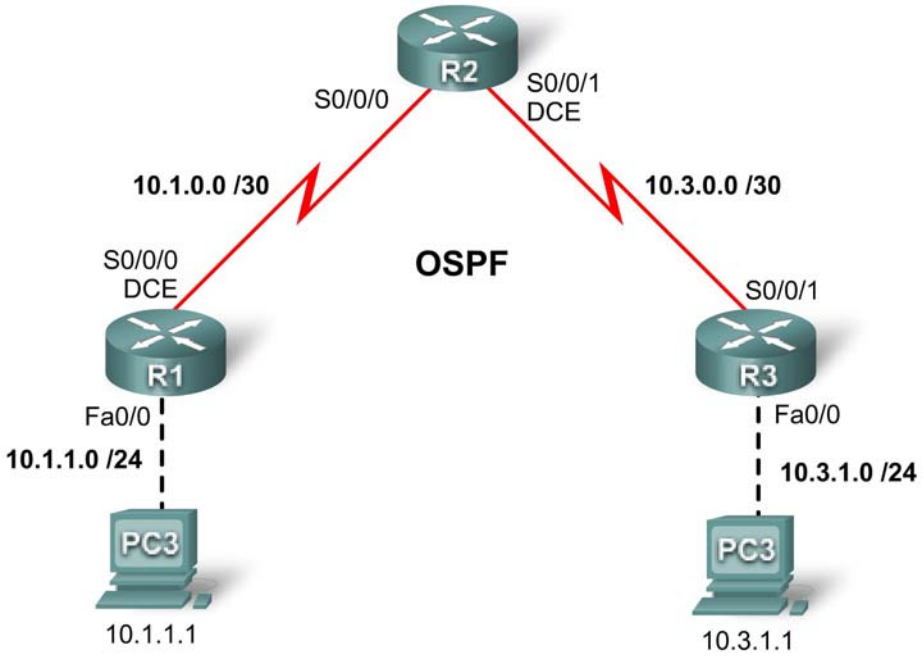
PT Activity 5.5.2: Challenge Access Control Lists

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.
- Configure standard ACLs.
- Configure extended ACLs.
- Verify ACLs.

Introduction

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

Task 1: Perform Basic Configurations

Step 1. Configure all devices.

Configure all devices according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an encrypted privileged EXEC password 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.
- Configure IP addressing and default gateways on each PC.
- Verify full IP connectivity using the **ping** command.

Step 2. Check results.

Your completion percentage should be 85%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configuring Standard ACLs

Step 1. Configure standard ACLs on R1 and R3.

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

_____

_____

_____

_____

_____

_____

_____

Step 2. Check results.

Your completion percentage should be 94%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configuring Extended ACLs

Step 1. Configure extended ACLs on R2.

Using extended ACLs on R2, complete the following requirements:

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

Document your ACL configuration

_____

_____

_____

_____

_____

_____

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Verifying ACLs

Step 1. Test telnet.

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

Step 2. Test traffic.

Pings between PC1 and PC3 should fail.

