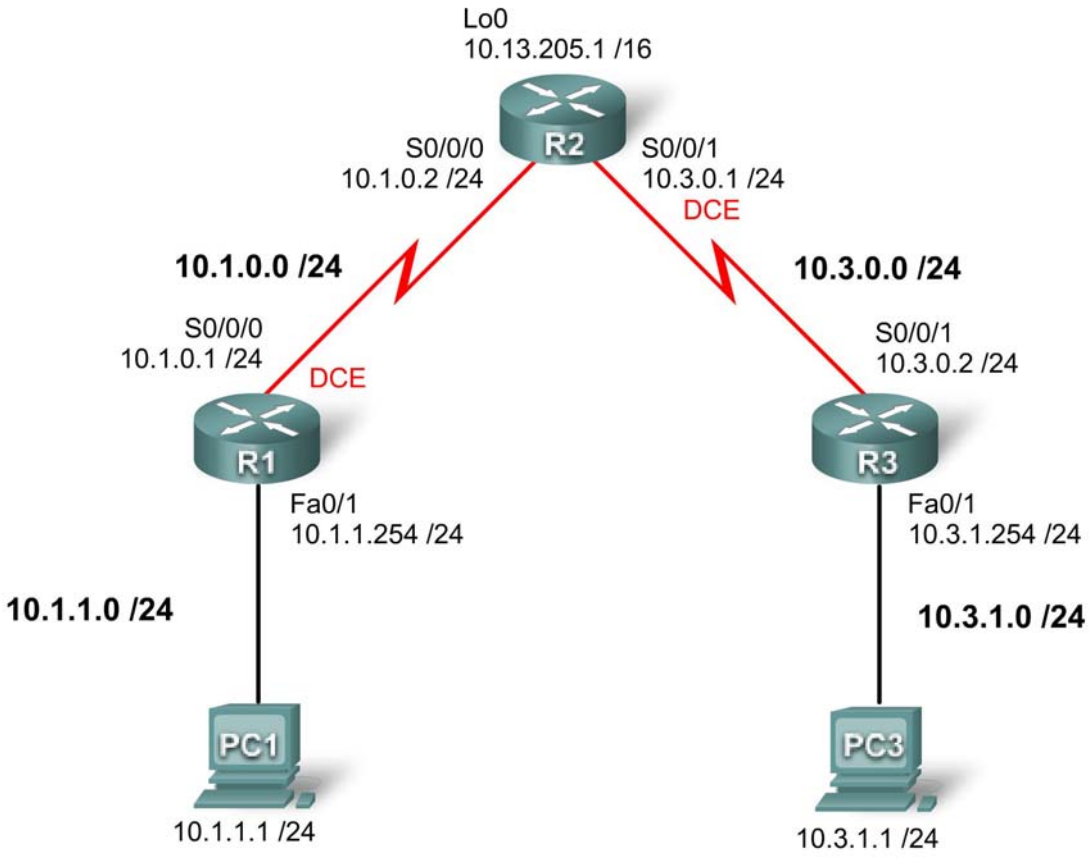
Lab 5.5.2: Access Control Lists Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**S0/0/0**	10.1.0.1	255.255.255.0	N/A
	Fa0/1	10.1.1.254	255.255.255.0	N/A
R2	**S0/0/0**	10.1.0.2	255.255.255.0	N/A
	S0/0/1	10.3.0.1	255.255.255.0	N/A
	Lo 0	10.13.205.1	255.255.0.0	N/A
R3	**S0/0/1**	10.3.0.2	255.255.255.0	N/A
	Fa0/1	10.3.1.254	255.255.255.0	N/A
PC 1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

To complete this lab:

- Design named standard and named extended ACLs.
- Apply named standard and named extended ACLs.
- Test named standard and named extended ACLs.
- Troubleshoot named standard and named extended ACLs.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: If you use a 1700, 2500, or 2600 router, the router outputs and interface descriptions may appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Configure IP addresses on all devices.
- Create a loopback interface on R2.
- Enable OSPF area 0 on all routers for all networks.
- Verify full IP connectivity using the **ping** command.

Task 3: Configuring Standard ACLs

Configure standard named ACLs on the R1 and R3 VTY lines, permitting hosts connected directly to their FastEthernet subnets to gain Telnet access. Deny and log all other connection attempts. Document your testing procedures.

_____

_____

_____

_____

Task 4: Configuring Extended ACLs

Using extended ACLs on R2, complete the following requirements:

- The LANs connected to R1 and R3 are used for student computer labs. The network administrator has noticed that students in these labs are playing games across the WAN with the remote students. Make sure that your ACL prevents the LAN attached to R1 from reaching the LAN at R3 and that the LAN on R3 cannot reach the LAN on R1. Be specific in your statements so that any new LANs added to either R1 or R3 are not affected.
- Permit all OSPF traffic.
- Permit ICMP traffic to the R2 local interfaces.
- All network traffic destined to TCP port 80 should be allowed. Any other traffic should be denied and logged.
- Any traffic not specified above should be denied.

Note: This may require multiple access lists. Verify your configuration and document your testing procedure.

Why is the order of access list statements so important?

_____

_____

Task 5: Verifying an ACL

Test each protocol that you are trying block, and make sure that permitted traffic is allowed.

Task 6: Document the Router Configurations

Task 7: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

