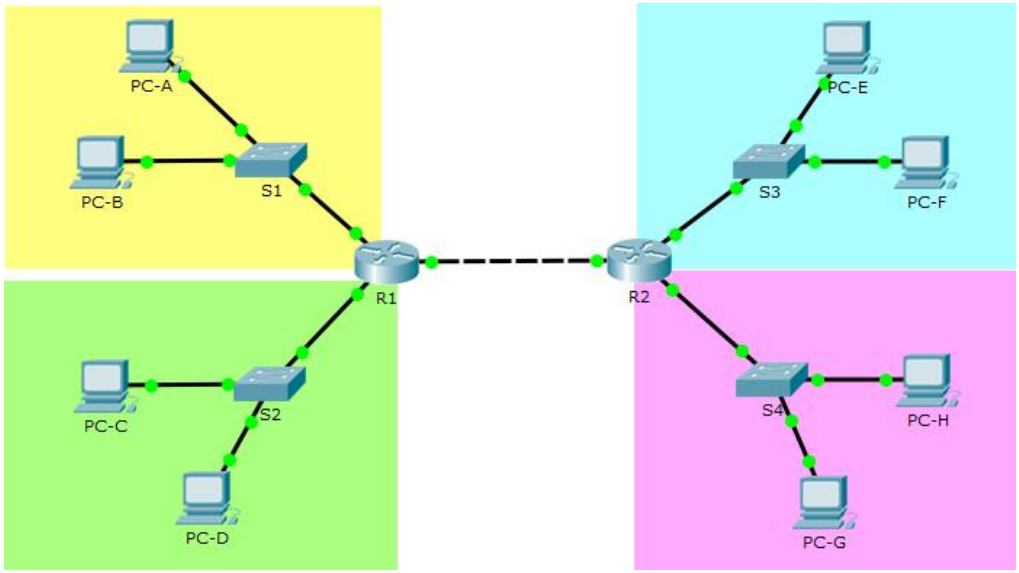
Lab 2 - Configure Standard IPv4 ACLs

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	G0/1	192.168.2.1	255.255.255.0	
	G0/2	192.168.250.1	255.255.255.0	
R2	G0/0	172.16.1.1	255.255.255.0	N/A
	G0/1	172.16.2.1	255.255.255.0	
	G0/2	192.168.250.2	255.255.255.0	
PC-A	NIC	192.168.1.100	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.150	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.50	255.255.255.0	192.168.2.1
PC-D	NIC	192.168.2.112	255.255.255.0	192.168.2.1
PC-E	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC-F	NIC	172.16.1.20	255.255.255.0	172.16.1.1
PC-G	NIC	172.16.2.100	255.255.255.0	172.16.2.1
PC-H	NIC	172.16.2.200	255.255.255.0	172.16.2.1

Lab 2 - Configure Standard IPv4 ACLs

Objectives

Restrict traffic on the network by configuring standard IPv4 ACLs.

Background / Scenario

An organization has recently decided to restrict traffic using standard IPv4 ACLs. As the network administrator, it is your job to configure two standard IPv4 ACLs to restrict traffic to the Pink LAN and the Blue LAN (see PT Topology Diagram). You must also configure a named standard IPv4 ACL to restrict remote access to router R1. Router interfaces and default/static routes have already been configured. Remote SSH access has also been enabled on the routers. You will need the following access information for console, VTY, and privileged EXEC mode:

Username: **admin01**

Password: **ciscoPA55**

Enable secret: **secretPA55**

Part 1: Configure a Standard IPv4 ACL to Restrict Access to the Pink LAN

In Part 1, you will configure and apply access list 10 to restrict access to the Pink LAN.

Step 1: Outline what you wish to accomplish with access list 10.

Access list 10 should have 4 access control entries to do the following:

1) Access list 10 should start with the following comment: ACL_TO_PINK_LAN
2) Permit PC-C to reach the Pink LAN
3) Permit only the first half of hosts on the Yellow LAN, so they can reach the Pink LAN
4) Permit all of the hosts on the Blue LAN to reach the Pink LAN

Access list 10 should be configured on the correct router, and applied to the correct interface and in the right direction.

Step 2: Create, apply, and test access-list 10.

After configuring and applying access list 10, you should be able to execute the following network tests:

1) A ping from PC-A to a host in the Pink LAN should be successful, but a ping from PC-B should be denied.
2) A ping from PC-C to a host in the Pink LAN should be successful, but a ping from PC-D should be denied.
3) Pings from hosts in the Blue LAN to hosts in the Pink LAN should be successful.

QUESTION 1 What message is sent back to the PCs when a ping is denied due to an ACL?

QUESTION 2 Which IP address on the Green LAN is permitted to ping hosts on the Pink LAN?

Before proceeding, go to the "Lab 2 - Configure Standard IPv4 ACLs - QUESTIONS" quiz on the Moodle page and enter your answer for questions 1 and 2. Leave the quiz open while you complete the rest of the lab sheet.

Part 2: Configure a Standard IPv4 ACL to Restrict Access to the Blue LAN

In Part 2, you will configure and apply access list 20 to restrict access to the Blue LAN.

Step 1: Outline what you wish to accomplish with access list 20.

Access list 20 should have 3 access control entries to do the following:

1) Access list 20 should start with the following comment: ACL_TO_BLUE_LAN
2) Permit PC-A to reach the Blue LAN
3) Deny the Yellow LAN from reaching the Blue LAN
4) Allow all other networks to reach the Blue LAN

Access list 20 should be configured on the correct router, and applied to the correct interface and in the right direction.

Step 2: Create, apply, and test access-list 20.

After configuring and applying access list 20 you should be able to execute the following network tests:

1) Only PC-A on the Yellow LAN can successfully ping the Blue LAN.
2) Pings from hosts in the Yellow LAN to the Blue LAN should fail.
3) Pings from hosts in the Green and Pink LANs to the Blue LAN should be successful.

Part 3: Configure a Named Standard IPv4 ACL

In Part 3, you will configure and apply a named standard IPv4 ACL to restrict remote access to router R1.

Step 1: Outline what you wish to accomplish with named standard ACL.

The named access list should do the following:

1) On R1 create a standard ACL named ADMIN_VTY
2) Permit a single host, PC-C
3) Apply the ACL to the VTY lines

Step 2: Test access-list ADMIN_VTY.

After configuring and applying access list ADMIN_VTY, you should be able to execute the following network test:

1) An SSH connection from host PC-C to R1 should be successful.
2) SSH connections from all other hosts should fail.

QUESTION 3 This lab features two standard ACLs to restrict traffic to the Pink and Blue LANs. If you needed to restrict traffic to the Yellow LAN, where would the ACL need to be created/placed?

QUESTION 4 If you needed to restrict traffic to the Green LAN, where would the ACL need to be created/placed?

Before proceeding, go to the "Lab 2 - Configure Standard IPv4 ACLs - QUESTIONS" quiz on the Moodle page and enter your answer for questions 3 and 4.

If you have correctly configured all parts of the lab your activity score should now be showing as 100%. If so, click on "check results" in the activity window. Return to the Moodle quiz one last time and enter the code into the appropriate question box (Q5) of the quiz.

You have completed the lab – please submit the Moodle quiz.