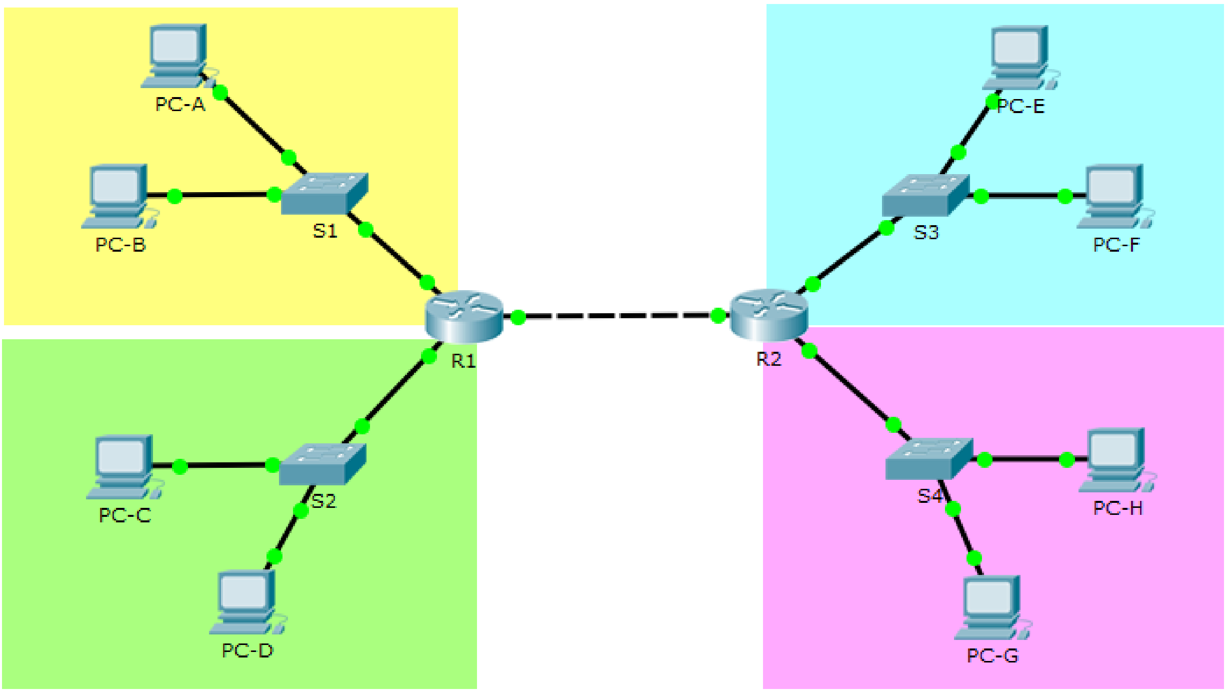
Packet Tracer – Configure Standard IPv4 ACLs (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

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

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.

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

____

A destination unreachable message.

Which IP addresses on the Yellow LAN are permitted to ping hosts on the Pink LAN?

____

Access list 10 permits pings to the Pink LAN from hosts 192.168.1.1 to 192.168.1.127 on the Yellow LAN.

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.

Step 3: Insert an ACE into access-list 20.

You need to make a change to access list 20. Insert an access control entry into access list 20 to permit PC-A to reach the Blue LAN. Insert the ACE prior to the other access list 20 permit and deny access control entries.

How do you insert or remove an ACE into a specific line of an ACL?

____

To insert or remove an ACE on a specific line enter the ACL using the *ip access-list* keywords and arguments as if the numbered ACL was a named ACL.

What line did you enter the ACE on?

____

Answers may vary but inserting the ACE on lines 1 through 9 would all work.

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.

Reflection

This lab features two standard ACLs to restrict traffic to the Pink and Blue LANs. Could you create 2 more standard ACLs to restrict traffic to the Yellow and Green ACLs and which router would those ACLs need to be created on?

____

____

Yes, you could create a standard ACL for G0/0 and G0/1 on router R1 to restrict access to the Yellow and Green LANs.

Script

R1

```
ip access-list standard ADMIN_VTY
 permit 192.168.2.50
line vty 0 4
 access-class ADMIN_VTY in
```

R2

```
access-list 10 remark ACL_TO_PINK_LAN
access-list 10 permit host 192.168.2.50
access-list 10 permit 192.168.1.0 0.0.0.127
```

```
access-list 10 permit 172.16.1.0 0.0.0.255
access-list 20 remark ACL_TO_BLUE_LAN
access-list 20 permit host 192.168.1.100
access-list 20 deny 192.168.1.0 0.0.0.255
access-list 20 permit any
interface gigabitEthernet0/0
 ip access-group 20 out
interface gigabitEthernet0/1
 ip access-group 10 out
```