**Unit 1 Performance Assessment 2 – ACLs**

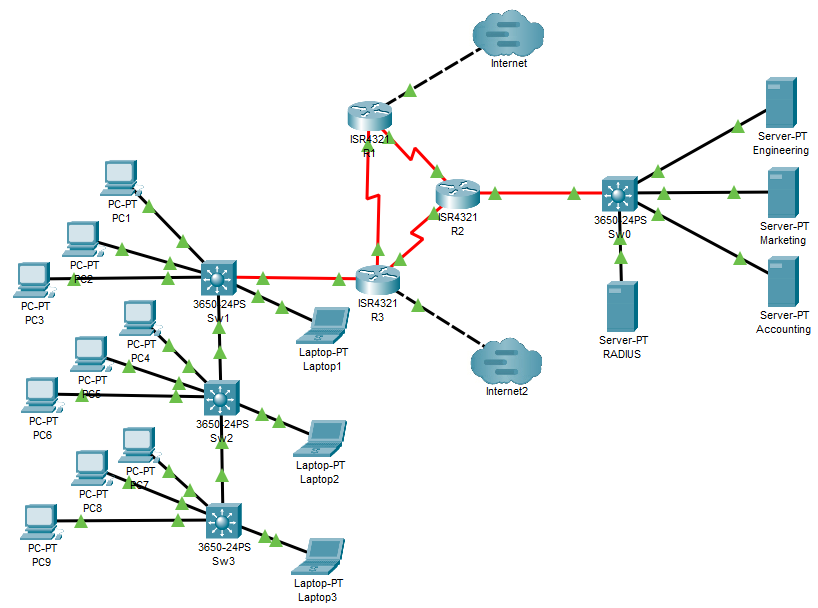
In this lab you will be reviewing the networking that you have learned in your program. You will be using Packet Tracer for the lab.

Your network will a class B network based on a number assigned by your professor, which you will be using for the duration of the class. In the lab anytime you see an underline you should fill in this number.

**Student network: 10.\_\_\_\_.0.0/16**

**Task 1 – Create the standard ACLs**

**Using the network you completed for 1.3 Performance Assessment: Review, you are going to create a standard ACL for each subnetwork that will allow us to limit access to the servers to only the groups that should have access.**



**Server access limiting**

A standard access-list uses the following three guidelines:

1. Standard Access-list is generally applied close to destination
2. Standard access-list uses the range 1-99 and 1300-1999
3. Standard access-list is implemented using source IP address only.

Add the access-list to the R2 router using the following commands

R2(config)# access-list 1 permit 10.\_\_\_.3.0 0.0.0.31

R2(config)# access-list 1 permit 10.\_\_\_.3.64 0.0.0.7

Now add the access list to the sub-interface

R2(config)# interface g0/0/0.10

R2(config-subif)# ip access-group 1 out

This ACL will allow only users in VLANs 10 and 40 to reach the Engineering Server. Test this ACL by pinging the Engineering Server from a user (laptop/PC) from each VLAN.

Now add a standard access list for interfaces g0/0/0.20 & g0/0/0.30 on R2.

R2(config)# access-list 2 permit 10.\_\_\_.3.32 0.0.0.15

R2(config)# access-list 2 permit 10.\_\_\_.3.64 0.0.0.7

R2(config)# access-list 3 permit 10.\_\_\_.3.48 0.0.0.15

R2(config)# access-list 3 permit 10.\_\_\_.3.64 0.0.0.7

R2(config)# interface g0/0/0.20

R2(config-subif)# ip access-group 2 out

R2(config)# interface g0/0/0.30

R2(config-subif)# ip access-group 3 out

Take a screenshot of all of the access-lists with a show run command on R2.

From a PC in VLAN 10 verify that your PC can reach the Engineering server but cannot reach the Marketing or Accounting servers. Take a screenshot of your successful ping to Engineering and your failed pings to Marketing and Accounting. Take three screenshots.

Perform the same task from a PC in VLAN 20 and a PC in VLAN 30.

Devices in VLAN 20 should be able to reach the Marketing server but cannot reach the Engineering or Accounting servers.

Devices in VLAN 30 should be able to reach the Accounting server but not the Engineering or Marketing servers.

Take three screenshots for each.

Verify that your laptop1 is able to reach each of the servers. Take three screenshots.

**Turn off Internet for Accounting**

The accounting office has asked that you do not allow their employees access to the Internet. Use a standard access list to deny them access to the Internet connections.

On the R1 router add the following ACL

R1(config)# access-list 1 deny 10.\_\_\_.3.48 0.0.0.15

R1(config)# access-list 1 permit any

Add the access list to the Internet interface.

R1(config)# interface g0/0/1

R1(config-if)# ip access-group 1 out

Create the same access control list for the R3 router for the Internet2 connection.

Verify you can no longer reach the Internet from you Accounting department. Take a screenshot of your failed ping to the Tier1 Internet Server.

**Deliverables**

* Screenshot of access-list from *show run* on the R2 router
* Screenshots of successful and failed pings
* Screenshots of access-list from *show run* on the R1 and R3 router
* Screenshot of failed ping to the Tier1 Internet Server from a PC in Accounting (VLAN 30)
* Screenshot of successful ping to the Tier 1 server from PCs in Engineering (VLAN 10) and Marketing (VLAN 20)

PASTE SCREENSHOTS BELOW- LABEL YOUR SCREENSHOTS

**Task 2 – Create the Extended ACLs**

Go back to R1, R2, and R3 and remove your standard ACLs and your access-groups from each interface.

R2(config)# no access-list 1

R2(config)# interface g0/0/0.10

R2(config-subif)# no ip access-group 1 out

Do the same for all access list and groups for each router.

An extended access-list uses the following five guidelines:

1. Extended access-lists are generally applied as close to source as possible.
2. Extended access-lists use the range 100-199 and 2000-2699.
3. Extended access-list can be implemented using source IP, destination IP, type of packet, and port number for the service.
4. Extended access-lists are by far the most common in use today.
5. Extended access-lists can use names as well as numbers.

Add the extended access-list to the R3 router using the following commands

R3(config)# access-list 100 deny ip any 10.\_\_\_.2.64 0.0.0.63

R3(config)# access-list 100 deny ip any 10.\_\_\_.2.128 0.0.0.63

R3(config)# access-list 100 permit ip any any

Now apply your access list to each of the subinterfaces

R3(config)# interface g0/0/0.10

R3(config-subif)# ip access-group 100 in

This extended access-list prevents users in VLAN 10 from accessing the Marketing and

Accounting servers.

Apply an access-list to each sub-interface on the R3 router to exclude access to the servers from the other groups.

R3(config)# access-list 101 deny ip any 10.\_\_\_.2.0 0.0.0.63

R3(config)# access-list 101 deny ip any 10.\_\_\_.2.128 0.0.0.63

R3(config)# access-list 101 permit ip any any

R3(config)# interface g0/0/0.20

R3(config-subif)# ip access-group 101 in

R3(config)# access-list 102 deny ip any 10.\_\_\_.2.0 0.0.0.63

R3(config)# access-list 102 deny ip any 10.\_\_\_.2.64 0.0.0.63

R3(config)# access-list 102 permit ip any any

R3(config)# interface g0/0/0.30

R3(config-subif)# ip access-group 102 in

This extended access-list prevents users in VLAN 30 from accessing the Engineering and Marketing servers.

Now it’s time to test your ACLs. Perform a ping to each server from a device from each VLAN (10, 20 and 30). Create a screenshot for each ping and make sure you label each screenshot. Which pings work? Why? Which pings don’t work? Why?

**Turn off Internet for Marketing**

The marketing office has asked that you do not allow their employees access to the Internet. Add an extended access list to deny them access to the Internet connections.

First remove the access list you applied to interface g0/0/0.20 in the previous section.

R3(config)#no ip access-group 101 in

Then on the R3 router add the following ACL:

R3(config)# access-list 199 deny ip any 11.1.1.0 0.0.0.255

R3(config)# access-list 199 permit ip any any

Add the access list to the Internet interface.

R3(config)# interface g0/0/0.20

R3(config-if)# ip access-group 199 in

Test this ACL by pinging the Tier1 Internet Server from a device in VLAN 20. What is the result? Can you ping the Tier1 Internet Server from the devices in other VLANs? Why or why not?

Verify you can no longer reach the Internet from you Marketing department. Take a screenshot of your failed ping to the Tier1 Internet Server.

**Deliverables**

* Screenshot of access-lists from show run on the R3 router
* Screenshots of successful and failed pings from VLANs 10, 20 and 30
* Screenshot of failed ping to the Tier1 Internet Server from a device in VLAN 20.
* Screenshot of successful ping to the Tier1 Internet Server from a device in VLAN 10 and 30
* Answer the questions.

PASTE SCREENSHOTS BELOW- LABEL YOUR SCREENSHOTS