Video Demonstration - Standard ACL Configuration Part 1 (8 min)

In this activity, we're going to configure standard IPV for access lists. According to the lab instructions, our first access list is access list 10 and it's going to be permitting or denying traffic to the pink LAN here. With a standard access list, we permit or deny based on source IPV for addressing and then the access list is placed closest to the destination. Since this access list is going to be affecting traffic to the pink LAN, the access list will be created on R2 and the interface it'll be placed on is this interface right here, outbound.

Let's get started and create this access list. I'll go into R2. I'll put in the username, admin01, which is in the instructions. The password is cisco, capital P-A 55. The enable secret is secret, capital P-A 55, and then I'll go to global config mode and I'm ready to create my access list. Now, I've already typed out my access list in notepad and following the instructions, the first line is a comment or in this case a remark, ACL_TO_PINK_LAN. This lets me know in this comment or remark what this access list is intending to do and it's an access list which is going to affect traffic to the pink LAN.

Then in the next line, I'm supposed to permit host PC C located at 192.168.2.50, so you can see it says here, access list 10 permit host 192.168.2.50. The next line is a little bit trickier. I'm supposed to permit half the first half of the host on the one network so that they can reach the pink LAN. The one network is a slash 24 network so what I've done is, instead of putting 192.168.1.0 with wildcard bit 0.0.0.255, I've changed it to 0.0.0.127. This is essentially changing the mask or the wildcard bits from slash 24 to slash 25. This will permit only half of the host addresses on that network. I'm using the masking or in the wildcard bits to effect which hosts are permitted.

The last one permits the entire 172161.0 network which is, we'll take a look, let me highlight this and copy it first. Control C. This effectively permits the first half of the host on the yellow network. Host PC C on the green network, and all of the hosts on the blue network to reach the pink LAN. In R2, all I have to do is basically right click and paste and there is my access list. To apply it I need to apply it to this interface right here. I can't tell what interface is this? To figure it out, you can look in the lab instructions or sometimes the running configuration will help you.

In the running config, you can see that it says, "Interface Gigabit 0/1 description PINK_LAN" so the description on the interface tells us what network it is so this is where we want to place our access list. I'll go into interface Gigabit 0/1 and put in the command, "IP Access group," the access list number is 10 outbound. Traffic leaving R2 headed towards the pink LAN and now the access list is applied.

In the next step, you'll need to test your access list to make sure that it works. We can do that by pinging from the network across. PC A is in the first half of the hosts in the yellow network and PC B is in the second half of the hosts in the yellow network so PC pings from PC A to PC H should be okay or be successful and a ping from PC B to PC H should fail. Let's try that out by using the simple PDU creator here. We just click from PC A to PC H and that should be successful and it is and if it's not successful and it fails, you'll have to do it a couple times and it'll eventually work and then I'll do another one from here to here and you can see that failed.

Then you can test using the same method from the green network to the pink network, PC C should be successful. PC D should fail and then both PC's here should be successful to reach the pink network. Time for our second access list. Now, our second access list is going to be access list 20 and it's going to permit or deny traffic to the blue LAN. To do this, I've also already written out the access list in Notepad which is a good habit to get into is to have it documented.

The first line access list 20 remark, this is a comment and it tells us what the access list is going to do and then the next line denies traffic from the one network. The one network, the entire one network meaning 192.168.1.0 with slash 24 worth of wildcard bits here. Then permitting every other network. I'll highlight that, copy, and I'll just paste this in here. I'm going to exit first. Go to global config and paste it. All right, now all I need to do is apply it. We looked in the running config and the running config showed us that the blue LAN which is where we want to permit and deny traffic to is on Gigabit 0/0. We'll just apply that to Gigabit 0/0, and IP access group 20 outbound.

Now we've applied that to this interface here. Outbound so as traffic comes from here and cross the router and starts to leave it, it should be denied, traffic from the yellow network. We'll just test that out really quickly.

Just go from here to here. Can see it failed and it also should fail from here to here and we can test that out and that also failed but everywhere else should be successful. We'll try that. Say from here to here. All right and that failed so it might take a second attempt. Let's see if it works the second time. It did so it's doing what we want to do.