Video Demonstration – Standard ACL Configuration Part 2 (7 min)

Now, in this access list in the instructions it says, "Uh-oh, you've changed your mind. You've decided after all you want to allow a single host on the yellow LAN, PC-A, to reach the blue LAN." How do you do that? How do you insert an additional line into the access list without having to rewrite the entire access list. In other words, if we look at the access list ... show access list, you can see that in access list 20 we want to add a line allowing one host on the one network. Now, if we just add one other line, it'll go at the bottom of the access list and the entire one network will be denied prior to permitting the single host. We need to add that line above this line right here.

To do this what we can do is, we can enter the access list as if it's a named access list and place it on a line number prior to ten. You can see how the access control entries are all given a line number, 10, 20, 30. Then for access list 20, this has given line number 10, line number 20. If we can insert that statement prior to line number 10 then we can have this work. Now to do that what we can do is, we'll go into the access list 20 as if it was a named access list. In other words, instead of saying access list 20, we say, "IP access-list standard 20." Then we're in, "Configure Standard Named Access List Mode," and we can put in the line number, we say, "line #5 permit host 192.168.1.100."

Now that should go prior, at the beginning essentially, of the access list. Let's see if that worked. We'll say, "Control-C," and show access list, and you can see that we've entered that line instead of it being it having it entered at the bottom of the access list which wouldn't have worked. We were able to successfully insert it on line five prior to any of the other lines even though it was a numbered access list, access list 20, we were able to insert it as if it was a named access list. That was pretty cool. Now that host should be permitted. We can test that out. Scroll down and you can see now it's allowed. Excellent. Now, the last access list that we'll need to create is a named ACL or a named standard ACL.

We're going to create it on R1 and apply it to the VTY lines or R1. This will restrict which hosts or which addresses are allowed to SSH or telnet into Router R1. Now, SSH has already been configured on R1 and all we need to do is restrict access so that only PC-C can SSH into R1. To do this, we'll need to create a named access list. What we'll do is, we'll put in the password, "admind01," is the username and the password is, "ciscoPA55." Then we'll put in the enable secret, "secretPA55," "secretPA55." Great, we're in. We'll go to "Global Config Mode," and we need to create our named access list. To do this, we'll put in the command, "ip access-list." It's going to be a standard ACL. The name of the ACL needs to be all caps, "ADMIN_VTY," so "ADMIN_VTY." Now we're in "Named Access List Mode."

All we need to do is, "permit host 192.168.2.50." Perfect. That's it. Our access list is actually finished. We want to just permit one IP address and we want to apply this access list, this names access list, to our VTY lines. To do that, we'll need to go to, "line vty 0 4," all the VTY lines. We'll put in the command. We'll put in a question mark, how about that. You can see here, "access-class filter connections based on an IP access list." Open the command, "access-class," and the a question mark, the IP access list name, "ADMIN_VTY," and then the direction, inbound, "Control-C," "Show run." We should, if we got to the bottom here, be able to see it, "line vty 0 4," "access-class ADMIND_VTY," inbound. It's applied. Notice the login is restricted to the local database of users and the transport input has been set to SSH, so only PC-C should be allowed to SSH into the router. Let's test out it.

Go to PC-C ... and, "ssh-l." Login the name, "admin01," and the address, let's see here, "192.168.2.1," and the password is, "ciscoPA55." We're in. Enable secret, "PA55," secret, "PA55." We have privileged exec access. Let's see if that will work. Copy. Now, that shouldn't work from PC-D. The desktop, "Command Prompt," paste that in there, "Connection refused by remote host." It's working. PC-C was allowed, PC-D wasn't, looks like our access list is working. Also, on this activity you can look at the completion percentage in the packet trace activity instructions and you should see, "Completion 100%."