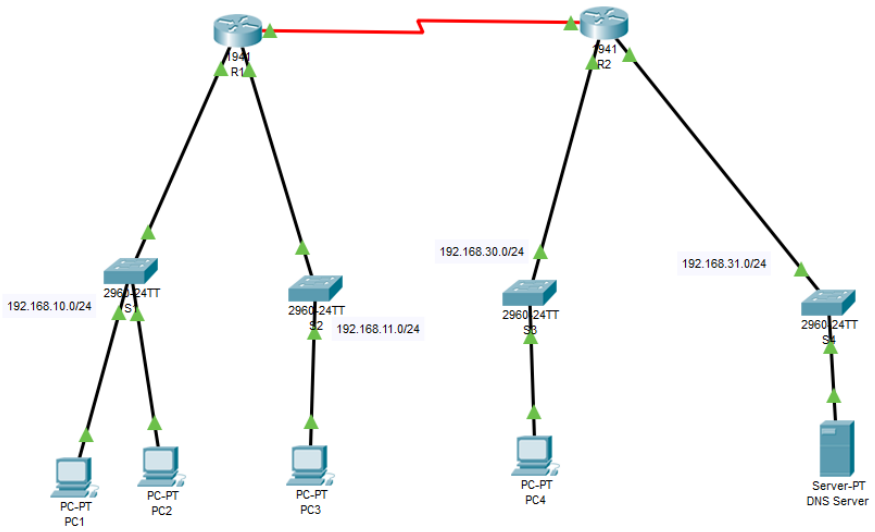
Week 9 Lab- ACL part 1- Solution: ACL Demonstration – show access-lists command

You may wish to link this exercise to the PPT document on BBL named Access Control Lists.

Topology



Remember: Before applying any ACLs to a network, it is important to confirm that we have full connectivity. Verify that the network has full connectivity by choosing a PC and pinging other devices on the network (or by route tracing). A confirmation can be in the form of being be able to successfully ping every device.

Background

An access control list (ACL) can be used to prevent a ping (instead of pinging you may prefer route tracing) from reaching hosts on remote networks. We may need to find out where the ACL is configured and remove it if necessary. Verify Local Connectivity and Test Access Control List

Step 1: Ping devices on the local network to verify connectivity.

a. From the command prompt of **PC1**, ping **PC2 (both are in the same LAN)**; and from the command prompt of **PC1**, ping **PC3 (in two different LANs / segments).** Why were the pings successful?

There is no policy filtering ICMP messages (and any other protocol message) between the two local networks. There is nothing restricting layers 1,2, and 3 technology and protocols, functions or services.

Step 2: Ping devices on remote networks to test ACL functionality.

a. From the command prompt of **PC1**, ping **PC4 (which is in a remote network); and f**rom the command prompt of **PC1**, ping the **DNS Server (the DNS server is also in a remote network)**.

Why did the pings fail? Where did the pings stop? (Hint: Use simulation mode or view the router configurations to investigate.) You may also repeat these steps and use PC2 to ping PC4 and DNS Server. The pings fail because R1 is configured with an ACL to deny any ping from exiting the serial 0/0/0 interface. This ACL does not affect 192.168.11.0/24.

Part 2: Remove ACL and Repeat Test

Step 1: Use show commands to investigate the ACL configuration.

a. To quickly view the current ACLs, use **show access-lists**. Enter the **show access-lists** command, followed by a space and a question mark (?) to view the available options:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

If you know the ACL number or name, you can filter the **show** output further. However, **R1** only has one ACL; therefore, the **show access-lists** command will suffice.

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

Can you explain what this ACL can do? Link you answer to the wildcard used (0.0.0.255 – what does such mask do?)

The first line of the ACL prevents any packets originating in the **192.168.10.0/24** network, which includes Internet Control Message Protocol (ICMP) echoes (ping requests). The second line of the ACL allows all other **ip** traffic from **any** source to transverse the router.

Use **show running-config** to yet view this ACL in the running configuration file? You should also see in which direction the ACP is applied. You can also use the command **show ip interface** to get such information. Outgoing traffic on S0/0/0.

Step 2: Remove access list 11 from the configuration

You can remove ACLs from the configuration by issuing the **no access list** [*number of the ACL*] command. The **no access-list** command deletes all ACLs configured on the router. The **no access-list** [*number of the ACL*] command removes only a specific ACL.

a. Under the Serial0/0/0 interface, remove access-list 11 previously applied to the interface as an **outgoing** filter:

```
R1(config)# int se0/0/0
R1(config-if)#no ip access-group 11 out
```

b. In global configuration mode, remove the ACL by entering the following command:

```
R1(config)# no access-list 11
```

c. Verify that **PC1** can now ping the **DNS Server** and **PC4**.