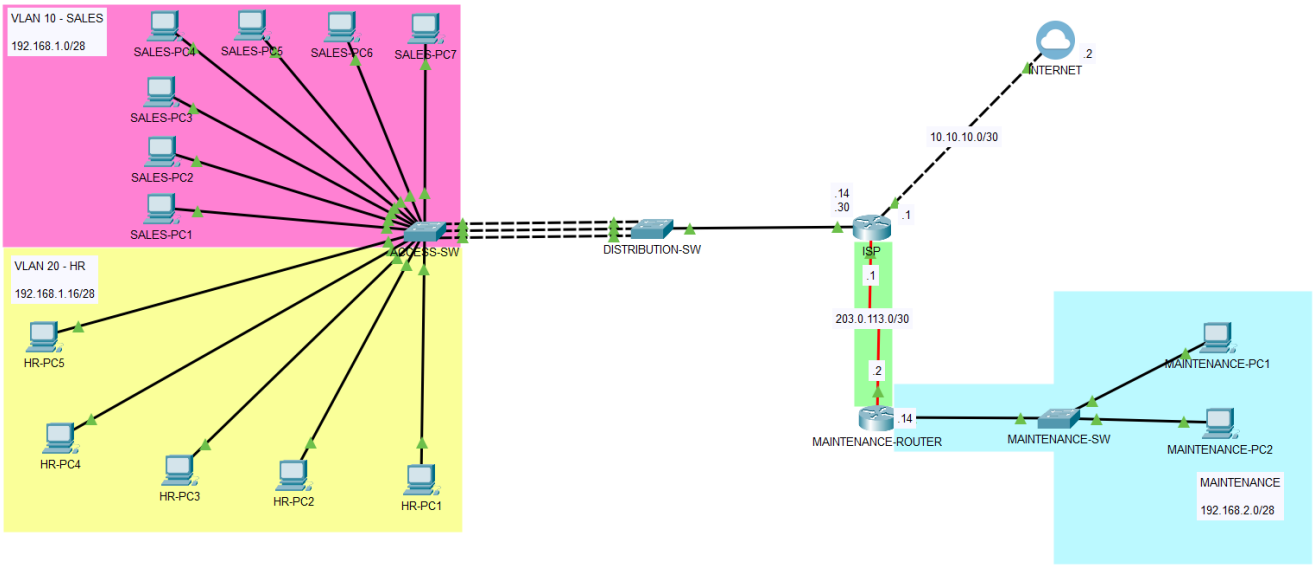
TROUBLESHOOTING LAB-1

Daniel Garcia Gata

Network Diagram



I set up this lab to practice with different concepts such as VLANs, Trunk interfaces, SSH access and ACL rules. On this small network, two main problems were found:

DHCP service is not available for users on HR (VLAN 20) so they are not able to access internet or communicate with the users from the SALES department (VLAN 10).

The steps I made to troubleshoot this issue are the following:

- I checked if there is a physical issue by checking if the right cables are used. Everything is fine.

- Since IP addresses are not dynamically obtained on VLAN 20 I set static IP addresses with their correct default gateway (192.168.1.30/28) but this wasn't the solution.

- I checked the DHCP server (configured on the ISP router) and the configurations are correct

SOLUTION:

After checking the interfaces from the access switch (ACCESS-SW), was to add VLAN 20 to the allowed interfaces on the trunk, this way the problem was solved. Now that we have DHCP service, we have full connectivity with every host in and outside the LAN.

MAINTENANCE department is having problems with restricted access on areas that are not supposed to be restricted and vice versa.

The expected configuration has to meet this requirements:

- Permit SSH access to ISP and MAINTENANCE-ROUTER to only MAINTENANCE-PC1 (192.168.2.1)
- Permit total access from the network 192.168.2.0/28 to the network 192.168.1.0/27 (SuperNet to cover both VLAN networks).
- Permit OSPF traffic
- Deny INTERNET access to MAINTENANCE department.

I checked the configurations and they are as follows:

ISP ACCESS LISTS

Extended IP access list OFFICE

10 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.3
20 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.15
30 permit ip any any

Standard IP access list 1

10 permit 192.168.2.0 0.0.0.15

MAINTENANCE-ROUTER ACCESS LISTS

Standard IP access list 1

30 permit 192.168.2.0 0.0.0.15

Extended IP access list MAINTENANCE

10 permit tcp 192.168.2.0 0.0.0.15 host 192.168.2.14 eq 22
20 permit tcp 192.168.2.0 0.0.0.15 host 203.0.113.1 eq 22
30 permit ospf any any
40 permit ip any any
50 deny ip 192.168.2.0 0.0.0.15 10.10.10.0 0.0.0.3

SOLUTION:

After checking the ACLs from both routers I saw the main problem on MAINTENANCE-ROUTER's Access List MAINTENANCE.
First, the only host that is allowed to have SSH on both routers is MANTENANCE-PC1 (192.168.2.1) while the first entry allows access to the whole 192.168.2.0 network. I changed that to:

- permit tcp host 192.168.2.1 host 192.168.2.14 eq 22
- permit tcp host 192.168.2.1 host 203.0.113.1 eq 22

The next thing to fix is the order of rules, the rule number 40 invalidates rule number 50 so I will place it on top.
The new set of rules looks like this:

- Permit TCP host 192.168.2.1 host 192.168.2.14 eq 22
- Permit TCP host 192.168.2.1 host 203.0.113.1 eq 22
- Permit OSPF any any
- Deny IP 192.168.2.0 0.0.0.15 10.10.10.0 0.0.0.3
- Deny TCP any any eq 22
- Permit IP any any

The ISP's Access List 1's rules were also modified, just in case with:

- Permit host 192.168.2.1 instead of Permit 192.168.2.0 0.0.0.15

Summary

With this lab I wanted to practice these concepts but also to practice reading the running configuration of every device to find problems. Although these were issues that required only small changes they meant a real problem for the integrity and connectivity of the network.