NWK780 – TRADITIONAL NETWORKS

Seneca | SCHOOL OF INFORMATION TECHNOLOGY ADMINISTRATION & SECURITY

GROUP 1:

[redacted]

Lab1 Basic Switch Management Group size =4

Prepared by:

Ali Abdulsattar Hussein
Majid Shahravan
Nagham Kubba

Lab Objectives

1. To gain skills for achieving basic management of a switch.
2. To configure the IP addresses of host computers.
3. To check the status of the interfaces of a switch.
4. To examine the MAC address table entries of a switch before and after running the ARP process.
5. To achieve a basic configuration of a switch.
6. To add security for accessing the configuration of a switch.
7. To enable remote access of a switch configuration within a simple Ethernet LAN.

Lab Instructions

1. **Mode of Operation:** This lab must be done **in person** with groups of **four** students.
2. **Lab contents:** This lab is the same as lab 1A except that it must be done on physical devices.
3. **Handle Equipment Carefully:** Cisco devices are delicate and expensive. Handle all equipment with care.
4. **Power Safety:** Ensure all devices are powered off before connecting or disconnecting cables to avoid electrical hazards.
5. **Avoid Physical Hazards:** Be mindful of cables to prevent tripping and ensure proper cable management to avoid entanglements.
6. Each group must **present** the results to the instructor to gain the mark of this lab.
7. **After finishing your lab:** Disconnect cables, return them to their proper place and power down all devices.

Network Topology

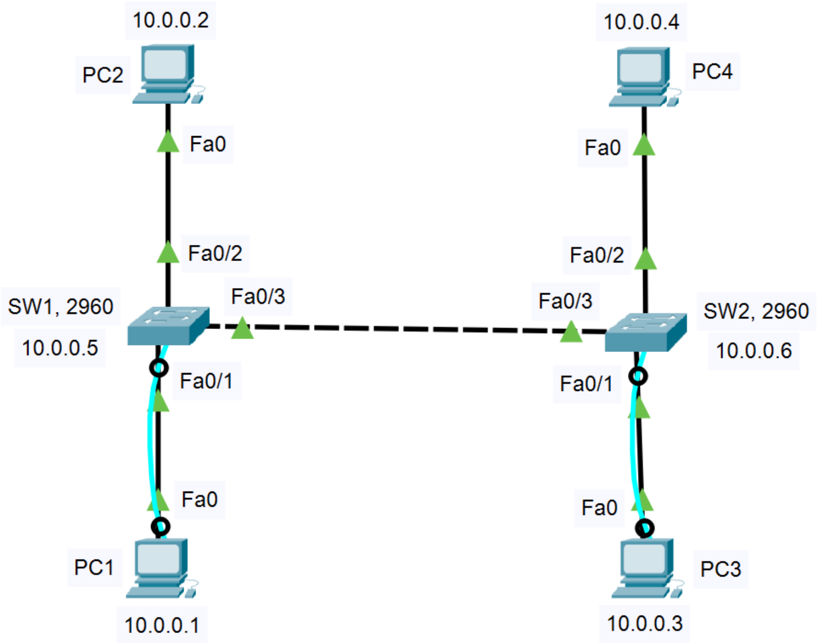

Figure 1 Topology of the Ethernet LAN network

Procedure

1. Connect the Network Topology shown in Figure 1
2. Use Straight through cables between PCs and switches
3. Use cross cables between the two switches.
4. For each PC, Fa0 means the FastEthernet port of the NIC of the PC.
5. The console cable must be connected to Fa0/3 of each switch.
6. Assign the following IP addresses to your PCs:
    a. PC1=10.0.0.0.1/8
    b. PC2=10.0.0.0.2/8
    c. PC3=10.0.0.0.3/8
    d. PC4=10.0.0.0.4/8
7. Open the Command Prompt of each PC and execute the command:

```
C:\>ipconfig /all
```

8. Figure out the MAC address (also called the Physical Address) of the NIC (FastEthernet0) of each PC and list the results in Table 1.

Table 1 MAC addresses of FastEthernet0 NIC of the PCs.

Host	MAC address of Fa0
PC1	**0013.3b4a.5a43**
PC2	**6c2b.59f1.ecb2**
PC3	**0013.3b4a.5965**
PC4	**6c2b.59f2.7229**

9. Connect the console of PC1 to the port of SW1, use PC1 to configure SW1
10. On PC1, run the PuTTY terminal emulator with default parameters.
11. Click OK to get into the CLI of SW1, once you gain access, click enter to be in the user execute mode of the switch

```
Switch>
```

12. Enter the command “enable” to alleviate the switch prompt to the privileged mode:

```
Switch>enable
Switch#
```

13. Now use the following command to list the status of all ports of the switch:

```
Switch#show interfaces status
```

Also, repeat the same practice of this step to SW2.

14. Display the MAC address table of SW1 using the command:

```
Switch#show mac address-table
```

Also, repeat the same practice of this step to SW2.

15. From the Command Prompt of PC1 ping the IP addresses of all other PCs. Here is the command to ping PC2:

```
C:\>ping 10.0.0.2
```

Immediately after the three ping operations indicated above display the MAC address table of SW1

Also inspect the MAC address table of SW2. Are the MAC addresses of the PCs in the CAM tables of SW1 and SW2 identical to those in Table 1?

16. **Check point 1:** Call your Instructor to show the above results.

Expanded configurations of CISCO switches

Apply the below steps to both switches, all the steps are written for SW1, when using the second switch, use SW2

17. In the CLI of SW1 enter into the global configuration mode:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

18. Set the hostname of the switch to SW1:

```
Switch(config)#hostname SW1

SW1(config)#
```

19. When you mistype a command in the CLI of a networking device the DNS name resolution process attempts to resolve the hostname which is the mistyped command into an IP address. This will make you wait for a minute of delay due to the error. Therefore, to disable the DNS resolution process enter the command:

```
SW1(config)#no ip domain-lookup
```

20. Now, configure "cisco" as the old plain text password to limit access to the privileged mode:

```
SW1(config)#enable password cisco
```

21. Enter the command "exit" two times to restart the console session and notice that you will start from the user execute mode. Enter the command "enable" and notice that you will be prompted to enter the password. In this case, enter the password "cisco" to get into the privileged mode.
22. Now, configure "class" as the new encrypted password to limit access to the privileged mode:

```
SW1(config)#enable secret class
```

23. Again, enter the command "exit" two times to restart the console session, and notice that you will start from the user execute mode. Enter the command "enable" and notice that you will be prompted to enter the password. In this case, enter the password "class" to get into the privileged mode. So, the new style secret password has overridden the old plain text password.
24. Now configure a password called "conpass" to limit access to the console session:

```
SW1(config)#line con 0
SW1(config-line)#password conpass
```

```
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#
```

25. The login command activates the configured password. Restart the console session as before and notice that you will be prompted to enter the password “conpass” needed to access the console session. Also to get into the privileged mode you will need to enter the “class” encrypted password as before.
26. To see all these details, display the running configuration of the switch

```
SW1# SW1# show run
Building configuration...

Current configuration : 1151 bytes (vary depending on device)
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
!
!
!
Other lines omitted
```

Notice that the enable password is shown as **cisco** while the secret password is **encrypted**.

When you have both passwords, the secret password will overwrite the enabled password.

27. Run the show run command again and keep clicking on the space bar until you reach the end of the running configuration.

```
SW1# show run
!
!
interface Vlan1
no ip address
shutdown
```

```
!
!
!
!
line con 0
password conpass
login
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

Notice the line **console** password shown at the end of the running configuration.

Deleting and Modifying Passwords

To change any password on CISCO switches and routers, you must delete the old one and then create a new one.

1. Delete the enable plain text password as follows:

   ```
   SW1(config)#no enable password
   ```

2. Delete the enable encrypted password as follows:

   ```
   SW1(config)#no enable secret
   ```

3. Delete the Console password as follows:

   ```
   SW1(config)#line con 0
   SW1(config-line)#no password
   SW1(config-line)#exit
   ```

4. Create a **plain** text password to limit access to the privileged mode, let it be **NWK780**
5. Create a **console** password to limit access to the console session, let it be **BTT**
6. **Check point 2:** Call your Instructor to show the above results.