Cisco Network Academy
CCNA 1 Introduction to Networks

Note: This lab guide is written by me using an example from the following website: http://www.danscourses.com/

- **Cisco IOS Command Hierarchy:**
  https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm

- **In this lab, you will learn how to configure the following tasks:**

IPv4 Addressing

1. Divide the 192.168.4.0 /24 network into the following subnets.
   Subnet A (not shown) : 52 hosts
   IP addr range: 192.168.4.0/26 ~ 192.168.4.63/26
   Subnet B (green): 50 hosts
   IP addr range: 192.168.4.64/26 ~ 192.168.4.127/26
   Subnet C (not shown) : 40 hosts
   IP addr range: 192.168.4.128/26 ~ 192.168.4.191/26
   Subnet D (yellow): 14 hosts
   IP addr range: 192.168.4.192/28 ~ 192.168.4.207/28

2. The router get the first usable address in the subnet

3. The PCs get 5th and 6th, usable address in the green subnet, and the 5th in the yellow subnet

4. The switches get the last usable address in the subnet.

5. The server gets the second address in the subnet

IPv6 Addressing

Green Network: 2001:DB8:CCCC:1::/64
R1 -- :1
PC0 -- :A
PC1 -- :B

Yellow Network: 2001:DB8:CCCC:2::/64
R1 -- :1
PC2 -- :A
Server -- :F

Link-local:
R1 -- FE80::1

Note: You will need to configure the router and both switches using the console connection and the desktop terminal program

Configuration Tasks

On R1, S1, S2:

1. hostnames: R1, S1, S2
2. R1 minimum password length 10 characters
3. user account: admin, encrypted password: danscourses
4. console line: login using local database
5. enable password: class12345 (encrypted)
6. password encryption on all lines
7. banner message of the day: No unauthorized access allowed!
8. domain name: danscourses.com
9. ssh version 2
10 timeout after 5 minutes on all console and vty lines
11 security keys: rsa 1024 modulus
12. R1: vty 0 4,
    S1: vty 0 15,
    secure SSH access using local database
13. enable ipv6 routing on R1
14. configure PCs with IPv4 and IPv6 addresses,
    network prefix or subnet mask, and default gateway
15. R1 interfaces with IPv4 and IPv6 addressing
16. S1 & S2 interface VLAN1 with IPv4 address
    and subnet mask
17. S1 & S2 with default gateway
18. backup R1, S1, S2 running-config to the tftp server
    (accept the default name)
19. Copy running-config to startup-config

Lab Guide

First of all, configure IP addresses on each PC as follows:

- Green Subnet (192.168.4.64/26 ~ 192.168.4.64/26)

  On PC0

  Click on the PC0 → select Desktop → select IP configuration

  (IP address) 192.168.4.69
  (Subnet Mask) 255.255.255.192
  (Default Gateway) 192.168.4.65

  (IPv6 Address) 2001:DB8:CCCC:1::A/64
  (IPv6 Gateway) FE80::1 ← link-local address of the router

  On PC1

  Click on the PC0 → select Desktop → select IP configuration

  (IP address) 192.168.4.70
  (Subnet Mask) 255.255.255.192
  (Default Gateway) 192.168.4.65

  (IPv6 Address) 2001:DB8:CCCC:1::B/64
  (IPv6 Gateway) FE80::1 ← link-local address of the router

- Yellow Subnet (192.168.4.192/28 ~192.168.4.207/28)

  On PC2

  Click on the PC0 → select Desktop → select IP configuration

  (IP address) 192.168.4.197
  (Subnet Mask) 255.255.255.240
  (Default Gateway) 192.168.4.193

  (IPv6 Address) 2001:DB8:CCCC:2::A/64
  (IPv6 Gateway) FE80::1 ← link-local address of the router

  On the TFTP Server

  Click on the PC0 → select Desktop → select IP configuration

  (IP address) 192.168.4.194
  (Subnet Mask) 255.255.255.240
  (Default Gateway) 192.168.4.193

  (IPv6 Address) 2001:DB8:CCCC:2::F/64
  (IPv6 Gateway) FE80::1 ← link-local address of the router

Now, we will configure the following tasks on R1, S1, and S2:

1. hostnames: R1, S1, S2
2. R1 minimum password length 10 characters
3. user account: admin, encrypted password: danscourses
4. console line: login using local database
5. enable password: class12345 (encrypted)
6. password encryption on all lines
7. banner message of the day: No unauthorized access allowed!
8. domain name: danscourses.com
9. ssh version 2
10 timeout after 5 minutes on all console and vty lines
11 security keys: rsa 1024 modulus
12. R1: vty 0 4,
    S1: vty 0 15,
    secure SSH access using local database
13. enable ipv6 routing on R1
14. configure PCs with IPv4 and IPv6 addresses,
    network prefix or subnet mask, and default gateway
15. R1 interfaces with IPv4 and IPv6 addressing
16. S1 & S2 interface VLAN1 with IPv4 address
    and subnet mask
17. S1 & S2 with default gateway
18. backup R1, S1, S2 running-config to the tftp server
    (accept the default name)
19. Copy running-config to startup-config

Now, we will configure the router R1.

```
Router>enable

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#security passwords min-length 10

R1(config)#username admin secret danscourses

R1(config)#line console 0

R1(config-line)#login local
R1(config-line)#exit

R1(config)#enable secret class1234
% Password too short - must be at least 10 characters. Password not configured.
R1(config)#enable secret class12345

R1(config)#service password-encryption

R1(config)#banner motd "No unautorised access allowed!"

R1(config)#ip domain-name danscourses.com

R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.

R1(config)#crypto key generate rsa
The name for the keys will be: R1.danscourses.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 0:55:50.968: %SSH-5-ENABLED: SSH 2 has been enabled

R1(config)#ip ssh version 2

R1(config)#line console 0
R1(config-line)#exec-timeout 5 0
R1(config-line)#exit
```

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exec-timeout 5 0

R1(config-line)#transport input ssh
R1(config-line)#exit

R1(config)#ipv6 unicast-routing

R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip address 192.168.4.65 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#ipv6 address 2001:DB8:CCCC:1::1/64
R1(config-if)#ipv6 address FE80::1 link-local

R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.4.193 255.255.255.240
R1(config-if)#no shut
R1(config-if)#ipv6 address 2001:DB8:CCCC:2::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#exit
R1(config)#exit

R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

R1#copy run tftp
Address or name of remote host []? 192.168.4.194
Destination filename [R1-confg]?

Writing running-config....!!
[OK - 1098 bytes]

1098 bytes copied in 3.004 secs (365 bytes/sec)

R1#show run
Building configuration...

Current configuration : 1098 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
service password-encryption
security passwords min-length 10
!
hostname R1
!
!
!
enable secret 5 $1$mERr$8BPXRaZKXzJUe84Ckfffz.
!
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username admin secret 5 $1$mERr$p3HOT7heFTqvFIYQsDEhe0
!
!
license udi pid CISCO1941/K9 sn FTX1524CPNG
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name danscourses.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 192.168.4.65 255.255.255.192
duplex auto
```

```
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CCCC:1::1/64
!
interface GigabitEthernet0/1
ip address 192.168.4.193 255.255.255.240
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:CCCC:2::1/64
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CNo unautorised access allowed!^C
!
!
!
!
line con 0
exec-timeout 5 0
login local
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
!
!
!
end


R1#ping 192.168.4.69

R1#ping 192.168.4.70

R1#exit
```

At this point, when you try to access the router R1 again by pressing <Enter> key, you will see the following:

No unautorised access allowed!

User Access Verification

Username: admin
Password: ← you need to type the password “danscourses”

R1>en
Password: ← you need to type the password “class12345”
R1#

At this point, please close the terminal and open the command prompt on PC0. Then, you can test if the ssh setup works.

PC> ssh -?
PC> ssh -l admin 192.168.4.65
Open
Password: ← you need to type the password “danscourses”

No unautorised access allowed!

R1>en
Password: ← you need to type the password “class12345”
R1#

After you complete up to this point, please submit your packet tracer file to the dropbox in D2L.

For your own practice, please continue to configure the switches S1 and S2.