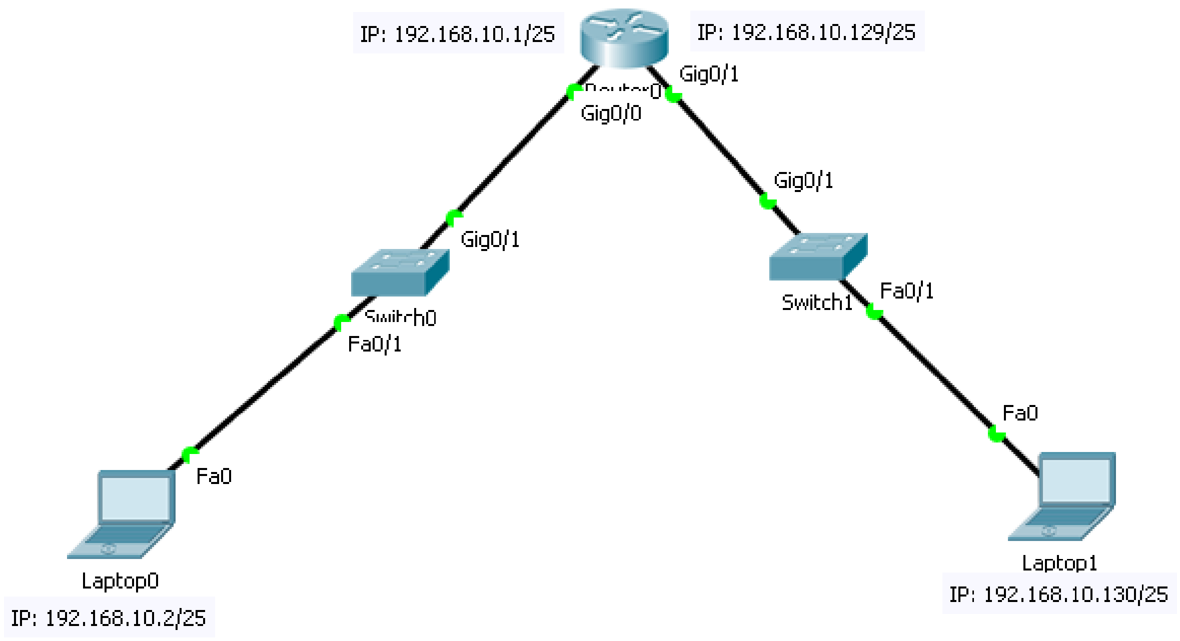
CCNA Sem01 Lab#06

Lab06 Topology (Secure Network)



Setup topology

Step 1: Connect topology devices as shown in figure.

1- Select straight-through Cable from connections in Cisco Packet Tracer.

Step 2: Variable Length Subnet Mask (VLSM)

- VLSM allows a network space to be divided in unequal parts.
- Subnet mask will vary depending on how many bits have been borrowed for a particular subnet.
- Network is first subnetted (Starting by a network which has the largest number of hosts), and then the subnets are subnetted again.
- Process repeated as necessary to create subnets of various sizes.
- Formula to determine number of useable hosts

$$2^n - 2$$

- **n** (where n is the number of zeros in the last octet) is used to calculate the number of hosts.
- **-2** for subnetwork ID and broadcast address cannot be used on each subnet.

In this topology, we will start by Network01

- The initial network is 192.168.10.0/24
- We will divide the initial network into two subnetworks, each one has 126 hosts
- $2^n - 2 \geq 126$ → n = 7 (# of zeros in the last octet)
- Subnet mask in binary: 11111111.11111111.11111111.10000000
- Subnet mask in decimal: 255.255.255.128

We will do the same for another network starting by network 192.168.10.128

Step 3: Configure Router R1.

1- Open router Router0
2- Select CLI tab.
3- Type “no” and Enter.

Step 4: Enter privileged EXEC mode of R1.

You can access all `Router` commands in privileged EXEC mode.
Enter privileged EXEC mode by entering the **enable** command.

```
1. Router> enable
2. Router#
```

The prompt changed from `Router` **>** to `Router`**#** which indicates privileged EXEC mode.

Step 5: Enter configuration mode of R1.

Use the **configuration terminal** command to enter configuration mode.

```
1. Router# configure terminal
2. Router(config)#
```

The prompt changed to reflect global configuration mode.

Step 6: Require that a minimum of 8 characters be used for all passwords on the R1

```
1. Router(config)# security passwords min-length 8
```

Step 7: The router blocks login attempts for set of seconds if someone fails to attempt.

The router blocks login attempts for 30 seconds if someone fails three attempts within 30 seconds.
This timer is set especially low for the purpose of this lab.

```
1. Router(config)# login block-for 30 attempts 3 within 30
```

Step 8: Set a password on the privileged EXEC mode of the R1

```
Encrypted, limits access to the privileged EXEC mode of the Router
   2. Router(config)# enable secret cisco123
```

Step 9: Set IPs for the interfaces of the R1.

```
1. Router(config)# interface G0/0
2. Router(config-if)# ip address 192.168.10.1 255.255.255.128
3. Router(config-if)# no shutdown
```

```
4. Router(config-if)# exit
5. Router(config)# interface G0/1
6. Router(config-if)# ip address 192.168.10.129 255.255.255.128
7. Router(config-if)# no shutdown
8. Router(config-if)# exit
9.  Router(config)# exit
```

Show interfaces status:

```
1. Router# show ip interface brief
```

Step 10: Configure Laptops

1- Set IP for Laptop0(Desktop -> IP configuration)
   a. IP address: 192.168.10.2
   b. Subnet Mask: 255.255.255.128
   c. Default Gateway: 192.168.10.1
2- Set IP for Laptop1(Desktop -> IP configuration)
   a. IP address: 192.168.10.130
   b. Subnet Mask: 255.255.255.128
   c. Default Gateway: 192.168.10.129

Step 11: Test Connectivity of laptops

1- Open Laptop0(Desktop ->CMD)
   a. Ping 192.168.10.130

2- Open Laptop1(Desktop ->CMD)
   a. Ping 192.168.10.2

Step 12: Enable SSH on router R1.

```
1. Change router hostname
      a. Router(config)# hostname R1
2. Add domain name to R1
      a. R1(config)# ip domain-name bfci.com
3. Generate RSA encryption
      a. R1(config)# crypto key generate rsa
      b. How many bits in the modulus [512]: 1024
4. Create local database on R1
      a. R1(config)# username Ahmed secret cisco123
5. Enable VTY inbound SSH session
      a. R1(config)# line vty 0 4
      b. R1(config-line)# login local
      c. R1(config-line)# exec-timeout 3 0 //time in minutes and seconds
      d. R1(config-line)# transport input SSH
      e. R1(config-line)# exit
```

Access R1 via SSH from Laptops:

1- Open CMD of the Laptop0 (Desktop -> Command prompt)
   a. **SSH -l Ahmed** 192.168.10.129
      Open
      Password: cisco123

R1>

2- Open CMD of the Laptop2 (Desktop -> Command prompt)

a. **SSH -l Ahmed** 192.168.10.1
Open
Password: cisco123
R1>

Step 13: Encrypting Password Display

```
1. R1(config)# service password-encryption
2. R1(config)# exit
```

Step 14: Save running configuration

```
1. R1# copy running-config startup-config.
```