IFT 266 Introduction to Network Information Communication Technology

Lab 41

IPv6 IoT & Wireless Security

Co-Authored by Samaria Simon

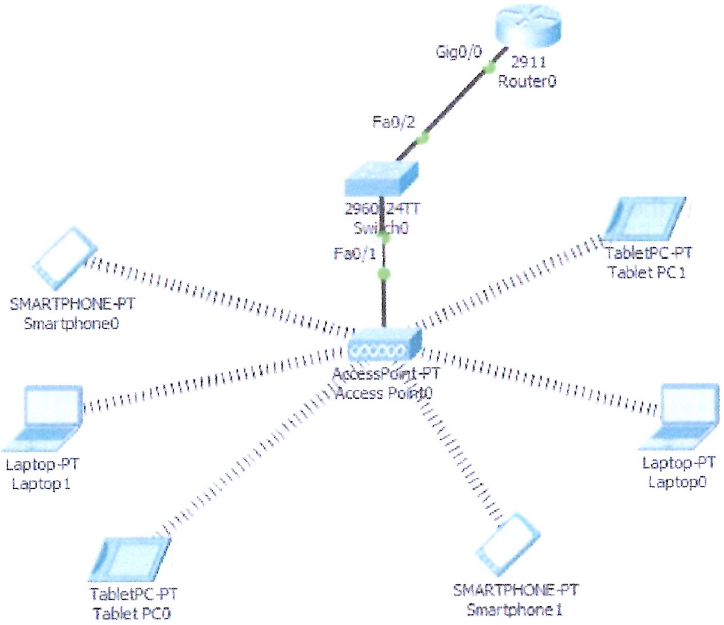
After you complete each step, put an 'x' in the completed box
or
Answer the open question
or
Attach a screenshot where required.

Objective: Today's average home has a network consisting of many devices "Internet of things". We will create customized IPv6 wireless network and some security to the network.

1. Setup the following topology in packet tracer.

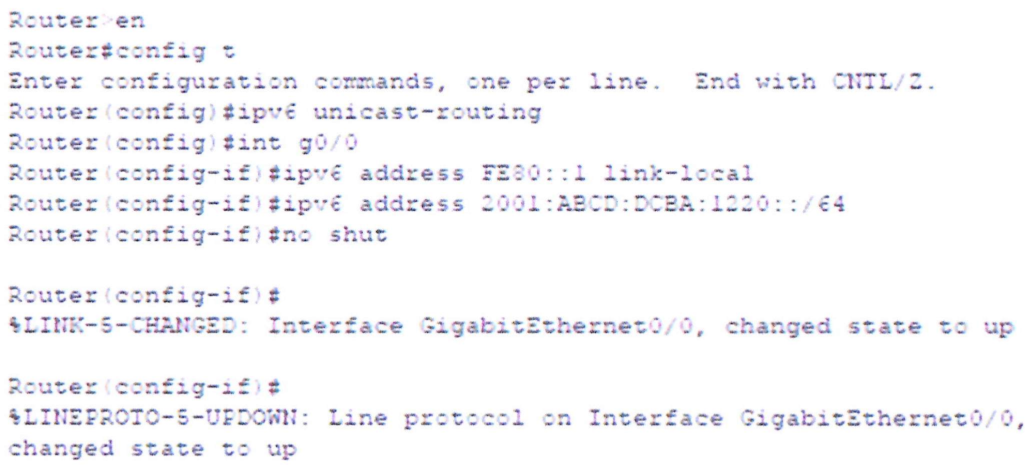
   The smartphones and tablets should automatically connect to the access point.

   You will need to remove the Ethernet module from the laptops and replace it with the wireless module (WPC300N).



Completed ☒

2. We will now configure the router with IPv6 link local and global unicast addresses. Navigate to the router's CLI and enter the following commands.



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#int g0/0
Router(config-if)#ipv6 address FE80::1 link-local
Router(config-if)#ipv6 address 2001:ABCD:DCBA:1220::/64
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

Completed ☒

3. Configure each of the smart devices (smartphones, tables and laptops) with an IPv6 global unicast address through the IPv6 Auto Config option on each device.

Completed ☒

4. We will now verify the IPV6 address of one of the laptops by typing the *ipv6config* command into the Command Line Interface under the Desktop tab on one of the laptops.

   Insert a screenshot of the command window below with the IPv6 configuration details.

5. We will now confirm an IPv6 connection between both laptops. Use the ping command to test the connection from Laptop0 to Laptop1

6. Insert a screenshot of your successful connection below.

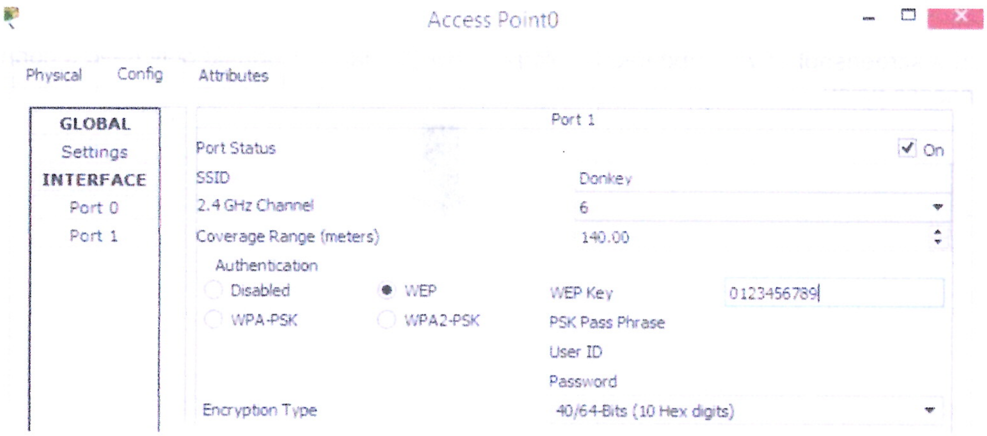
⬇

7. So far, we have created small IPv6 wireless network. However, it is not very secure.

   We used the default SSID with no authentication.

   We will now change the SSID and enable WEP authentication on the laptops.

   Go into the Access Point and change the SSID to “Donkey” and enable WEP and provide a 10-digit key of your choosing (as in the image below)



Port 1

Port Status ☑ On

SSID Donkey

2.4 GHz Channel 6

Coverage Range (meters) 140.00

Authentication

○ Disabled ● WEP

○ WPA-PSK ○ WPA2-PSK

WEP Key 0123456789

PSK Pass Phrase

User ID

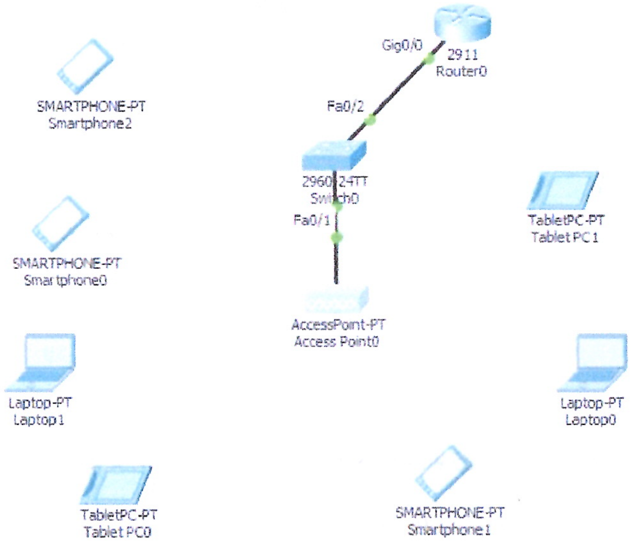
Password

Encryption Type 40/64-Bits (10 Hex digits)

Completed ☒

8. Notice now how all the wireless connections from the smart devices have disappeared from the topology.

   This is because the SSD and WEP key on the smart devices no longer match settings on the Access point.



Completed ☒

9. Reconfigure the wireless settings on both laptops so they both have a successful connection to the access point.

   Insert a screenshot of your updated topology below (the laptops should only have a connection to the access point).

⬇

Extra Credit (30 points)

Play around with the other authentication methods (strategies) on the access point and then implement another strategy on the smart devices.

1. What strategy did you select and why?

   ____

   ____

   ____

2. Insert a screenshot of both the access point (new wireless security configurations) and of the smart device of your choosing (new wireless security configurations).

⬇