CSCI 5010 – Fundamentals of Data Communications

Lab 8

Wireless Lab

University of Colorado Boulder

Department of Computer Science

Professor Levi Perigo, Ph.D.

# Objectives

* Learn how wireless (Wi-Fi) technology works.
* Learn how to simulate roaming in wireless network.
* Learn how to configure wireless networks.
* Learn about wireless security protocols.

# Summary

Wireless LANs enable users to communicate without the need cables. Each WLAN needs a wireless Access Point (AP) to transmit and receive data. Unlike a wired network which operates at full-duplex (send and receive at the same time), a wireless network operates at half-duplex, so sometimes an AP is referred as a Wireless Hub.

# This lab will provide a basic understanding of configuring wireless networks that comprise of AP’s, a switch, and a router on Cisco Packet Tracer. IPv4 DHCP scopes will be created for the new users connecting to the wireless network. The lab expands on the “Router-on-a-Stick framework to include roaming scenarios in WLAN networks.

# Objective 1: Creation of wireless topology in Cisco Packet Tracer (CPT)

1. Please create the following topology (Figure 1) in CPT:

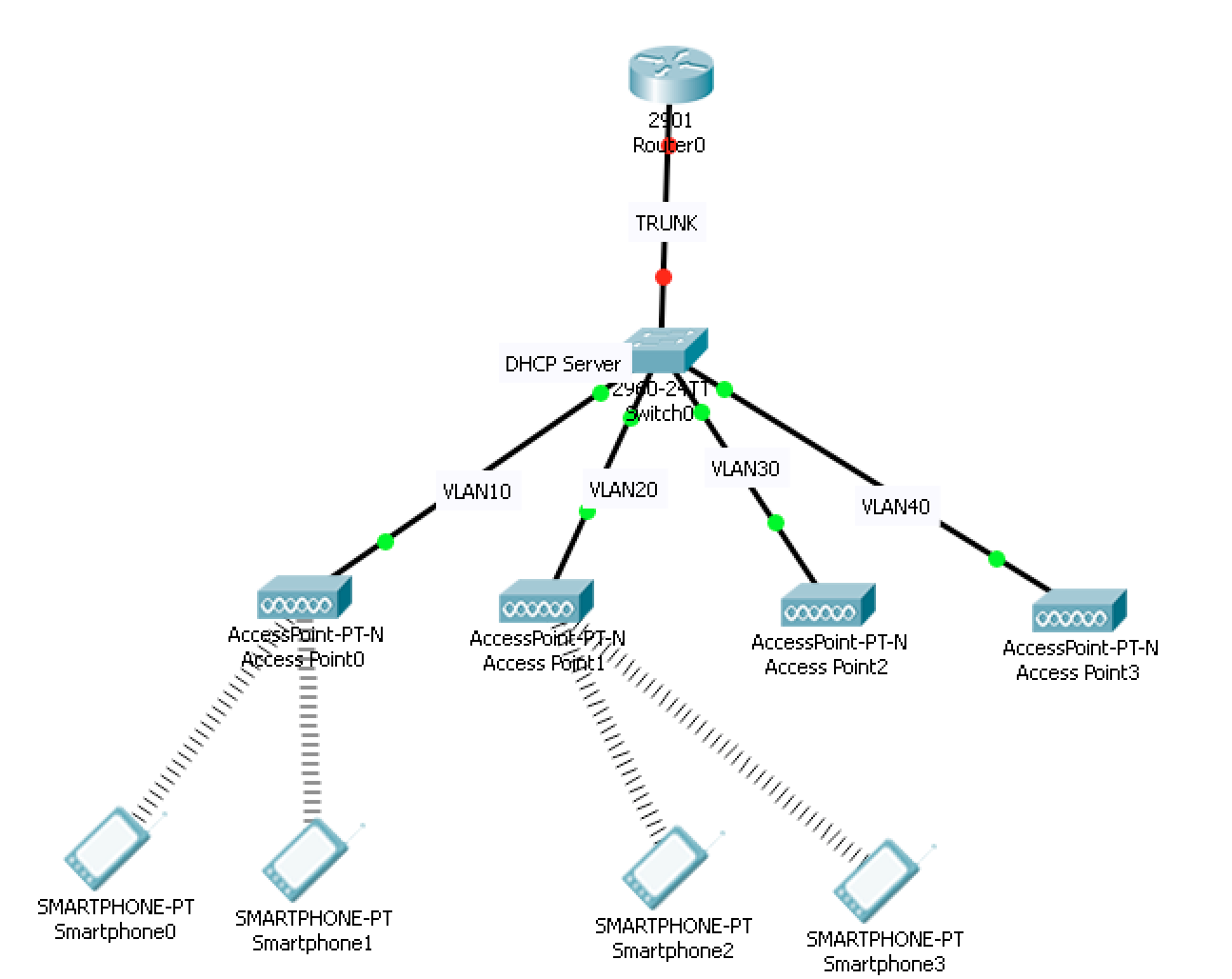


Figure 1: Wireless topology

1. The Access Points (AP’s) and wireless terminals (Smartphones) are located in the “Wireless Devices” section of CPT. Please drag and drop appropriately as indicated in Figure 1. The wireless terminals may connect randomly to AP’s. Please disregard it at this point. Paste the screenshot of the created topology from CPT **[20 points]**.

A diagram of a network

Description automatically generated

# Objective 2: Wireless Network Configuration

1. Access Point and Smartphone configuration
   1. Configure AP0 in a way that its SSID is “NetEng,” and works on channel no. 6, coverage as “250 meters,” and WEP Authentication key as “ABDCE12345.” Similarly, Smartphones 0 and 1 should be configured to authenticate to “NetEng” with WEP key as “ABCDE12345.” Paste screenshot of configuration. **[10 points]**

AP:

A screenshot of a computer

Description automatically generated

Smartphone:

A screenshot of a computer

Description automatically generated

* 1. Configure AP1 in a way that its SSID is “NetEng,” works on channel no. 11, coverage as “250 meters,” and Authentication as “Disabled.” Similarly, Smartphones 2 and 3 should be configured to connect with “NetEng” with no Authentication. Paste screenshot of configuration**. [10 points]**

AP:

**A screenshot of a computer

Description automatically generated**

Smartphone:

A screenshot of a computer

Description automatically generated

* 1. Configure AP2 in a way that its SSID is “Default,” works on channel no. 6, coverage as “250 meters,” and Authentication as “Disabled.”Paste screenshot of configuration. **[10 points]**

A screenshot of a computer

Description automatically generated

* 1. Configure AP3 in a way that its SSID is “NetEng,” works on channel no. 1, coverage as “250 meters,” and Authentication as “Disabled.” Paste screenshot of configuration. **[10 points]**

**A screenshot of a computer

Description automatically generated**

1. Configure Cisco switch 0 in a fashion that each of its four switch ports are in separate VLAN’s as shown in Figure 1 and the port connected to the router 0 as “TRUNK” port. Additionally, configure the switch as DHCP server having four different pools for it to assign IP addresses for the connecting wireless devices/terminals. Paste the screenshot of configuration window of all Smartphones highlighting received DHCP address. **[20 points]**

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A close up of a text

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A close-up of a sign

Description automatically generated

1. In order to bring connectivity between different wireless devices, configure sub-interfaces on Router 0. *Hint: Router on a Stick configuration*
2. Try to ping Smartphone 0 from Smartphone 2. Did it ping? If so why? Paste the screenshot of the output of the ping command. **[20 points]**

*Hint: You can access command line terminal in a smartphone by navigating to “Desktop” tab after double-clicking on the device.*

It did work. It worked because I configured the router on the stick configuration to allow for inter-vlan routing.

A computer screen with white text

Description automatically generated

# Objective 3: Roaming Scenario Simulation

1. Change the coverage on AP1 to be “10 meters.” Did you notice any change in topology? If so, what behavior did you notice? Paste the screenshot of the changed topology. **[10 points]**

I did notice changes in the topology. The behavior I noticed was that smartphone 2 and 3 changed its wireless connection from AP1 to AP3.

A diagram of a network

Description automatically generated

1. What is the reason that caused the wireless smartphones to switch to an alternative AP? Explain using a real-world scenario. **[10 points]**

Let’s say someone was on the boulder campus inside the CASE building. Right next to us is the UMC building. The CASE building’s AP connection radius was suddenly changed to 10 meters. The user who was originally connected to the CASE AP has been disconnected because that AP was >10 meters away from their smartphone. Now because the smartphone is broadcasting an SSID out to the wireless world, any network configured to match that SSID wants to connect that smartphone. While I am in the CASE building, I am only 100 meters away from the AP that is inside the UMC building. Given that our config says that the range for the UMC building AP is 250 meters, it will then go ahead and connect to that AP because it is in range.

1. Why do you think the smartphones switched to a particular AP as opposed to other nearby AP’s? Explain the process considering wireless configuration present on all AP’s. **[20 points]**

This behavior was observed because AP1 and AP3 both have the SSID name ‘NetEng’ and require no authentication to connect. AP0 does have the same SSID but requires authentication. AP2’s SSID is set to ‘Default’. Because the smartphones were configured to only accept SSIDs matching ‘NetEng’ with no authentication, it switched to the AP that matched that configuration.

1. What are the different WLAN modes? Which mode resembles the topology presented in this lab? **[5 points]**

Ad hoc mode:

* + Independent Basic Service Set (IBSS)
    - Mobile clients connect directly to each other

Infrastructure mode:

* + Basic Service Set (BSS)
    - Mobile clients using a single AP to connect each other or to the network
  + Extended Service Set (ESS)
    - >2 BSSs connected by a common distro system, typically a switch.

The infrastructure mode: ESS best resembles the topology that was created in the lab.

1. How do we overcome interference caused by multiple AP’s in a network having same SSID? **[5 points]**

We overcome interference caused by multiple Aps in a network having same SSID by hosting the SSID on different channels for every AP. Like we did in the lab, AP1 was on channel 11 and AP3 was on channel 1 so they would not overlap traffic.

1. Differentiate between WLAN Security Standard briefly. Which one did we use in this lab? **[5 points]**

SSID – Identifier of the network

WEP – Wired Equivalent Privacy. Only protects against from man in the middle.

WPA/WPA2 – Wi-Fi protected Access.

MAC filtering – Allow only certain MAC addresses to access the network.

We used the WEP standard.

1. Name the two unlicensed spectrum bands? **[2 points]**

2.4 Ghz & 5 Ghz.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/157