Polytechnic University of Puerto Rico

Department of Electrical Engineering

Hato Rey

Module 10 Project COE 4331

Computer Networks Laboratory

January 31, 2025

Schmidt Montilla, Coral S., Student ID: 148830

Professor: Juan Tovar

Table of Contents

Introduction

This lab focuses on the practical implementation of configuring a wireless router's firewall settings to enhance network security and manage external access. The key objectives include enabling MAC filtering to restrict wireless network access, configuring a DMZ (Demilitarized Zone) to allow external access to a specific internal server, and setting up Single Port Forwarding to limit exposed ports for security. These configurations are essential in real-world network administration, where maintaining security while ensuring accessibility is crucial. By following a step-by-step approach, this lab provides hands-on experience in managing firewall rules, securing wireless networks, and optimizing internal and external connectivity.

Method

Packet Tracer - Identify MAC and IP Addresses

Objectives

- Configure MAC Filtering on a wireless router.
- Configure DMZ on a wireless router.
- Configure Single Port Forwarding on a wireless router.

Introduction

In this activity, you will configure a wireless router to:

- Rely on MAC filtering to increase security
- Allow access to a server in the DMZ
- Disable the DMZ and configure support for Single Port Forwarding

Instructions

Connect to the wireless router.

Step 1: Connect to the wireless router configuration web page at **192.168.0.1** from **PC0**.

Step 2: Use **admin** for both the user name and password.

Step 3: Navigate to wireless settings to determine the SSID and passphrase for connection to WRS1. Record the SSID and passphrase below.

Questions:

SSID: aCompany

Passphrase: aCompWiFi

Configure laptop as wireless client.

Step 1: Connect **Laptop0** to the **WRS1** wireless network using the security settings configured on the wireless router. Click **Desktop** > **PC Wireless**. Select **Connect** tab. Press **Refresh**. Select the desired SSID and click **Connect**. Provide the passphrase and select **Connect**.

Step 2: Close the **PC Wireless** window and click **Command Prompt**.

Step 3: At the prompt, enter **ipconfig /all** and record the IP and MAC addresses of **Laptop0** below.

Questions:

Laptop0 IP Address: 192.168.0.105

MAC address: 00:01:97:94:EB:38

Step 4: Repeat the above steps to connect **Laptop1** to **WRS1**.

Configure WRS1 to support MAC filtering.

Step 1: On **PC0**, go to the wireless router's configuration page at 192.168.0.1.

Step 2: Navigate to **Wireless > Wireless MAC Filter**.

Step 3: Select **Enabled** and **Permit PCs listed below to access wireless network**.

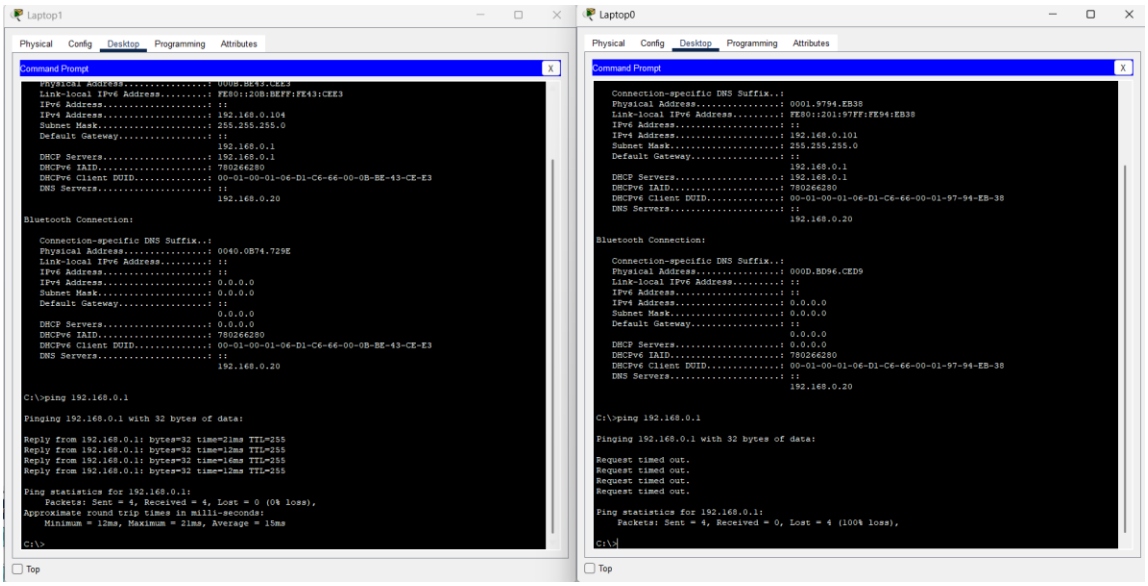
Step 4: Type in the MAC address **for Laptop0** in the **MAC 01:** field. Notice the MAC address must be in the **XX:XX:XX:XX:XX:XX** format. Click **Save Settings**.

Step 5: To verify connectivity, open a command prompt. Issue the ping command to the default gateway to 192.168.0.1 from **Laptop0** and **Laptop1**.

```
C:\> ping 192.168.0.1
```

Question:

Were both laptop able to connect to the WRS1 network? Why are you unable to associate with the access point?



No, both laptops were not able to connect to the WRS1 network. Laptop1 successfully connected, as indicated by the successful ping to 192.168.0.1 with 0% packet loss, confirming that it has access to the network. However, Laptop0 failed to connect, as shown by the 100% packet loss in the ping test, meaning it could not communicate with the wireless router. The reason for Laptop0's inability to associate with the access point is that MAC Filtering was enabled on the wireless router (WRS1), and only Laptop1's MAC address was added to the allowlist. Since Laptop0's MAC address was not listed, the router blocked its access to the network. This confirms that MAC Filtering is working correctly by restricting access to only authorized devices.

Test connectivity through the Telco Cloud.

Step 1: Open a **Command Prompt** on **Laptop0**.

Step 2: In **Laptop0**, test connectivity to **Remote PC** by issuing the **ping 209.165.201.29** command. The first few pings may fail while the network converges. Issue the command again if you did not get successful replies.

Step 3: Open **Remote PC** and then browse to the address of the internal web page hosted at **Server0**, which is **www.acompany.com**. A **Request Timeout** message should display. A webpage requests

from **Remote PC** to **Server0** is not successful because **WRS1** does not know which internal device should receive it. Port forwarding must be configured on **WRS1**.

Configure DMZ.

A demilitarized zone (DMZ) is where a portion of the company network is exposed to an untrusted external network, such as the internet.

Step 1: On **PC0**, reconnect to the wireless router's configuration page.

Step 2: Navigate to **Application & Gaming** > **DMZ**.

Step 3: Click **Enabled**.

Step 4: In the Destination: field, enter **20** for the IP address **192.168.0.20**.

Step 5: Scroll to the bottom and save the settings.

Step 6: Browse to **www.acompany.com** from **Remote PC**. You should now see the web page hosted by **Server0**.

Step 7: After you have verified that you were able to reach the webpage, disable **DMZ** and save the settings.

Configure WRS1 to forward a single port to Server0.

Depending on the router model, the open ports of a server in the DMZ can be exposed to an untrusted external network. To limit the number of exposed ports, single port forwarding can be configured on the router.

Step 1: On **PC0**, reconnect to the wireless router's configuration page. Navigate to **Application & Gaming** > **Single Port Forwarding**.

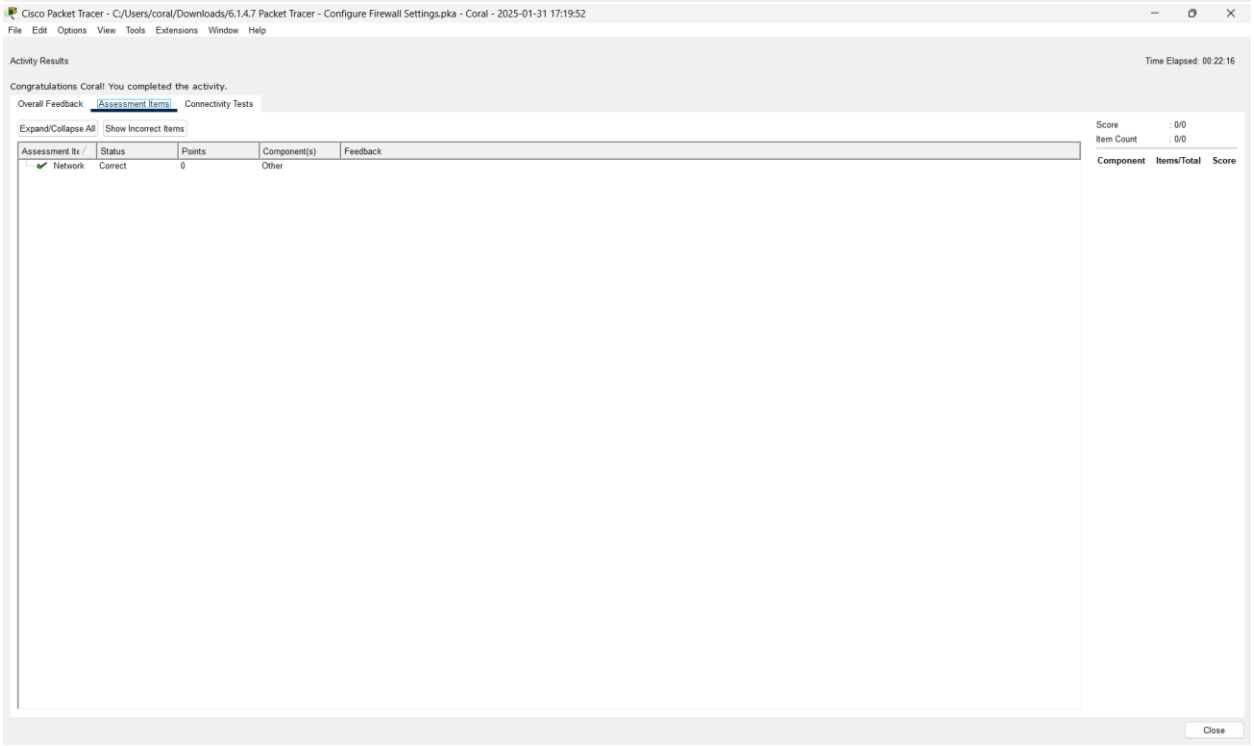
Step 2: On the left-hand menu, choose **HTTP** from the first drop-down box. Change the **To IP Address** to match **Server0**'s IP address, **192.168.0.20**. Also, check the **Enabled** checkbox at the end of the row.

Step 3: Scroll to the bottom of the window and click **Save Settings**.

Step 4: You should now be able to reach the webpage hosted on **Server0**. Browse to **www.acompany.com** on **Remote PC**. You should now see the web page hosted by **Server0**.

Lab Results


Cisco Packet Tracer - C:/Users/coral/Downloads/6.1.4.7 Packet Tracer - Configure Firewall Settings.pka - Coral - 2025-01-31 17:19:52
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:21:53
Congratulations Coral! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations on completing this activity!
Close


Cisco Packet Tracer - C:/Users/coral/Downloads/6.1.4.7 Packet Tracer - Configure Firewall Settings.pka - Coral - 2025-01-31 17:19:52
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:22:16
Congratulations Coral! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Ite
Status
Points
Component(s)
Feedback
Network
Correct
0
Other
Score : 0/0
Item Count : 0/0
Component
Items/Total
Score
Close

Conclusion

This lab provided an in-depth understanding of firewall configuration on a wireless router, covering MAC filtering, DMZ setup, and Single Port Forwarding. Through hands-on tasks, we successfully restricted network access using MAC filtering, allowing only authorized devices to connect. The DMZ configuration demonstrated how to expose a specific server to external networks while keeping the rest of the network secure. Additionally, Single Port Forwarding was implemented to refine access control, minimizing security risks while maintaining service availability. These configurations are critical for ensuring secure and efficient network operations, emphasizing the importance of proper firewall rules, access management, and security best practices in a professional networking environment.

References

[1] Cisco CCNA Packet Tracer Ultimate labs: SNMP CCNA Lab. Answers! (n.d.). www.youtube.com. Retrieved from https://youtu.be/5h0fN0j2XS8

[2] Taller Cisco Packet Tracer Configure Firewall Settings. (n.d.). www.youtube.com. Retrieved from https://youtu.be/yN5VqT6IhTs