

NAME: KELVIN NAMBALE

REG NO: I231/G/1729/21

COURSE NAME: FIREWALLS AND NETWORK AND DEFENCE SECURITY

LAB ASSIGNMENT

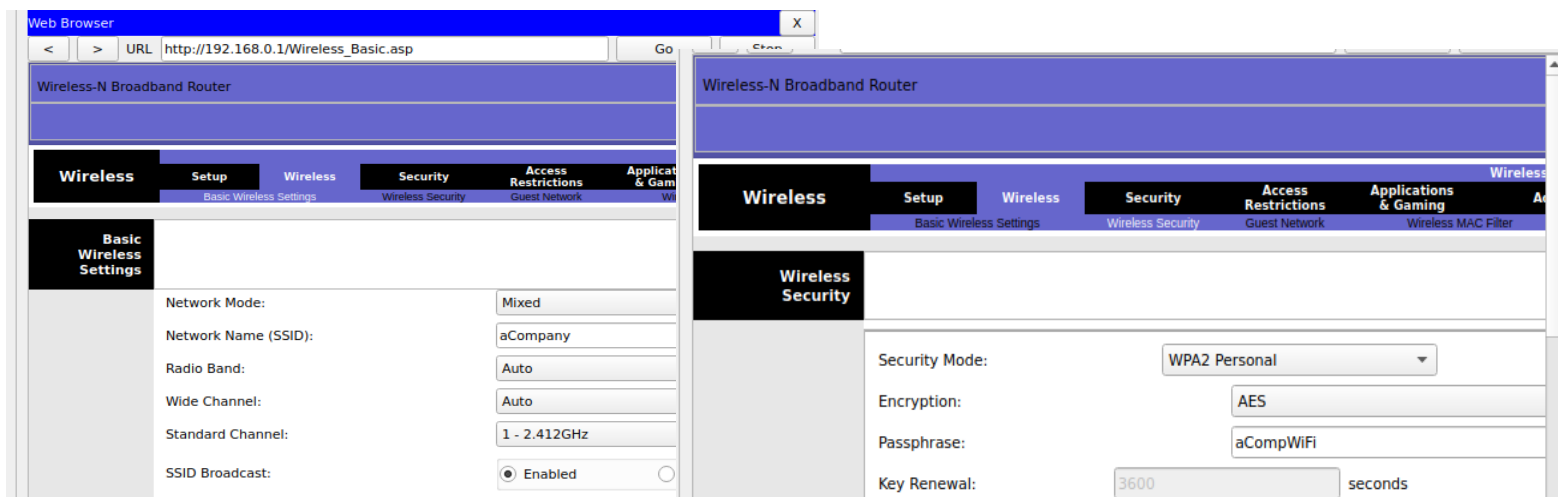
OBJECTIVES:

MAC filtering, Configuring DMZ, Disabling DMZ and configuring single port forwarding

Steps involved

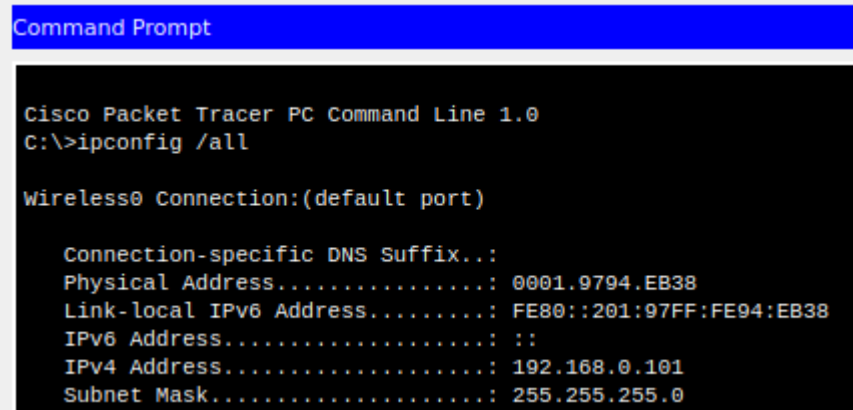
Step 1. Connecting to the wireless router configuration web page at 192.168.0.1 from PC0 then determining the SSID and passphrase.

SSID= aCompany passphrase= aCompWiFi



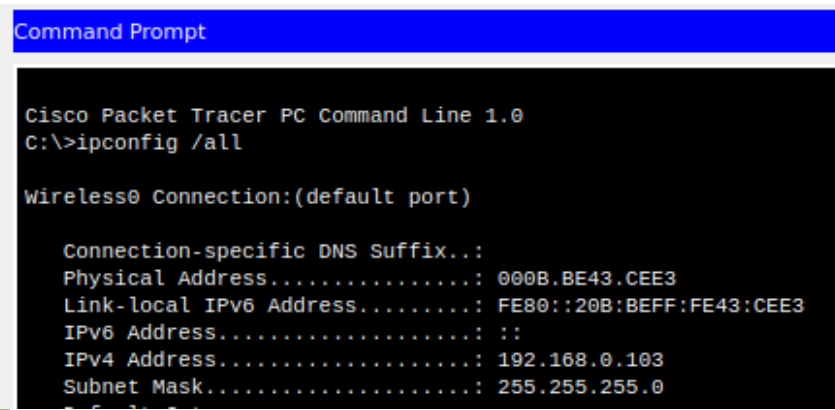
Step 2. Configuring laptop 0 as wireless client and note the ip and mac address

Laptop 0: IP address=: 192.168.0.101 MAC address=:0001.9794.EB38

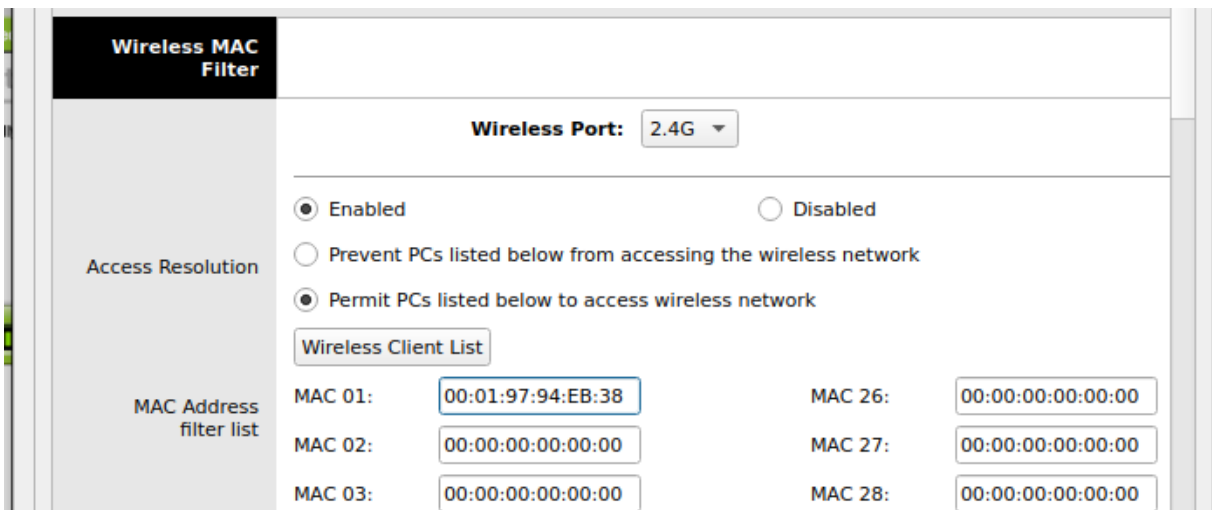


Laptop 1 configured as a wireless client

Laptop 1: *IP address:* 192.168.0.103 *MAC address:* 000B:BE43.CEE3



Step 3. Configuring MAC filtering on WRS1



Verifying connectivity for both laptops

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=78ms TTL=255
Reply from 192.168.0.1: bytes=32 time=55ms TTL=255
Reply from 192.168.0.1: bytes=32 time=45ms TTL=255
Reply from 192.168.0.1: bytes=32 time=31ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 78ms, Average = 52ms
```

Pinging from laptop0

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pinging from laptop1

Question:

Were both laptop able to connect to the WRS1 network? Why are you unable to associate with the access point? Laptop0 connected since the MAC address was configured on the access point WRS1. Laptop1 didn't connect since the MAC address wasn't configured on the access point.

Step 4. Testing connectivity through the telco cloud

Testing connectivity of remote pc (209.165.201.29). Connection was successful.

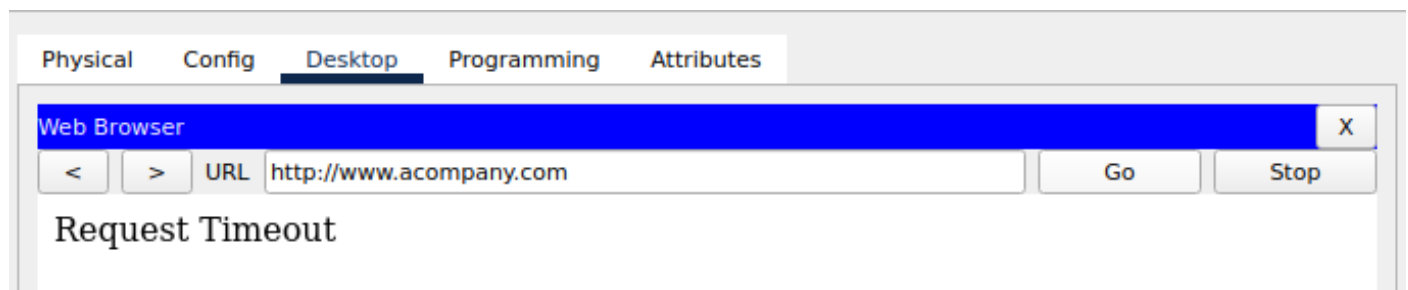
```
C:\>ping 209.165.201.29

Pinging 209.165.201.29 with 32 bytes of data:

Reply from 209.165.201.29: bytes=32 time=76ms TTL=126
Reply from 209.165.201.29: bytes=32 time=50ms TTL=126
Reply from 209.165.201.29: bytes=32 time=47ms TTL=126
Reply from 209.165.201.29: bytes=32 time=50ms TTL=126

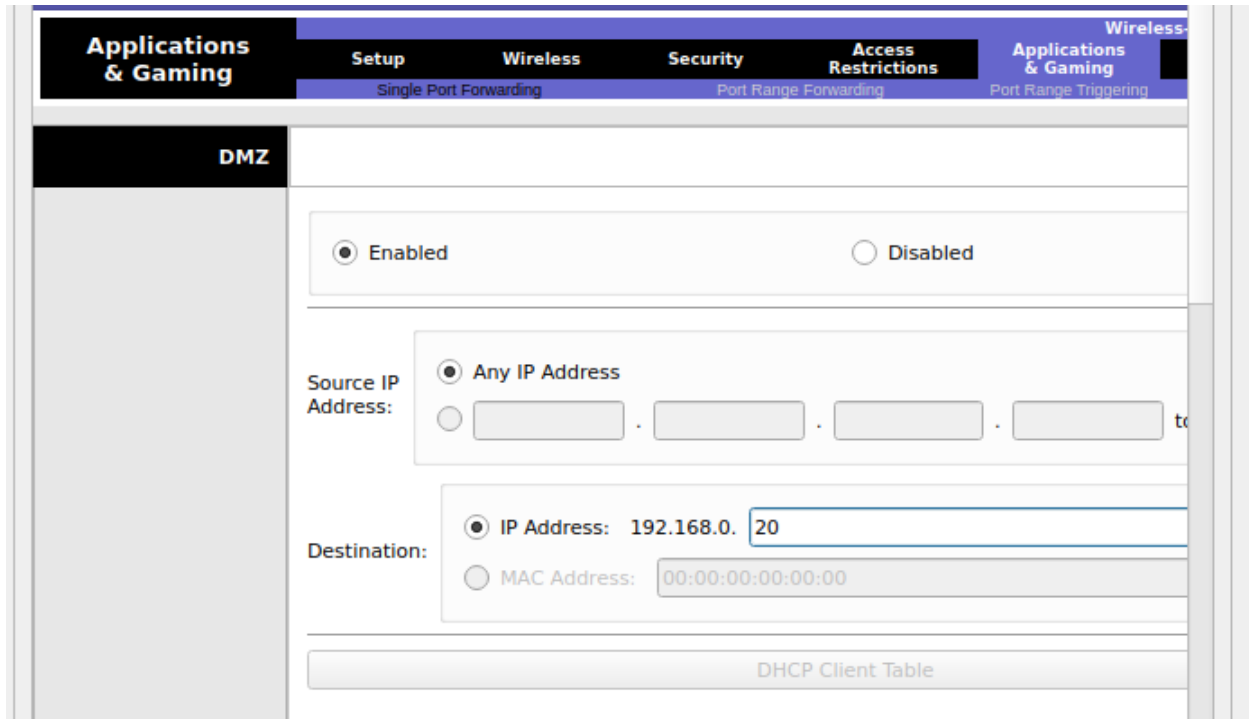
Ping statistics for 209.165.201.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 76ms, Average = 55ms
```

Browsing to the address of the internal web page hosted at Server0, which is www.acompany.com. A ***“Request timeout”*** message was displayed.



Step 5: Configuring DMZ.

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



The screenshot shows a router's configuration interface. The top navigation bar includes 'Applications & Gaming', 'Setup', 'Wireless', 'Security', 'Access Restrictions', and 'Wireless'. Under 'Applications & Gaming', there are sub-tabs for 'Single Port Forwarding', 'Port Range Forwarding', and 'Port Range Triggering'. The 'DMZ' section is active, showing a 'DMZ' tab on the left. The main content area has two radio buttons: 'Enabled' (selected) and 'Disabled'. Below this, there are two sections: 'Source IP Address' and 'Destination'. The 'Source IP Address' section has a radio button for 'Any IP Address' (selected) and a text input field for a specific IP address. The 'Destination' section has a radio button for 'IP Address' (selected) with a text input field showing '192.168.0.20', and a radio button for 'MAC Address' with a text input field showing '00:00:00:00:00:00'. At the bottom, there is a 'DHCP Client Table' section.

Browsing the www.acompany.com on remote pc; webpage was displayed as shown below:



Step 6: Configure WRS1 to forward a single port to Server0.

Configuring single port forwarding on the WRS1 to limit the number of exposed ports.

The screenshot shows the 'Applications & Gaming' tab in the WRS1 configuration interface. The 'Single Port Forwarding' sub-tab is selected. On the left, the 'Application Name' is set to 'HTTP'. The main table lists two forwarding rules:

External Port	Internal Port	Protocol	To IP Address	Enabled
---	---	---	192.168.0. 20	<input checked="" type="checkbox"/>
---	---	---	192.168.0. 0	<input type="checkbox"/>

Web page www.acompany.com on server 0 was reached from remote pc and is displayed as shown below:

