Edge Hill University

Faculty of Arts and Science

The Department of Computer Science

CIS2707 Computer Networks

Level 5

Coursework 1 – Task: 2

Home Wireless Network Scenario

2024/2025

Thomas Mason

26040247

Module Leader: Hamed Balogun

☎ 01695 65 6795

Email: hamed.balogun@edgehill.ac.uk

Administrators:

☎ 01695 65 7603

Table of Contents

Improvements from Task 1:

VLAN Implementation for the Network:

- Implemented VLAN 10 (Main) and VLAN 20 (Guest).

Internet Simulation:

- Built a custom internet simulation.

Firewall/ACL Implementation:

- Implemented ACL 110 to deny guest VLAN access to the main network.
- Allow internet access for both networks.

DHCP and IP Planning:

- DHCP pools were implemented per VLAN.
- Static IP are assigned to key devices (e.g TV, Router, Gaming Console).

Coverage and Hardware Placement:

- Access Points were positioned to provide floor-based coverage (2.4 GHz up, 5 GHz down).

Documentation & Screenshots

IP Interface on Router for VLANs:

```
HomeRouter>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual up                    up
GigabitEthernet0/0.10  192.168.1.1     YES manual up                    up
GigabitEthernet0/0.20  192.168.2.1     YES manual up                    up
GigabitEthernet0/1     203.0.113.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
HomeRouter>
```

Note: 203.0.113.1 is used for WAN simulation.

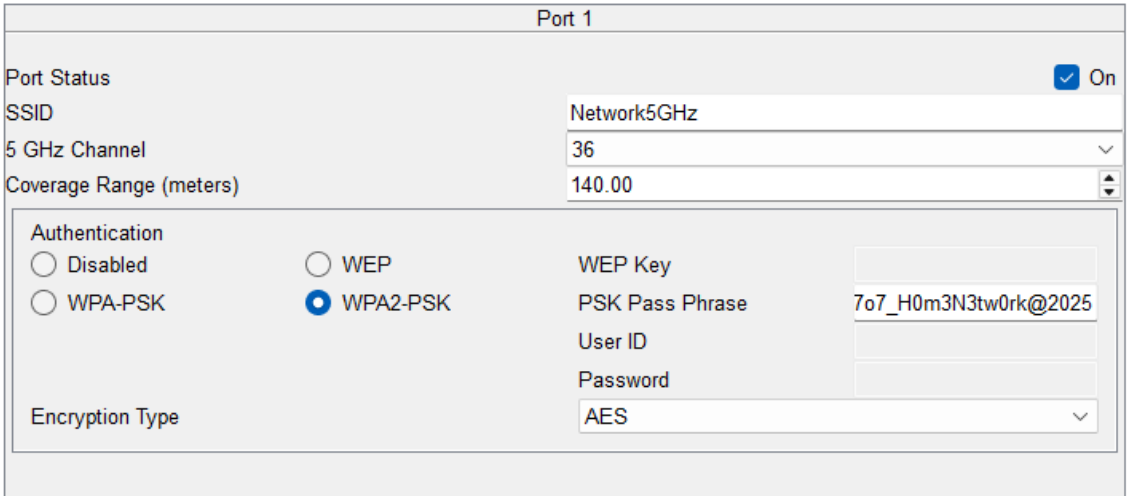
IP DHCP Pool for both the Main and Guest Networks:

```
HomeRouter>show ip dhcp pool

Pool MAIN_WIFI_POOL :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 8
 Excluded addresses              : 2
 Pending event                   : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     8    / 2     / 254

Pool GUEST_WIFI_POOL :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 5
 Excluded addresses              : 2
 Pending event                   : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.2.1          192.168.2.1      - 192.168.2.254     5    / 2     / 254
HomeRouter>
```

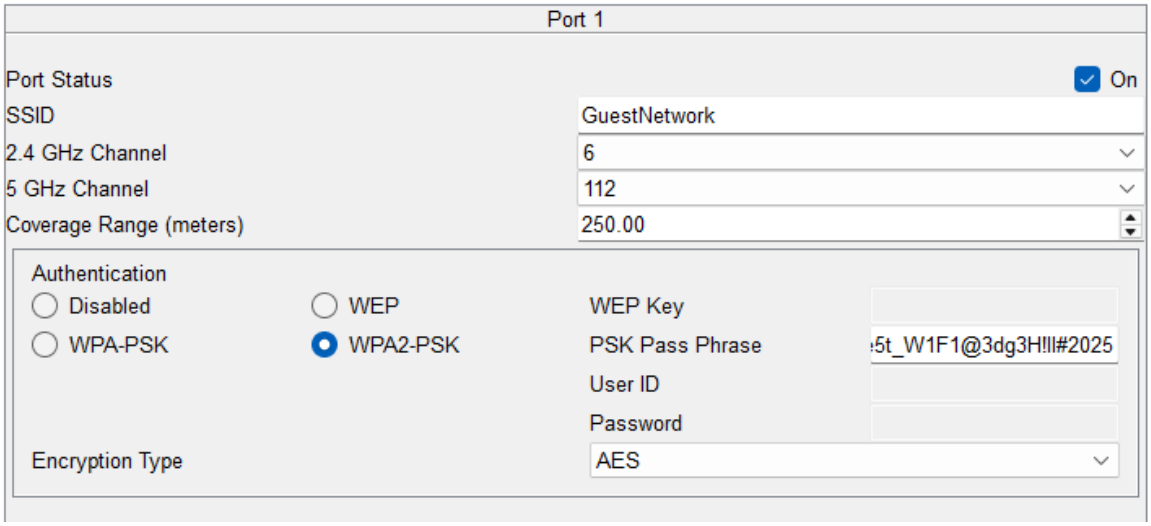
DHCP leases from both pools:

```
HomeRouter>show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.102    0001.9790.2CBB            --                    Automatic
192.168.1.101    00D0.D32B.B36E            --                    Automatic
192.168.1.100    000B.BE42.3023            --                    Automatic
192.168.1.104    00D0.9721.B4C7            --                    Automatic
192.168.1.103    00E0.F7E7.6300            --                    Automatic
192.168.1.105    0030.A39A.C61E            --                    Automatic
192.168.1.106    0001.4230.427B            --                    Automatic
192.168.1.107    0007.EC26.1528            --                    Automatic
192.168.2.13     00E0.B098.0B2B            --                    Automatic
192.168.2.10     00E0.F7BB.933D            --                    Automatic
192.168.2.11     00E0.8F2D.55C3            --                    Automatic
192.168.2.12     00E0.F753.70E4            --                    Automatic
192.168.2.14     000C.CF3D.4E6B            --                    Automatic
HomeRouter>
```

Access Point Configurations:



Note: The SSID would be hidden in a real-world application; however, Cisco Packet Tracer does not allow the application to save without it.



Switch VLAN setup:

```
Switch>show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
10   MAIN_WIFI                         active    Gig0/2
20   GUEST_WIFI                        active    Fa0/1
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch>
```

Trunk port configuration allowing VLAN 10 & 20 for Main and Guest:

```
Switch>show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20

Switch>
```

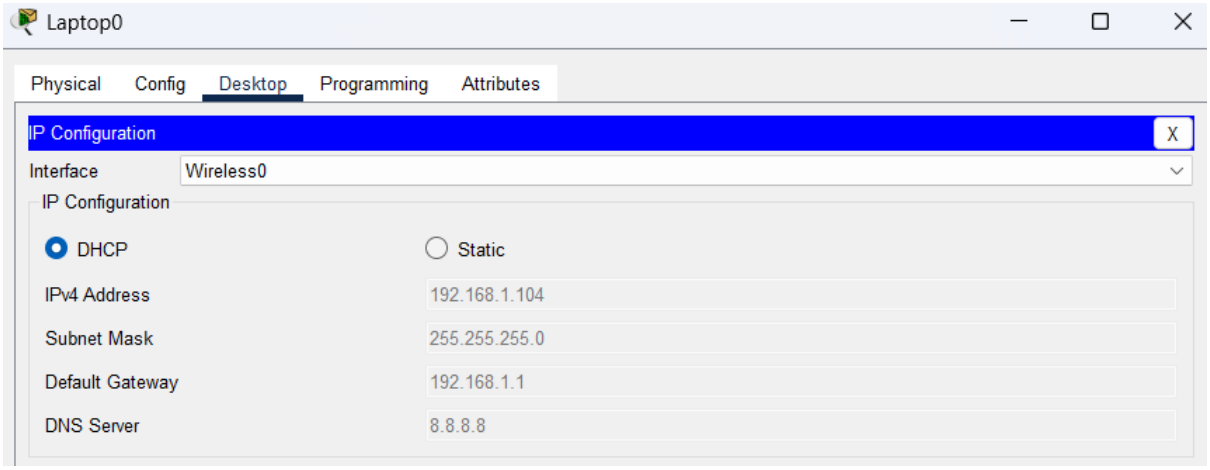
Access List configuration - Guest network traffic is blocked from Main:

```
HomeRouter>enable
HomeRouter#show access-lists
Extended IP access list 110
    10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
    20 permit ip any any (10 match(es))

HomeRouter#
```

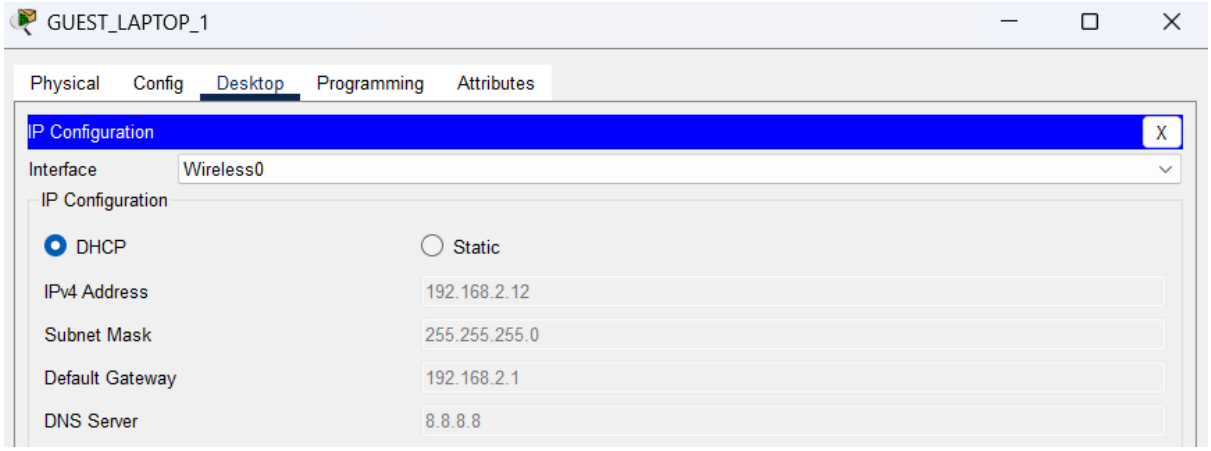
ACL 110 is applied inbound to the VLAN 20 Guest Network, preventing access to the Main Network while still allowing internet access:

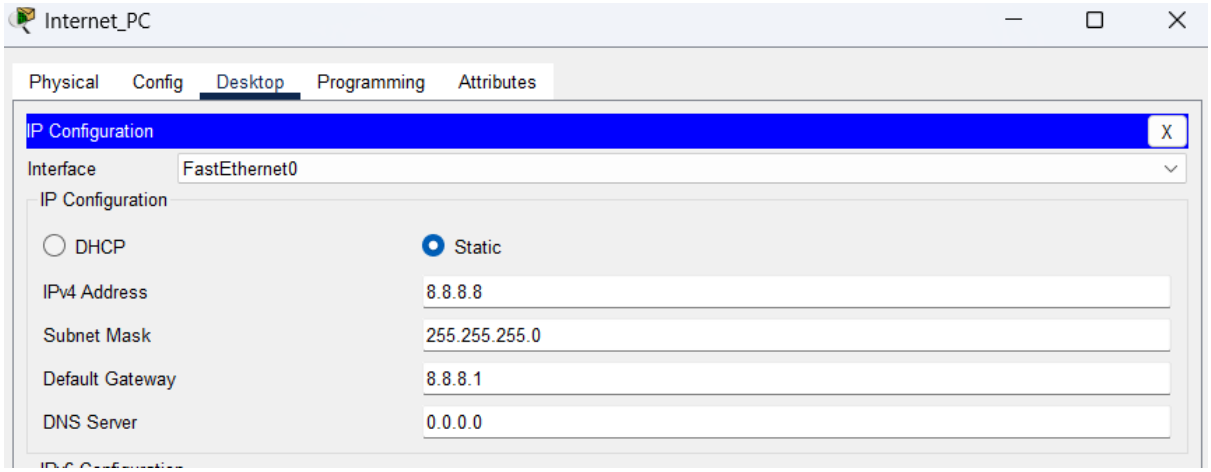
```
HomeRouter#show run | include access-group
 ip access-group 110 in
```

Device IP Configuration Main, Guest, & Internet PC:



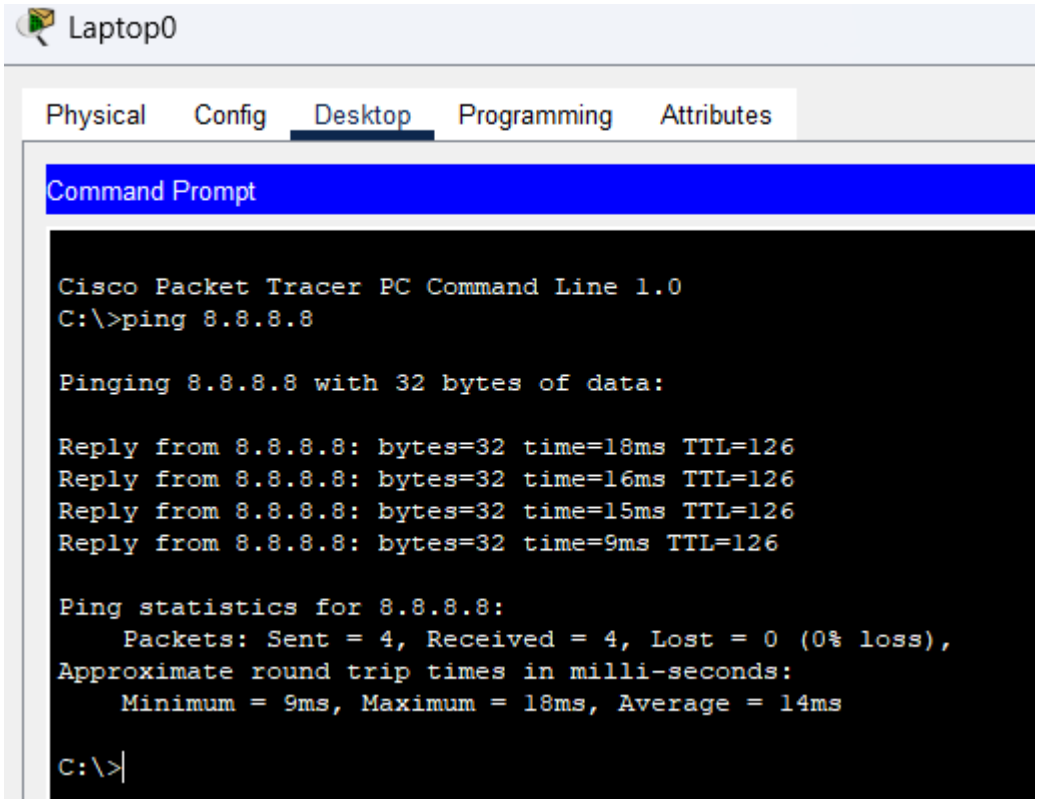
Home Wireless Networks: TASK 2



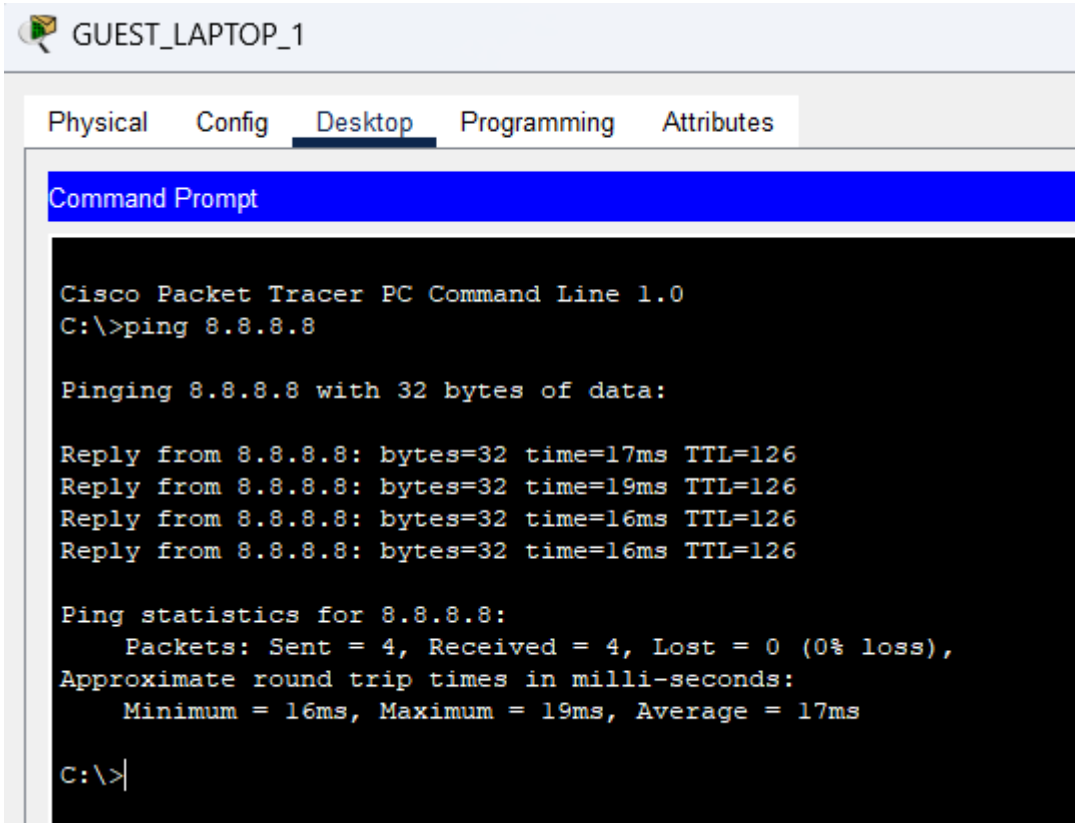


Network Ping Testing:

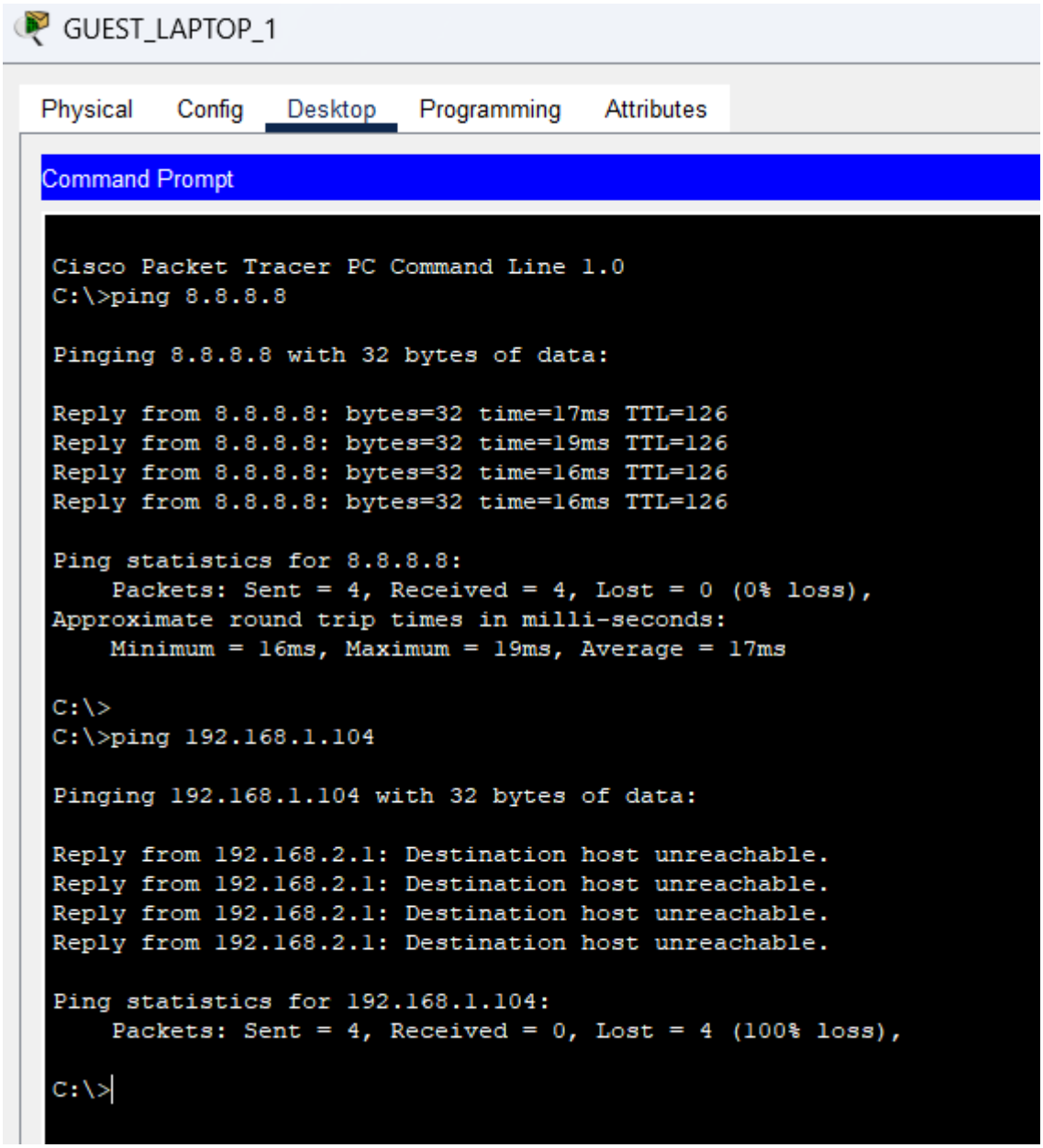
Main to Internet:



Guest to Internet:



Guest to Main:



MAC Address Filtering:

To further enhance wireless security on the main network (5GHz), MAC address filtering was initially intended to be implemented. This feature only allows specific trusted devices to connect to the wireless network based on their hardware (MAC) address.

However, due to Cisco Packet Tracer limitations, MAC address filtering is not available within the standard AccessPoint-PT-AC. On the other hand, in a real-world scenario, MAC filtering could be implemented with the following:

- Filter Mode: Allow only listed MAC addresses.
- Device Examples: Laptop0 (MAC: 00D0.9721.B4C7), Laptop1 (MAC: 00D0.D32B.B36E).