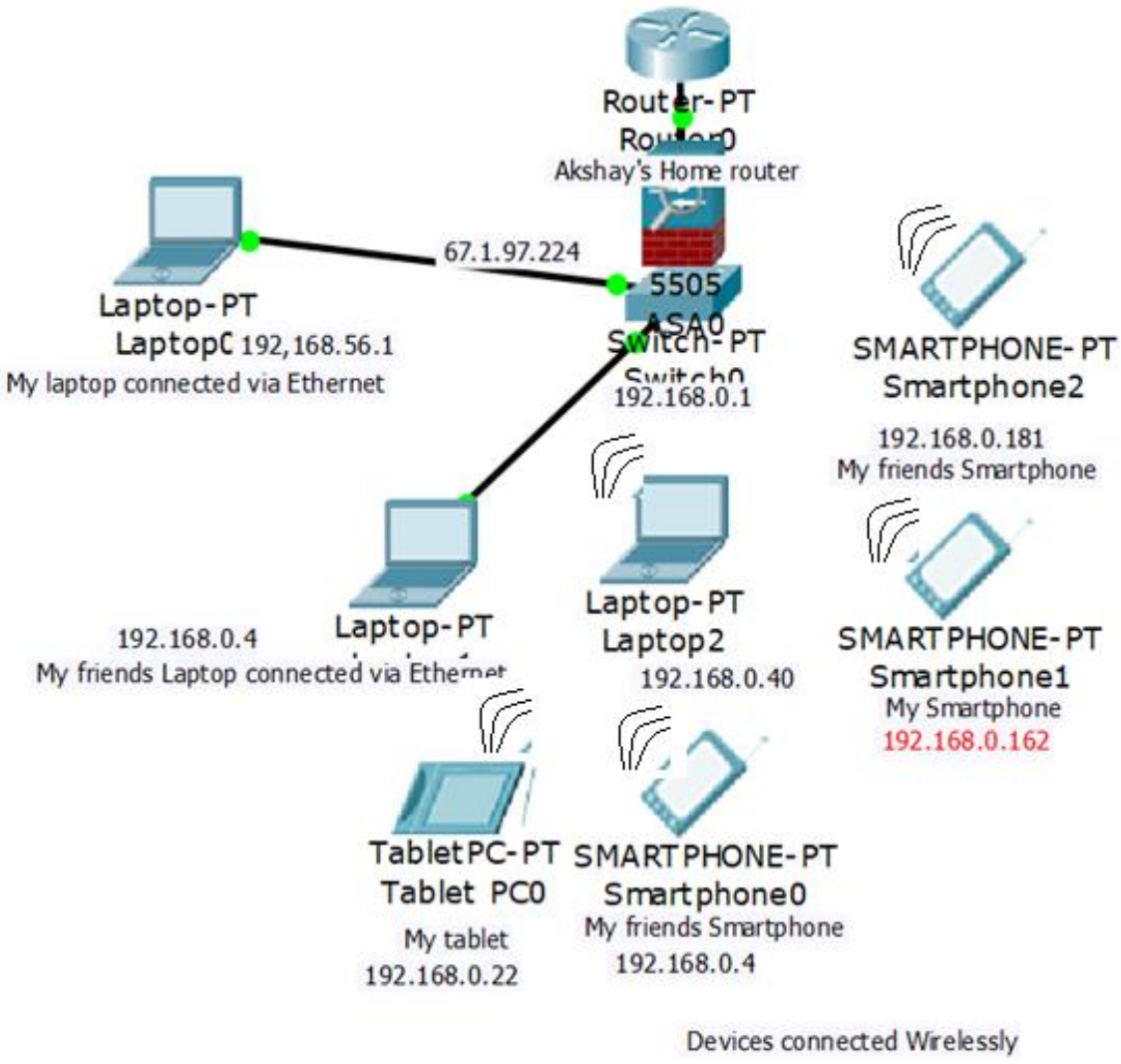
SIE 471/571 – Homework Network Sniffing

Akshay A Nayak

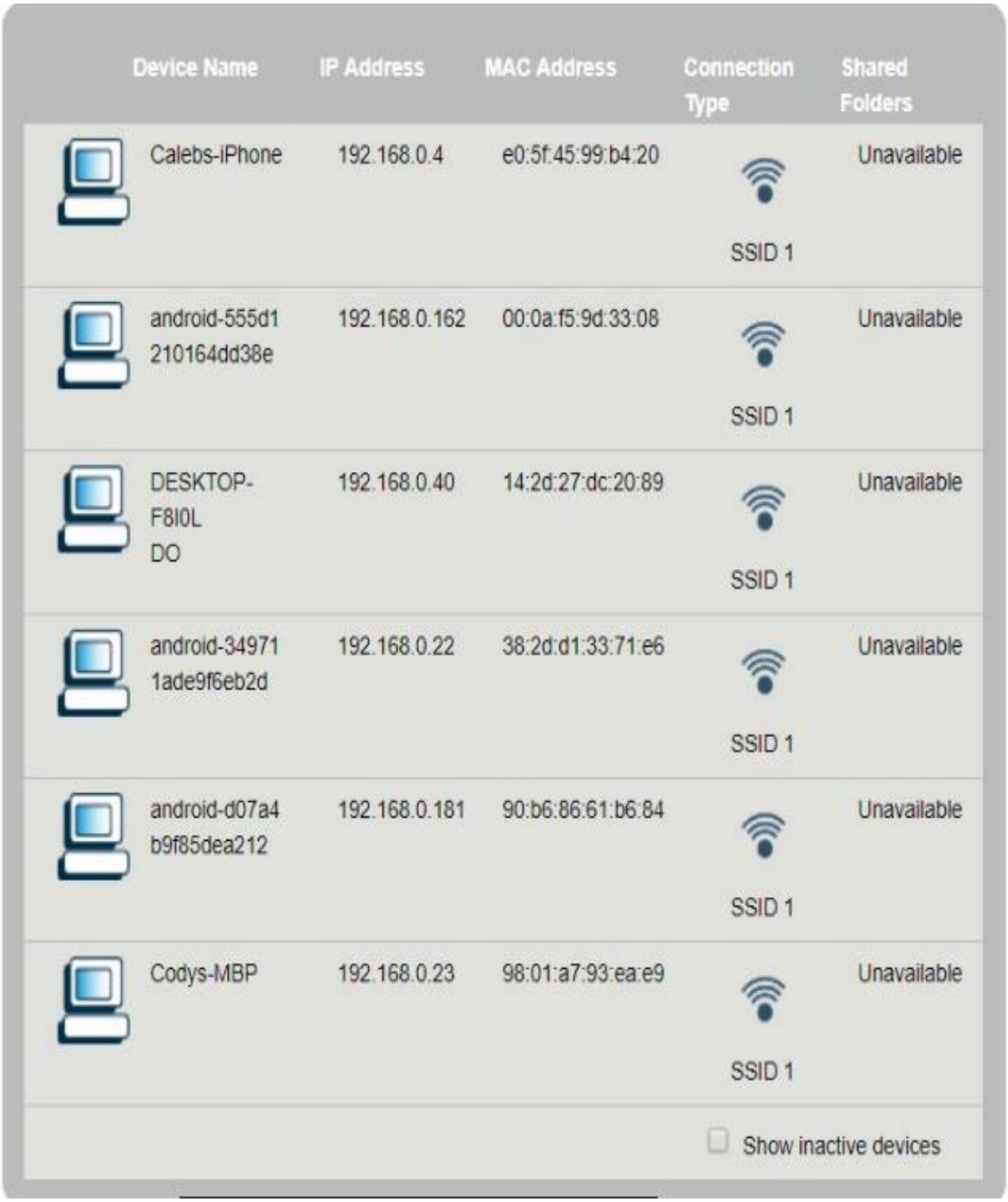
Student Id: 23368873

Personnel WIFI network



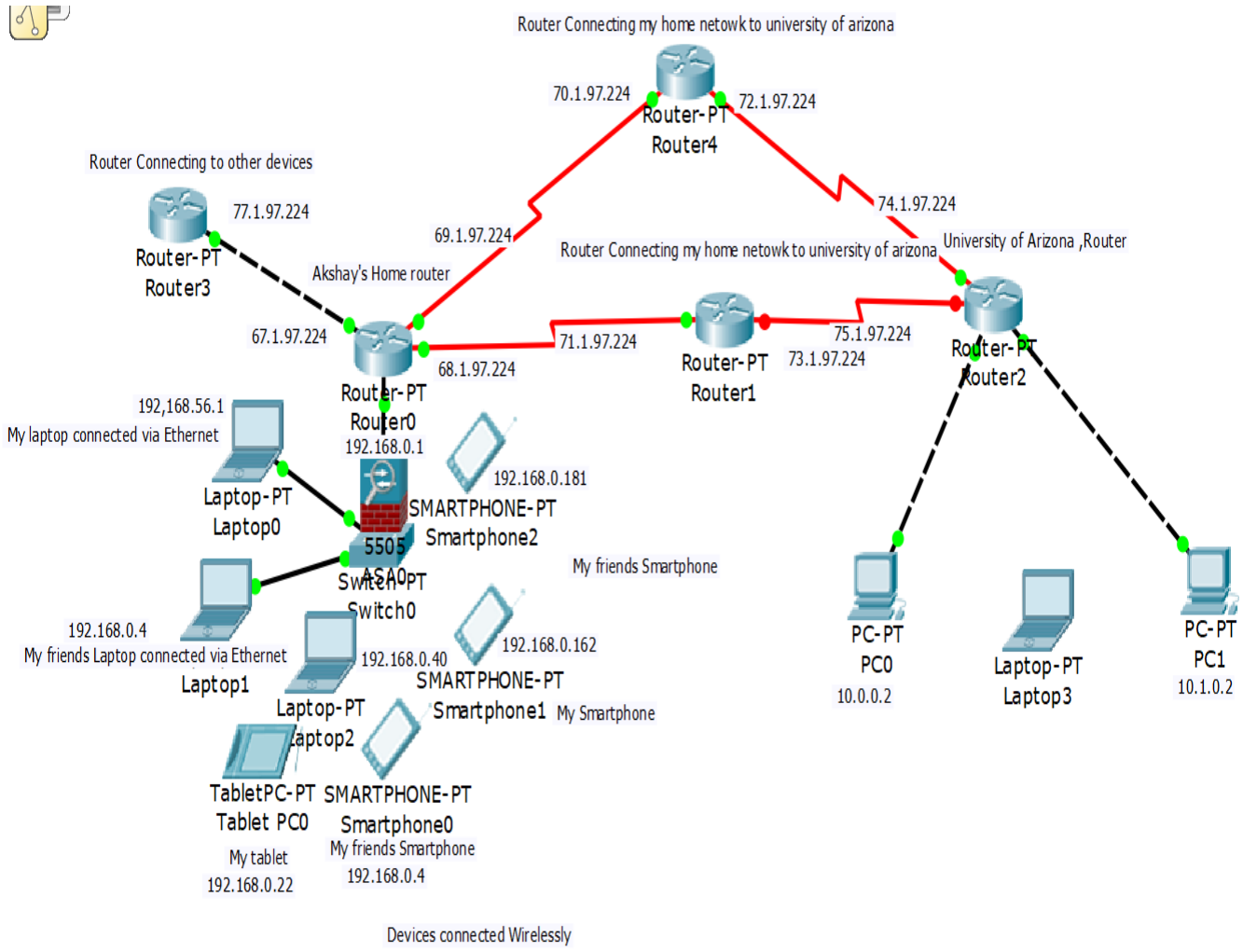
The above diagram shows my personnel WIFI network. I have a Laptop, smart phone and a tablet. I am sharing my apartment with 2 other friends who have a laptop and a smartphone respectively.

I found the IP address of all the WIFI connected devices my signing onto my router using the username and password. The IP address of all connected devices were found to be as shown below



I used the IP address that I found from my router to draw my Personnel WIFI network. (Figure shows all devices Connected to my home router)

My home router has an inbuilt modem, and a firewall feature in it. I have shown the separation of Router, modem and switch. Me and my friend use ethernet wire which is represented as lack of connection, in networking terms it is also called as a crossover cable. I have also shown the connection between my home network to the U of A WIFI network, which would look like the one shown below.



The above figure shows a possible path of connection from my laptop connected in my home to the U of A router. The U of A has certain devices connected via ethernet and few devices connected wirelessly.

I have shown 2 different paths, to connect to the U of A network, however there are many paths and many routers between my home and U of A network. The red wires represent the serial communication, we use cross over cable for the connection. The green dot shows that the connection is proper, while you can see a red rot that shows that the connection is not proper and the packets take a different route. The routers use EIGRP protocol to communicate within a small area and BGP protocol to communicate between areas. I configured the same in the above diagram. The routers between then home network and the U of A, WIFI was found using the **tracert** command:

```
1    21 ms     2 ms    19 ms  modem.Home [192.168.0.1]
2    73 ms    26 ms    21 ms  tcso-dsl-gw26.tcso.qwest.net [75.160.240.26]
3    38 ms    27 ms    24 ms  tcso-agw1.inet.qwest.net [75.160.241.201]
4    37 ms    67 ms     *     tcs-edge-05.inet.qwest.net [67.14.23.10]
5   120 ms   181 ms   167 ms  204.132.144.18
6    30 ms    26 ms    38 ms  206.207.226.158
7     *        *        *     Request timed out.
8     *        *        *     Request timed out.
9     *        *        *     Request timed out.
```

The request timed out is because, U of A firewall does not allow ping or tracert command.

The properties/Features of my WIFI is as shown below

SSID: R2C (Service set identifier- Can be changed)

Protocol: 802.11n

The properties of this protocol are that, it is faster (Used multiple input multiple output, can use two data channels at the same time. Better than the older version 802.11n as quality of wireless link is better), less prone to interference (Uses 2.4Ghz to communicate with older version devices and 5GHz to communicate with newer devices,5GHz channel is less crowded and thus quality of data is better) and has increased security (This feature make it difficult to obtain unauthorized access , it also has inbuilt IDS tools).

Security type: WPA2-Personal

WPA2 is advanced version of WPA.WPA-Personal 9pre shared key). The network device encrypts the data from a 128-bit encryption key that is generated from a 256-bit shared key. Uses AES encryption algorithm for authentication and data encryption.

Network band: 2.4 GHz

Network channel: 6

IPv4 address: 192.168.0.10

IPv4 DNS Servers: 192.168.0.1

205.171.3.25

Manufacturer: Broadcom

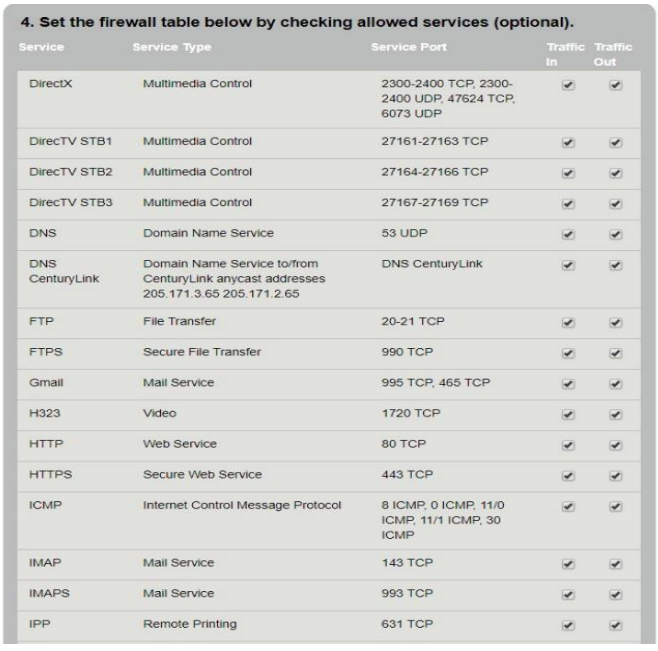
Description: Broadcom BCM43142 802.11 bgn Wi-Fi Adapter

Driver version: 7.35.352.0

Physical address (MAC): 14-2D-27-DC-20-89

It is the hardware address of my laptop. It is a unique 48-bit number, where the first half represent the manufacturer number. MAC number plays a vital role in packet forwarding to the destined location.

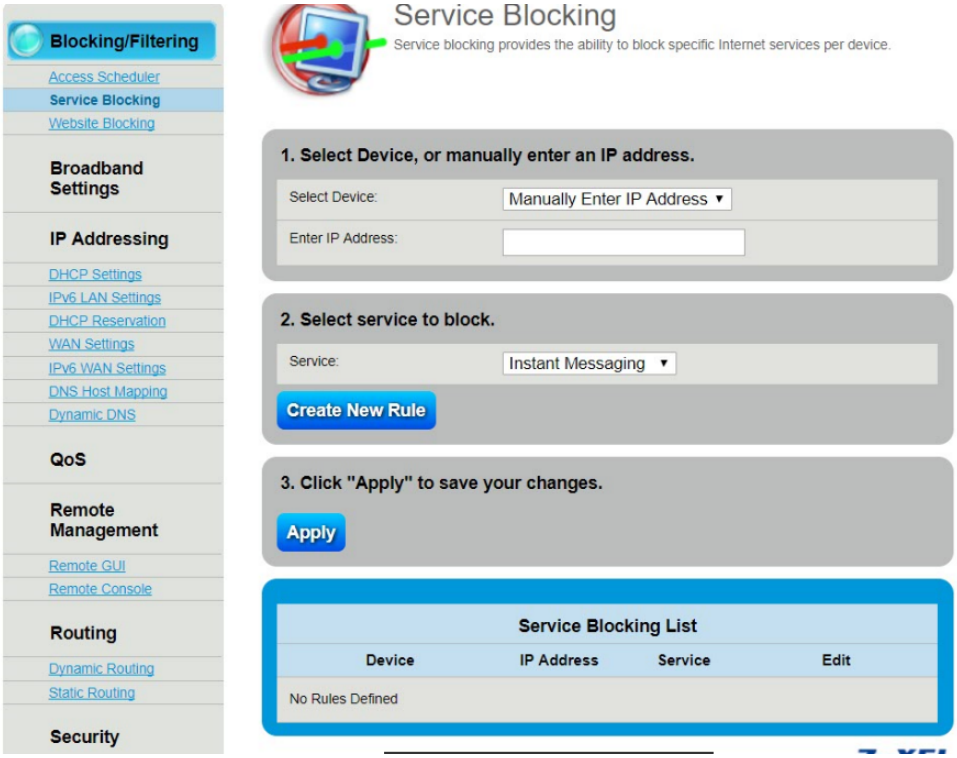
Also, there are two layers of firewall before reaching my computer for an external attacker. The first firewall exists in my home router. I am attaching screen shots of the same. The below figure shows the list of services that are allowed. I can add and remove the services to increase my security

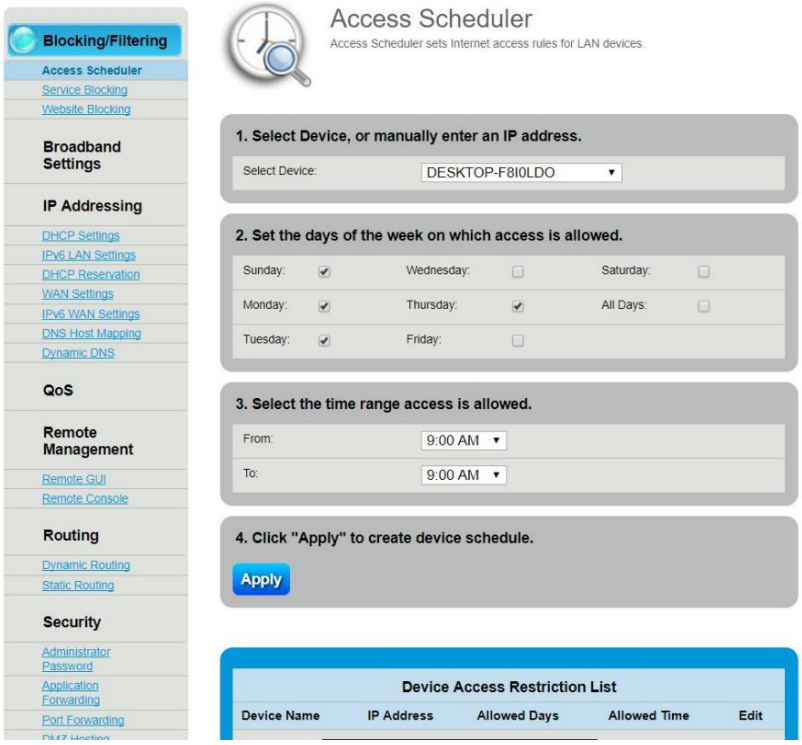


4. Set the firewall table below by checking allowed services (optional).

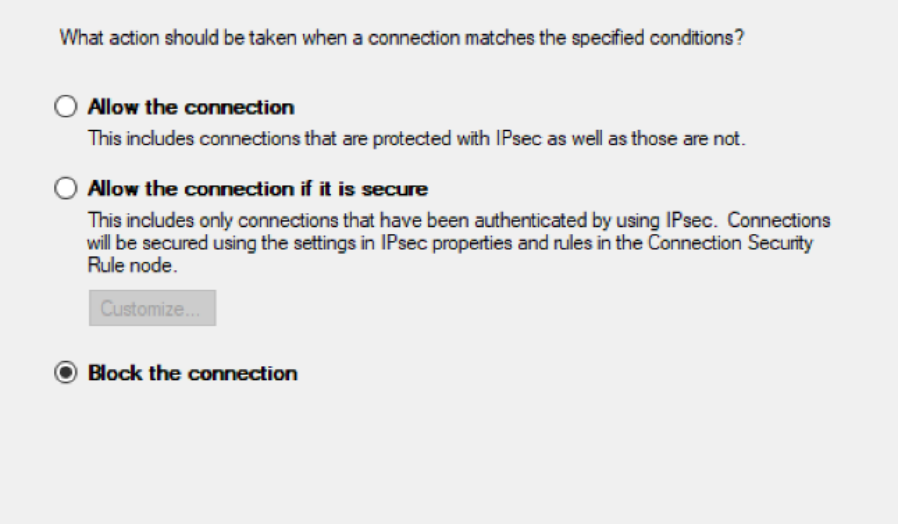
Service	Service Type	Service Port	Traffic In	Traffic Out
DirectX	Multimedia Control	2300-2400 TCP, 2300-2400 UDP, 47624 TCP, 6073 UDP	✓	✓
DirecTV STB1	Multimedia Control	27161-27163 TCP	✓	✓
DirecTV STB2	Multimedia Control	27164-27166 TCP	✓	✓
DirecTV STB3	Multimedia Control	27167-27169 TCP	✓	✓
DNS	Domain Name Service	53 UDP	✓	✓
DNS CenturyLink	Domain Name Service to/from CenturyLink anycast addresses 205.171.3.65 205.171.2.65	DNS CenturyLink	✓	✓
FTP	File Transfer	20-21 TCP	✓	✓
FTPS	Secure File Transfer	990 TCP	✓	✓
Gmail	Mail Service	995 TCP, 465 TCP	✓	✓
H323	Video	1720 TCP	✓	✓
HTTP	Web Service	80 TCP	✓	✓
HTTPS	Secure Web Service	443 TCP	✓	✓
ICMP	Internet Control Message Protocol	8 ICMP, 0 ICMP, 11/0 ICMP, 11/1 ICMP, 30 ICMP	✓	✓
IMAP	Mail Service	143 TCP	✓	✓
IMAPS	Mail Service	993 TCP	✓	✓
IPP	Remote Printing	631 TCP	✓	✓

The below two figures show about the blocking and access feature. Using the access feature, I can allow a user to connect to my WIFI only for a certain time of a week and using the blocking feature I can block a certain IP device holder from gaining access to my network.





The second layer of security is offered by the windows firewall on my PC. I always ensure that the firewall is on. The windows firewall has an inbuilt set of rules for inbound and outbound connections. We can add the rules if necessary. We can block applications from accessing the data or close a port if needed. For example, adding a new outbound rule on port 80 and 443 to block a connection would block port 80(HTTP) AND 443(HTTPS) and deprive my laptop from having a internet connection. The below diagram represents the same.

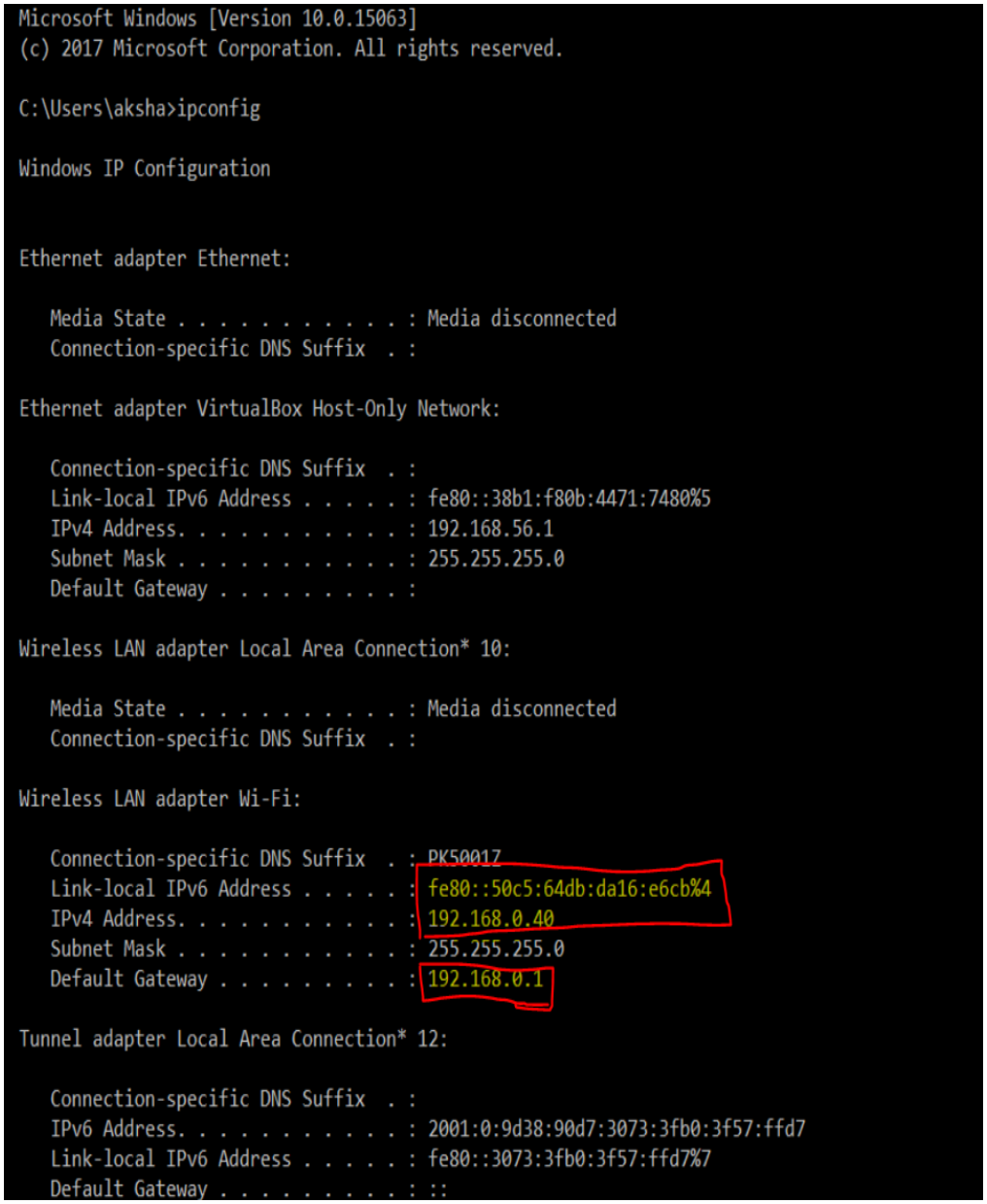


Yes, I would change my architecture of my network, I would add a physical firewall device after my router so that no external entity would be able to access my network. I would also enable port block feature on the switches that will turn off the port if an unknown MAC address bearing device try to connect to a switch.

I had enabled the feature to connect automatically to WIFI when I am in range, I found that this would be risky as it might make me vulnerable to an attack.

Part C- Mapping our Home Network

Step 1: In the command line type ipconfig to check the IP address of our device(laptop) and the default gateway (Usually Router IP address – The IP address is the private IP address and not the actual public IP address). There are two types of IP address IPV4 and IPV6 both are show using the ipconfig command.
The NAT process is used to convert private IP to public IP address. NAT is the reason because of which IPV4 address is still not exhausted.



I used a wireless LAN, I found out my IP address to be 192.168.0.40(IPV4) and IPV6 address to be fe80::50c5:64db: da16:e6cb(Expressed as a hexadecimal value – 128 bit long . :: -represent that 0's are placed here) .

The default gateway, represent my routers IPV4 address and it is found to be 192.168.0.1(private IP address, however router communicates with the outside world using private IP address).

The subnet mask is found to be 255.255.255.0, which states that I could connect 254 host in the same LAN, the first 3 number defines the network park while the last part defines the host part.

Step 2: Ping someone in our network

I connected my tablet to the same network, and found out its IP address to be 192.168.0.22 . I used ping command to send data packets from my laptop to my tablet and found my tablet was also within the same subnet.

```
C:\Users\aksha>ping 192.168.0.22

Pinging 192.168.0.22 with 32 bytes of data:
Reply from 192.168.0.22: bytes=32 time=526ms TTL=64
Reply from 192.168.0.22: bytes=32 time=29ms TTL=64
Reply from 192.168.0.22: bytes=32 time=373ms TTL=64
Reply from 192.168.0.22: bytes=32 time=72ms TTL=64

Ping statistics for 192.168.0.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 526ms, Average = 250ms

C:\Users\aksha>
```

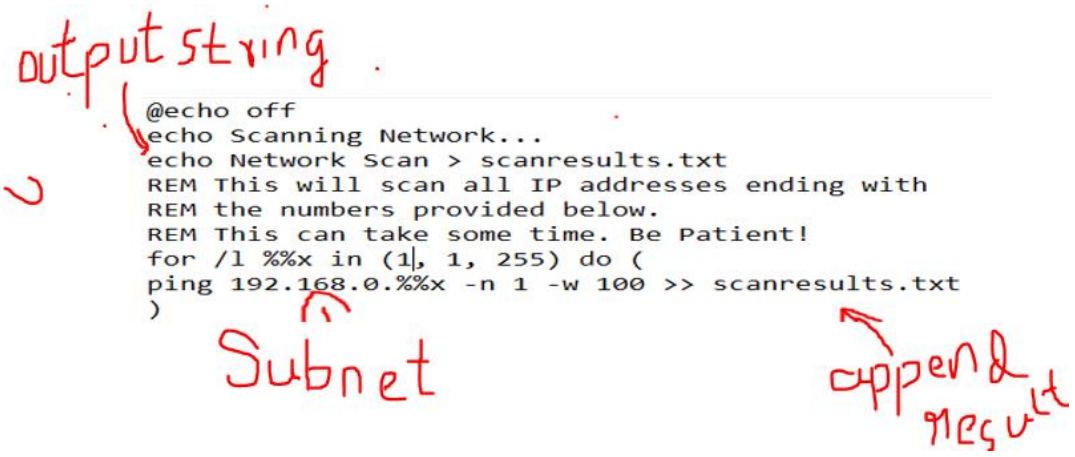
Since the Netmask is 255.255.255.0, all devices that are in 192.168.0. xx fall in the same subnetwork.

Step 3: To store results

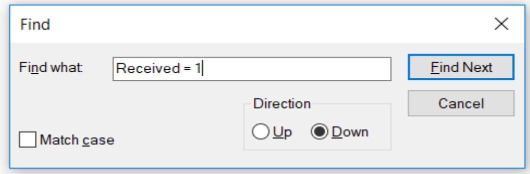
Use > and >> to store results,>> appends a new value while > overwrites a value in text file. I stored the result in a fil named hello.txt.

```
C:\Users\aksha>echo Hello Class! >hello.txt

C:\Users\aksha>type hello.txt
Hello Class!

C:\Users\aksha>echo Hello Akshay! >>hello.txt

C:\Users\aksha>type hello.txt
Hello Class!
Hello Akshay!

C:\Users\aksha>echo bye good night >hello.txt

C:\Users\aksha>type hello.txt
bye good night

C:\Users\aksha>
```

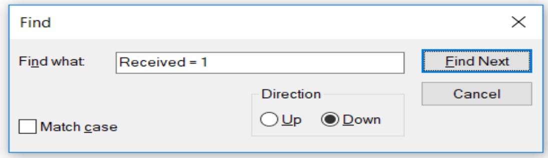
Step 4:



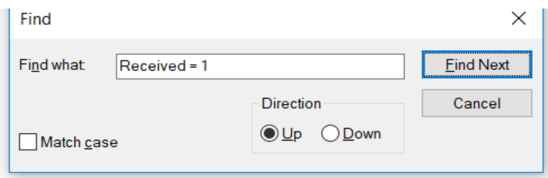
```
Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

Pinging 192.168.0.2 with 32 bytes of data:
Request timed out.
```



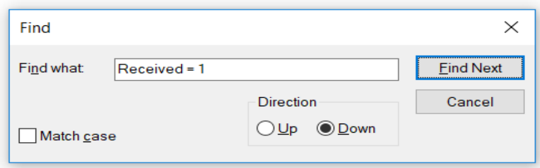

```
Ping statistics for 192.168.0.22:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 89ms, Maximum = 89ms, Average = 89ms

Pinging 192.168.0.23 with 32 bytes of data:
Reply from 192.168.0.23: bytes=32 time=102ms TTL=32

Ping statistics for 192.168.0.23:
```




```
Pinging 192.168.0.40 with 32 bytes of data:
Reply from 192.168.0.40: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.40:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pinging 192.168.0.41 with 32 bytes of data:
```



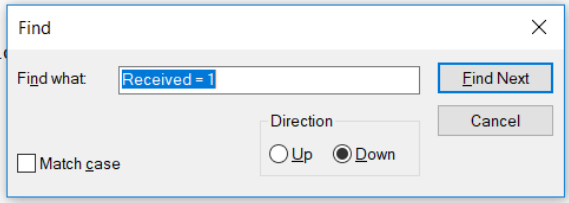

```
Ping statistics for 192.168.0.181:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 96ms, Maximum = 96ms, Average = 96ms

Pinging 192.168.0.182 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.182:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Pinging 192.168.0.183 with 32 bytes of data:
Request timed out.
```



The above code pings to all the devices in my subnet 192.168.0.1 to 192.168.0.254. 192.168.0.1 and 192.178.0.255 form the network ID and broadcast ID of my network. When the device with particular IP address is present in my network I hear back from them , and thus I receive the Received == 1 message.
The result obtained shows that I could ping devices with IP address 192.168.0.x, There were 4 active devices in my subnet when I executed my code, I got a reply from these devices. The 192.168.0.1 is the IP address of my router, while other packets received are due to the 3 devices connected in my subnet.
To verify the code, I ran the same code by disconnecting all devices except my laptop, and found that only twice the packets were received, one for the router IP and other for my laptop IP.

```
@echo off
echo Scanning Network...
echo Network Scan > scanresults.txt
REM This will scan all IP addresses ending with
REM the numbers provided below.
REM This can take some time. Be Patient!
for /l %%x in (1, 1, 255) do (
ping 192.168.0.%%x -n 1 -w 100 >> scanresults.txt
)
```

```
Reply from 192.168.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% l
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pinging 192.168.0.11 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.0.11:
```



The IP address of devices are assigned dynamically, by DHCP. So, the IP address of individual devices change. Usually a lease time of about 1 hour is allocated for a IP address.