Logo, company name

Description automatically generated

***Portfolio-Second Draft***

**Submitted By:**

**Name:** Khalid Hasan Seum

**Student ID:** 12176368

**Subject:** NETWORKED INFRASTRUCTURE FOUNDATIONS

**Course:** BACHELOR OF INFORMATION TECHNOLOGY (Major in Cyber Security)

**Submitted To:**

**Name:** Jahan Hassan

**E-mail:** j.hassan@cqu.edu.au

**Week 4:** Network Topologies and Technologies.

**Summary:**

In this week we are learned about the Wireshark tool. The tool is used for the packet capture. It can be used for the network troubleshooting, analysis, development of software and communications protocol development, and education. It can capture network traffic and analyzing packets at an extremely granular level.

.Graphical user interface, application

Description automatically generated

*Pic 1: The front page of Wireshark Network Analyzer.*

In the picture 1, we can see the front page contains different type of connection, If we use Wi-Fi and wants to capture the packets from the Wi-Fi, then we have to select Wi-Fi and if we use ethernet then we have to press ethernet. After that we can see in the upper line a option called capture. We have to press there and after that we have to press start. Then the Wireshark will start capturing. In the picture 2 we can see that.

Graphical user interface, text

Description automatically generated

*Pic 2: Wireshark capturing the packet of the WI-FI.*

Then, we can perform ipconfig /all to see our network configuration and besides we have to do it so that we can see the configuration is match with the Wireshark or not. Then we have to use ping command to the command prompt so that Wireshark can capture that packet and we can analyze that.

Text

Description automatically generated

*Pic 3: Using ipconfig /all to see the network configuration.*

Text

Description automatically generated

*Pic 4: Using ping to trace the root and for Wireshark so that Wireshark can capture this data.*

In the capture option there are many capture list. So, for the specific capture list we have to use filter. We used the filter for icmp and then we found the result that is shown in the picture 5.

Table

Description automatically generated

*Pic 5: We are using filter to see the icmp result.*

In the picture 5, we can see the Frame, Ethernet details, internet protocol and internet control message protocol.

Graphical user interface, text, application

Description automatically generated

*Pic 6: we are right click on the Frame, Ethernet, and all other option to see more details.*

In the picture 6, If we tap the options like Frame, Ethernet then we can see more details. We can see each and every details of those options.

Graphical user interface, text, application, email

Description automatically generated

*Pic 7: We filter the http to see the http packet that captured by the Wireshark.*

**Reflection:**

In the last week, I understood most of the week’s materials and the topics of that week was network hardware essentials, but I wants to go deeper down of advantages and disadvantages of a repeater. Though we know repeater helps a lot by extend the network’s total distance. But it has disadvantages too. But why ?

If we look into advantages of the repeater, we can see the repeater extend a network’s total distance, it’s never seriously affect network performance, it’s simple to connect and cost effective, it has the ability to boost the digital to retransmit, some of them can connect networks using different physical media.

If we look at the disadvantage then we can see repeater are unable to reduce network traffic, there are limitation in the number of repeater, repeater does not segment the network. Repeater cannot connect difference network architecture, it does not separate the device in the collision domain and most of them on a network produce noise on the wire and increase the possibility of packet collisions.

So, we can see there are some disadvantages beside the huge advantages.

**Reference:**

https://www.ecstuff4u.com/2020/05/advantages-disadvantages-repeater.html

**Week 5: Network Media**

**Summary:**

The main tool used in this tutorial for week five was WI-FI analyzer. This tool is used for analyze the WI-FI. It can be installed in the android and the iOS device.

In the picture 1 we can see my SSID is: Hola and in this WI-FI analyzer app it’s marked as Grey color. We can also see the signal strength.

Diagram

Description automatically generated

*Pic 1: Graph of WI-FI Aps and the gray color marked is my WI-FI AP.We can also see the signal strength of those APs.*

In the picture 2 we can see there are also graph of Wi-Fi routers SSID and their signal strength.

Chart, histogram

Description automatically generated

*Pic 2: Graph of WI-FI routers APs and their signal strength.*

In the picture 3, we can see the signal strength of my W*-FI router*, we can put the individual Wi-Fi SSID here and test the signal strength. If it’s goes to the green, then the signal of WI-FI router is very good but if it goes to yellow, then the signal strength is not much good as the green one and if it goes to gray one, then the signal strength is poor.

A picture containing diagram

Description automatically generated

*Pic 3: WI-FI router signal strength test meter*

In the picture 4, we can see how many APs are within the range of my phone. We can see there are total 19 APs around the range of my phone. Some of the Aps have better signal than the others. We can see the mac address of those WI-FI router and the channel of those routers. I can see my AP have -59 dBm

A screenshot of a computer

Description automatically generated with medium confidence

*Pic 4: WI-FI routers APs list.*

In the picture 5, we can see and analyze which channel is best for our Wi-Fi router.

Graphical user interface, text, application

Description automatically generated

*Pic 5: WI-FI router channel list which showing which channel is better for our router by analyzing others router.*

**Reflection:**

In the last week, I understood most of the week’s materials and the topic was network topologies and technologies, but I wants to go deeper down of WI-FI band 5 GHz and 2.4 GHz. There are some advantages to shift 5 GHz from 2.4 GHz. But why?

There are pros in both band such as in 5 GHz, we get higher speed, less commonly used that means less interference from others and our microwave ovens will not interfere with signal.

Besides, in 2.4 GHz have longer range, better penetration through walls and have compatibility with older device which doesn’t support 5 GHz.

If we compare both we see for more speed, lower interference with other device and no interfere with other device, we must have to use 5GHz. We can also get a lower ping in 5GHz. If we keep the 5 GHz only for the gaming while using the 2.4 GHz for the other devices, The ping and performance of internet will be lot better as most devices use 2.4 GHz but and they’re not using 5 GHz.

**Reference:**

<https://www.quora.com/How-come-my-2-4GHz-WiFi-has-a-better-ping-but-my-5GHz-WiFi-downloads-quicker>

<https://www.quora.com/Is-5g-or-2-4-g-better-for-gaming>

**Week 6: Network Protocols**

**Summary:**

The main tool used in this week 6 is command prompt, ipconfig/all, and arp -a, and arp -d. In this week at command prompt we find out my IPv4 address, NIC MAC address, the address of default gateway, the address of one of my DNS servers. We’ll discover so many thing by using “arp-a” command.

We’re using ipconfig/all for find out all the details of our network.

Text

Description automatically generated

*Pic 1: In command prompt we’re using ipconfig/all.*

Text

Description automatically generated

*Pic 2: The existing result of ipconfig/all.*

In the command prompt if we write the command of ipconfig/all then we can see the IPV4 address of our router. My IPV4 address is: 192.168.1.109

Text

Description automatically generated with medium confidence

*Pic 3: IPV4 Address of mine by using ipconfig/all.*

In the command prompt if we write the command of ipconfig/all then we can see the NIC MAC address of our router. My NIC MAC address is: D0-AB-D5-68-17-1C

A picture containing text

Description automatically generated

*Pic 4: NIC MAC address of my laptop.*

In the command prompt if we write the command of ipconfig/all then we can see the default gateway of our router. My Default Gateway is: 192.168.1.1

A picture containing text

Description automatically generated

*Pic 5: Default Gateway of my laptop.*

In the command prompt if we write the command of ipconfig/all then we can see the DNS Servers of our router. My DNS Servers is: 192.168.1.1

Text

Description automatically generated with medium confidence

*Pic 6: DNS Servers of my laptop.*

DNS full form is Domain Name System. DNS server is use for match website hostnames to their corresponding IP addresses and it contains database of the public Internet Protocol(IP) corresponding domain name.

In the picture 7 we can see my DHCP Server is 192.168.1.1(marked as Yellow) and DNS Server is 192.168.1.1(marked as Green) and the Gateway is 192.168.1.1(marked as Pink).

Text

Description automatically generated

*Pic 7: DHCP Server IP address, DNS Servers IP address, and Gateway of my laptop*

We can use arp -a command to the command prompt to see the current ARP table. We can see many IP address , physical address and the type of those IP address such as dynamic, static. The current entries exist because they are used recently , some of the are broadcast nature and some of them are fixed nature.

A picture containing calendar

Description automatically generated

*Pic 8: Using arp -a to see the ARP table.*

We can use arp -d to delete this ARP table.



*Pic 9: Using arp -d for delete the ARP table.*

Then, we have to ping a website and the again we have to use arp -a command to see the changes in the ARP table.

A picture containing calendar

Description automatically generated

*Pic 10: Using ping command and then again using arp -a to see the changes after using ping.*

**Reflection:**

In the last week, I understood most of the week’s materials and the topics was network media, but I wants to go deeper down of WI-FI 5 and WI-FI 6. Which will give us more advantage and why ?

Wi-Fi 6 has a maximum throughput of 9.6 gigabits per second (Gbps) across multiple channels, compared to 3.5 gigabits per second (Gbps) for Wi-Fi 5. A Wi-Fi 6 enabled router may theoretically achieve rates of almost 250 percent faster than current Wi-Fi 5 devices.

Wi-Fi 6's increased speed is due to technology such as orthogonal frequency division multiple access (OFDMA); MU-MIMO; beamforming, which allows higher data rates at a given range to increase network capacity; and 1024 quadrature amplitude modulation (QAM), which increases throughput for emerging, bandwidth-intensive uses by encoding more data in the same amount of spectrum.

So, we can see there are advantage in WI-FI 6.

**Reference:**

https://www.minim.com/blog/wifi-6-vs-wifi-5-speed

**Week 7: The Internet Protocols**

**Summary:**

In this week the main tool is Command Prompt, ipconfig, and tracert. By this we can find out IPv4 address and network details.

Text

Description automatically generated

*Pic 1: Using command prompt and running the ipconfig command.*

In the picture 1, my IPv4 address is: 192.168.1.109 and I have to convert it from decimal to binary.

* 192.168.1.109
* 11000000.10101000.00000001.01101101

There is total five classes of IPv4. Those are A, B, C, D.

In class A the public IP Range: 1.0.0.0 to 127.0.0.0

In class B, the public IP Range: 128.0.0.0 to 191.255.0.0

In class C, the public IP Range: 192.0.0.0 to 223.255.255.0

In class D, the public IP Range: 224.0.0.0 to 239.255.255.255

In class E, the public IP Range: 240.0.0.0 to 255.255.255.255

So, after all of that my IPv4 is matched with class C.

A private IP address is our network router assigns to our device. Private IP addresses allows devices connected to the same network which communicate with each other without connection to the whole internet. It’s makes it more difficult for the external host, user to establish the connection. Private IP always help bolster security within in a specific network, like our office and home.

In this class identified in 2.2, C addresses from 192.168.0 to 192.168.255 and the addresses in the following ranges can’t be routed across the internet because they are reserved as the private IP address.

Tracert is a network diagnostic tool which is used to track in real-time pathway which is taken by a packet on an IP network from source to destination.

Text

Description automatically generated

*Pic 2: Using tracert in Command Prompt for trace the path a website*

The server IP address is: 142.250.204.14

IP address of the gateway in my network: 192.168.1.1

ARCHER\_VR1600V

[192.168.1.1]

lo10.lns22.sydnmtc.nsw.vocus.network

[203.134.4.206]

ae2-111.per02.sydnmtc.nsw.vocus.network

[203.134.2.52]

26.72.core.vocus.network

[203.134.72.26]

as15169.cor01.sydnmtc.nsw.vocus.network [203.134.8.247]

108.170.247.33

142.251.64.177

syd09s25-in-f14.1e100.net

[142.250.204.14]

*Diagram 1: Showing the “google.com” trace path by diagram.*

Tracert trace the path and is reporting the IP addresses of all the routers it pinged in between. Tracert records the time taken for each hop the packet makes during its route the destination.

**Answer to the question no. 3:**

We’re using the ipconfig tool for find out the Subnet Mask (highlighted by sky blue). The Subnet Mask is: 255.255.255.0

A picture containing text

Description automatically generated

*Pic 3: using ipconfig in command prompt and then find out Subnet Mask.*

Then we can also see there is IPv4 address(which is highlighted by Green color). The IPv4 Address is: 192.168.1.109

Text

Description automatically generated with medium confidence

*Pic 4: using ipconfig in command prompt and then find out IPv4 Address.*

My IPv4 Address is: 192.168.1.109 and we can divided them into two parts. One part is network part and another part is host part. As the IPv4 address in class C so there’re different rules to findout the Netowork ID part and Host ID part.

Network ID part: 192.168.1.

Host ID part: 109

Host ID part

Network ID part

*Diagram 2: Diagram of Network ID part and Host ID part.*

Subnetting can divide a single large network in to the multiple small networks. The main reason of subnetting is keep the internet routing tables of a manageable size. There are also many advantage such as easy network management, avoid the IP Address wastage, increase the network security, avoid the network broadcast storm or network collision and to boost the network performance.

**Reflection:**

In the last week, I understood most of the week’s materials and the topics was network protocols, but I wants to go deeper down of IPv4 and IPv6. Is IPv6 better than the IPv4 ?

Autoconfiguration is a new feature in IPv6, which allows a device to generate an IPv6 address as soon as it lights up and connects to the network. The device looks for an IPv6 router first. If one is available, the device can create both a local and a globally routable address, providing connection to the internet. The procedure of adding devices to IPv4-based networks is frequently done manually.

IPv6 allows devices to connect to several networks at the same time. This is owing to the hardware's interoperability and configuration capabilities, which allow it to issue several IP addresses to the same device automatically.

A public signature key — one half of an asymmetric encryption system, the other being the private key — can be bound to an IPv6 address using IPv6. The user can utilise the Cryptographically Generated Address to show "proof of ownership" for a certain IPv6 address and authenticate their identity. With the existing 32-bit address space restriction, retrofitting this feature to IPv4 is unfeasible.

The new protocol also enables end-to-end communication at the IP layer by removing the need for Network Address Translation (NAT), which was previously used to save IPv4 addresses. This change allows for the introduction of new and valued services. Peer-to-peer networks are becoming easier to set up and manage, and services like VoIP and QoS are becoming more reliable.

Furthermore, IPv6 provides the opportunity to belong to numerous networks at the same time, each with its own unique address, as well as the possibility to integrate various enterprise networks without readdressing.

The Internet Protocol form 6 (IPv6) is further developed and has better highlights contrasted with IPv4. It has the ability to give an endless number of addresses. It is supplanting IPv4 to oblige the developing number of organizations worldwide and assist with taking care of the IP address depletion issue.

**Reference:**

<https://www.avast.com/c-ipv4-vs-ipv6-addresses#gref>

https://www.linksys.com/us/support-article?articleNum=139604