

COSC 4436: Computer Networks

Team #9

Performance Analysis of online
streaming

Navesh Kanna Koneswaran 199693480

Isara Senaratne 199663120

Aditi Malviya 189632440

Equal Contribution by everyone

Introduction

Streaming became very popular after the fame of YouTube in December 2005. After Saturday Night Live aired its first video short, it got viral and became a talk of town. The other platform Netflix had started producing binge worthy shows which were only available on NETFLIX. This resolved a lot of copyright issues and gave a raw platform for some of the best content.

Netflix had 2.2 million new paid subscribers between the time period of July and September of 2020. As well as there were several movies and tv series released in online streaming platforms during the pandemic. This resulted in Netflix and other streaming platforms becoming a mainstream entertainment during and after covid-19. This came to our attention to analyze the data packets that transfer over the network in WIFI and mobile data connection.

In this Performance Analysis of online streaming, we will be capturing the data packets of tcp using a network analysis tool known as Wireshark. Wireshark will show us enough details of the data packets to see the difference among the packets captured over wireless connections such as WIFI and mobile data. The reason to use wireless connection to analyze the performance is because that is the medium of the network that is being used by most of the users around the world and whereas streaming of a video can be done anywhere around the world where you have wireless connection (WIFI or mobile data).

The initial plan of this analysis is to use several different streaming platforms and compare the data. Due to insufficient information about routing protocols and architectures of other platforms, the analysis was done by using only Netflix video streams.

Netflix uses a simple routing protocol where the Netflix servers all around the world send the video packets to the client with the shortest and efficient path possible. They use such protocols in order to provide high quality video streaming. Netflix does use AWS to deploy thousands of servers and terabytes of storage within minutes

What is tcp?

TCP stands for Transmission Control Protocol. This basically is a standard or set of rules which defines how the network conversation will take place between applications. TCP works hand in hand with Internet Protocol (IP) which defines how computers send packets and receive data. The two of this form the rules which totally define the internet. The work of TCP is to take the data or messages from an application or a server and then divide them into small packages or packets in order to send them over the network by different devices like switches, routers and security gateways to the destination. The other task of the TCP is to number the packets before sending them over. It reassembles all the packets before sending them. As the TCP is connection-oriented it ensures that the connection is established between the

application/servers for sending and receiving the data and until its complete. The process of transmitting the data can be seen as: -

Step-1

1- Establishing a connection

When there is a need of sending the data over TCP the computers need to establish a connection using a three-way handshake.

The first computer sends a packet with SYN bit set to 1 (SYN = "Synchronize?"). The second computer sends back a packet with ACK or ACKnowledge bit set to 1 plus the SYN bit set to 1 as well.

Step-2

2- Send packets of data

When data is sent over TCP the recipient must acknowledge what they have received. When the first computer sends the data in packets with sequence numbers, the second computer acknowledges it and increases the Acknowledgement number by the length of the data received.

3- Close the Connection

Any of the two computers can close the connection if they no longer want to have the transfer.

The TCP also can detect lost packets using timeout. Handling of out of order packets is also looked after by TCP.

What is ipv6?

IPv6 is the latest and newest version of the Internet Protocol (IP). This version is designed to supply IP addresses and to control the additional security and to support the IoT and emerging areas like autonomous driving. IPv6 uses the hex digits where each digit represents 4 bits. IPv6 allows ISPs to accumulate all the customers' prefixes to a single prefix and present only that one prefix out to the IPv6. This reduces the routing table size. For now, many networks will implement IPv6 concurrently with IPv4 in a dual stack design. The fresh networks will be compatible with IPv6 and the IPv4 together. The current government mandates these new IP addresses.

What is IPv4?

This is the fourth version of the standard that routes Internet traffic and other packet-switched networks. An IPv4 address is a series of four eight-bit binary numbers separated by a decimal point. Most commonly you see IP addresses expressed in dot-decimal notation. Classless Inter-Domain (CIDR) gave greater flexibility for allocating blocks of addresses. To identify the leading bits, a suffix is added to the IP address. IPv4 is numbered between 0 and 32. It was last distributed in 2011.

Differences between ipv4 vs ipv6

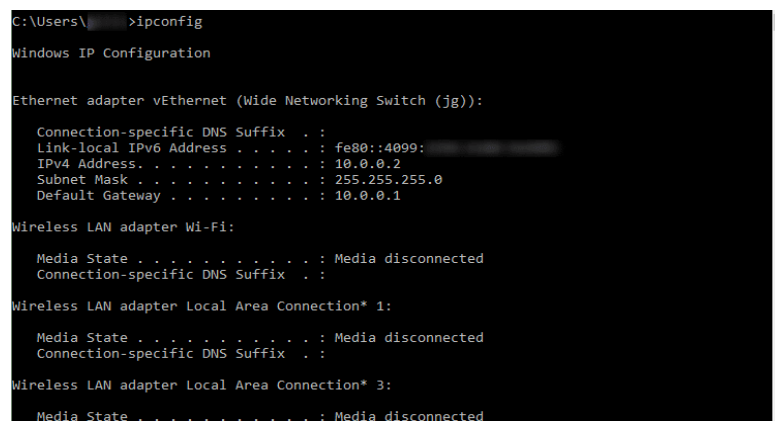
The most important difference between IPv4 and IPv6 is that IPv4 has only numeric addresses whereas in IPv6 there can be virtually limitless number of addresses. There are 5 classes in IPv4 that are from A to E whereas in IPv6 there are a limitless number of addresses. IPv4 has 3 types of addresses, Unicast, Multicast and broadcast. Whereas in the IPv6 there are unicast, multicast and anycast. IPv4 has 12 header fields whereas in IPv6 there are 8. The packet size for an IPv4 is 576 bytes whereas minimum packet size for an IPv6 is 1028 bytes. IPv4 uses the address resolution protocol (ARP) to map an IP address to the media access control (MAC) address. IPv6 uses the neighbor discovery protocol (NDP) to map the IP to MAC address. Security depends on the application in IPv4 whereas IPv6 has an internet protocol security (IPsec) built into the protocol to provide automatic security.

How were the packets captured?

We used command prompt in windows or terminal in MacOS to find the respective IP addresses of the local device and Netflix. The method of getting the IP addresses using command prompt or terminal is shown below.

Looking up IP versions (Windows)

1. Open Command Prompt.
2. Type ipconfig and enter.
3. The IP address of the local device will be shown in the name of Default gateway in IPV4, whereas IPV6 will be shown in the name of Link-Local IPV6 Address. The below screenshot shows the information.



```

C:\Users\>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Wide Networking Switch (jg)):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4099:
    IPv4 Address. . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

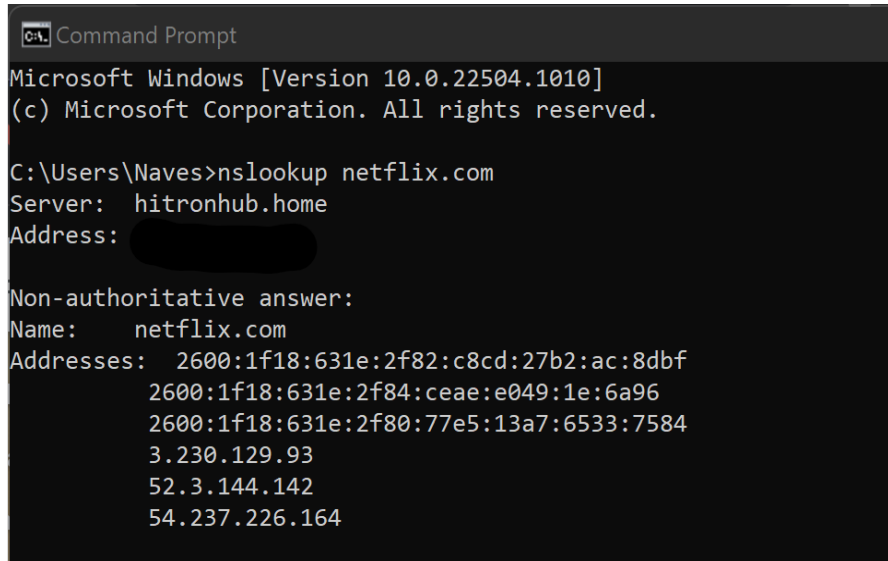
Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
  
```

4. Open command Prompt
5. Type `nslookup netflix.com`
6. The IP address of Netflix will be shown, there will be several IP addresses in both IPV4 IPV6 versions. The below screenshot shows the information.



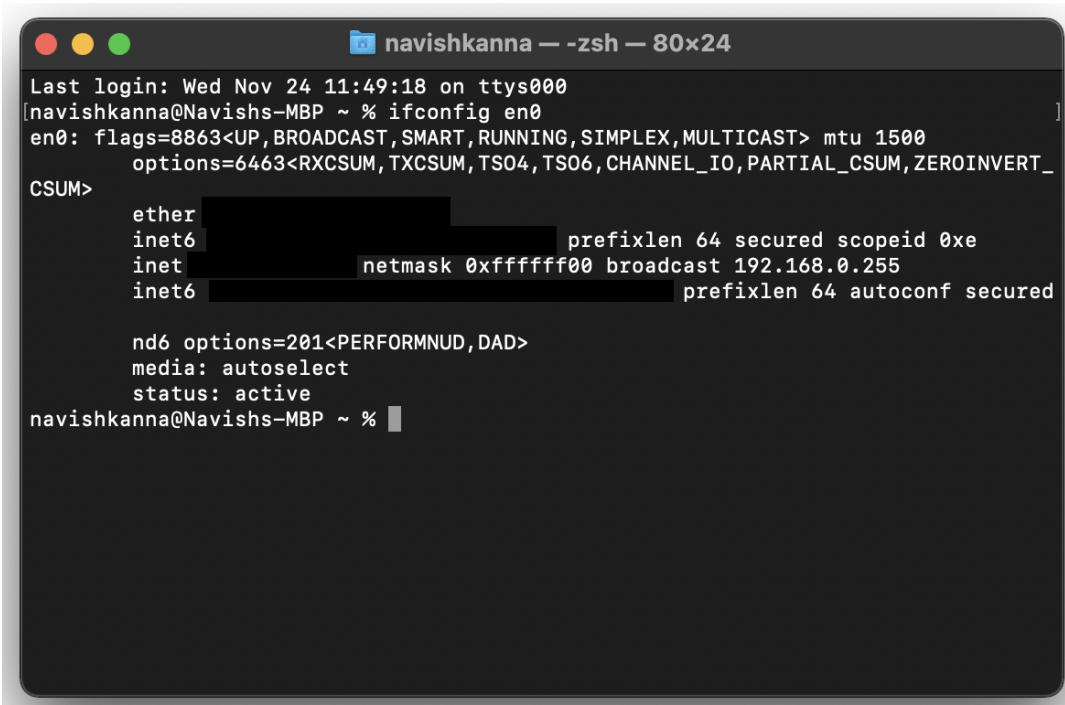
```

C:\Users\Naves>nslookup netflix.com
Server: hitronhub.home
Address: ██████████

Non-authoritative answer:
Name:    netflix.com
Addresses: 2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf
           2600:1f18:631e:2f84:ceae:e049:1e:6a96
           2600:1f18:631e:2f80:77e5:13a7:6533:7584
           3.230.129.93
           52.3.144.142
           54.237.226.164
  
```

Looking up IP versions (MacOS)

1. Open Terminal
2. Type `ifconfig en0` and enter.
3. The IP address of the local device will be shown in the name of inet in IPV4, whereas IPV6 will be shown in the name of inet6. The below screenshot shows the information.



```

navishkanna — -zsh — 80x24
Last login: Wed Nov 24 11:49:18 on ttys000
[navishkanna@Navishs-MBP ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=6463<RXCSUM, TXCSUM, TS04, TS06, CHANNEL_IO, PARTIAL_CSUM, ZEROINVERT_
CSUM>
    ether ██████████
    inet6 ██████████ prefixlen 64 secured scopeid 0xe
    inet ██████████ netmask 0xffffffff broadcast 192.168.0.255
    inet6 ██████████ prefixlen 64 autoconf secured

    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
navishkanna@Navishs-MBP ~ %
  
```

4. Open Terminal.

5. Type nslookup netflix.com
6. The IP address of Netflix will be shown.

```
navishkanna@MBP14inch2021 ~ % nslookup netflix.com
Server:
Address:

Non-authoritative answer:
Name:   netflix.com
Address: 3.211.157.115
Name:   netflix.com
Address: 54.160.93.182
Name:   netflix.com
Address: 3.225.92.8
```

IP address of Netflix(source) and IP address of local device(destination) were shown as follow:

Over WIFI

Source: 3.225.92.8

Destination: 10.8.70.204

Over Mobile Data

Source: 2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf

Destination: 2605:8d80:5c1:1cde:172:2f0:ccee:f492a

The data packets that were captured over WIFI showed the ip address of the destination and source in ipv4 whereas the data packets that were captured over mobile data showed the ip address of the destination and source in ipv6.

Using Wireshark, we captured the data packets while streaming a Netflix video on a local device (Apple MacBook). First, the data was captured using WIFI. We have used AlgomaU public WIFI for this, which has several devices connected and there is huge traffic. Next, the local device (Windows Laptop) was connected to a mobile hotspot, where a Netflix video was playing in the background.

The display filters in Wireshark are used to filter out the information out of the captured packets. First, the TCP packets that were captured in the Netflix IP address were filtered. An I/O graph was created using that filter to compare with the total number of TCP packets captured.

Later another I/O graph was created to check the TCP stream rate to compare the speed of the TCP packets transfer speed over WIFI and mobile Data.

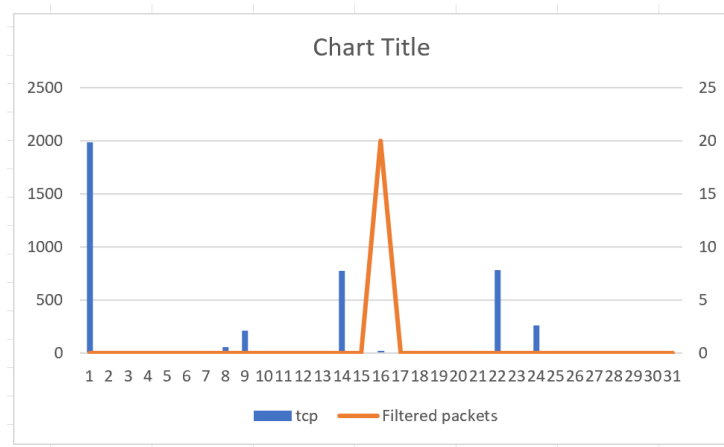
The filters that were used are mentioned below:

- Filtering the TCP packets of Netflix on WIFI: ip.addr == 3.225.92.8

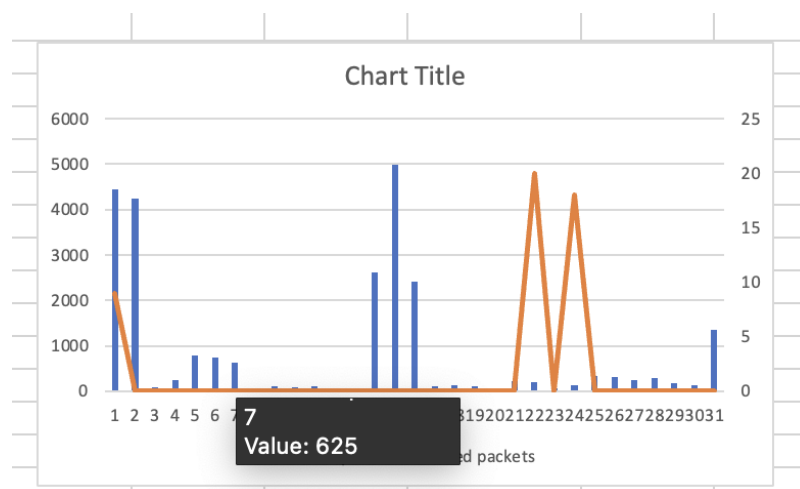
- Filtering the TCP packets of Netflix on Mobile data: `ipv6.addr == 2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf`
- To monitor TCP packets stream: `tcp.stream eq 0`

Differences compared.

When using mobile data, the ip address of Netflix was captured in ipv6 whereas the WIFI ip address of Netflix was in ipv4. This shows that mobile data uses a secure protocol to transfer data.

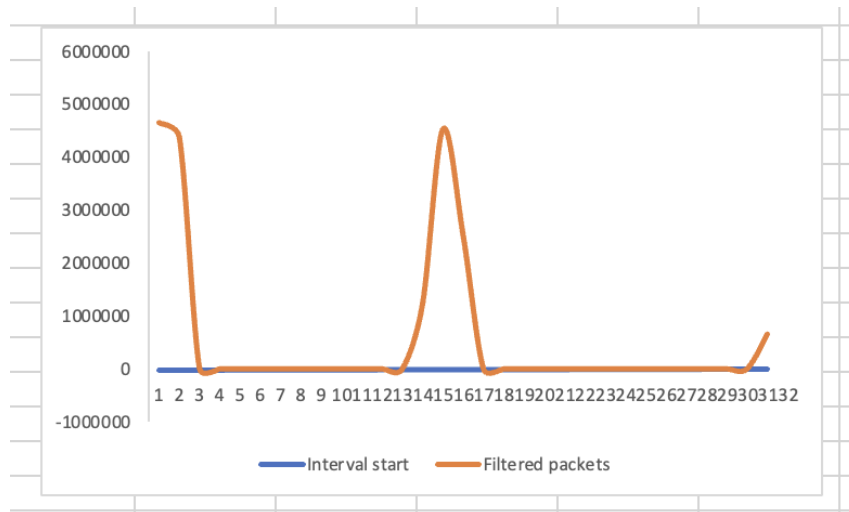


TCP vs Filtered Packets (`ipv6.addr == 2600:1f18:631e:2f82:c8cd:27b2:ac:8dbf`)

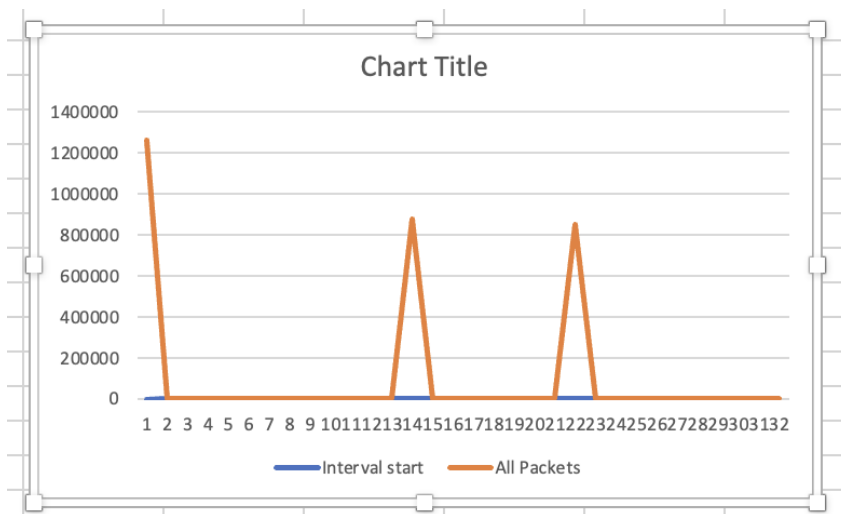


TCP vs Filtered Packets (`ip.addr == 3.225.92.8`)

Out of the tcp packets that were captured from using mobile data, all the packets were about Netflix streaming data, whereas in WIFI there were other data packets captured in tcp. This concludes that the mobile data only focused on Netflix data packets, while WIFI was sending data packets over tcp even when Netflix was working.



TCP Stream transfer Rate over Wi-Fi



TCP Stream transfer Rate over Mobile Data

By observing the above graphs, the transfer rate or the speed of the packet transfer can be analyzed. Even though the WIFI was a public network, and there was huge traffic the speed was fast, whereas the mobile data was a closed network and less traffic the speed was slow on the packet transfer.

The packets that are transferred in between can be analyzed by playing the videos in different video qualities (1080p, 720p etc..). Netflix is a smart service, which allows the video to low the quality during a less bandwidth and get back to normal quality during a proper bandwidth. Hence, it was hard to analyze such activity.

References

<https://www.techtarget.com/searchnetworking/definition/TCP>
<https://www.sdxcentral.com/resources/glossary/transmission-control-protocol-tcp/>
<https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp>
<https://www.cisco.com/c/en/us/solutions/ipv6/overview.html>
<https://www.uptrends.com/what-is/ipv4>
<https://help.netflix.com/en/node/85>
<https://aws.amazon.com/solutions/case-studies/netflix-case-study/#:~:text=AWS%20enables%20Netflix%20to%20quickly,mobile%20devices%20such%20as%20iPhones.>
<https://www.parallels.com/blogs/ras/difference-between-ipv4-and-ipv6/>