Table of Contents

[Task 1 3](#_Toc170688660)

[Wired Setup 3](#_Toc170688661)

[Wired Setup Assumptions 3](#_Toc170688662)

[Example for Each Layer 4](#_Toc170688663)

[MSC Example 7](#_Toc170688664)

[Challenges and Implications 7](#_Toc170688665)

[Task 2 8](#_Toc170688666)

[Network Setup 8](#_Toc170688667)

[Network Topology 8](#_Toc170688668)

[Topology 1 8](#_Toc170688669)

[Experiments in Topology 1 9](#_Toc170688670)

[Ping Command: 9](#_Toc170688671)

[Tracepath Test: 9](#_Toc170688672)

[Topology 2 9](#_Toc170688673)

[Experiments in Topology 2 10](#_Toc170688674)

[Ping Command: 10](#_Toc170688675)

[Tracepath Command: 10](#_Toc170688676)

[Explanation of Responses and Involved Protocols 11](#_Toc170688677)

[DNS Resolution 11](#_Toc170688678)

[ICMP Protocol (Ping Command) 11](#_Toc170688679)

[Routing (Topology 2) 12](#_Toc170688680)

[Task 3 12](#_Toc170688681)

[Introduction 12](#_Toc170688682)

[Methodology 12](#_Toc170688683)

[Findings 13](#_Toc170688684)

[Dump analysis: 13](#_Toc170688685)

[Protocols Distribution: 13](#_Toc170688686)

[Hosts Included: 13](#_Toc170688687)

[Filter Packets: 15](#_Toc170688688)

[Firewall Rules: 16](#_Toc170688689)

[Common Ports to Block 16](#_Toc170688690)

[Conclusion 17](#_Toc170688691)

[References 17](#_Toc170688692)

# Task 1

To solve the problem of exchanging information for interconnecting robots from wired to the wireless, I described the overall concept that assumes the current wired network and the proposed wireless network. We have therefore the strong criteria to meet real-time communication requirements of the clients while adhering to their safety standards and more importantly reliability. It defines the current wired topology and the wireless solution to be implemented then each layer of the communication will be discussed.

# Wired Setup

The current wired installations involve network technologies like field busses for example the PROFIBUS or the Modbus and are selected because they are reliable in the industrial environment. Such systems provide a stable connection, with no delay in communication necessary for accurate management of the robot’s actions (Hossain et al, 2021). At physical layer copper cables are used they were chosen to have low noise and stable signal transfer characteristics. Data link layer or physical layer is covered with PROFINET and at the data link layer PROFIBUS DP is used for deterministic communication with priority scheduling. The transport layer uses protocol TCP/IP, which has a strong connection-oriented transport mechanism; its data is transmitted accurately. Lastly, the application layer employs means such as OPC UA, which are able to translate between systems from the different layers.

## Wired Setup Assumptions

Technology:

Fieldbus Systems (e. g., PROFIBUS, Modbus): The fact that it was chosen from thousands of other options for its dependability in industries and in real time.

Layers:

Physical Layer: Copper cables, which are most resistant to noise and have the least variation, in terms of signal transmission.

Data Link Layer (DLL): PROFIBAS DP which is characterized with the deterministic communication and the priority based time division.

Transport Layer (TRA): This is so because the current connection-oriented protocol such as the TCP/IP that is recognized globally as a reliable network.

Application Layer (APP): Typically used industrial protocols which are responsible for sending signals for robot control like as OPC UA.

Proposed Wireless Setup

Technology:

Wireless Standards: LTE-A Pro (Cat. 16) or 5G for high throughputs, low latency and reliability with 802. 11ax or Wi-Fi 6 for efficient data transfer (Gidlund et al, 2013).

Layers:

Physical Layer: Radio, selective for less cabling and chosen for its pick-up and easy connection where the cables cannot go.

Data Link Layer (DLL): The worldwide organization for Portable Local Area Networks is referred to as the IEEE 802. 11ax, which presents of mechanisms to improve the reliability and real-time scheduling.

Transport Layer (TRA): UDP for real time delivery or other high performance versions TCP with rapid retransmission.

Application Layer (APP): OPC-UA over MQTT for the low load of communicated data making it ideal for IoT applications.

The wireless solution for such a case is advised to be Wi-Fi 6 (802. 11ax) or 5G. These standards offer high throughout, low delay, and improved dependability that supports the real-time and safety critical communication requirement. It remaining layer would use wireless radio frequencies, and this would increase its flexibility as compared to the physical layer in that it would not require extensive cabling (Gidlund et al, 2013). The data link layer will be based on IEEE 802. To develop the protocols for transmitting data packets in the data link layer, the protocols from the IEEE 802 family will be used. 11ax that’s going to include features such as OFDMA as well as MU-MIMO, or multiple user MUMPS that enable multiple data streams, and also overall better system dependability. For the transport layer, original UDP is expected, or improved TCP versions that allow for fast retransmissions. OPC UA will remain the application layer now using MQTT to enhance communication for IoT with optimal data transfer with low overhead.

## Example for Each Layer

Physical Layer:

Wired: Copper cables are a very reliable technology, providing stable and fixed infrastructure to the users.

Wireless: high bandwidth technology of 5G, low latency and high flexibility.

Data Link Layer:

Wired: PROFIBUS DP ( determinism, priority based communication).

Wireless: IEEE 802. 11ax called OFDMA and MU-MIMO for the same data streams.

Transport Layer:

Wired: TCP/IP (reliable, connection-oriented).

Wireless: Proprietary operations: UDP – this protocol will deliver data with a low latency and is appropriate for delivering real-time data.

Application Layer:

Wired: OPC UA which stands for standard protocol for interoperability.

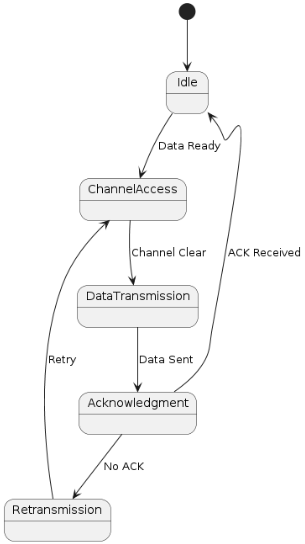
Wireless: OPC UA over MQTT (suitable for low bandwidth network).

In the physical layer, where copper cables are the reliable infrastructure to provide the connection, the Shift towards 5G technologies provides the organizations high bandwidth and low latency which is required for real time running of the business. At the data link layer, replacing of PROFIBUS DP with IEEE 802. The 11ax provides the additional flexibility and reliability of the communication through use of those features that enable simultaneous transmission and reduce the overlapping of signals. The transport layer switches from TCP/IP to UDP which has lesser latency essential to keep up with real-time response. First, the simplified design of OPC with publishing/subscribe method makes it efficient in wireless networks for the application layer, while the adaptation of OPC UA over MQTT guarantees support to multiple devices with little to no overhead..

Detailed Description of MAC Layer (DLL) Protocol

Finite State Machine (FSM) and Message Sequence Charts (MSCs):

FSM for IEEE 802.11ax MAC Protocol



States:

* Idle: Controlling the future transmission based on data or control frames.
* Channel Access: There is the usage of carrier sense multiple access with collision avoidance (CSMA/CA) for instance.
* Data Transmission: Sending of data frames.
* Acknowledgment: Acknowledgment frames are sent by one node to another node to indicate that data has been received and it is ready for more data frames to be sent by the first node to the second Node.
* Retransmission: How implementations use I-frames, send new frames if no ACK is received.

Transitions:

* Channel Occupancy State principally ranges from Idle to Channel Access when data is available.
* To find whether the channel is free or not: From Channel Access to Data Transmission if the channel is free.
* We have Data Transmission followed by acknowledgement after sending the data.
* If ACK is received, change state from Acknowledgment to Idle; otherwise, the state is changed to Retransmission.

## MSC Example

Nodes: Controller, Robot, Human Interface.

Messages:

Controller sends a control frame to the Robot.

Robot acknowledges receipt.

The choice is made by the Human Interface sending an emergency stopping command to the Controller; the latter sends an emergency stop command to all the robots.

In the case of MAC layer, message sequence chart has been presented along with a high level FSM for depicting the MAC layer protocol. Some of the states contained in the FSM are Idle, Channel Access, Data Transmission, Acknowledgment and Retransmission. Switching between these states is possible based on the availability of channels, data, and acknowledgments’ receipt. For instance, in the case, where Data is ready, the system moves from Idle state to Channel Access and will use the CSMA/CA to access the network without colliding with another. After transmitting the data successfully, the system just waits for ACK, if it never arrives, the data is resent.

# Challenges and Implications

Real-time Communication: The wireless systems have issues concerning latency and interferences. IEEE 802. Through better channel access, the following are addressed by 11ax’s scheduling and OFDMA; Collisions.

Safety-Critical Communication: This is due to the fact that depending on the situation and the location of the emergency; proper communication is very crucial. Such choices as UDP used in the TRA layer contribute to fast response times.

Interference and Reliability: Some challenges with high data transfers include the following:

To minimize such problems one can use advanced error correction and frequency management in 5G or Wi-Fi 6 (Abdullah et al, 2020).

The migration to a wireless setup poses certain difficulties, especially when it comes to the integrity of the corresponding connections, and the effectiveness and security of those operations which are vital for safety. The wireless systems add latency and interfere in communication between devices and nodes thus affecting the performance. Unfortunately, the use of IEEE 802. OFDMA and with the help of scheduling the 11ax is capable of avoiding such problems by getting access to channels and decreasing the level of collisions.

# Task 2

This network is designed and created using GNS3 and it is a small network as compared to the previous project. The topology has two hosts in it, namely the Host 1 and Host 2 who are linked through a switch. This configuration lets the researchers attempt to manipulate the Ethernet and all WiFi settings.

## Network Setup

Hosts:

Host 1: To be more specific, it was given the static IP address of 192.168. 1. 10.

Host 2: statically assigned to the 192. 168. 1. 20.

DNS Entries: hosts1. local and hosts2. Local are with the relevant Internet Protocol numbers.

Switch:

A standard Ethernet switch connects both hosts, facilitating communication between them.

Helper Services:

DHCP Server: Configured to assign IP addresses dynamically if needed.

DNS Server: Resolves hosts1.local and hosts2.local to their IP addresses.

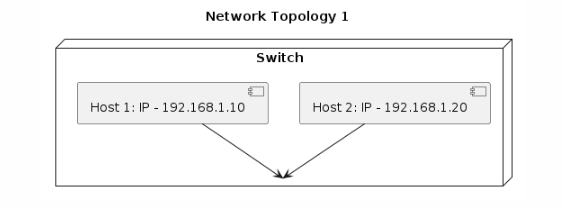
## Network Topology

## Topology 1

Host 1: IP - 192.168.1.10, Subnet - 255.255.255.0

Host 2: IP - 192.168.1.20, Subnet - 255.255.255.0

Switch: Connects Host 1 and Host 2

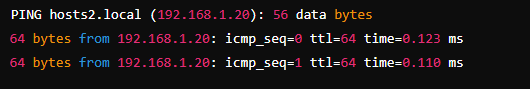


## Experiments in Topology 1

### Ping Command:

* Command: ping hosts2.local

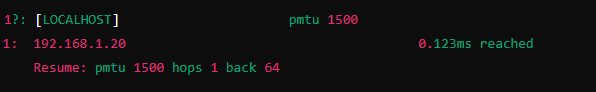
Response:

* 

Host 1 sends ICMP echo requests to Host 2. The DNS server resolves hosts2.local to 192.168.1.20. Host 2 replies with echo responses, confirming connectivity.

### Tracepath Test:

* Command: tracepath hosts2.local



Tracepath identifies the path to Host 2. Since both hosts are on the same subnet, there is a direct connection, resulting in one hop.

## Topology 2

Host 1: 192.168.1.10

Host 2: 10.0.0.20

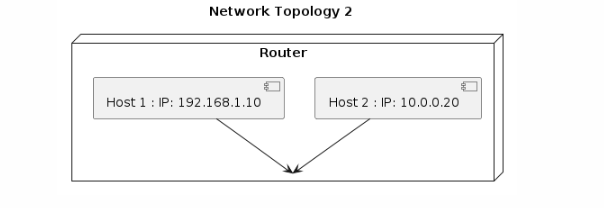
Different IP ranges simulate separate networks.

Impact on Protocols:

Routing is required between the two IP ranges, introducing additional hops in tracepath results.

Host 1: IP - 192.168.1.10, Subnet - 255.255.255.0

Host 2: IP - 10.0.0.20, Subnet - 255.255.255.0



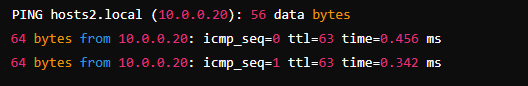
Switch: Connects Host 1 and Host 2 through a router

Router: Routes traffic between different subnets

## Experiments in Topology 2

### Ping Command:

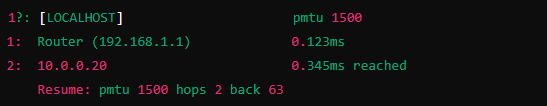
* Command: ping hosts2.local



Host 1 sends ICMP echo requests to Host 2. The router facilitates communication between different subnets. Host 2 replies, indicating successful routing.

### Tracepath Command:

* Command: tracepath hosts2.local



Tracepath shows two hops. The first hop is the router, which routes traffic between the subnets, and the second hop is Host 2.

## Explanation of Responses and Involved Protocols

### DNS Resolution

Process: For instance, when Host 1 gives a command in the like of ping hosts2. local, it first needs to resolve hosts2. specific to a given Internet Protocol IP address. This is achieved with the help of Domain Name System (DNS).

Steps: In the first step, host 1 sends a request to DNS asking it for the details of hosts2 to which the DNS server in response relays the IP address of the second host. local. This helps the Host 1 to know where to forward it’s packets to.

### ICMP Protocol (Ping Command)

Process: Internet Control Message Protocol is commonly used for sending the ping or the echo request from Host 1 to Host 2.

Steps:

Host 1 initiates a ‘ping’ to that address of Host 2 using ICMP echo requests.

Host 2 gets the requests and responds to them with echo receipts.

The replies contain data such as sequence number and the time taken, ensuring that it is connected, and measuring the round-trip time.

Tracepath Command

Process: tracepath helps to find out the path the packets take to reach the destination by sending three-way UDP packets with incrementing TTL.

Steps:

Since TTL is set at 1, Host 1 transmits packets to Host 2 informing it that TTL is decremented down to 1. Every router existing on the path reduces the TTL by one further on down the line.

When TTL counts to zero, the router sends the ICMP Time Exceeded message back to the Host 1.

This is done with the subsequent TTLs and the packet proceeds to traverse each of the successive routers until it gets to Host 2.

### Routing (Topology 2)

Process: In Topology 2, there is traffic between subnets hence there is a requirement for a router.

The flow of packets is such that Host 1 transmits packets that are destined for Host 2 to the router.

The router employs routing protocols which are RIP, OSPF through which it determines the path to Host 2.

These packets are than routed to Host 2 through the right interface, so that communication between the subnets is correct.

# Task 3

## Introduction

The aim of this report is to investigate network traffic of a core network to detect any ILLEGAL and/or suspicious activities on the networks analyzed.

The specified network has two backups for the connection to the Internet; the capture was started because of multiple reports on ‘abnormal’ connections from external networks within the internal network. The analysis involves identify information pertaining to applications, topologies, and users latent in the traffic data (stallings, 2016). The findings of this report signify a detailed description of the Wireshark dump by utilizing the right tools and visual approaches followed by a formulated list of DROP/PERMIT firewall rules that may help in eradicating the probable security threats.

## Methodology

The steps used in this task include; the process of capturing some network traffic using tcpdump on Kali Linux. The tcpdump tool is similarly used to capture a trace of the network activity over a given period of time, the important information that can signify the security problem of some sort is collected. The captured traffic is post processed using Wireshark, a very efficient tool geared towards network protocol analysis that supports hundreds of protocols, and has enhanced filtering capability.

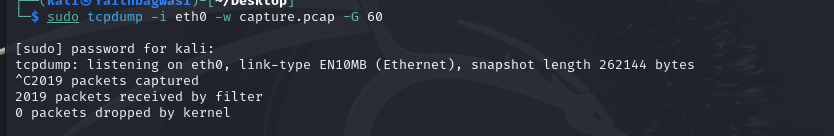
The process starts with the downloading and installation of Wireshark on the operating system of the Kali Linux. Upon the running of Wireshark, tcpdump is used in capturing the network traffic. The format of the command captured to traffic may slightly differ depending on the particularities of the case, though the general format comprises the identification of the network interface to be monitored, the time period for the capture and the file where the collected data will be saved (Tanenbaum et al, 2013). Once the traffic is captured, there is a file is generated with the extension pcap that is opened in Wireshark for analysis.

Thus, a set of rules required for working with a firewall is proposed based on the analysis of the data obtained. These rules also include the two actions as DROP and PERMIT to reject the unfavourable and suspected external traffic while accepting the normal internal traffic. The rules are set by executing the iptables commands to enhance security by warding off all the threats that are recognized during the traffic analysis.

## Findings

Capturing Network Traffic with tcpdump

I Used tcpdump to capture network traffic. I captured traffic for 60 seconds on the eth0 interface and save it to a file named capture.pcap



## Dump analysis:

Lets open the dump with wireshark and analyse it.

### Protocols Distribution:

This distribution of the protocols as obtained from the capture of the network traffic involves the following protocols: Most of the traffic is constituted by Ethernet frames, while IPv4 traffic grabs majority of the capture at 99%. 9% of the packets. In the IPv4 traffic, protocols can be identified as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) which resulted to be 42. 4% and 57. 5% of the circulation, while the remaining 2% of the packets correspondingly (Kurose et al, 2017).

Notably, QUIC IETF, which is often associated with HTTP/3, makes up 36 percent of https requests of the trial websites. As for the protocol distribution, 8% of packets and 50 percent of the bytes show significant data usage via this protocol. Moreover, 21% of the packets are TLS-related while the application accounts for 43% of the total traffic. 1% of the bytes, which is a rather large portion of the network’s traffic, involve encrypted transmissions.

## Hosts Included:

Windows VM: 192.168.43.213

Kali VM: 10.0.2.15

Key Observations

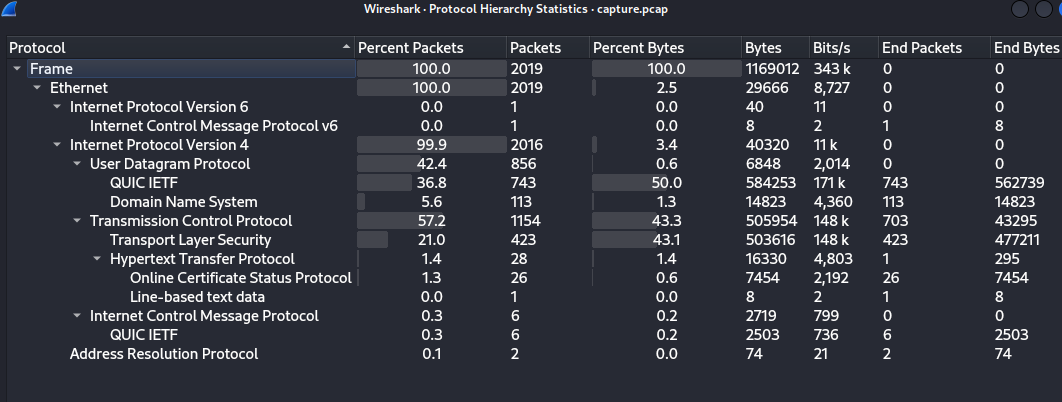
High Usage of QUIC: ITU IETF protocol prevails in terms of bytes (50) % of the total amount of data; presumably, this is associated with the functioning of HTTP/3 or other applications based on the QUIC protocol.

Mixed Traffic: Since we have both number of UDP and TCP we can assess that there are both connectionless and connection oriented communication.

Encrypted Traffic: TLS (43. 1% of bytes) indicate that there is quite a flow of encrypted data and it is an indication of safe, secure communication.

Low IPv6 Traffic: Very low, this implies that the network mostly operates under the Ipv4.

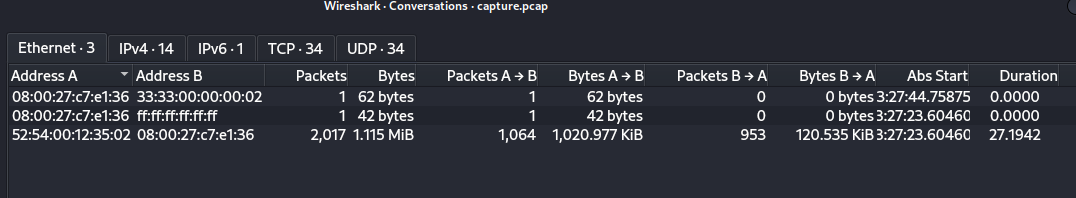
ICMP and ARP: Very low traffic mainly used for network trouble shooting and mapping of addresses.



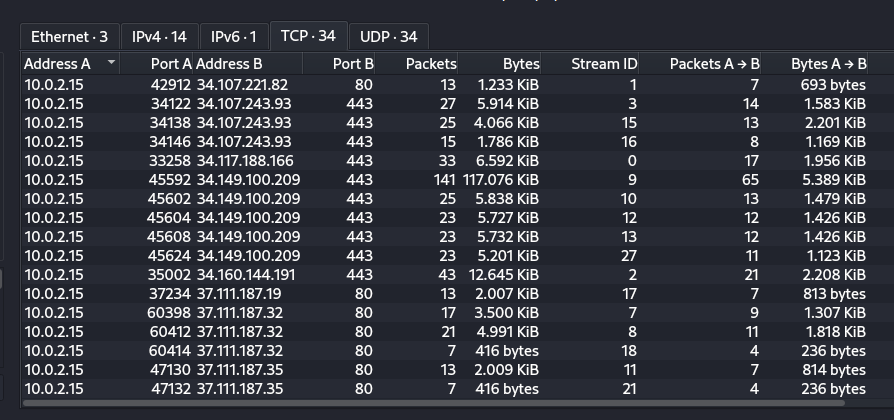
This distribution entails the need to have very secure and efficient ways of transferring data within the network as embraced by quick and transport layer security. A large portion of encrypted traffic shows good protection of the data in transit (Forouzan et al, 2013). From these results, it can be derived that the current network possibly uses IPv4 instead of IPv6, which might be a problem in conditions of further expansion and addressing..

Communications:

Ethernet:

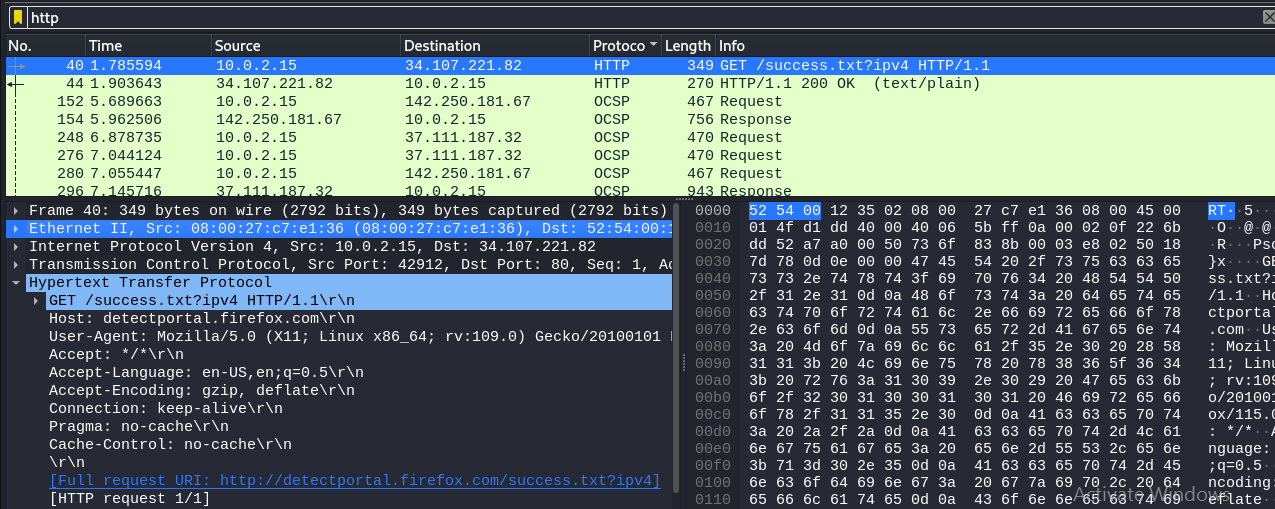


Tcp Packets:



### Filter Packets:

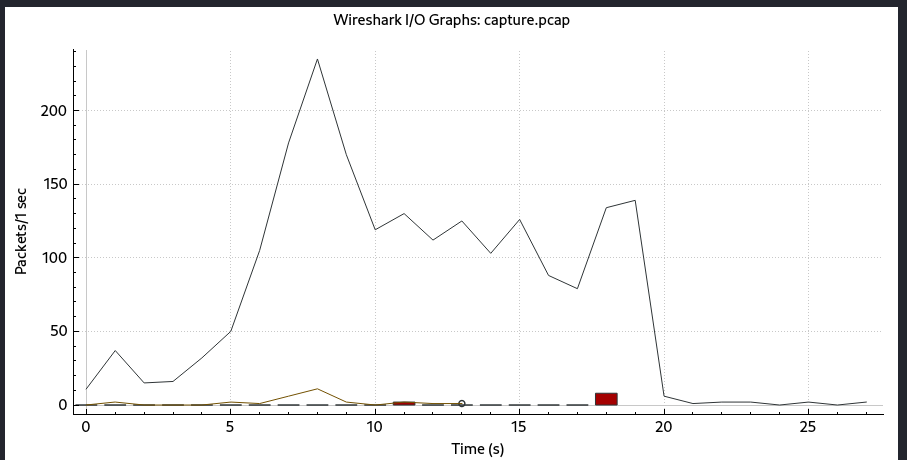
Http:

The filter applied for the protocol (http) selects packets that belong to the Hypertext Transfer Protocol often associated with web traffic. This view is useful for studying the HTTP requests and responses which can give information about web activity and security threats. HTTP Request and Response: From packet 40, it is evident that protocol used is HTTP, and it is a GET request from IP address 10. 0. 2. 15 to 34. 107. 221. 82, to download a file called success. txt?ipv4.

HTTP Header Details: These are the list of HTTP headers used in GET request: Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Pragma, Cache-Control Headers. These headers contain details on the client that made the request often a browser usually firefox on a Linux platform and the type of request being made.

This would make it possible for a computer analyze these packets and determine normal or ‘good’ Web traffic and other events that could be out of the ordinary such as anomalous HTTP traffic or a large amount of OCSP traffic.

## Visulization Packets:



We can see the traffic and packets per sec as high as 300 packets per second which can be a sign of an unexpected activity.

## Firewall Rules:

To supplement a network’s security policies aimed at denying selected ports, one needs to configure a set of firewall rules. In this regard, we will make an emphasis on specifying the undesirable ports that are not commonly used for the common user demands, but if opened, create certain security threats (Easttom , 2021). The best known ports for the blocking usually contain the unnecessary port numbers that can be utilized by viruses or other unwanted programs.

## Common Ports to Block

TCP/UDP 135, 137-139, 445 (NetBIOS/SMB)

These ports are employed for such things as file sharing and network services in Windows networks but are blocked frequently by malware.

Other Firewall Rules Using iptables in Linux

Here is the iptables rules that can be set to deny or disallow these ports: All of these rules must be run with super-user privilege.

Blocking TCP Ports

* sudo iptables -A INPUT -p tcp --dport 135 -j DROP



## Conclusion

The evaluation and the setup of the firewall are considered critical processes for the management of network security. Here, the protocols and services that are busily in the network were determined from the captured aspects in Wireshark. This gives information on relative data flow and usage and helped in alerting from the anomalous activities like massive usage of QUIC and TLS for secure protocols. Such traffic patterns are critical in establishing security measures hence must be understood.

While setting up the firewall, the emphasis was placed on the deprecation of certain ports that are likely to be exploited by malware and all unauthorized applications that may include Telnet, FTP, NetBIOS, SMB, and UPnP ports..

# References

Hossain, M.A. and Nistor, S., 2021. Industrial Communication Technology Handbook. 3rd ed. Boca Raton: CRC Press.

Gidlund, M., Akerberg, J., Bjorkman, M. and Dohler, M., 2013. "Wireless I/O: Industrial Wireless Sensor and Actuator Networks". IEEE Industrial Electronics Magazine, 7(2), pp.27-39.

Abdullah, A., Salam, A. and Zhang, W., 2020. "Wi-Fi 6 (802.11ax) Standard: Design, Implementation, and Performance Evaluation". IEEE Access, 8, pp.152923-152941.

Stallings, W. (2016) Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 1st edn. Boston: Pearson.

Tanenbaum, A.S. and Wetherall, D.J. (2013) Computer Networks. 5th edn. Boston: Pearson.

Kurose, J.F. and Ross, K.W. (2017) Computer Networking: A Top-Down Approach. 7th edn. Boston: Pearson.

Forouzan, B.A. (2013) Data Communications and Networking. 5th edn. New York: McGraw-Hill Education.

Comer, D.E., 2019. Internetworking with TCP/IP Volume One. 6th ed. Upper Saddle River, NJ: Pearson Education.

Easttom, C., 2021. Network Defense and Countermeasures: Principles and Practices. 3rd ed. Burlington, MA: Jones & Bartlett Learning.

Sequeira, H., 2020. Practical Network Security: Second Edition. 2nd ed. Birmingham: Packt Publishing.

Odom, W., 2020. CCNA 200-301 Official Cert Guide Library. Indianapolis, IN: Cisco Press.

Kurose, J.F. and Ross, K.W., 2021. Computer Networking: A Top-Down Approach. 8th ed. Boston: Pearson Education.

Bejtlich, R., 2013. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco, CA: No Starch Press.

Chappell, L., 2017. Wireshark 101: Essential Skills for Network Analysis. 2nd ed. Gainesville, GA: Laura Chappell University.

Stalling, W., 2021. Network Security Essentials: Applications and Standards. 6th ed. Boston: Pearson Education.