School

of

Electronics and Communication Engineering

Minor-2 Project Report

on

Prioritizing SHE Packets for Emergency Response

By:

1. **Aishwarya B Kalatippi** 01FE21BEI016
2. **Babusingh Rajput** 01FE21BEI018
3. **Rahul B Sajjan** 01FE21BEI024
4. **Vinayak Suresh Bhajantri** 01FE21BEI028

Semester: VI, 2023-2024

Under the Guidance of

Prof. Kiran M R

K.L.E SOCIETY'S
KLE Technological University,
HUBBALLI-580031
2023-2024

SCHOOL OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **"Prioritizing SHE Packets for Emergency Response"** is a bonafide work carried out by the student team of **"Aishwarya B Kalatippi (01FE21BEI016), Babusingh Rajput (01FE21BEI018), Rahul B Sajjan (01FE21BEI024), Vinayak Suresh Bhajantri (01FE21BEI028)"**. The project report has been approved as it satisfies the requirements with respect to the minor project work prescribed by the university curriculum for BE (VI Semester) in School of Electronics and Communication Engineering of KLE Technological University for the academic year 2023-2024

Prof.Kiran M R	**Dr. Suneeta V Budihal**	**Dr. B.S. Anami**
Guide	**Head of School**	**Registrar**

External Viva:

Name of Examiners **Signature with date**

1.

2.

ACKNOWLEDGEMENT

The project Prioritizing SHE packets for emergency response becomes successful with many individuals' kind support and constant help. We the team under Computer-Networking extends our sincere thanks to each one respectfully. The team expresses sincere appreciation to all the people who have assisted us in completing this project. All their contributions are deeply appreciated and acknowledged. The team would like to thank Dr. Suneeta Budihal, Head, School of Electronics and Communication Engineering for allowing extending our skills in the direction of this project. The team expresses heartfelt gratitude to our guide Prof. Kiran M R, whose valuable insights proved to be vital in contributing to the success of this project

-Project Team

ABSTRACT

In recent years, natural disasters like earthquakes, tsunamis, floods, and storms have happened frequently, causing severe damage. These disasters have shown how crucial it is to have reliable communication for rescue operations. Often, disasters damage communication network. The heavy demand for data transfer on the Internet is pushing its infrastructure to the limit, making it difficult to respond quickly to emergencies and disasters. To solve this problem, Internet networks need to prioritize certain types of data traffic: Security, Health, and Emergency (SHE) data traffic. These specialized networks work in private domains to support specific tasks for particular groups of users. We proposed network flow priority management system based on Software-Defined Networking (SDN) to give SHE data traffic the highest priority. Using the Mininet simulator, we tested our system extensively. The results show significant improvements in handling SHE data traffic, ensuring that during network congestion, SHE data is transmitted quickly, improving the effectiveness of emergency response efforts.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Disasters like earthquakes, floods, heavy rains, and accidents often mess up communication systems, which are super important during emergencies. We really need systems that help people like first responders, firefighters, and medical teams talk quickly and effectively to help those in trouble. Sometimes, people caught up in disasters can't reach their families or call for help, so we need communication systems that can keep working no matter what happens. Making these systems better at staying up and working well is crucial for helping out during emergencies.

Nowadays, alongside the threat of terrorism, natural disasters are causing big problems. To make things better, countries need good communication networks they can rely on. These networks give top priority to important packets like security, health, and emergency messages, which helps save lives and keep the country safe. To send these urgent messages over the internet, they have to go through phone networks, and that means using lots of different up-to-date technologies.

SHE networks can exist in two types: stationary infrastructure networks and non-stationary infrastructure networks. Stationary infrastructure networks rely on a fixed setup where data traffic is routed to a base station along predefined paths. These networks are relatively expensive and unsuitable for hostile conditions such as disaster response applications (e.g., extreme weather forecasting, earthquakes, volcanoes). In contrast, non-stationary networks do not rely on fixed network devices and include wireless networks like Ad-hoc, security, and health networks. These networks operate within a closed domain, allowing users to communicate efficiently only within this domain. If non-stationary networks fail, they can use Internet links to send information, but their data traffic does not get high priority. To address this issue, emergency data should be given the highest priority by network devices for routing during emergencies.

To get the best performance possible, this procedure needs the use of different and cutting-edge technologies in communication networks, such as Software-Defined Networking (SDN). In the event of a communication interruption, the first priority must be given to ensuring the effective data transfer of SHE networks over public Internet links.

Our contribution aims to improve packet traffic forwarding during SHE network failures using the Internet. We propose a new method for managing traffic priority by selecting specific header bits from the traffic class field instead of checking the entire header (320 bits). This method ensures that the most important SHE traffic gets the highest priority. By controlling the differentiated service and assured forwarding bits in a packet header, we can set the desired priority for specific traffic. This approach, based on selected header bits, helps prioritize traffic flows according to the levels set by the Differentiated Services Code Point (DSCP) and network administrator policies. Our traffic management method shows improvements in processing time,

power consumption, and server load.

As technology gets better and faster, we need to come up with quick solutions for handling emergencies. Old ways of doing things are often too slow, unreliable, and expensive. That's why this report suggests using something called Software-Defined Networking (SDN) as a solution. This could really help out developing countries, which often suffer the most during disasters, by making their emergency response much better.

1.1 Motivation

The motivation behind undertaking the project As we noticed how disasters like earthquakes and floods often leave people without any way to communicate, making it hard for help to reach them quickly. We want to find a way to make communication better during these tough times, so we can save more lives and keep people safer. We saw that current communication systems sometimes fail during emergencies, leaving people stranded and unable to get help. This motivated us to come up with a solution that can keep working even when things get really bad. We believe that everyone deserves to have access to reliable communication, especially during emergencies when it's needed the most. By improving communication during disasters, we can make sure that help gets to people faster, reducing the impact of these disasters. Our goal is to create a system that is easy to use and can be quickly deployed in any emergency situation. We want to give people peace of mind knowing that they can reach out for help when they need it most. This project is driven by a desire to make a positive impact on the world by helping communities stay connected and safe during times of crisis. We hope that our efforts will contribute to saving lives and minimizing the damage caused by natural disasters and other emergencies.

1.2 Objectives

- Ensure the prioritized transfer of Security, Health, and Emergency (SHE) packets over the communication network.
- To provide uninterrupted communication and data exchange for effective emergency response.
- To develop an easy-to-use communication network that works even when things are really tough.

1.3 Literature survey

The paper proposed by Fouad A.Yaseen and team suggests a unique method for SDN-based ML traffic prioritisation for SHE data that makes use of machine learning and software-defined networking. Compared to older approaches, SDN provides more control and flexibility; yet, current systems may not have optimal traffic scheduling, particularly in emergency situations. The suggested system combines SDN and ML to close this gap. SDN establishes priority for SHE data packets in accordance with network administrator requirements, while ML classifies SHE data packets by analysing traffic header bits. This strategy should greatly improve emergency response efficiency by lowering packet loss and queue time for SHE data transmission. [1].

The reliable network architecture presented in this study combines cloud computing and layered reinforcements with already-existing infrastructure. This method offers quick ICT service deployment while minimising logical and physical redundancy. The parallel, reinforced

infrastructure that cloud processing offers makes this approach especially appealing to underdeveloped nations looking for reliable, affordable communication during emergencies. Current literature investigates a range of approaches for communication networks that are resilient to disasters, such as utilising cloud technology and taking network design into account. By putting forth a tiered architecture designed especially for quick deployment and effective resource use in underdeveloped nations, our work expands on that foundation. [2].

The development of smart sensor technology and microelectromechanical systems has made wireless sensor communication a hot topic for research. Despite its enormous promise for a wide range of applications, a number of obstacles prevent it from developing further. Increasing network lifetime, controlling energy use, and guaranteeing affordable hardware and software are important concerns. Consideration must also be given to network coverage, security risks, dependability, and bandwidth constraints. In order to solve these issues, this article offers detailed recommendations along with a comparison of current approaches. This research intends to pave the road for further breakthroughs in wireless sensor communication by emphasising common problems, suggesting solutions through analysis, and maybe suggesting particular techniques[3].

The paper "QoS-aware Traffic Classification Architecture Using Machine Learning and Deep Packet Inspection in SDNs" by Changhe Yu et al. presents a novel approach that integrates Deep Packet Inspection (DPI) and semi-supervised machine learning to classify network flows into different Quality of Service (QoS) categories, enabling fine-grained adaptive QoS traffic engineering in Software-Defined Networks (SDNs). By maintaining a dynamic flow database and periodically re-training the classifiers, the system can effectively adapt to evolving network applications and traffic patterns, ensuring high classification accuracy. Experimental validation confirms the architecture's efficiency in achieving accurate traffic classification, with the heteroid tri-training mechanism outperforming traditional techniques in precision, F1 score, and Area Under the Curve (AUC) metrics. The study underscores the importance of combining DPI and machine learning in SDNs for QoS-aware traffic engineering, suggesting future research directions to enhance scalability and real-time performance for more precise network management systems.[4].

The paper "A Survey of Traffic Classification in Software Defined Networks" by Jinghua Yan and Jing Yuan delves into the realm of traffic classification within Software Defined Networks (SDN), highlighting its importance in network management, service measurements, design, security monitoring, and advertising. The document reviews traditional techniques like port-based and payload-based classification, noting their limitations and the shift towards more sophisticated methods like Deep Packet Inspection (DPI). It also explores recent advancements in SDN traffic classification, discussing frameworks, feature extraction, and classification algorithms proposed by researchers like Anderson Santos da Silva et al. The paper concludes by addressing future directions for SDN traffic classification, emphasizing the need for improved classification strategies, handling encrypted traffic, and enhancing real-time classification capabilities to meet the evolving demands of network traffic analysis.[5].

1.4 Problem statement

Addressing the challenge of maintaining resilient networking infrastructure during disasters to ensure uninterrupted communication and data exchange for effective emergency response.

1.5 Application in Societal Context

Prioritizing Security, Health, and Emergency (SHE) packets in our communication systems can really help out in emergencies. It means making sure that important messages, like those from hospitals or emergency services, get through first. This can make a big difference in keeping people safe and informed during tough times like floods or accidents. By sending these messages quickly, we can help emergency services respond faster and help those who need it most. It's like giving a special lane on the road to ambulances so they can get to the hospital faster. This way, everyone can stay safer and get the help they need when they need it most.

1.6 Organization of the report

In Chapter 1, discusses about the motivation of the project carried on with Objectives and Literature Survey. The Problem statement is described, followed by the applications in societal context, project planning .

In Chapter 2, describes about Functional block diagram , followed by algorithm and flowchart.
In Chapter 3, focuses about the results.

In Chapter 4, presents about the conclusion and future scope of the project.

Chapter 2

System design

In this chapter, we will be looking towards the final system architecture which is being implemented and is described by the algorithm and flowchart.

2.1 Block diagram

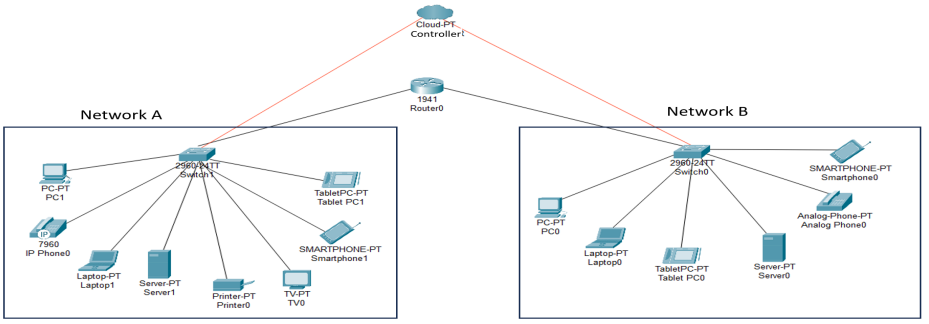

Figure 2.1: Block diagram

Fig 2.1 shows block diagram of our project work. It consist of Network A and B with switches, PCs, Laptops, Servers, Tablets, Smart phones etc connected to Router and SDN controller.

Figure 2.2: Block diagram

Currently, Internet traffic is heavily burdened by demanding applications like multimedia streaming, network storage, and real-time video games, pushing network resources to their limits. During emergencies, it is crucial to prioritize network traffic to and from SHE (Smart Home Environment) networks to manage large civilian gatherings, disasters, and pandemics effectively. The COVID-19 pandemic highlighted this need as it led to unprecedented data traffic, causing significant congestion. Thus, there is a pressing need for a system that ensures priority for emergency data traffic. Our solution aims to address this by prioritizing SHE network traffic, ensuring high priority and quality of service (QoS) across various Internet infrastructures. While SDN (Software-Defined Networking) technology is prevalent among service providers, not all Internet infrastructures use it. Hence, our proposal focuses on administrative domains that have implemented SDN technology.

Create Two Networks Named A and B with SDN Controller
First, we set up two separate networks named A and B, both managed by a Software-Defined Networking (SDN) controller. This involves defining the structure of each network, which includes switches, routers, and devices like computers, servers, mobiles, telephones etc. All devices are configured to communicate with this central controller, allowing for easier and more flexible management of network traffic.

Destroy Any End Device's Connection with Switch (Disaster Has Occurred)
Next, we simulate a disaster by disconnecting one of the end devices from its switch. This could represent a real-life issue like a hardware failure or a network outage. To do this, we select an end device and either physically or programatically disconnect it from the switch. The SDN controller, which monitors the network in real time, detects this disconnection. This simulation helps us test how well the network can handle unexpected disruptions.

Immediate Response is Required. Packets Are Routed Based on Priority Assigned by DSCP Bits
When the SDN controller detects the disconnection, it needs to respond immediately to ensure important services continue to work. It does this by prioritizing network traffic using Differentiated Services Code Point (DSCP) bits. These DSCP bits assign different priority levels to packets. High-priority traffic, like voice calls or critical data, is given higher DSCP values. The SDN controller uses these values to reroute traffic, making sure that high-priority packets are delivered first, even during a disruption.

If No Link is Destroyed, Packets Move As Usual
If no disruptions occur, the network operates normally. The SDN controller monitors the network continuously but does not change the flow of traffic. Standard routing methods, such as shortest path routing, are used to direct packets. This ensures efficient and reliable network performance under normal conditions, allowing all traffic to move smoothly without the need for special handling.

Finally, after the disruption is handled, we check all network connections and device statuses to ensure everything is back to normal. We generate reports on what happened, how it was handled, and how the network recovered. This process helps us evaluate the effectiveness of our response and make any necessary improvements to our disaster recovery plan, enhancing the network's ability to deal with future issues.

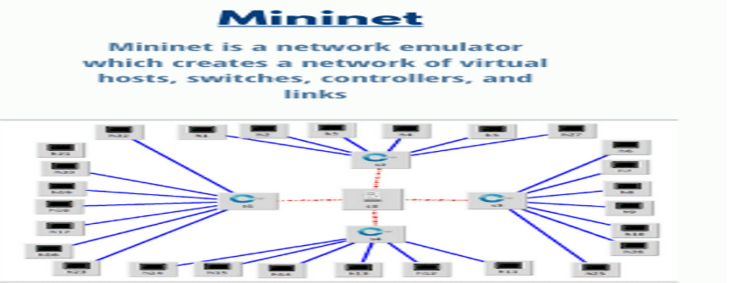

Figure 2.3: Software mininet

2.2 Implementation details

Figure 2.2 shows mininet software. Mininet is a network emulator that creates virtual networks on a single computer. It allows users to simulate different network setups and test new protocols and applications. With Mininet, you can run real code, making the simulations very realistic. It is scalable, supporting both small and large networks, and works with OpenFlow. Mininet is easy to use, with simple commands and Python scripts for quick setup and testing. It is commonly used for teaching, network design, and testing, making it a valuable tool for developers, researchers, and educators in networking.

2.3 Flowchart

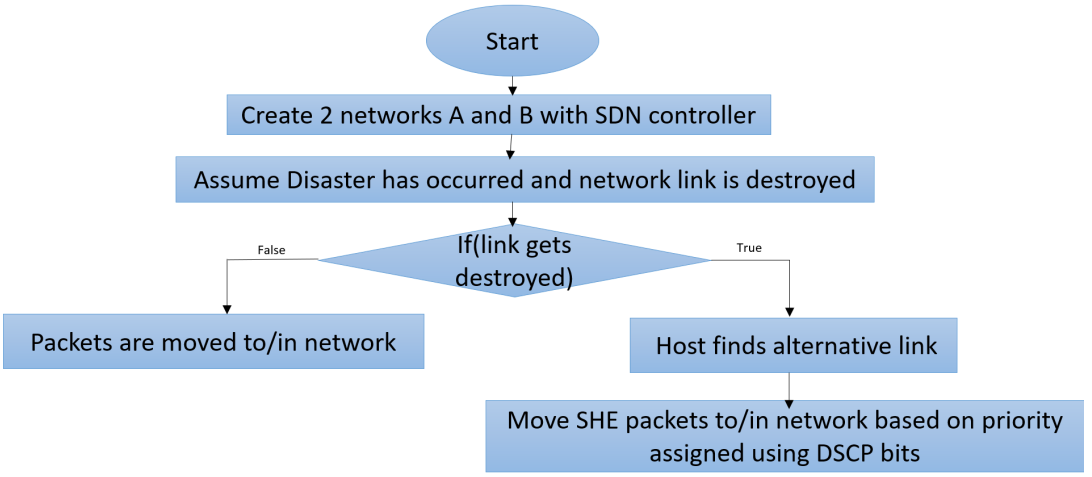

Figure 2.4: Flowchart

Fig 2.3 shows flowchart of our project. Create 2 networks named A and B which includes end devices like TVs, PCs, Mobiles etc connected to switch and SDN controller. To show disaster has occurred we are manually diconnecting any of the end device with switch, so immediate response is needed in such case. Forward SHE packets to area based on priority assigned using DSCP bits.

2.4 Algorithm

- Start
- Create two networks named A and B with SDN controller.
- Destroy any end device's connection with switch.(Disaster has occured).
- Immediate response is required. Packets are to network based on priority assigned by DSCP bits.
- If no link is destroyed. Packets move as usual.
- End

Chapter 3

Results and discussions

3.1 Simulation Results

```
vinayak@vinayak-VirtualBox:~/code$ sudo python3 dscp_link.py
mininet> links
h1-eth0<->s1-eth1 (OK OK)
h2-eth0<->s1-eth2 (OK OK)
h3-eth0<->s2-eth1 (OK OK)
h4-eth0<->s2-eth2 (OK OK)
s1-eth3<->s2-eth3 (OK OK)
s3-eth1<->s4-eth1 (OK OK)
s2-eth4<->s3-eth2 (OK OK)
s2-eth5<->s4-eth2 (OK OK)
h2-eth1<->s2-eth6 (OK OK)
h1-eth1<->s4-eth3 (OK OK)
```

Figure 3.1: Creating network

Fig 3.1 shows how network has created. There are 4 switches and 4 hosts connected through ethernet. Host1 is connected to switch1. Host2 is connected to switch2. Host3 connected to switch3. Host4 connected to switch4. All switches and hosts are internally connected.

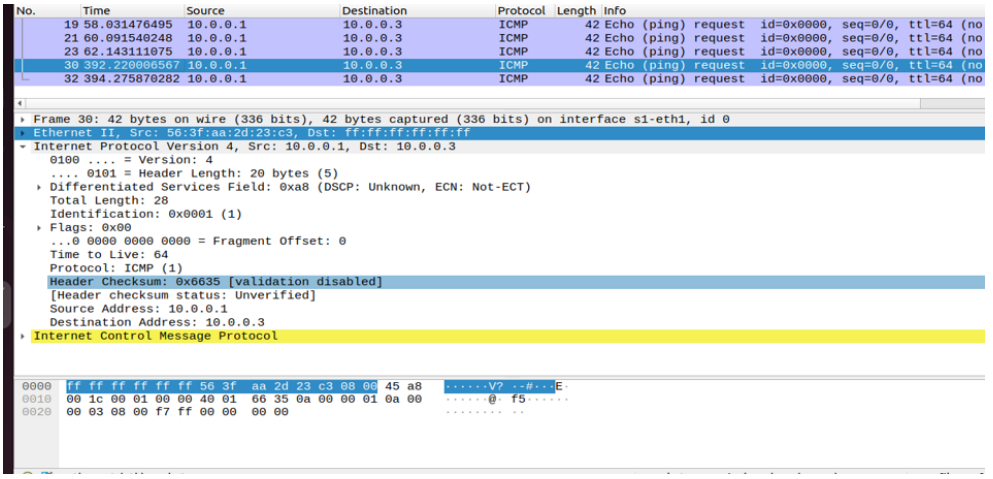

Figure 3.2: No priority set

Fig 3.2 shows the the movement of packets. Here the priority is yet not set as disaster has not occured. So packets will move asusual. As it can be seen the packet is set to "DSCP:Unknown".

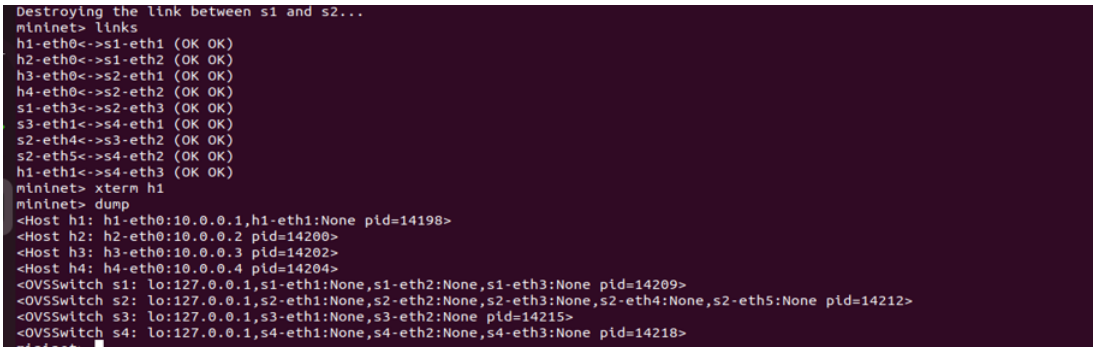

Figure 3.3: Destroying link

Fig3.3, The link is destroyed to show disaster has occured and further action will be taken. Here link between switch1 and switch2 is lost. It finds alternative path to transfer SHE packets further.

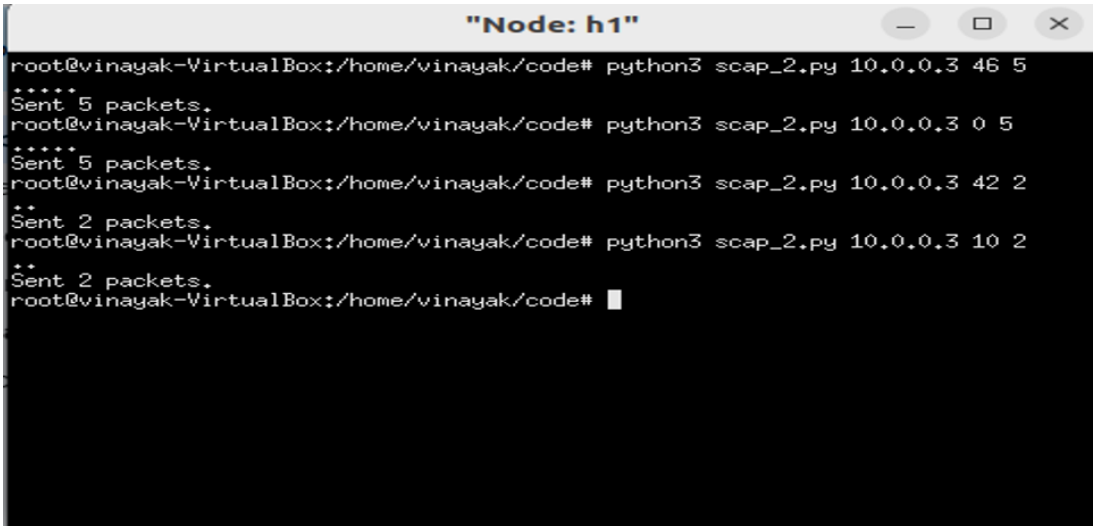

Figure 3.4: DSCP bits set

Fig3.4 shows the result of DSCP bits being set. 46, 0, 42, 10 are set. When disaster occurs these bits are set and packets move accordingly. Even number of packets can be mentioned.

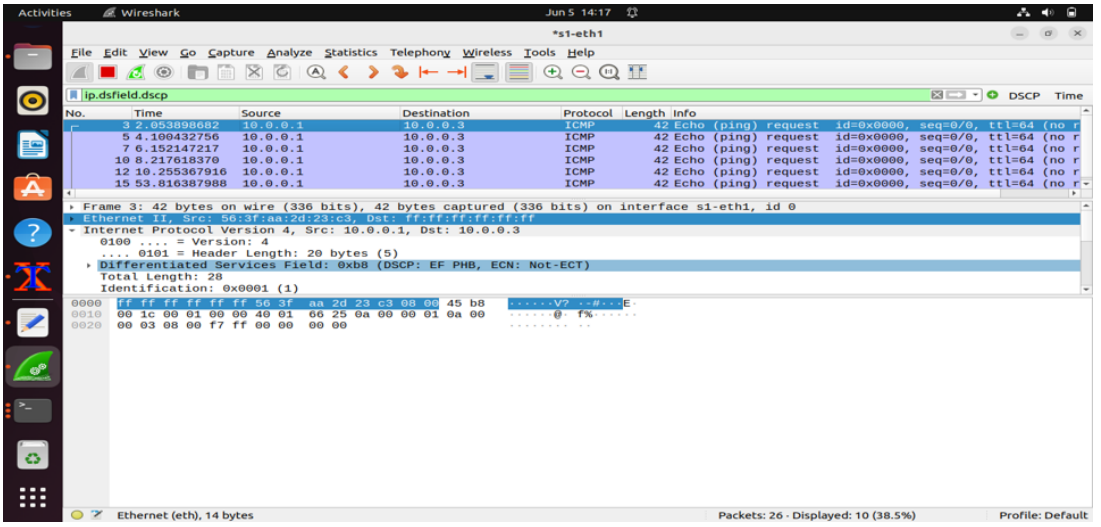

Figure 3.5: DSCP bit 46(EF) set

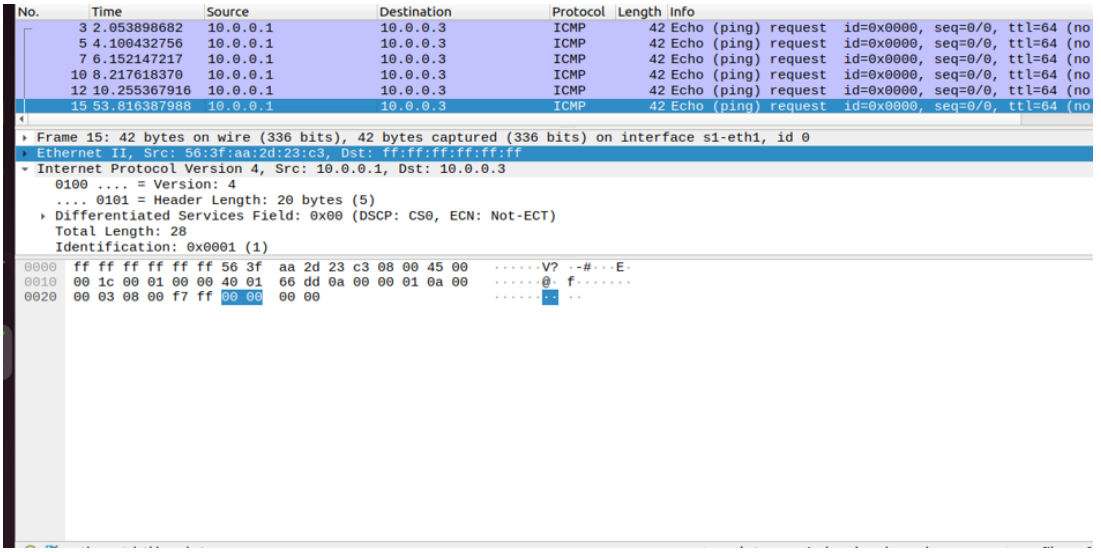

Figure 3.6: DSCP bit 00(CS0) set

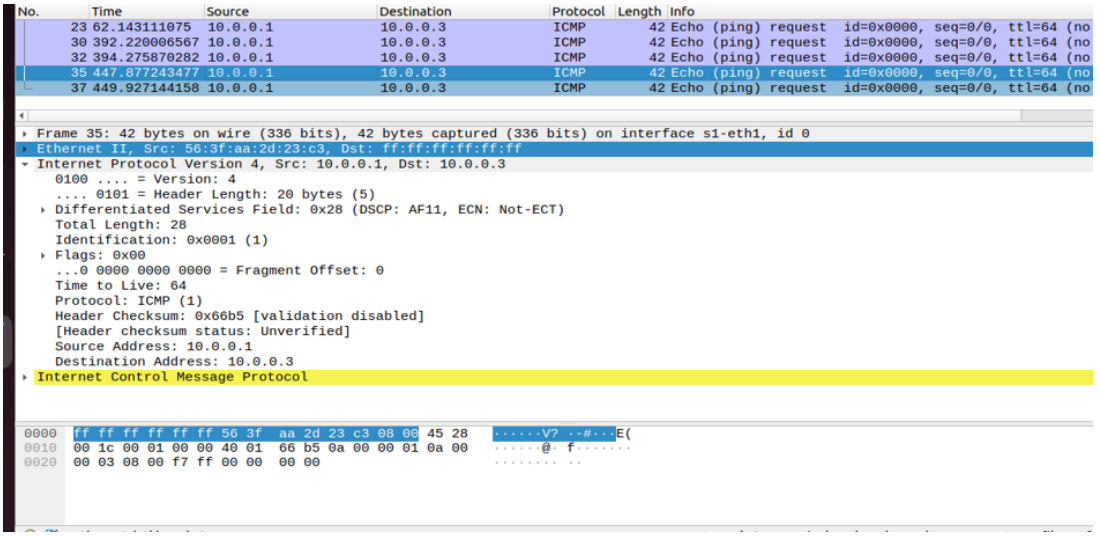

Figure 3.7: DSCP bit 10(AF11) set

Fig3.5, Fig3.6 and Fig3.7 shows results how DSCP bits are sent with precedence, the highest priority is set for 46 which is SHE packet i.e, 2. And for rest of the packets the priority is 1 by default. In a network utilizing DSCP (Differentiated Services Code Point) for traffic prioritization, packets are marked with specific DSCP values to determine their handling priority. The highest priority is assigned to packets with a DSCP value of 46, which corresponds to the Expedited Forwarding (EF) class. This ensures that critical packets, such as those requiring Special Handling (SHE), receive top priority (priority 2) and are forwarded with minimal delay. All other packets are marked with a default DSCP value, typically 0, and are assigned a lower priority (priority 1). This scheme allows network devices to differentiate and appropriately manage traffic, ensuring that high-priority packets are expedited through the network while standard packets receive regular best-effort service.

Chapter 4

Conclusion and future scope

4.1 Conclusion

In conclusion, giving priority to Security, Health, and Emergency (SHE) packets in our communication networks is very important for keeping people safe and managing disasters better. By using Software-Defined Networking (SDN), we can make sure that important messages from emergency services get through quickly, improving response times during crises like natural disasters and accidents. This means help can reach people faster, saving lives and reducing harm. It also helps communities become stronger and ensures that those most in need get timely assistance. Overall, prioritizing SHE packets with the help of SDN is a key step in making our emergency response systems more effective and protecting everyone in our communities. The output is simulated in Mininet software.

4.2 Future scope

The future of prioritizing Security, Health, and Emergency (SHE) packets using Software-Defined Networking (SDN) looks very promising. This method can be used worldwide and integrated into national emergency response systems. Better algorithms and AI can make traffic management and response times even faster. Connecting SDN with Internet of Things (IoT) devices will give real-time data and improve awareness during disasters. Ensuring the security of these networks will protect against cyber threats and help different emergency teams work together smoothly. Making this technology affordable will make it available to developing countries and smaller communities. Continuous research will keep improving the technology, making emergency communication systems stronger and more efficient, which will ultimately save more lives.s

Bibliography

4.3 Reference

[1] Yaseen, F.A., Alkhalidi, N.A. and Al-Raweshidy, H.S., 2022. She networks: Security, health, and emergency networks traffic priority management based on ml and sdn. IEEE Access, 10, pp.92249-92258.

[2] Ali, K., Nguyen, H.X., Vien, Q.T. and Shah, P., 2015, March. Disaster management communication networks: Challenges and architecture design. In 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops) (pp. 537-542). IEEE.

[3] Paul, S.P. and Vetrithangam, D., 2022, November. A Comprehensive Analysis on Issues and Challenges of Wireless Sensor Network Communication in Commercial Applications. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 377-382). IEEE.

[4] Yu, C., Lan, J., Xie, J. and Hu, Y., 2018. QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs. Procedia computer science, 131, pp.1209-1216.

[5] Faezi, S. and Shirmarz, A., 2023. A comprehensive survey on machine learning using in software defined networks (SDN). Human-Centric Intelligent Systems, 3(3), pp.312-343