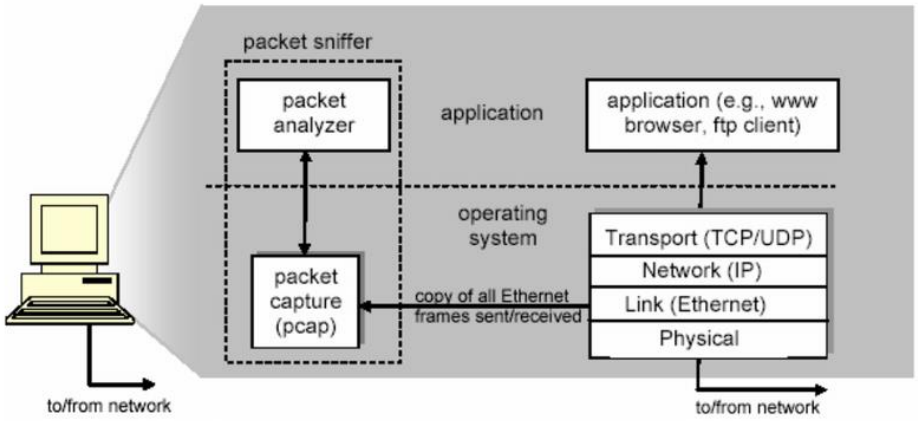
BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

Name	Arushi Jain
UID no.	2023800035
Experiment No.	3

Program 1	
PROBLEM STATEMENT :	**Analyze communication over the network with Wireshark.**
ASSIGNMENT :	**1. DNS Queries and Responses**



DNS Queries:
The majority of the traffic has DNS queries from 192.168.88.61 to 192.168.88.1 (port 53) for the domain time.nist.gov. These queries are sent repeatedly, indicating a retry mechanism due to failures.
Example:

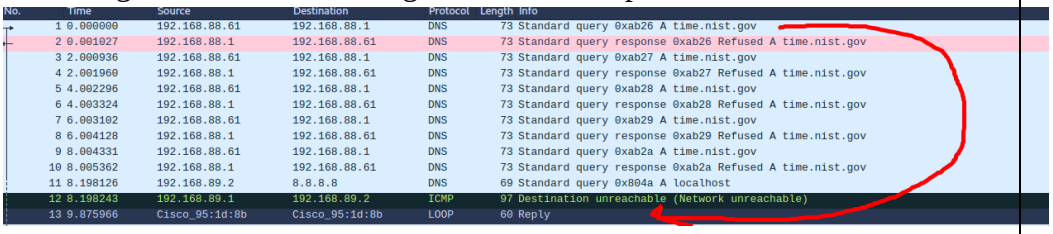
```
2015-10-20 20:40:34.524710 IP 192.168.88.61.949 > 192.168.88.1.53: 43814+ time.nist.gov. (31)
```

The + symbol indicates that the DNS query is requesting a recursive resolution.
DNS Responses:
The DNS server at 192.168.88.1 responds with a "Refused" message, indicating that it is unable or unwilling to resolve the query.

Example:

```
2015-10-20 20:40:34.525737 IP 192.168.88.1.53 > 192.168.88.61.949: 43814 (31)
```

This response suggests that the DNS server is either misconfigured, does not have access to the requested domain, or is intentionally refusing the query.The client (192.168.88.61) retries the DNS query multiple times, indicating that it is not receiving a successful response.



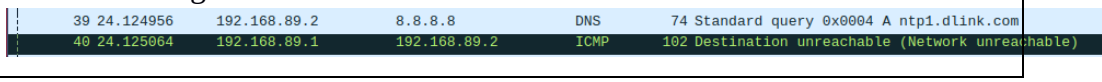
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab26 A time.nist.gov
2	0.001027	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab26 Refused A time.nist.gov
3	2.000936	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab27 A time.nist.gov
4	2.001960	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab27 Refused A time.nist.gov
5	4.002296	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab28 A time.nist.gov
6	4.003324	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab28 Refused A time.nist.gov
7	6.003102	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab29 A time.nist.gov
8	6.004128	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab29 Refused A time.nist.gov
9	8.004331	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab2a A time.nist.gov
10	8.005362	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab2a Refused A time.nist.gov
11	8.198126	192.168.89.2	8.8.8.8	DNS	69	Standard query 0x804a A localhost
12	8.198243	192.168.89.1	192.168.89.2	ICMP	97	Destination unreachable (Network unreachable)
13	9.875966	Cisco_95:1d:8b	Cisco_95:1d:8b	LOOP	60	Reply

2. ICMP Unreachable Messages
ICMP Destination Unreachable:
Several ICMP "Destination Unreachable" messages are sent from 192.168.89.1 to 192.168.89.2, indicating that the destination (8.8.8.8) is unreachable.
Example:

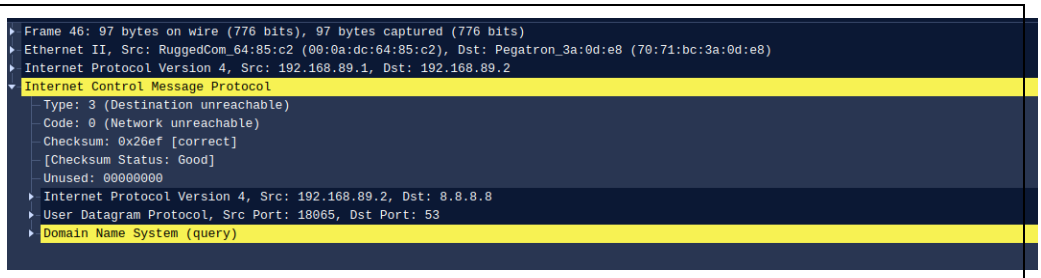
```
2015-10-20 20:40:42.722953 IP 192.168.89.1 > 192.168.89.2: ICMP net 8.8.8 length 63
```

This suggests that 192.168.89.2 is attempting to reach 8.8.8.8 (Google's public DNS server), but the network path is broken or blocked.
Implications:
The ICMP unreachable messages indicate a network connectivity issue, possibly due to:

- A misconfigured gateway
- Firewall rules blocking the traffic
- Routing issues



39	24.124956	192.168.89.2	8.8.8.8	DNS	74 Standard query 0x0004 A ntp1.dlink.com
40	24.125064	192.168.89.1	192.168.89.2	ICMP	102 Destination unreachable (Network unreachable)



3. ARP Requests and Replies

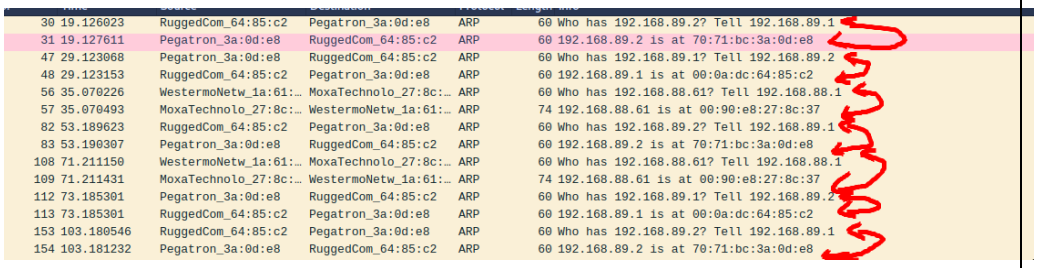
ARP Requests:

Several ARP requests and replies occur between devices on the 192.168.88.1 and 192.168.89.2 networks. ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses.

Example:

```
2015-10-20 20:41:03.647778 ARP, Request who-has 192.168.89.1 tell 192.16
2015-10-20 20:41:03.647863 ARP, Reply 192.168.89.1 is-at 00:0a:dc:64:85:c
```

These ARP messages are normal and indicate that devices are discovering each other's MAC addresses for communication.

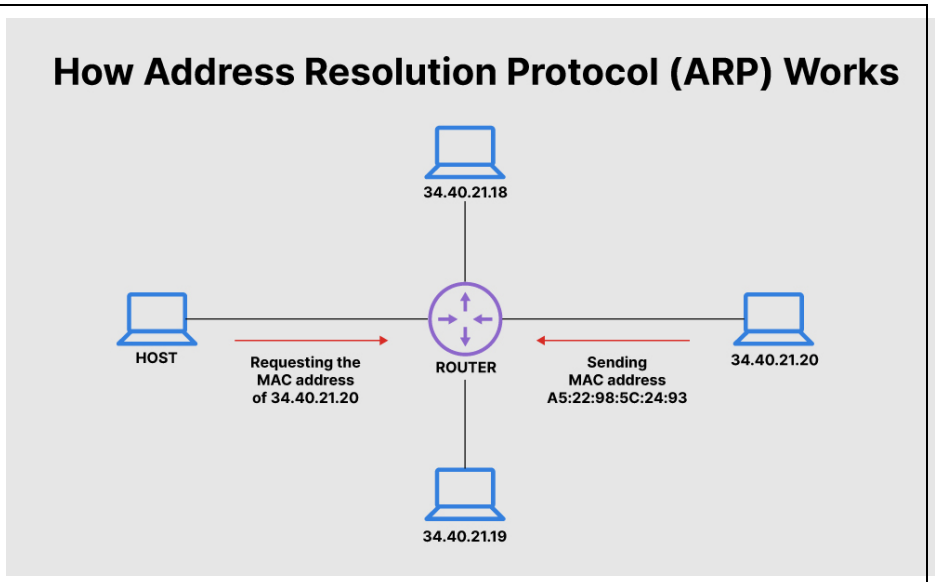


30	19.126023	RuggedCom_64:85:c2	Pegatron_3a:0d:e8	ARP	60 Who has 192.168.89.2? Tell 192.168.89.1
31	19.127611	Pegatron_3a:0d:e8	RuggedCom_64:85:c2	ARP	60 192.168.89.2 is at 70:71:bc:3a:0d:e8
47	29.123068	Pegatron_3a:0d:e8	RuggedCom_64:85:c2	ARP	60 Who has 192.168.89.1? Tell 192.168.89.2
48	29.123153	RuggedCom_64:85:c2	Pegatron_3a:0d:e8	ARP	60 192.168.89.1 is at 00:0a:dc:64:85:c2
56	35.070226	WestermoNetw_1a:61:…	MoxaTechnolo_27:8c:…	ARP	60 Who has 192.168.88.61? Tell 192.168.88.1
57	35.070493	MoxaTechnolo_27:8c:…	WestermoNetw_1a:61:…	ARP	74 192.168.88.61 is at 00:90:e8:27:8c:37
82	53.189623	RuggedCom_64:85:c2	Pegatron_3a:0d:e8	ARP	60 Who has 192.168.89.2? Tell 192.168.89.1
83	53.190307	Pegatron_3a:0d:e8	RuggedCom_64:85:c2	ARP	60 192.168.89.2 is at 70:71:bc:3a:0d:e8
108	71.211150	WestermoNetw_1a:61:…	MoxaTechnolo_27:8c:…	ARP	60 Who has 192.168.88.61? Tell 192.168.88.1
109	71.211431	MoxaTechnolo_27:8c:…	WestermoNetw_1a:61:…	ARP	74 192.168.88.61 is at 00:90:e8:27:8c:37
112	73.185301	Pegatron_3a:0d:e8	RuggedCom_64:85:c2	ARP	60 Who has 192.168.89.1? Tell 192.168.89.2
113	73.185301	RuggedCom_64:85:c2	Pegatron_3a:0d:e8	ARP	60 192.168.89.1 is at 00:0a:dc:64:85:c2
153	103.180546	RuggedCom_64:85:c2	Pegatron_3a:0d:e8	ARP	60 Who has 192.168.89.2? Tell 192.168.89.1
154	103.181232	Pegatron_3a:0d:e8	RuggedCom_64:85:c2	ARP	60 192.168.89.2 is at 70:71:bc:3a:0d:e8

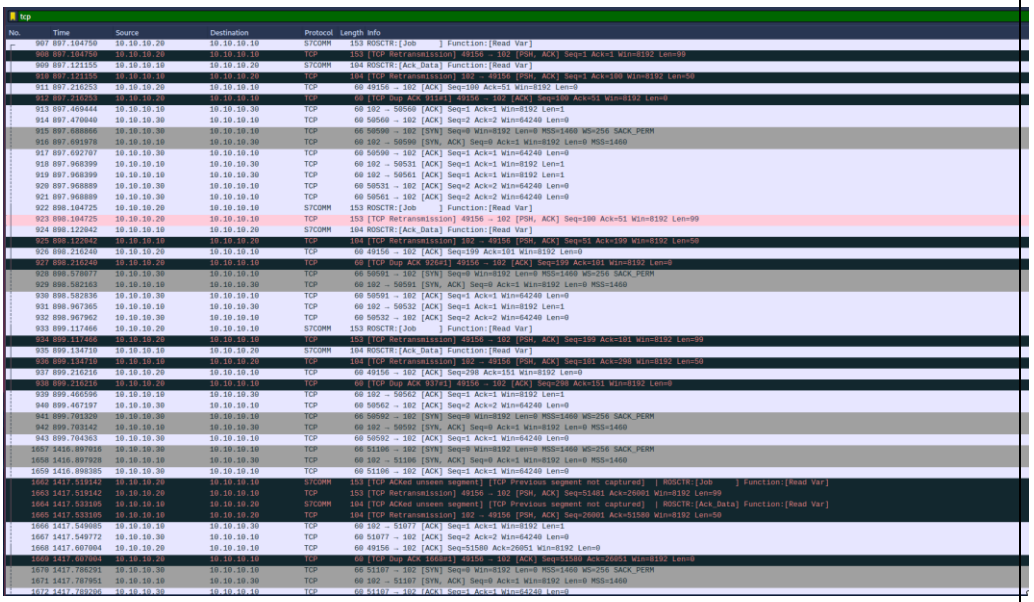
ARP Cache Maintenance:

The frequent ARP requests and replies suggest that:

- The ARP cache on some devices may be expiring quickly
- Intermittent connectivity issues are causing devices to re-resolve MAC addresses



4. TCP Behavior



The network capture shows communication between two devices:

- **Source:** 10.10.10.20
- **Destination:** 10.10.10.10

The primary protocol used in this communication is **S7COMM**, a protocol used for communication with Siemens PLCs (Programmable Logic Controllers). The transport layer protocol is **TCP**, ensuring reliable data transmission. The captured packets suggest that 10.10.10.20 is sending **S7COMM Read Var** requests to 10.10.10.10, which is likely responding with requested data.

Packet Acknowledgment and Failures

Normal TCP Handshake & Acknowledgment

The TCP handshake is established through the following steps:

1. **SYN** – The client (10.10.10.20) initiates a connection to the server (10.10.10.10).
2. **SYN-ACK** – The server acknowledges the request.
3. **ACK** – The client confirms the connection is established.

Once established, data transmission occurs, where every TCP segment sent requires an acknowledgment (ACK) from the receiver. The communication includes sequences of **S7COMM Read Var** requests and corresponding acknowledgment responses.

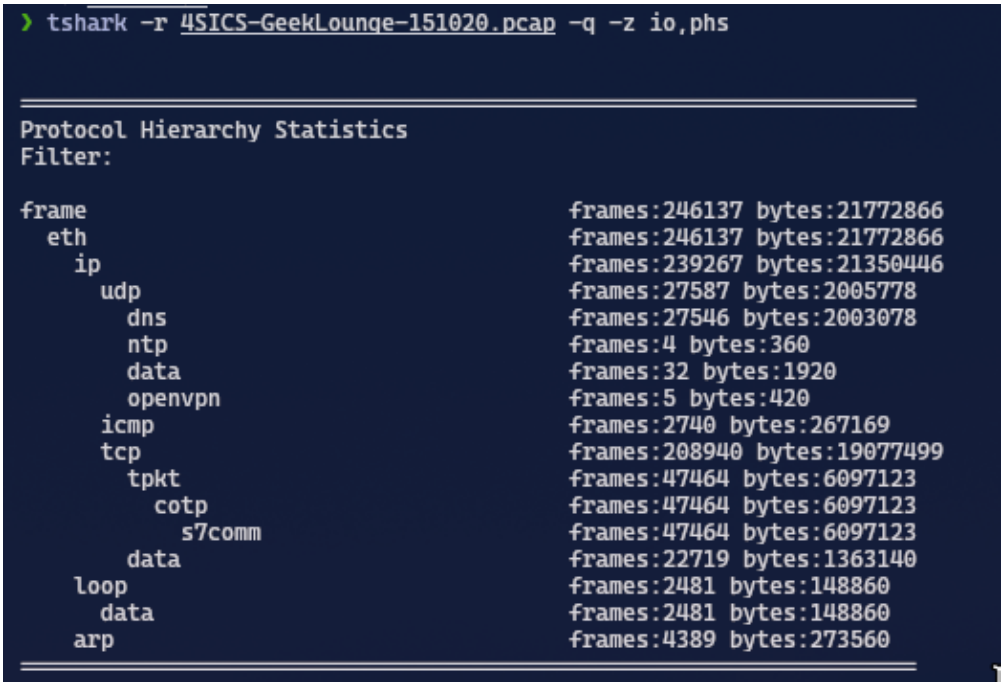
Packet Loss and Retransmissions

There's a lotta retransmission tcp in the capture tho. Retransmissions occur when the sender does not receive an acknowledgment within the expected timeframe, indicating **packet loss** or **network congestion**.

- Innn packet **923**, we see a **TCP Retransmission** of sequence 49156 -> 102 with **PSH, ACK** flags, meaning that the previously sent data was not acknowledged, forcing the sender to resend the packet.

Additionally, **duplicate acknowledgments (Dup ACKs)** appear in response to lost packets, confirming missing data segments. The presence of **"Previous segment not captured"** messages indicates potential packet drops at the capture point.

The above is visible throughout the capture.



We can see our protocol stats above.

There does not appear to be any password leakages in the data.

CONCLUSION:

One major observation is the persistent DNS queries to time.nist.gov, repeatedly met with "Refused" responses. This suggests a misconfiguration or intentional filtering at the DNS server, which could impact time synchronization and dependent services. Similarly, multiple ICMP "Destination Unreachable" messages indicate routing or firewall restrictions, preventing access to external services like Google's DNS (8.8.8.8) and

	potentially disrupting connectivity. ARP traffic appears normal, but the frequent exchanges suggest ARP cache expiration or intermittent connectivity, possibly affecting stability. In TCP analysis, particularly within S7COMM protocol exchanges, the three-way handshake functions correctly, but a high number of retransmissions and duplicate acknowledgments point to packet loss and congestion issues. This could stem from bandwidth limitations, latency, or inefficient TCP configurations, affecting real-time communication. Overall, these findings highlight areas for improvement in DNS settings, routing stability, ARP cache management, and TCP performance. Addressing these concerns will enhance network reliability, efficiency, and security, ensuring smooth communication and external connectivity.