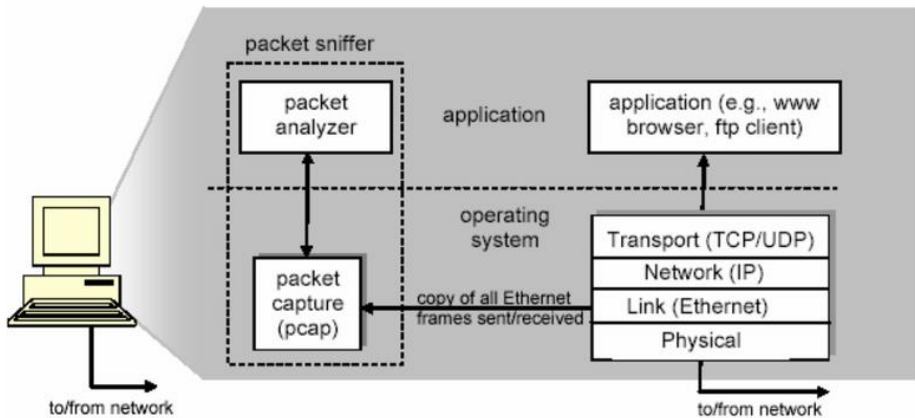




BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

Name	Arushi Jain
UID no.	2023800035
Experiment No.	3

Program 1	
PROBLEM STATEMENT :	Analyze communication over the network with Wireshark.
ASSIGNMENT :	<div><p>1. DNS Queries and Responses</p><p>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.</p><p>Example:</p><pre>2015-10-20 20:40:34.524710 IP 192.168.88.61.949 > 192.168.88.1.53: 43814 time.nist.gov. (31)</pre><p><u>The + symbol indicates that the DNS query is requesting a recursive resolution.</u></p><p>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.</p></div>



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

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	0.000936	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab27 A time.nist.gov
4	0.001960	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab27 Refused A time.nist.gov
5	0.002996	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab28 A time.nist.gov
6	0.003324	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab28 Refused A time.nist.gov
7	0.003102	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab29 A time.nist.gov
8	0.004128	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab29 Refused A time.nist.gov
9	0.004331	192.168.88.61	192.168.88.1	DNS	73	Standard query 0xab2a A time.nist.gov
10	0.005362	192.168.88.1	192.168.88.61	DNS	73	Standard query response 0xab2a Refused A time.nist.gov
11	0.198126	192.168.89.2	8.8.8.8	DNS	60	Standard query 0x804a A localhost
12	0.198243	192.168.89.1	192.168.89.2	ICMP	97	Destination unreachable (Network unreachable)
13	0.875966	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)



BHARATIYA VIDYA BHAVAN'S SARDAR PATEL INSTITUTE OF TECHNOLOGY

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

Department of Computer Engineering

```
Frame 46: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
Ethernet II, Src: RuggedCom_64:85:c2 (00:0a:dc:64:85:c2), Dst: Pegatron_3a:0d:e8 (70:71:bc:3a:0d:e8)
Internet Protocol Version 4, Src: 192.168.89.1, Dst: 192.168.89.2
Internet Control Message Protocol
  Type: 3 (Destination unreachable)
  Code: 0 (Network unreachable)
  Checksum: 0x26ef [correct]
  [Checksum Status: Good]
  Unused: 00000000
Internet Protocol Version 4, Src: 192.168.89.2, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 18065, Dst Port: 53
Domain Name System (query)
```

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 192.168.88.1
2015-10-20 20:41:03.647863 ARP, Reply 192.168.89.1 is-at 00:0a:dc:64:85:c2
```

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

No.	Time	Source	Destination	Protocol	Length	Info
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

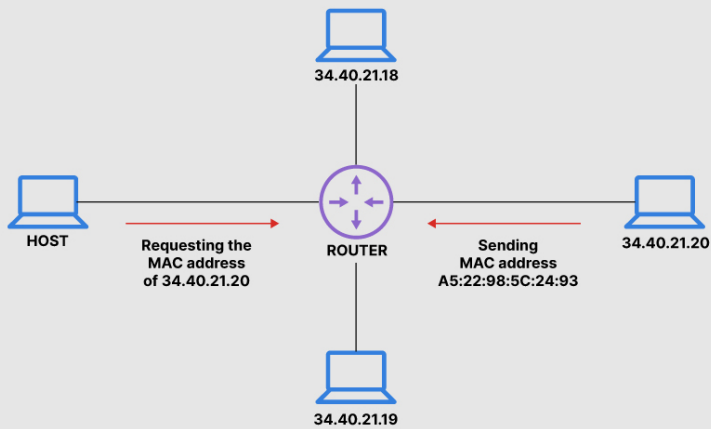


BHARATIYA VIDYA BHAVAN'S SARDAR PATEL INSTITUTE OF TECHNOLOGY

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

Department of Computer Engineering

How Address Resolution Protocol (ARP) Works



4. TCP Behavior

No.	Time	Source	Destination	Protocol	Length	Info
897	897.104750	10.10.10.20	10.10.10.10	STCOWH	153	RSCSTR:[Job] Function:[Read Var]
898	897.104750	10.10.10.10	10.10.10.20	STCOWH	153	RSCSTR:[Job] Function:[Read Var]
899	897.121155	10.10.10.10	10.10.10.20	STCOWH	154	RSCSTR:[Ack Data] Function:[Read Var]
900	897.121155	10.10.10.10	10.10.10.20	TCP	104	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=0
901	897.121253	10.10.10.20	10.10.10.10	TCP	60	49150 -> 102 [ACK] Seq=100 Ack=8192 Len=0
902	897.121253	10.10.10.20	10.10.10.10	TCP	60	[TCP Seq ACK 8191] 49150 -> 102 [ACK] Seq=100 Ack=8192 Len=0
903	897.400444	10.10.10.10	10.10.10.10	TCP	60	392 -> 50500 [ACK] Seq=1 Ack=1 Win=8192 Len=1
904	897.470640	10.10.10.10	10.10.10.10	TCP	60	50500 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
905	897.480846	10.10.10.10	10.10.10.10	TCP	60	50500 -> 102 [SYN] Seq=8 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
906	897.605378	10.10.10.10	10.10.10.10	TCP	60	392 -> 50500 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
907	897.602707	10.10.10.10	10.10.10.10	TCP	60	50500 -> 102 [ACK] Seq=1 Ack=1 Win=84240 Len=0
908	897.900300	10.10.10.10	10.10.10.10	TCP	60	392 -> 50501 [ACK] Seq=1 Ack=1 Win=8192 Len=1
909	897.900399	10.10.10.10	10.10.10.10	TCP	60	392 -> 50501 [ACK] Seq=1 Ack=1 Win=8192 Len=1
910	897.900889	10.10.10.10	10.10.10.10	TCP	60	50501 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
911	897.900889	10.10.10.10	10.10.10.10	TCP	60	50501 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
912	898.104725	10.10.10.10	10.10.10.10	STCOWH	153	RSCSTR:[Job] Function:[Read Var]
913	898.104725	10.10.10.10	10.10.10.10	TCP	153	[TCP Retransmission] 49150 -> 102 [PSH, ACK] Seq=100 Ack=51 Win=8192 Len=99
914	898.122042	10.10.10.10	10.10.10.10	STCOWH	154	RSCSTR:[Ack Data] Function:[Read Var]
915	898.122042	10.10.10.10	10.10.10.10	TCP	104	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=0
916	898.216240	10.10.10.10	10.10.10.10	TCP	60	49150 -> 102 [ACK] Seq=100 Ack=8192 Len=0
917	898.216240	10.10.10.10	10.10.10.10	TCP	60	[TCP Seq ACK 8191] Seq=100 Ack=8192 Len=0
918	898.500377	10.10.10.10	10.10.10.10	TCP	60	50501 -> 102 [SYN] Seq=8 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
919	898.500263	10.10.10.10	10.10.10.10	TCP	60	392 -> 50501 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
920	898.502636	10.10.10.10	10.10.10.10	TCP	60	50501 -> 102 [ACK] Seq=1 Ack=1 Win=84240 Len=0
921	898.907805	10.10.10.10	10.10.10.10	TCP	60	392 -> 50502 [ACK] Seq=1 Ack=1 Win=8192 Len=1
922	898.907802	10.10.10.10	10.10.10.10	TCP	60	50502 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
923	898.117466	10.10.10.10	10.10.10.10	STCOWH	153	RSCSTR:[Job] Function:[Read Var]
924	898.117466	10.10.10.10	10.10.10.10	TCP	153	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=99
925	899.134739	10.10.10.10	10.10.10.10	STCOWH	154	RSCSTR:[Ack Data] Function:[Read Var]
926	899.134739	10.10.10.10	10.10.10.10	TCP	104	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=0
927	899.216219	10.10.10.10	10.10.10.10	TCP	60	49150 -> 102 [ACK] Seq=100 Ack=8192 Len=0
928	899.216219	10.10.10.10	10.10.10.10	TCP	60	[TCP Seq ACK 8191] Seq=100 Ack=8192 Len=0
929	899.400556	10.10.10.10	10.10.10.10	TCP	60	392 -> 50502 [ACK] Seq=1 Ack=1 Win=8192 Len=1
930	899.407197	10.10.10.10	10.10.10.10	TCP	60	50502 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
931	899.703239	10.10.10.10	10.10.10.10	TCP	60	50502 -> 102 [SYN] Seq=8 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
932	899.703142	10.10.10.10	10.10.10.10	TCP	60	392 -> 50502 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
933	899.704463	10.10.10.10	10.10.10.10	TCP	60	50502 -> 102 [ACK] Seq=1 Ack=1 Win=84240 Len=0
934	899.807016	10.10.10.10	10.10.10.10	TCP	60	51186 -> 102 [SYN] Seq=8 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
935	899.807020	10.10.10.10	10.10.10.10	TCP	60	392 -> 51186 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
936	899.808265	10.10.10.10	10.10.10.10	TCP	60	51186 -> 102 [ACK] Seq=1 Ack=1 Win=84240 Len=0
937	899.811014	10.10.10.10	10.10.10.10	STCOWH	153	[TCP Seq ACK 8191] Seq=100 Ack=8192 Len=0
938	899.811014	10.10.10.10	10.10.10.10	TCP	153	[TCP Retransmission] 49150 -> 102 [PSH, ACK] Seq=100 Ack=8192 Len=99
939	899.811014	10.10.10.10	10.10.10.10	STCOWH	154	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=0
940	899.811014	10.10.10.10	10.10.10.10	TCP	104	[TCP Retransmission] Seq=49150 [PSH, ACK] Seq=100 Ack=8192 Len=0
941	899.811014	10.10.10.10	10.10.10.10	TCP	60	392 -> 51187 [ACK] Seq=1 Ack=1 Win=8192 Len=1
942	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
943	899.811014	10.10.10.10	10.10.10.10	TCP	60	49156 -> 102 [ACK] Seq=51500 Ack=2651 Win=8192 Len=0
944	899.811014	10.10.10.10	10.10.10.10	TCP	60	392 -> 51187 [ACK] Seq=1 Ack=1 Win=8192 Len=1
945	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
946	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
947	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
948	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
949	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
950	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
951	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
952	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
953	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
954	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
955	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
956	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
957	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
958	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
959	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
960	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
961	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
962	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
963	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
964	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
965	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
966	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
967	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
968	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
969	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
970	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
971	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
972	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
973	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
974	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
975	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
976	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
977	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
978	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
979	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
980	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
981	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
982	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
983	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
984	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
985	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
986	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
987	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
988	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
989	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
990	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
991	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
992	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
993	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
994	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
995	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
996	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
997	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
998	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0
999	899.811014	10.10.10.10	10.10.10.10	TCP	60	51187 -> 102 [ACK] Seq=2 Ack=2 Win=84240 Len=0

The network capture shows communication between two devices:



**BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY**

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

Department of Computer Engineering

- **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**.

- In 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.



**BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY**

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

Department of Computer Engineering

```
> tshark -r 4SICS-GeekLounge-151020.pcap -q -z io,phs

Protocol Hierarchy Statistics
Filter:

frame                                frames:246137 bytes:21772866
  eth                                frames:246137 bytes:21772866
    ip                                frames:239267 bytes:21350446
      udp                             frames:27587 bytes:2005778
        dns                           frames:27546 bytes:2003078
          ntp                          frames:4 bytes:360
            data                       frames:32 bytes:1920
              openvpn                  frames:5 bytes:420
                icmp                   frames:2740 bytes:267169
                  tcp                  frames:208940 bytes:19077499
                    tpkt                frames:47464 bytes:6097123
                      cotp              frames:47464 bytes:6097123
                        s7comm          frames:47464 bytes:6097123
                          data          frames:22719 bytes:1363140
                            loop         frames:2481 bytes:148860
                              data       frames:2481 bytes:148860
                                arp       frames:4389 bytes:273560
```

We can see our protocol stats above.

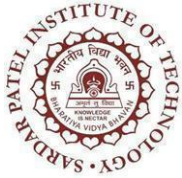
```
> tshark -r 4SICS-GeekLounge-151020.pcap -Y 'data.text contains "password"'
> tshark -r 4SICS-GeekLounge-151020.pcap -Y 'http.authorization'
> tshark -r 4SICS-GeekLounge-151020.pcap -Y 'frame contains 70617373776F7264'
> tshark -r 4SICS-GeekLounge-151020.pcap -q -z credentials
```

Packet	Protocol	Username	Info
~/Downloads			

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



**BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY**

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

Department of Computer Engineering

	<p>potentially disrupting connectivity.</p> <p>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.</p> <p>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.</p>
--	--