Packet Analysis(ARP & ICMP) using wireshark

2023005439-Ronanki Trivikram

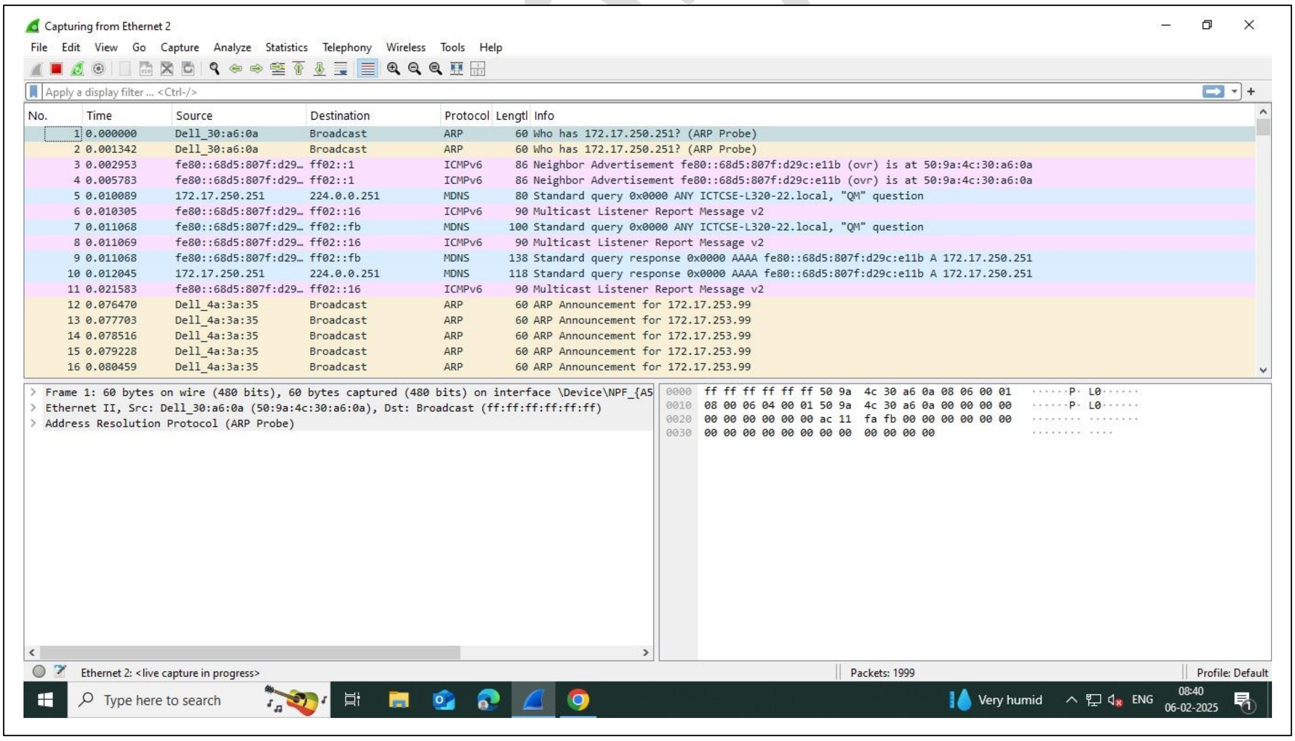
GITAM

Abstract

This project explores network communication protocols, specifically ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol), through packet analysis using Wireshark. The objective is to gain a practical understanding of how these protocols function at the packet level. ARP's role in mapping IP addresses to MAC addresses within a local network is examined by capturing and analyzing ARP requests and responses. ICMP, used for network diagnostics and error reporting, is investigated by analyzing various ICMP message types, such as echo requests/replies (ping) and destination unreachable messages. This project demonstrates the use of Wireshark to capture and dissect network traffic, providing insights into the structure and behavior of ARP and ICMP packets. By analyzing the captured data, the project aims to solidify understanding of these fundamental networking protocols and their importance in network operation and troubleshooting.

Steps:

Step1:open wireshark it will start analysing the packet


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source                   Destination   Protocol Lengtl Info
    1 0.000000  Dell_30:a6:0a            Broadcast     ARP       60 Who has 172.17.250.251? (ARP Probe)
    2 0.001342  Dell_30:a6:0a            Broadcast     ARP       60 Who has 172.17.250.251? (ARP Probe)
    3 0.002953  fe80::68d5:807f:d29… ff02::1       ICMPv6    86 Neighbor Advertisement fe80::68d5:807f:d29c:e11b (ovr) is at 50:9a:4c:30:a6:0a
    4 0.005783  fe80::68d5:807f:d29… ff02::1       ICMPv6    86 Neighbor Advertisement fe80::68d5:807f:d29c:e11b (ovr) is at 50:9a:4c:30:a6:0a
    5 0.010089  172.17.250.251           224.0.0.251   MDNS      80 Standard query 0x0000 ANY ICTCSE-L320-22.local, "QM" question
    6 0.010305  fe80::68d5:807f:d29… ff02::16      ICMPv6    90 Multicast Listener Report Message v2
    7 0.011068  fe80::68d5:807f:d29… ff02::fb      MDNS     100 Standard query 0x0000 ANY ICTCSE-L320-22.local, "QM" question
    8 0.011069  fe80::68d5:807f:d29… ff02::16      ICMPv6    90 Multicast Listener Report Message v2
    9 0.011068  fe80::68d5:807f:d29… ff02::fb      MDNS     138 Standard query response 0x0000 AAAA fe80::68d5:807f:d29c:e11b A 172.17.250.251
   10 0.012045  172.17.250.251           224.0.0.251   MDNS     118 Standard query response 0x0000 AAAA fe80::68d5:807f:d29c:e11b A 172.17.250.251
   11 0.021583  fe80::68d5:807f:d29… ff02::16      ICMPv6    90 Multicast Listener Report Message v2
   12 0.076470  Dell_4a:3a:35            Broadcast     ARP       60 ARP Announcement for 172.17.253.99
   13 0.077703  Dell_4a:3a:35            Broadcast     ARP       60 ARP Announcement for 172.17.253.99
   14 0.078516  Dell_4a:3a:35            Broadcast     ARP       60 ARP Announcement for 172.17.253.99
   15 0.079228  Dell_4a:3a:35            Broadcast     ARP       60 ARP Announcement for 172.17.253.99
   16 0.080459  Dell_4a:3a:35            Broadcast     ARP       60 ARP Announcement for 172.17.253.99
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A5
> Ethernet II, Src: Dell_30:a6:0a (50:9a:4c:30:a6:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (ARP Probe)
```

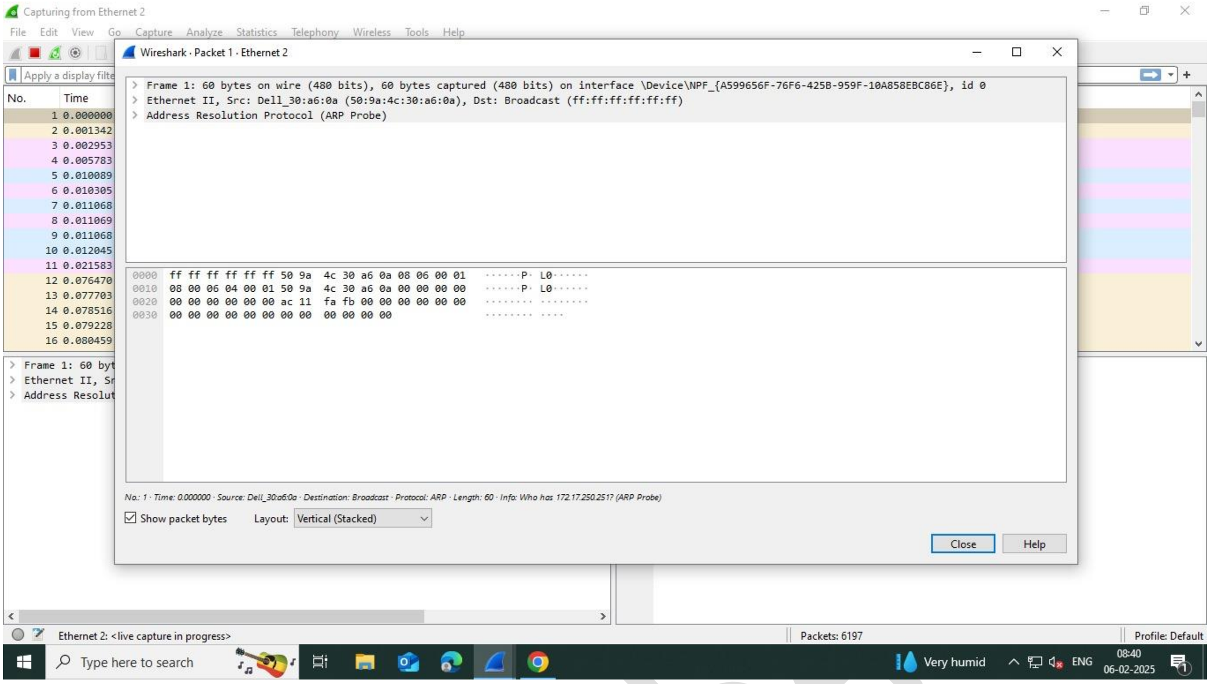
```
0000  ff ff ff ff ff ff 50 9a  4c 30 a6 0a 08 06 00 01   ······P· L0······
0010  08 00 06 04 00 01 50 9a  4c 30 a6 0a 00 00 00 00   ······P· L0······
0020  00 00 00 00 00 00 ac 11  fa fb 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Ethernet 2: <live capture in progress>

Packets: 1999

Profile: Default

Step 2: now search for ARP and ICMP Packets in the search bar


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filte
Wireshark · Packet 1 · Ethernet 2
Close
Help
Type here to search
Very humid
ENG
08:40
06-02-2025

```
No.  Time
  1 0.000000
  2 0.001342
  3 0.002953
  4 0.005783
  5 0.010089
  6 0.010305
  7 0.011068
  8 0.011069
  9 0.011068
 10 0.012045
 11 0.021583
 12 0.076470
 13 0.077703
 14 0.078516
 15 0.079228
 16 0.080459
```

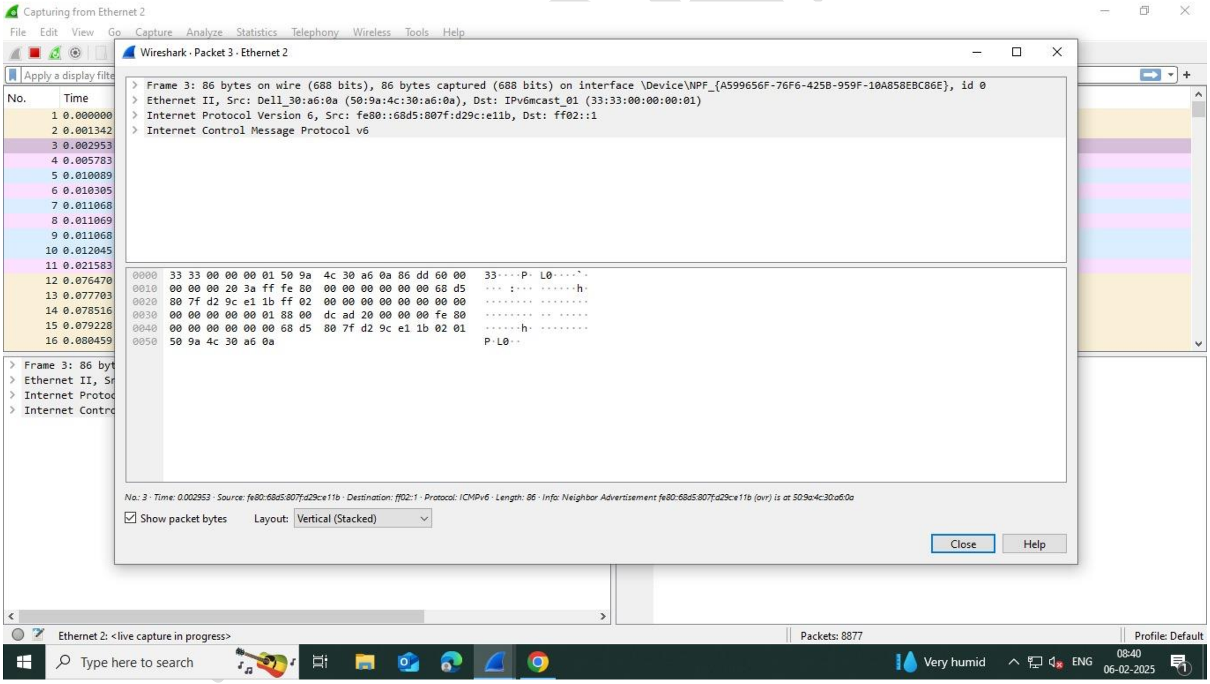
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A599656F-76F6-425B-959F-10A858EBC86E}, id 0
> Ethernet II, Src: Dell_30:a6:0a (50:9a:4c:30:a6:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (ARP Probe)
```

```
0000  ff ff ff ff ff ff 50 9a  4c 30 a6 0a 08 06 00 01   ······P· L0······
0010  08 00 06 04 00 01 50 9a  4c 30 a6 0a 00 00 00 00   ······P· L0······
0020  00 00 00 00 00 00 ac 11  fa fb 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

No.: 1 · Time: 0.000000 · Source: Dell_30:a6:0a · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 172.17.250.251? (ARP Probe)

☑ Show packet bytes Layout: Vertical (Stacked)

Ethernet 2: <live capture in progress> Packets: 6197 Profile: Default


Capturing from Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filte
Wireshark · Packet 3 · Ethernet 2
Close
Help
Type here to search
Very humid
ENG
08:40
06-02-2025

```
No.  Time
  1 0.000000
  2 0.001342
  3 0.002953
  4 0.005783
  5 0.010089
  6 0.010305
  7 0.011068
  8 0.011069
  9 0.011068
 10 0.012045
 11 0.021583
 12 0.076470
 13 0.077703
 14 0.078516
 15 0.079228
 16 0.080459
```

```
> Frame 3: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{A599656F-76F6-425B-959F-10A858EBC86E}, id 0
> Ethernet II, Src: Dell_30:a6:0a (50:9a:4c:30:a6:0a), Dst: IPv6mcast_01 (33:33:00:00:00:01)
> Internet Protocol Version 6, Src: fe80::68d5:807f:d29c:e11b, Dst: ff02::1
> Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 01 50 9a  4c 30 a6 0a 86 dd 60 00   33····P· L0····`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 68 d5   ··· :··· ······h·
0020  80 7f d2 9c e1 1b ff 02  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 88 00  dc ad 20 00 00 00 fe 80   ········ ·· ·····
0040  00 00 00 00 00 00 68 d5  80 7f d2 9c e1 1b 02 01   ······h· ········
0050  50 9a 4c 30 a6 0a                                  P·L0··
```

No.: 3 · Time: 0.002953 · Source: fe80::68d5:807f:d29c:e11b · Destination: ff02::1 · Protocol: ICMPv6 · Length: 86 · Info: Neighbor Advertisement fe80::68d5:807f:d29c:e11b (ovr) is at 50:9a:4c:30:a6:0a

☑ Show packet bytes Layout: Vertical (Stacked)

Ethernet 2: <live capture in progress> Packets: 8877 Profile: Default

Significance

Understanding ARP and ICMP is fundamental to network functionality and troubleshooting. ARP (Address Resolution Protocol) maps IP addresses to MAC addresses within a local network, enabling devices to communicate. Without it, devices wouldn't know the physical location of others, hindering communication. Analyzing ARP packets with Wireshark helps diagnose connectivity issues, identify bottlenecks, and detect attacks like ARP spoofing.

ICMP (Internet Control Message Protocol) is crucial for network diagnostics and error reporting. Tools like ping use it to test connectivity. Routers also use ICMP to communicate network status and errors, such as "destination unreachable." Analyzing ICMP traffic helps identify outages, latency, and routing problems. It's also vital for security, as some ICMP messages can be exploited in attacks.

Wireshark allows detailed packet inspection. Analyzing ARP and ICMP packets provides practical insights into their function, importance, and vulnerabilities. This knowledge is invaluable for network professionals, enabling them to build, maintain, and secure networks. It allows proactive problem identification, minimizing downtime and ensuring smooth operation. By understanding these core protocols, network professionals can effectively troubleshoot connectivity issues, optimize network performance, and implement robust security measures.

Thank you