

To demonstrate the different Network-Layer techniques shown in the Wireshark trace, this report will display three different techniques that can be found in this trace.

Addressing

The figure below shows the Internet Protocol Version 4 (IPv4) section with its respective source and destination addresses. This demonstrates the Network-Layer technique of addressing of the RFC 791 Internet Protocol Standard of the DARPA Internet Program. [1]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.19.32.52	255.255.255.255	UDP	492	2021 → 2021 Len=450
2	1.024080	fe80::1855:c3de:96...	ff02::1:2	DHCPv6	120	Information-request
3	1.844738	62:a7:79:9a:7b:d4	Apple_d8:d0:cb	ARP	60	Who has 172.19.33.189
4	1.844796	Apple_d8:d0:cb	62:a7:79:9a:7b:d4	ARP	42	172.19.33.189 is at


```
> Frame 1: Packet, 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
> Ethernet II, Src: AMPAKTechnol_67:dc:ac (50:41:1c:67:dc:ac), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.19.32.52, Dst: 255.255.255.255
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xcf7f (53119)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x9d48 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.19.32.52
    Destination Address: 255.255.255.255
    [Stream index: 0]
```

Figure 2

As seen above, RFC 791 defines the IPv4 header files, i.e. Address, TTL (Time to Live), header checksum, in which is a type of “addressing” technique in the Network Layer.

Routing – Decreasing TTL values across packets

No.	Time	Source	Destination	Protocol	Length	Info
10	5.324619	10.4.48.232	224.0.0.1	IGMPv2	60	Membership Quer
12	6.664096	58.136.190.31	172.19.33.189	TCP	74	80 → 50132 [SYN
15	6.673462	58.136.190.31	172.19.33.189	TCP	66	80 → 50132 [ACK
16	6.673488	58.136.190.31	172.19.33.189	HTTP	385	HTTP/1.1 200 OK


```
> Frame 10: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_16:8d:bc (2c:3f:0b:16:8d:bc), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
> Internet Protocol Version 4, Src: 10.4.48.232, Dst: 224.0.0.1
  0100 .... = Version: 4
  .... 0110 = Header Length: 24 bytes (6)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 32
    Identification: 0x1735 (5941)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: IGMP (2)
    Header Checksum: 0xf1f5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.4.48.232
    Destination Address: 224.0.0.1
  > Options: (4 bytes), Router Alert
    [Stream index: 3]
```

Figure 3

No.	Time	Source	Destination	Protocol	Length	Info
10	5.324619	10.4.48.232	224.0.0.1	IGMPv2	60	Membership Quer
12	6.664096	58.136.190.31	172.19.33.189	TCP	74	80 → 50132 [SYN
15	6.673462	58.136.190.31	172.19.33.189	TCP	66	80 → 50132 [ACK
16	6.673488	58.136.190.31	172.19.33.189	HTTP	385	HTTP/1.1 200 OK


```
> Frame 15: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: 62:a7:79:9a:7b:d4 (62:a7:79:9a:7b:d4), Dst: Apple_d8:d0:cb (98:01:a7:d8:d0:cb)
> Internet Protocol Version 4, Src: 58.136.190.31, Dst: 172.19.33.189
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x48 (DSCP: AF21, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x090f (2319)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: TCP (6)
    Header Checksum: 0x74f5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 58.136.190.31
    Destination Address: 172.19.33.189
    [Stream index: 4]
  > Transmission Control Protocol, Src Port: 80, Dst Port: 50132, Seq: 1, Ack: 376, Len: 0
```

Figure 4

Figure 3 & 4 displays two different packets that were filtered using `ip.ttl < 64`. This is to display the TTL or Time-To-Live values in that they are below the initial TTL values of 64 or 128. As specified in RFC 791, every router decrements TTL by at least one before forwarding a packet [3], therefore, the TTL values of the packets display that multiple routing hops were involved, demonstrating active network-layer routing behavior.

Network-layer error reporting

Figure 5 displays the ICMP section, in which, shows its type to be 3 or “Destination Unreachable”. This is specified in RFC 792 where it defines Type 3 and codes, returned internet header + 64 bits to allow the sender to match the error to an originating process. [2]

No.	Time	Source	Destination	Protocol	Length	Info
3258	106.393224	103.11.12.145	172.19.33.189	ICMP	110	Destination unreachable (Network unreachable)
[Header checksum status: Unverified]						
Source Address: 103.11.12.145						
Destination Address: 172.19.33.189						
[Stream index: 41]						
Internet Control Message Protocol						
> Type: Destination unreachable (3)						
Code: 0 (Network unreachable)						
Checksum: 0x070 (correct)						
[Checksum Status: Good]						
Unused: 00						
Length: 17						
[Length of original datagram: 68]						
Unused: 0000						

Figure 5

References

- [1] J. Postel, **Internet Protocol**, RFC 791, Sep. 1981. (See §1.4 *Operation*, §2.3 *Addressing*, pp. 1–6 for addressing, TTL, fragmentation).
- [2] J. Postel, **Internet Control Message Protocol**, RFC 792, Sep. 1981. (See “*Destination Unreachable Message*” and “*Time Exceeded Message*”, pp. 4–6 — packet formats, Type/Code meanings, and the requirement to include the original IP header + 64 bits.)
- [3] J. Postel, **Internet Protocol**, RFC 791, Sep. 1981. (See §3.2.1 *Time to Live*, pp. 14–15 — TTL decrement by each router; packet lifetime limitation; hop-by-hop forwarding behavior.)