# Tutorial 9: Common Questions for P3

# How to identify the IP of ultimate destination?

- Take group1-trace1.pcap for an example

| | | | | | |
|---|---|---|---|---|---|
| 17 | 0.624666000 | Cisco_79:fd:00 | Spanning-tree-(for-… | STP | 60 RST. Root = 8192/0/00:16:9c:b4:8 |
| 18 | 0.757215000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 45344 → 33434 Len=32 |
| 19 | 0.757242000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 48975 → 33435 Len=32 |
| 20 | 0.757258000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 40110 → 33436 Len=32 |
| 21 | 0.757272000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 46241 → 33437 Len=32 |
| 22 | 0.757286000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 60688 → 33438 Len=32 |
| 23 | 0.757300000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 45930 → 33439 Len=32 |
| 24 | 0.757313000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 60038 → 33440 Len=32 |
| 25 | 0.757327000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 48895 → 33441 Len=32 |
| 26 | 0.757340000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 41564 → 33442 Len=32 |
| 27 | 0.757354000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 42541 → 33443 Len=32 |
| 28 | 0.757367000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 41326 → 33444 Len=32 |
| 29 | 0.757381000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 38441 → 33445 Len=32 |
| 30 | 0.757394000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 53293 → 33446 Len=32 |

- The destination IP of these UDP packets is 8.8.8.8, which is the ultimate destination

# How to verify whether you make a correct match?

- Still take group1-trace1.pcap for an example

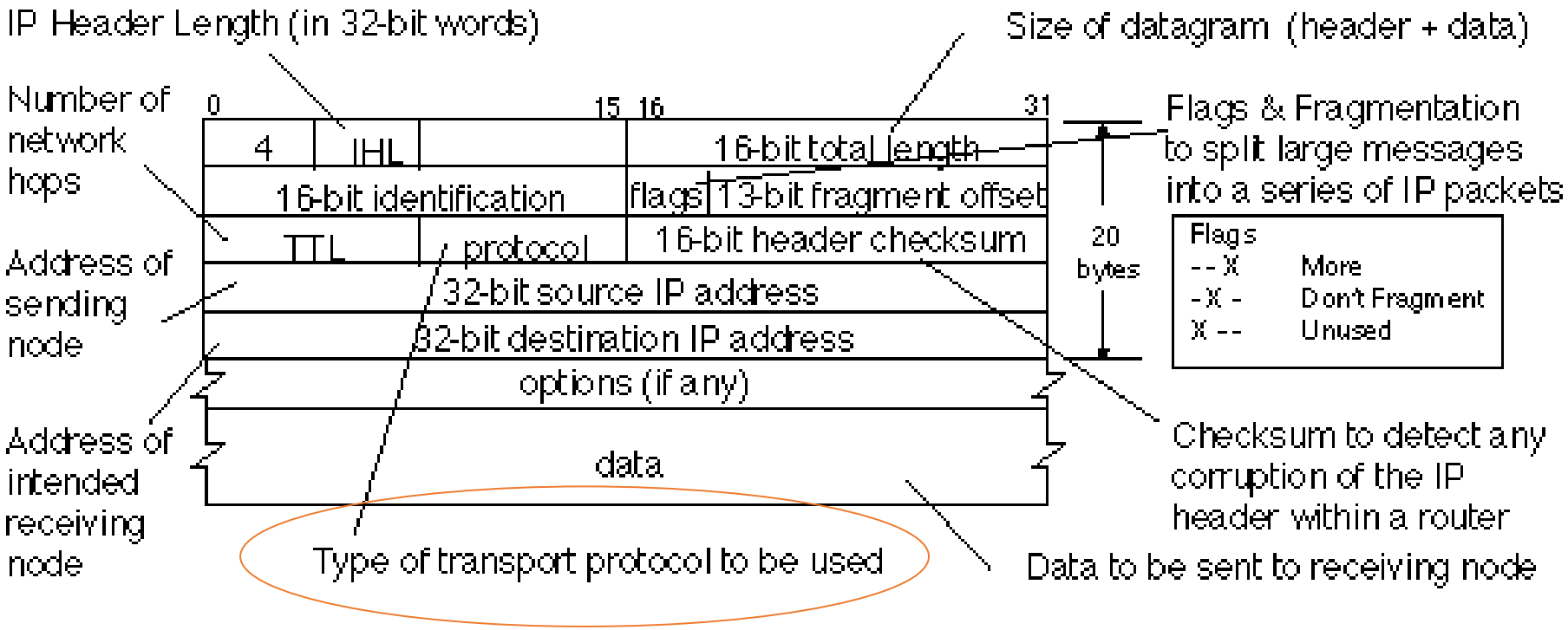
| | | | | | |
|---|---|---|---|---|---|
| 17 | 0.624666000 | Cisco_79:fd:00 | Spanning-tree-(for-… | STP | 60 RST. Root = 8192/0/00:16:9c:b4:89:40 Cost = 1 Port = 0x8091 |
| 18 | 0.757215000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 45344 → 33434 Len=32 |
| 19 | 0.757242000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 48975 → 33435 Len=32 |
| 20 | 0.757258000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 40110 → 33436 Len=32 |
| 21 | 0.757272000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 46241 → 33437 Len=32 |
| 22 | 0.757286000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 60688 → 33438 Len=32 |
| 23 | 0.757300000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 45930 → 33439 Len=32 |
| 24 | 0.757313000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 60038 → 33440 Len=32 |
| 25 | 0.757327000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 48895 → 33441 Len=32 |
| 26 | 0.757340000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 41564 → 33442 Len=32 |
| 27 | 0.757354000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 42541 → 33443 Len=32 |
| 28 | 0.757367000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 41326 → 33444 Len=32 |
| 29 | 0.757381000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 38441 → 33445 Len=32 |
| 30 | 0.757394000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 53293 → 33446 Len=32 |
| 31 | 0.757407000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 59062 → 33447 Len=32 |
| 32 | 0.757421000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 59977 → 33448 Len=32 |
| 33 | 0.757434000 | 192.168.100.17 | 8.8.8.8 | UDP | 74 43296 → 33449 Len=32 |
| 34 | 0.768327000 | 142.104.68.167 | 192.168.100.17 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 35 | 0.768611000 | 142.104.68.167 | 192.168.100.17 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 36 | 0.768877000 | 142.104.68.167 | 192.168.100.17 | ICMP | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 37 | 0.768930000 | 192.168.100.17 | 8.8.8.8 | DNS | 87 Standard query 0x4062 PTR 167.68.104.142.in-addr.arpa |

In Wireshark, the match between UDP and ICMP TTL Exceeded has been automatically created

# Messages that can be neglected

- We only care about UDP and ICMP messages. Other messages can be neglected, e.g.,
- TCP messages
- DNS messages
- Spanning-Tree Packet
  which is used to build a loop-free logical topology for Ethernet networks

# Protocol field in IP header




- 8-bit Protocol field, you only need to care about two values:

- 1 for ICMP,17 for UDP

# The type field in ICMP header


- You only need to care about four types:

Type 0:  Echo reply

Type 3:  (code3) Port number unreachable

Type 8 :  Echo (ping) request

Type 11: Time exceeded

messages