Using Wireshark to Analyze IPv4, IPv6, and ICMP

Chris Greer
NETWORK ANALYST

@packetpioneer www.packetpioneer.com

Module Overview

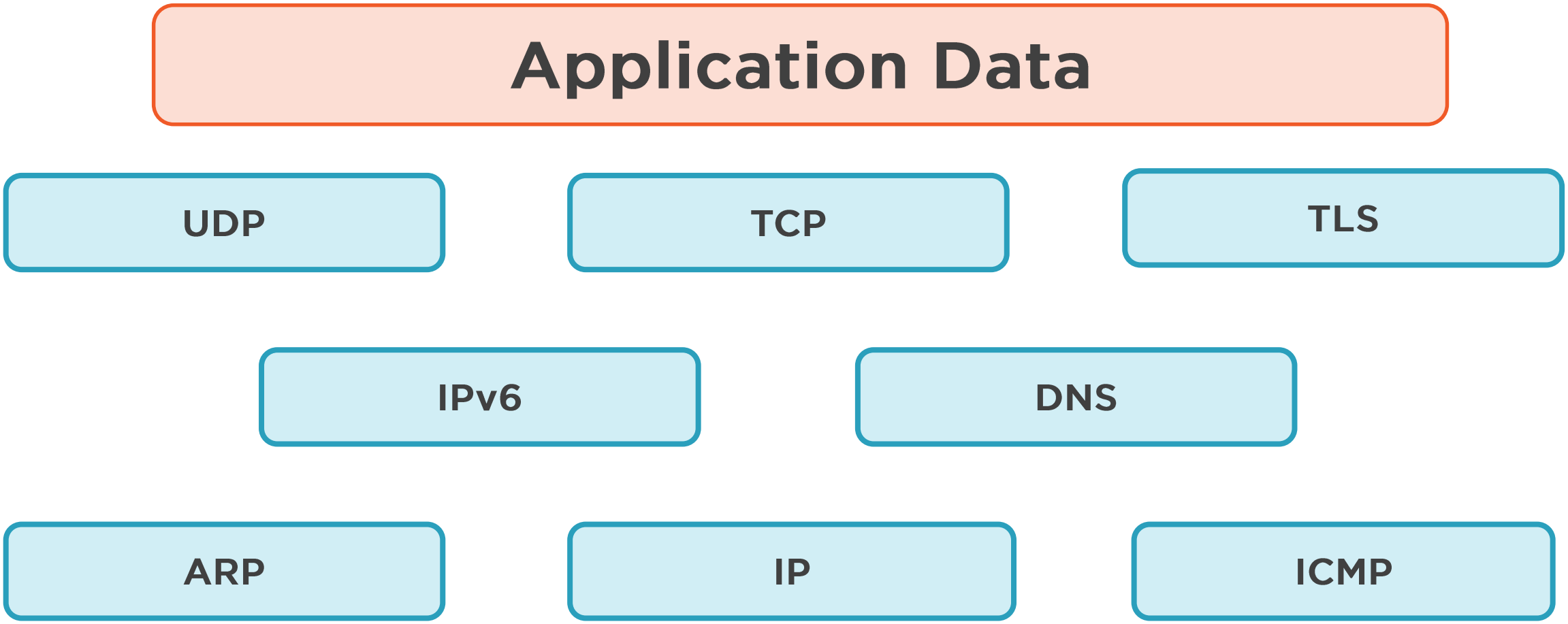
Let's talk IPv4

- TTL
- Fragmentation

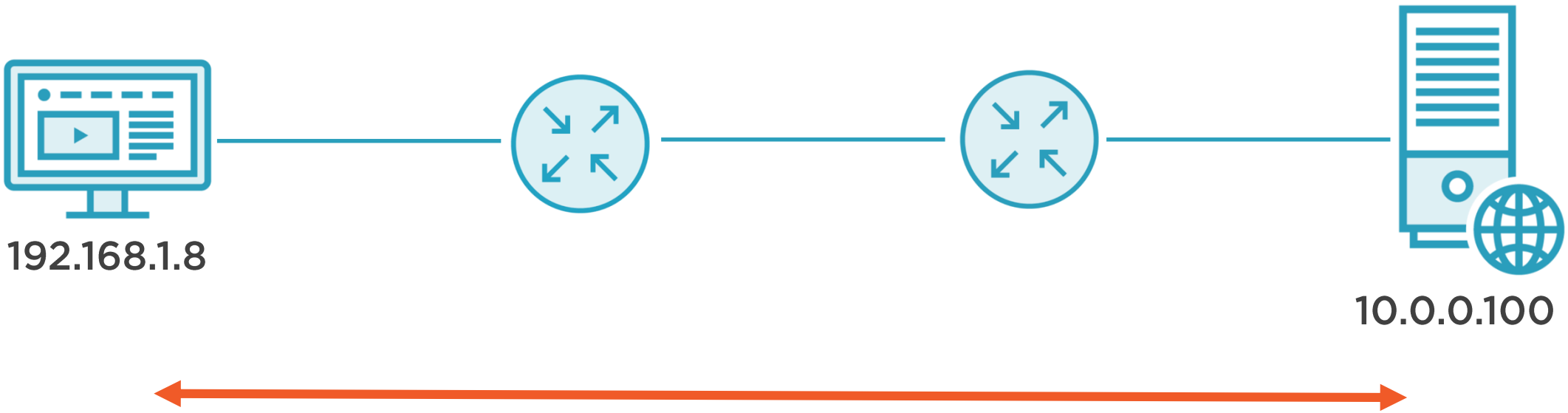
Examining ICMP messages

Analyzing IPv6

Core Protocols - ICMP



The Internet Protocol

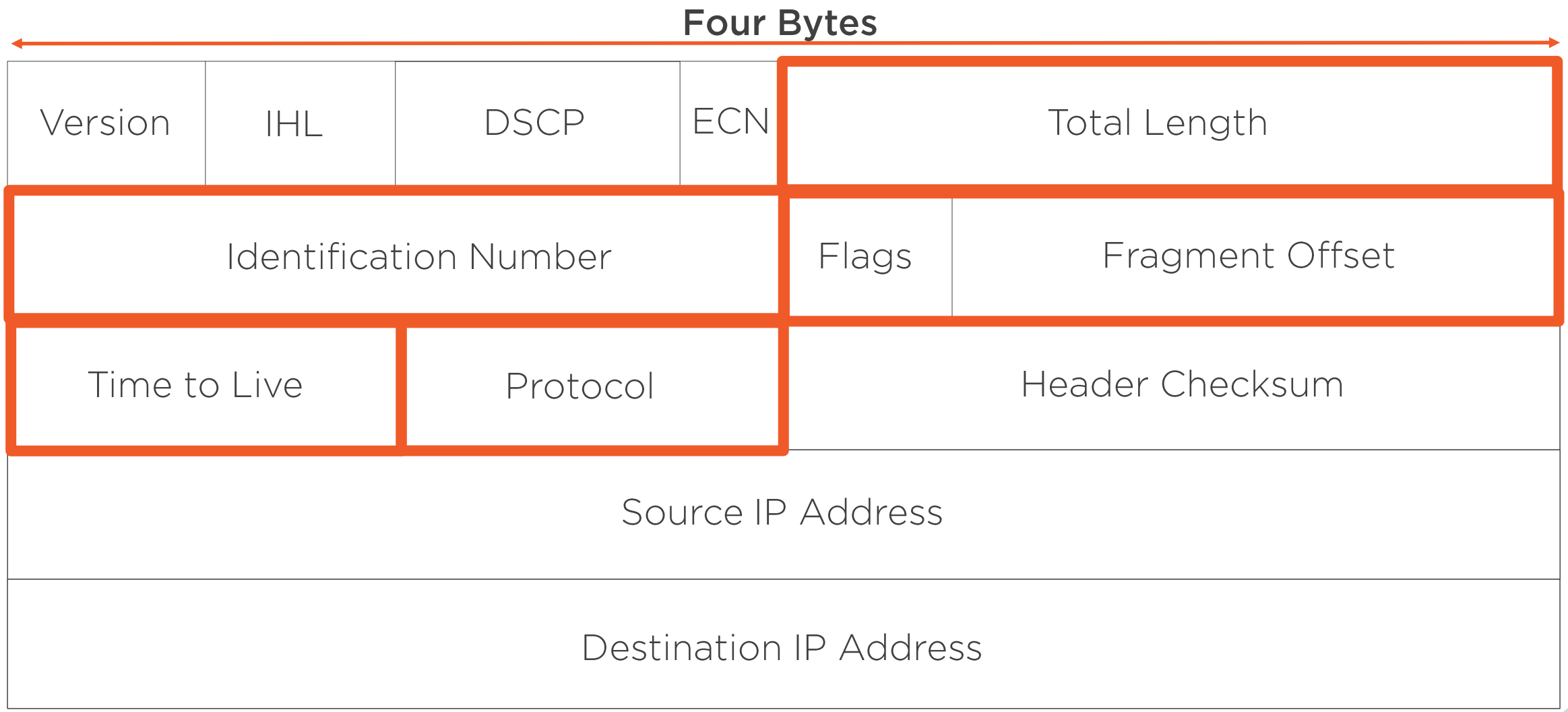


The IP Address

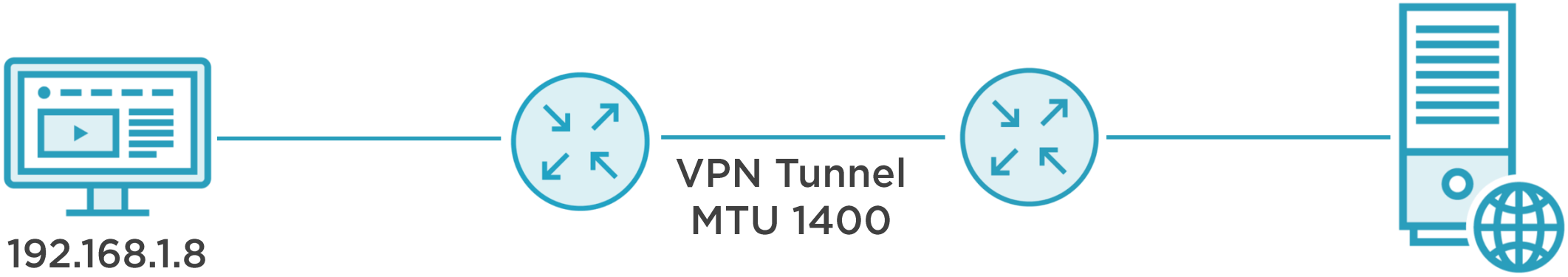
192.168.1.8

255.255.255.0

IP Header Structure



IP Fragmentation



1500 Bytes

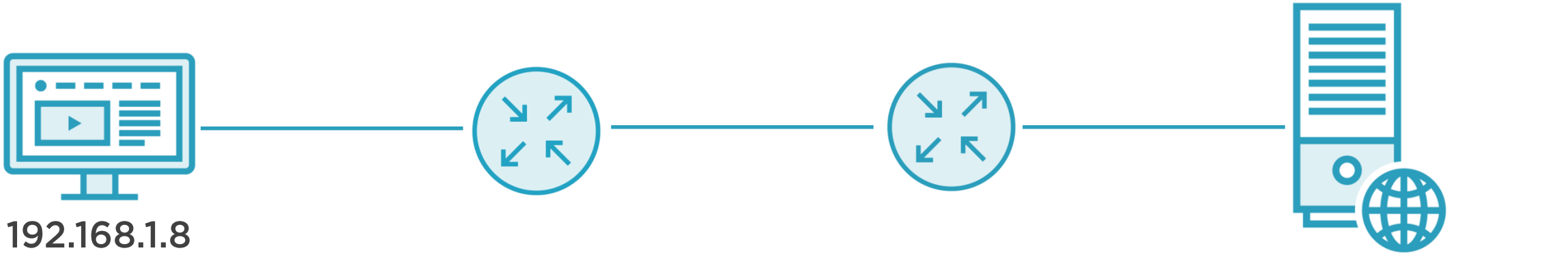
100

1400 Bytes

IP Fragmentation

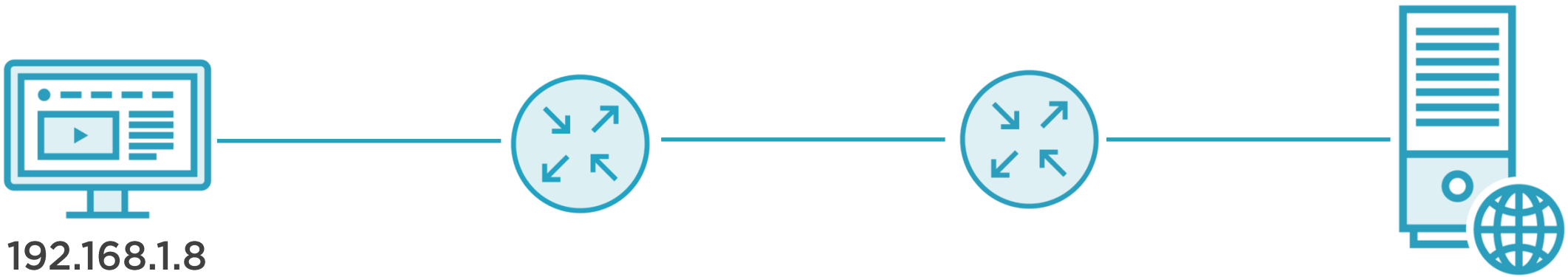
```
▼ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x5000 (20480)
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xd971 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 10.0.0.1
```

IP Time to Live




```
ChrisBook:~ chris$ ping www.pluralsight.com
PING www.pluralsight.com.cdn.cloudflare.net (104.19.161.127): 56 data bytes
64 bytes from 104.19.161.127: icmp_seq=0 ttl=51 time=55.678 ms
64 bytes from 104.19.161.127: icmp_seq=1 ttl=51 time=48.153 ms
64 bytes from 104.19.161.127: icmp_seq=2 ttl=51 time=47.932 ms
64 bytes from 104.19.161.127: icmp_seq=3 ttl=51 time=49.524 ms
64 bytes from 104.19.161.127: icmp_seq=4 ttl=51 time=49.225 ms
```

IP Time to Live



TTL 255

TTL 254

TTL 253

TTL 253

TTL 255

255, 128, or 64

The Time to Live field is useful to determine how many router hops away a station is

Demo

Let’s look at how TTL works

Answer the questions in Statistics | Capture File Properties

Demo

Let’s look at how fragmentation works

The ICMP Protocol

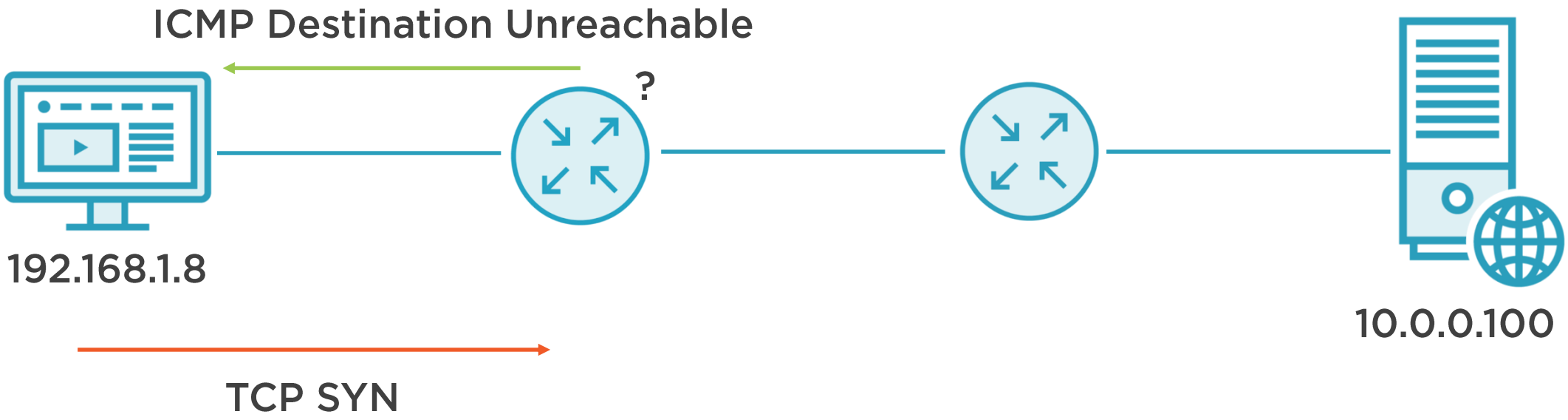
The ICMP Protocol

Messaging suite for IP

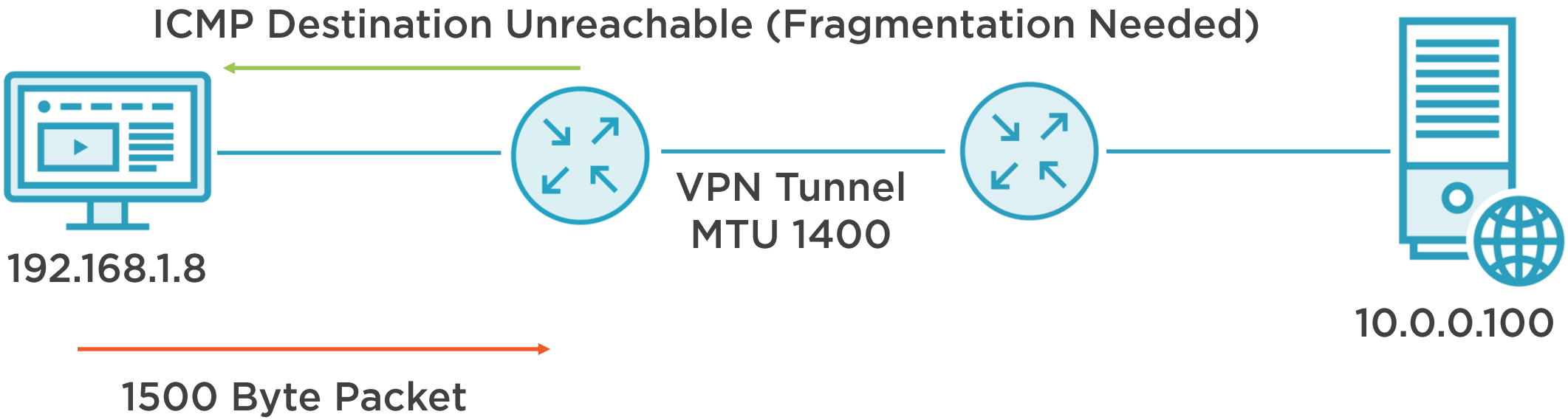
Used by both endpoints and infrastructure

Communicates network problems, outages, routing issues, port unavailable, and more

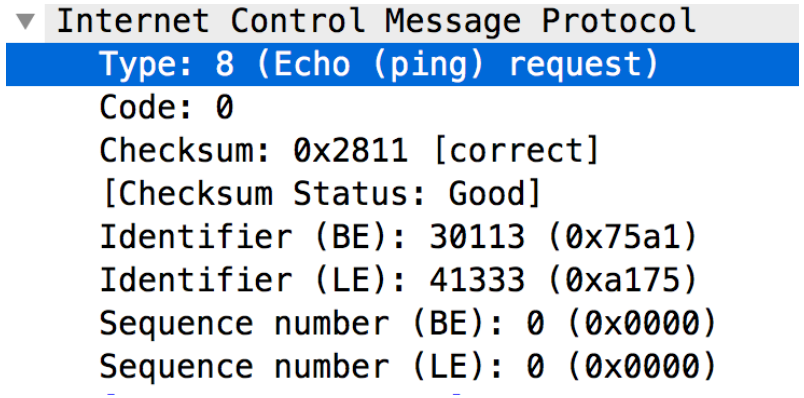
ICMP – Destination Unreachable



ICMP – Fragmentation Needed



ICMP Types



0 = Echo reply

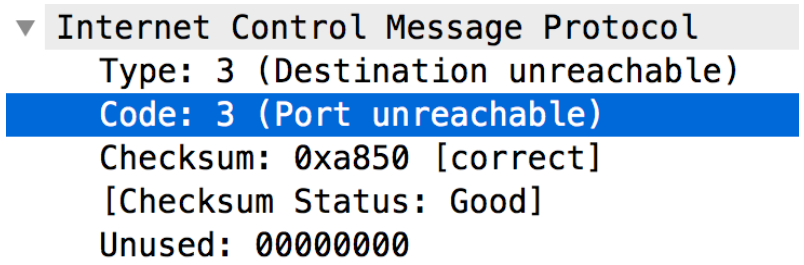
3 = Destination unreachable

5 = Redirect

8 = Echo request

11 = Time to live exceeded

ICMP Codes – Destination Unreachable



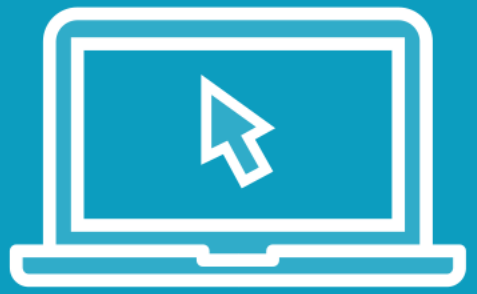
0 = Network unreachable

1 = Host unreachable

3 = Port unreachable

4 = Fragmentation needed

Demo



Analyzing ICMP with Wireshark

Answer the questions in Statistics | Capture File Properties

The IPv6 Protocol

IPv6

IPv4 – 4.3 Billion Addresses

32 Bit Address

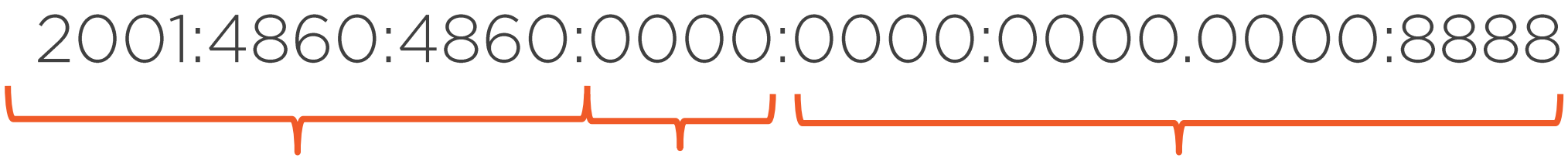
NAT Has Extended Use

IPv6 – 340 Trillion Trillion Trillion Addresses

128 Bit Address

More Efficient

The IPv6 Address



The IPv6 Address

2001:4860:4860:0000:0000:0000.0000:0088

2001:4860:4860::88

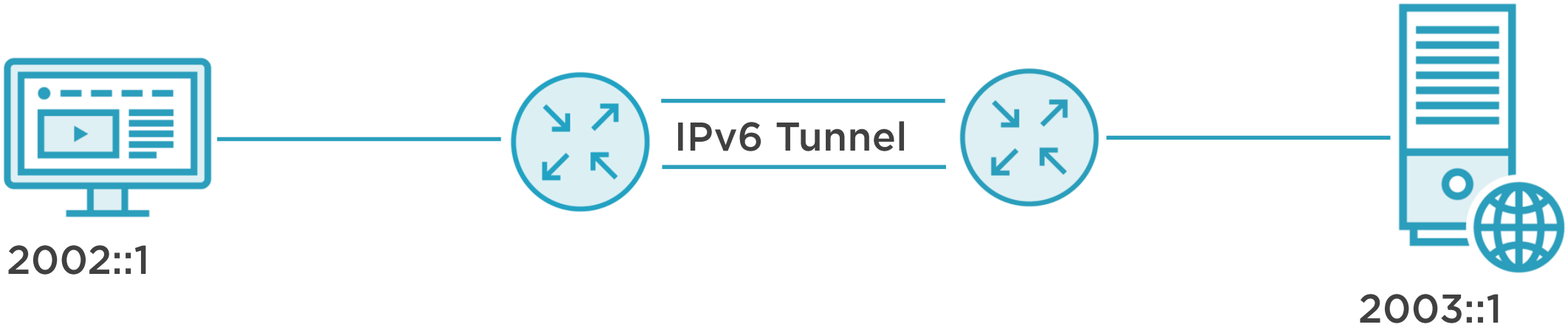
The IPv6 Address

Link Local Address Range: fe80::/64

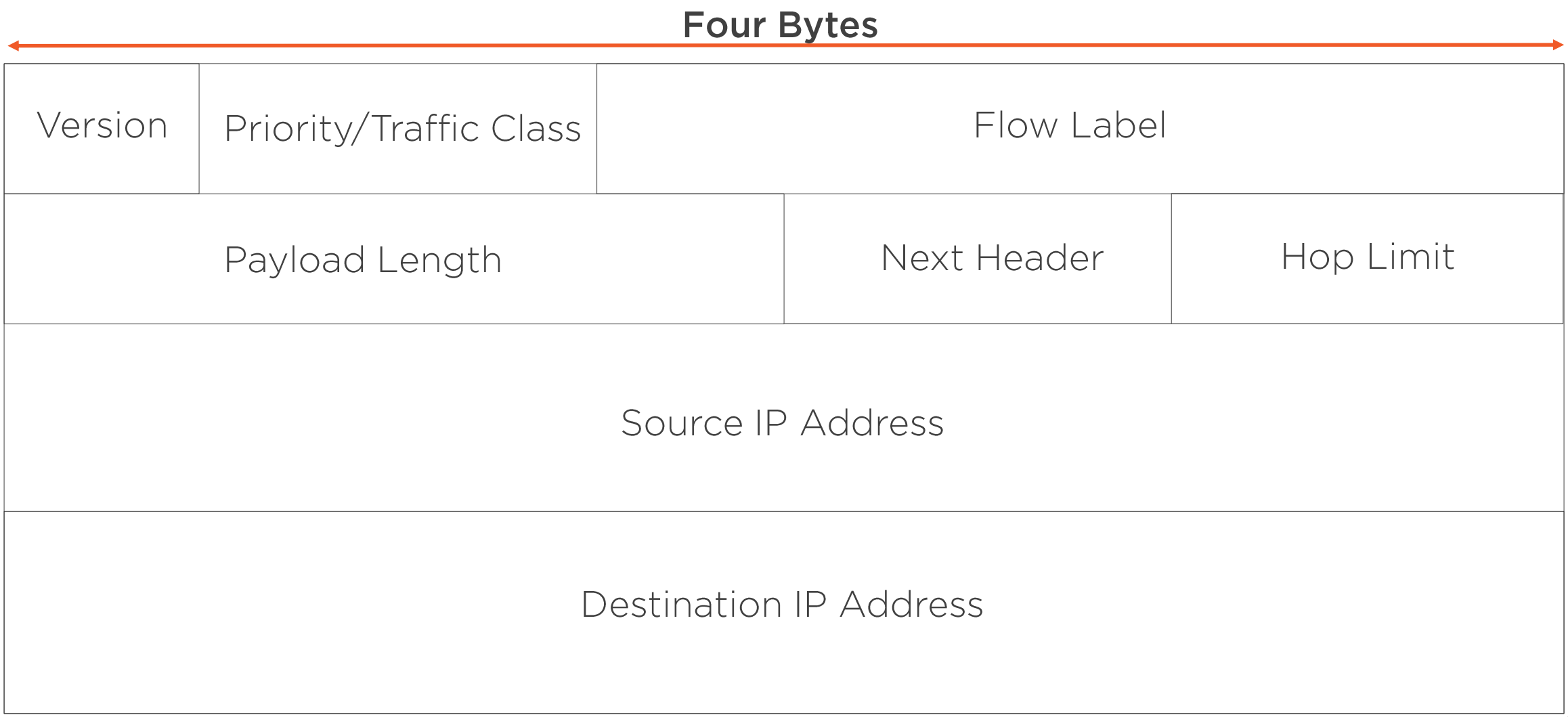
Global Address Range: 2000::/3

Unique Local Address Range: fc00::/7

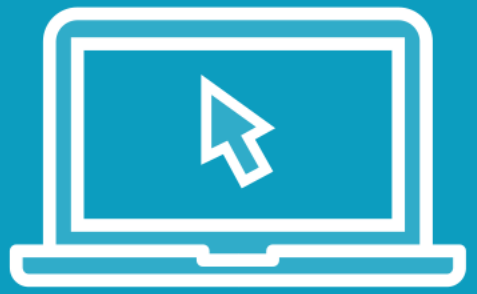
IPv6 Today – IPv4 Across IPv6



IPv6 Header Structure



Demo



Analyzing IPv6 with Wireshark