IP security

CS642: Computer Security

Moving up the network stack

Fragmentation

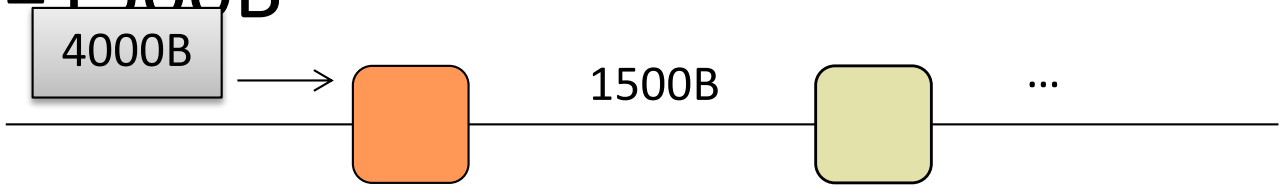
DoS attacks, Networking telescopes

A closer look at fragmentation

- Every link has a “Maximum Transmission Unit” (MTU)
  - largest number of bits it can carry as one unit
- A router can split a packet into multiple “fragments” if the packet size exceeds the link’s MTU
- Must reassemble to recover original packet

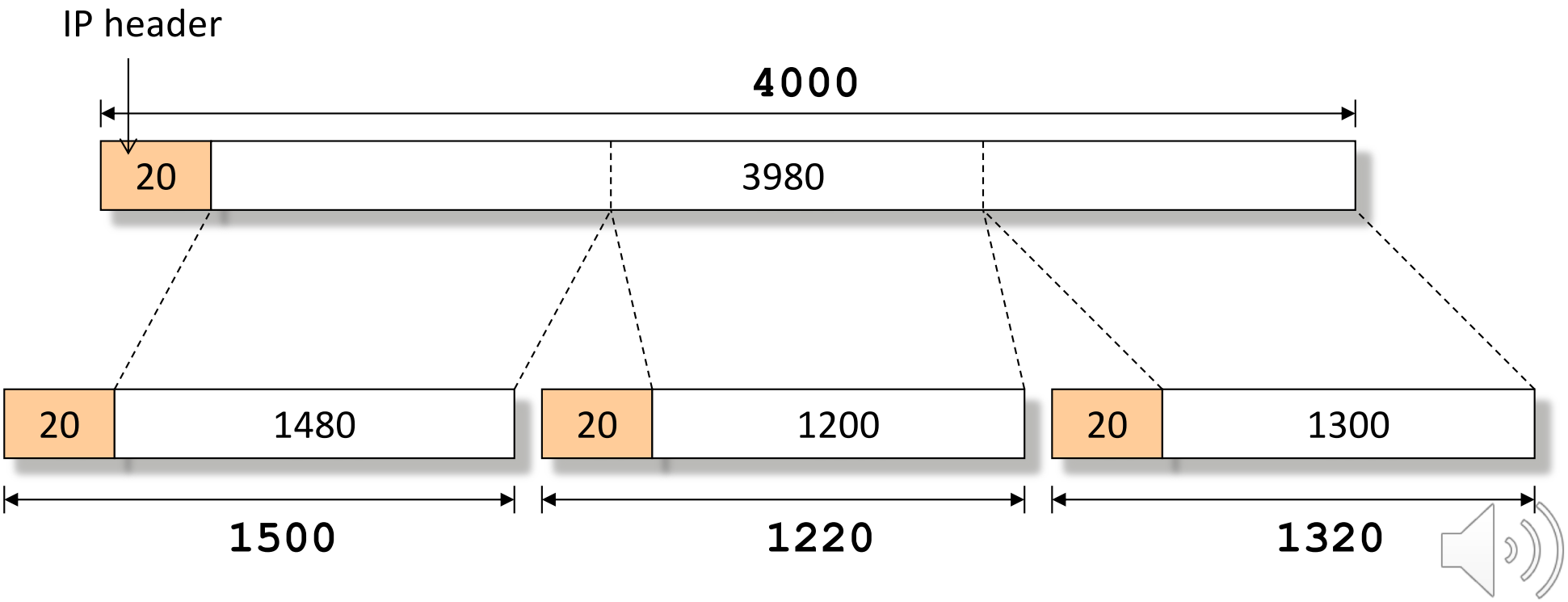
Example of fragmentation

- A 4000 byte packet crosses a link w/ MTU=1500B

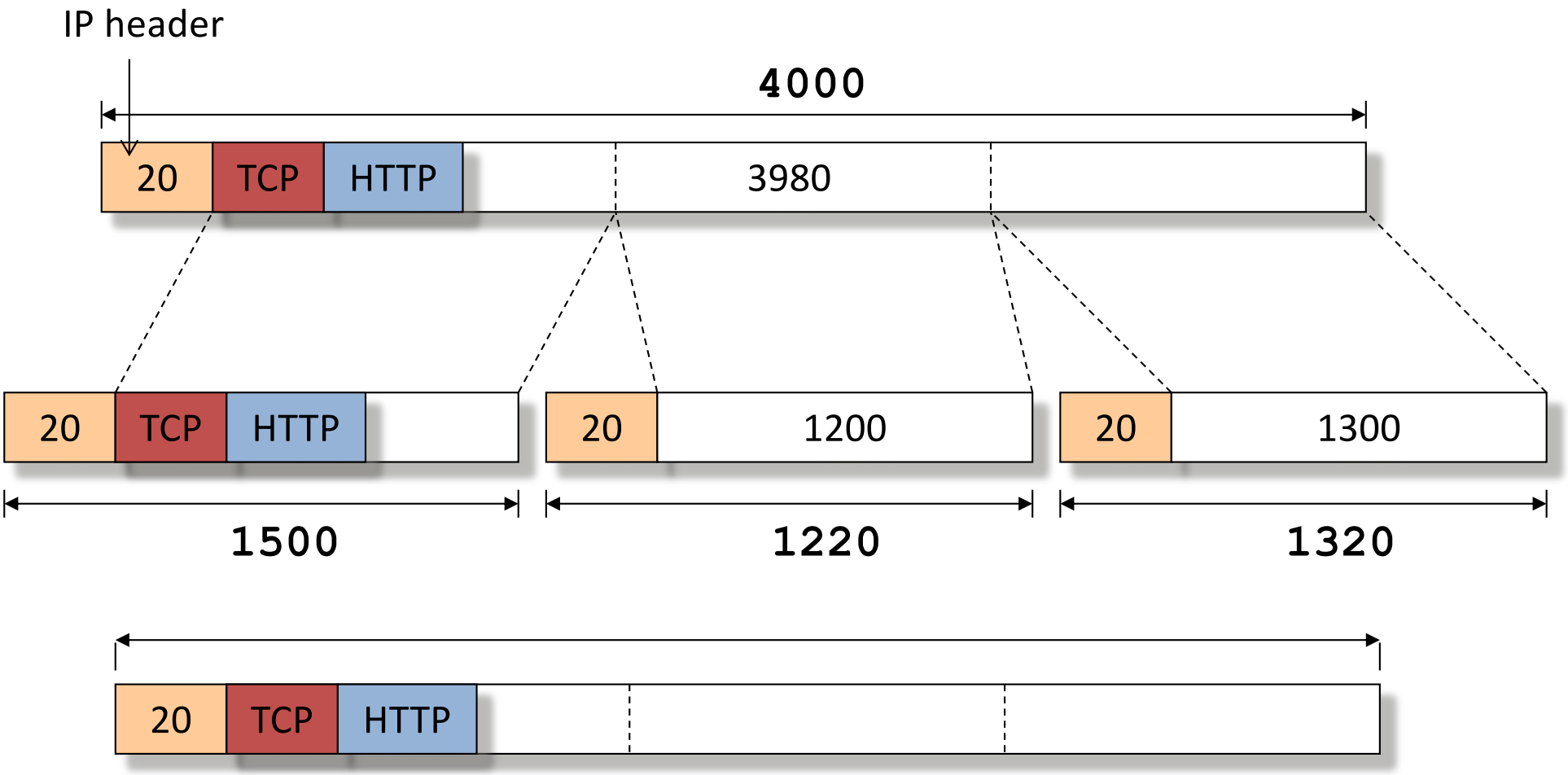


Example of fragmentation

- A 4000 byte packet crosses a link w/ MTU=1500B



Why reassemble?



Must reassemble before sending the packet to the higher layers

A few considerations

- Where to reassemble?
- Fragments can get lost
- Fragments can follow different paths
- Fragments can get fragmented again

Where should reassembly occur?

Classic case of E2E principle

- At next-hop router imposes burden on network
  - *complicated reassembly algorithm*
  - *must hold onto fragments/state*
- Any other router may not work
  - *Fragments may take different paths*
- Little benefit, large cost for network reassembly

- Hence, reassembly is done at the destination

Reassembly: what fields?

- Need a way to identify fragments of the packet
  → introduce an identifier

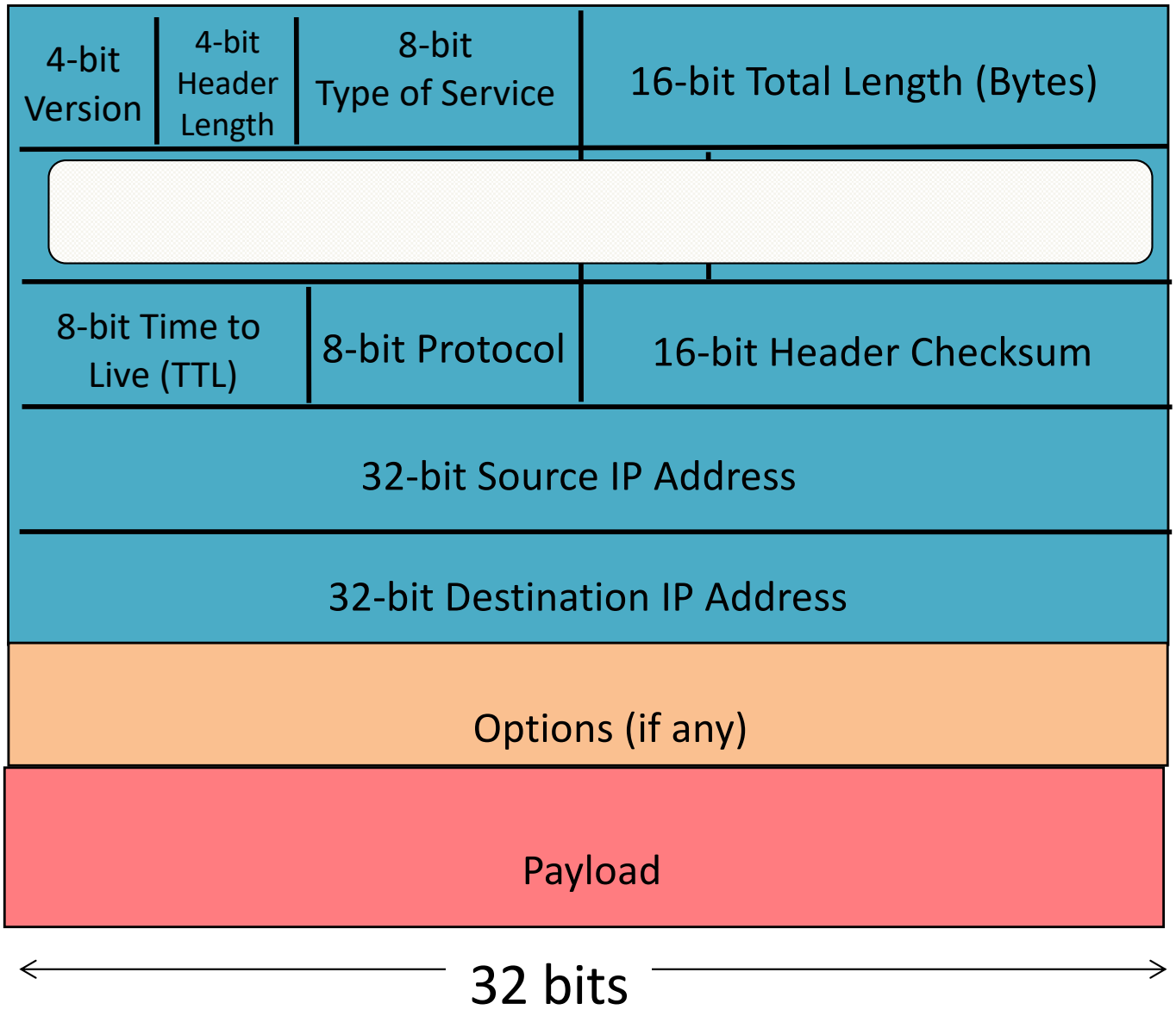
- Fragments get lost?
  → need some form of sequence number or offset?

- Sequence numbers / offset
  - How do I know when I have them all? (need max seq# / flag)
  - What if a fragment gets re-fragmented?

IPv4's fragmentation fields

- **Identifier**: which fragments belong together
- **Flags**:
  - **R**eserved: ignore
  - **D**F: don't fragment
    - *may trigger error message back to sender*
  - **M**F: more fragments coming
- **Offset**: portion of original payload this fragment contains
  - in 8-byte units

IP Packet Structure

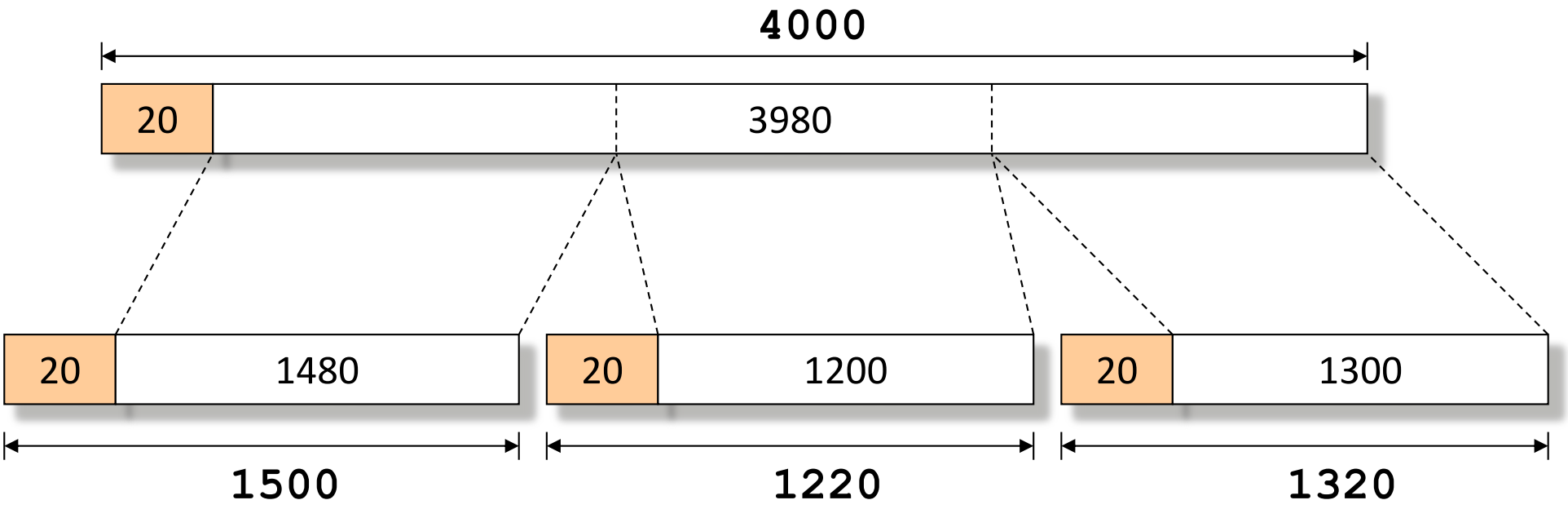


Why This Works

- Fragment without MF set (last fragment)
  - Tells host which are the last bits in original payload
- All other fragments fill in holes
- Can tell when holes are filled, regardless of order
  - Use offset field
- Q: why use a byte-offset for fragments rather than numbering each fragment?
  - Allows further fragmentation of fragments

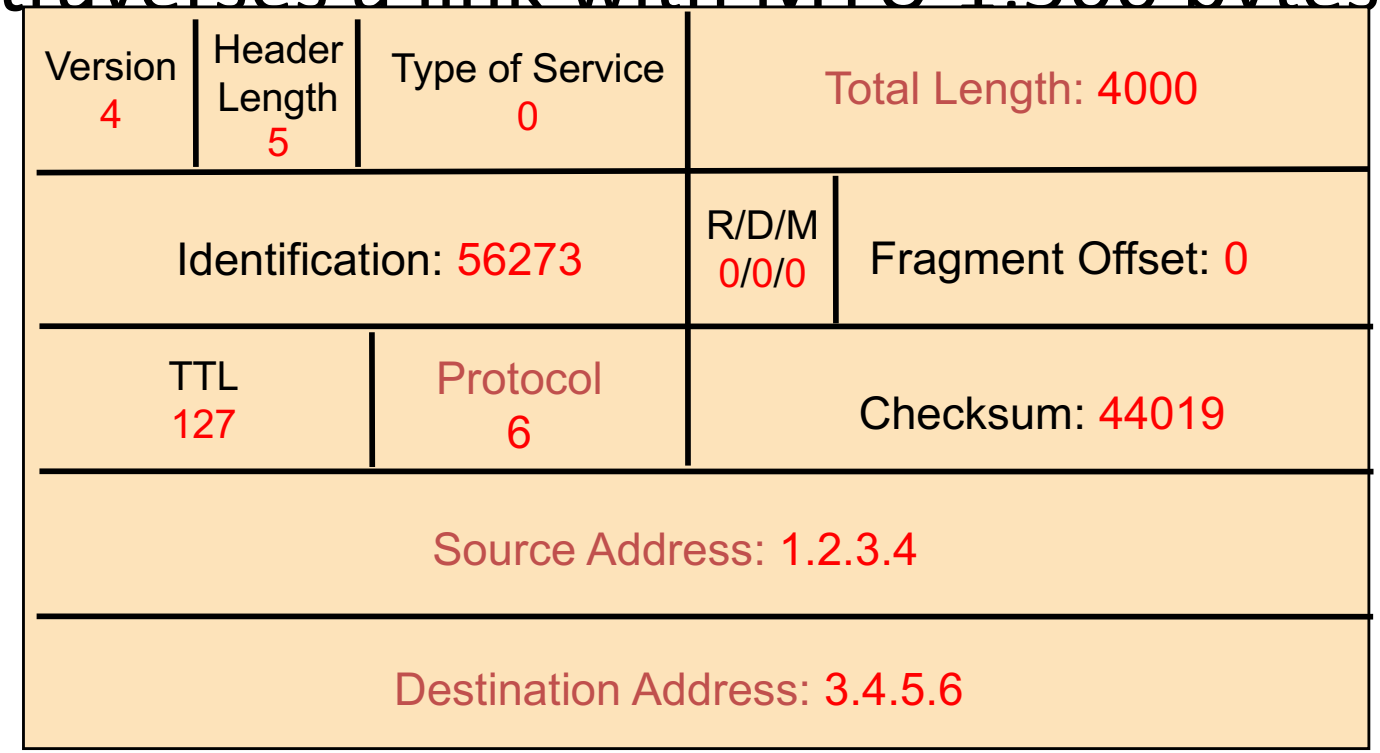
Example of fragmentation (contd.)

- Packet split into 3 pieces
- Example:



Example of fragmentation, contd.

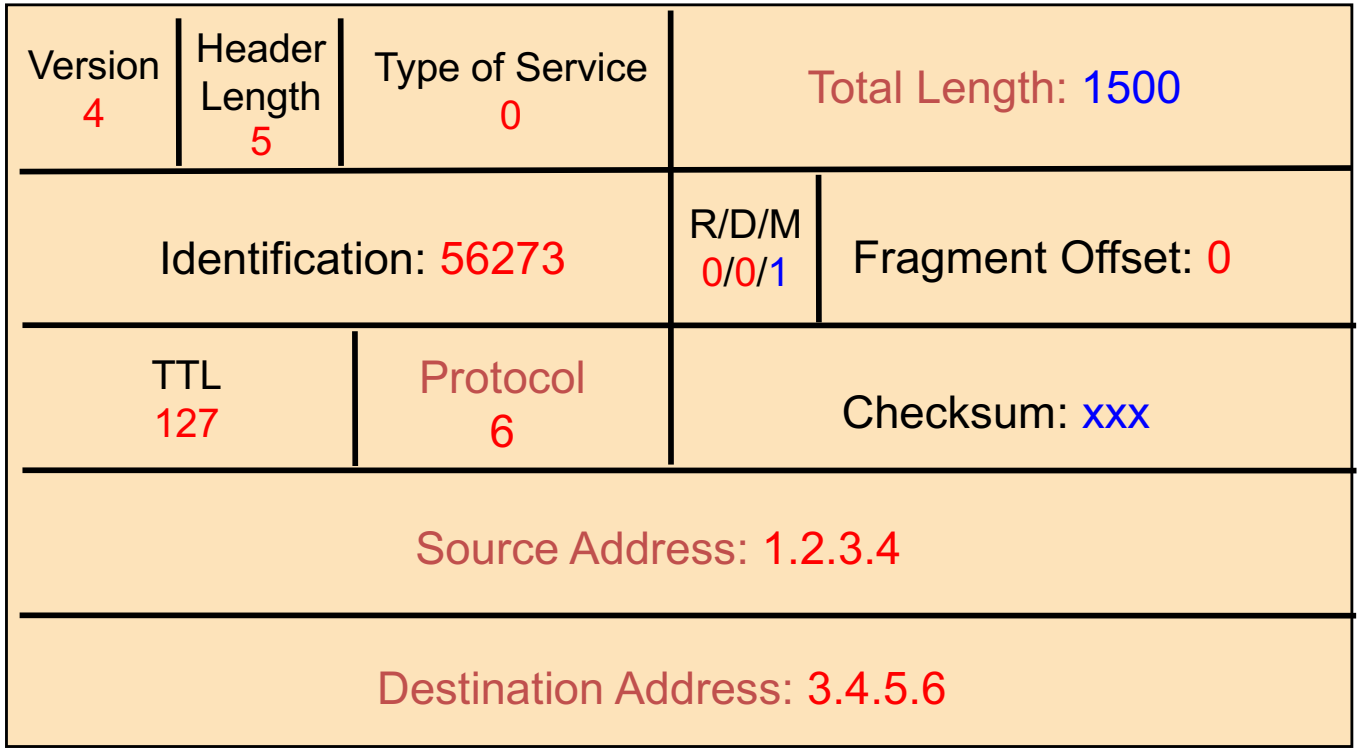
- 4000 byte packet from host 1.2.3.4 to 3.4.5.6 …
- … traverses a link with MTU 1,500 bytes



(3980 more bytes of payload here)

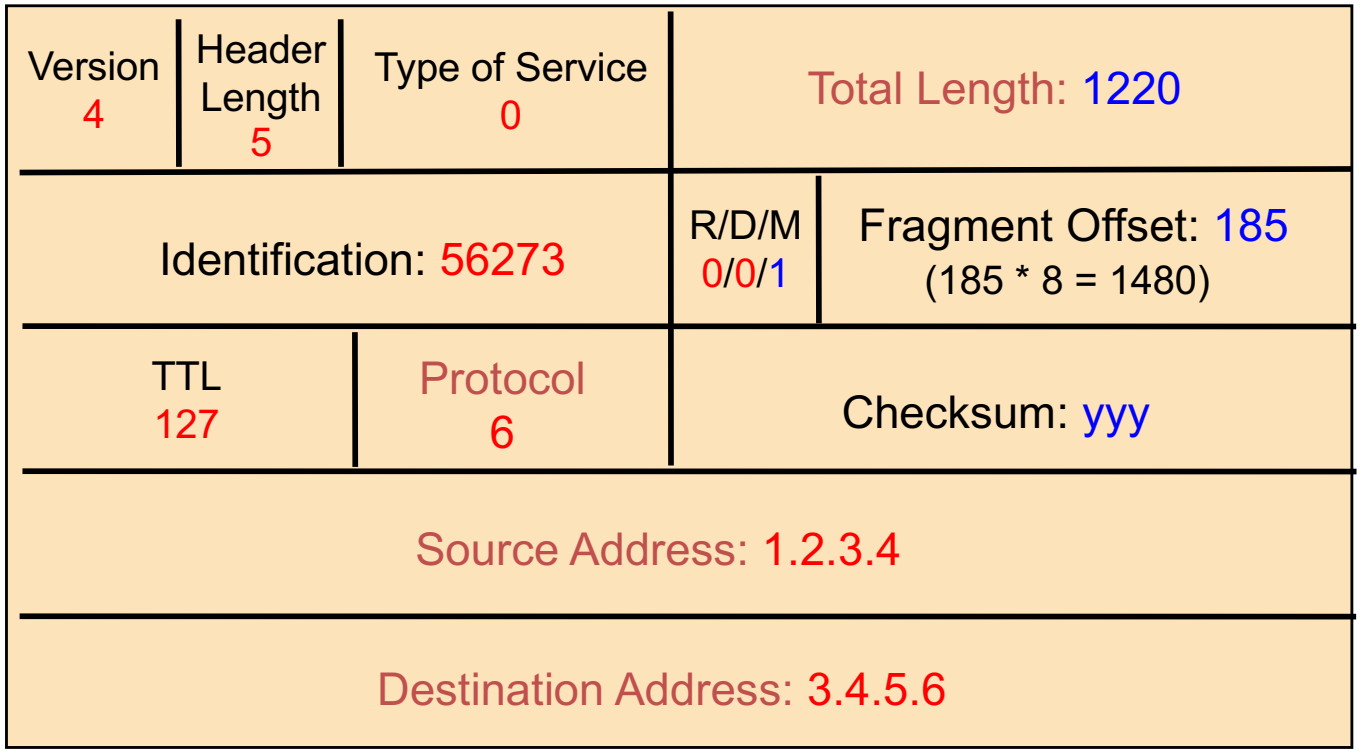
Example of fragmentation, contd.

- Datagram split into 3 pieces. Possible first piece:



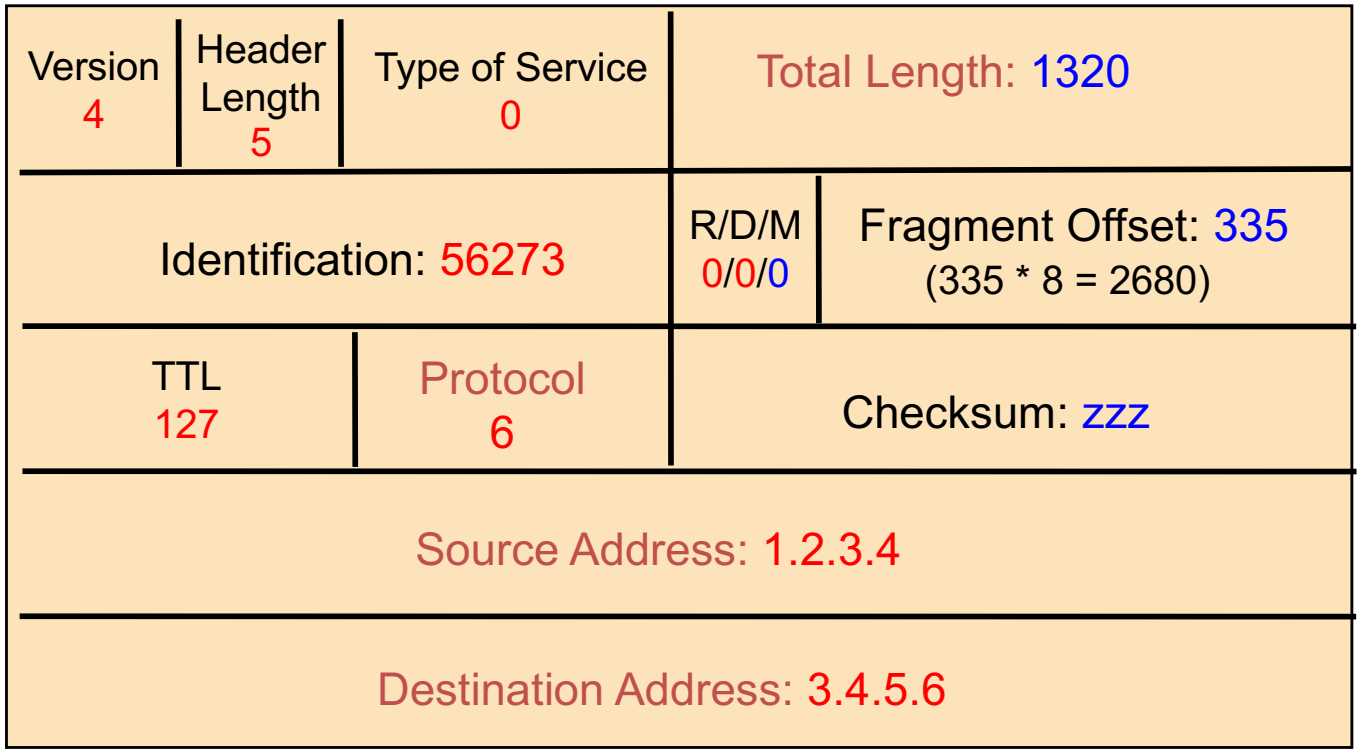
Example of fragmentation, contd.

- Possible second piece: Frag#1 covered 1480bytes



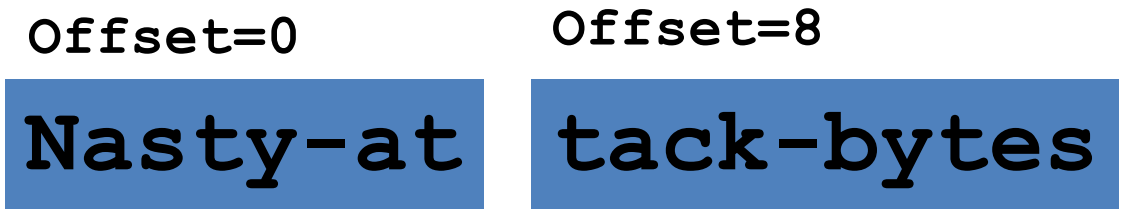
Example of fragmentation, contd.

- Possible third piece: 1480+1200 = 2680

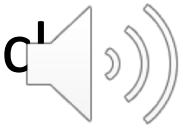


Security Implications of Fragmentation?

- Allows **evasion** of network monitoring/enforcement
- E.g., split an attack across multiple fragments
  - Packet inspection won't match a "signature"

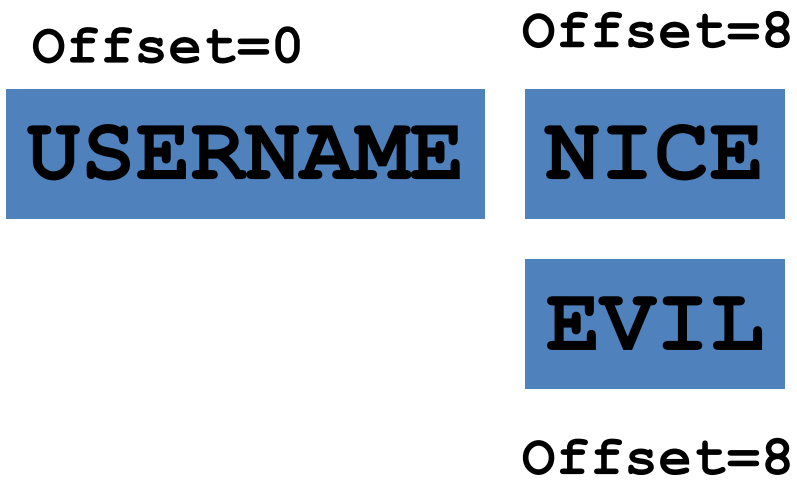


- Monitor must remember previous fragments
  - But that costs **state**, which is another vector of attac



More Fragmentation Attacks

- What if 2 overlapping fragments are inconsistent?

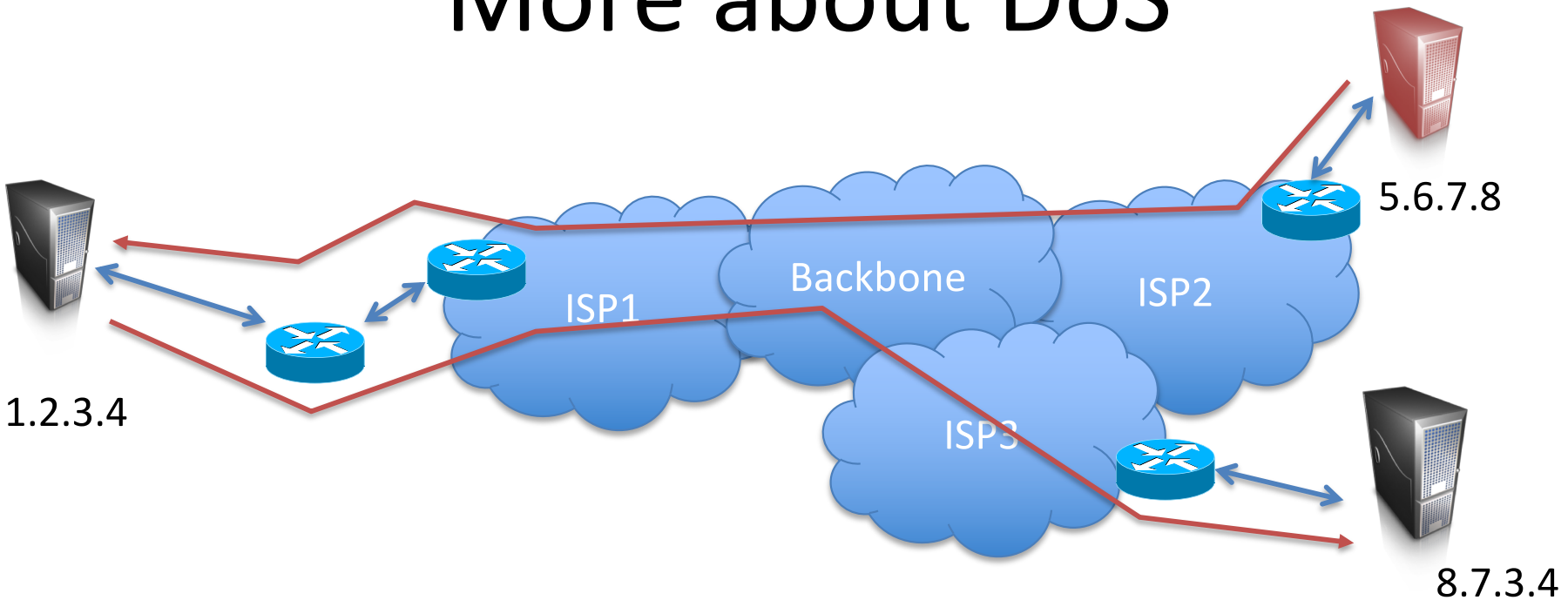


- How does network monitor know whether receiver sees **USERNAME NICE** or **USERNAME EVIL**?

Even More Fragmentation Attacks

- What happens if attacker doesn't send all of the fragments in a packet?
- Receiver (or firewall) winds up holding the ones they receive for a long time
  - **State-holding** attack

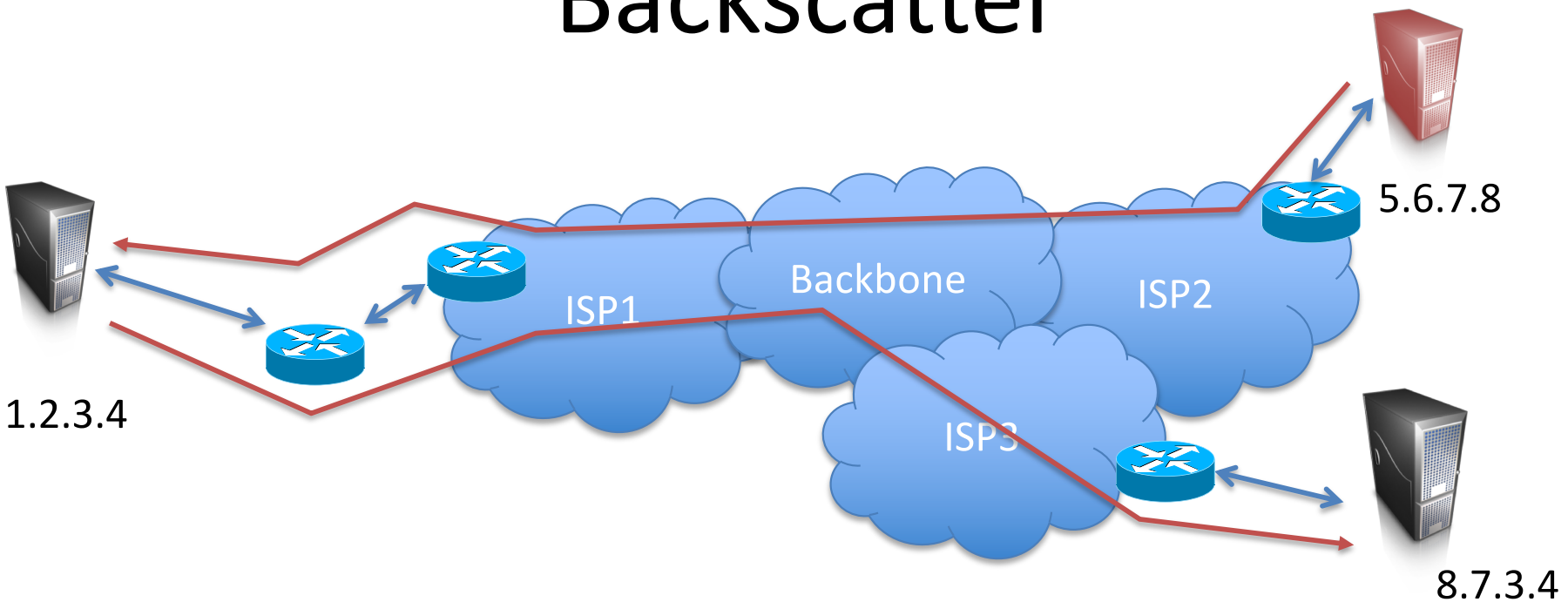
More about DoS



DoS is still a big problem

How big?

Backscatter



Can we measure the level of DoS attacks on Internet?

- Suppose 5.6.7.8 spoofs 8.7.3.4 when attacking 1.2.3.4
- If we can measure spurious packets at 8.7.3.4, we might infer something about DoS at 1.2.3.4

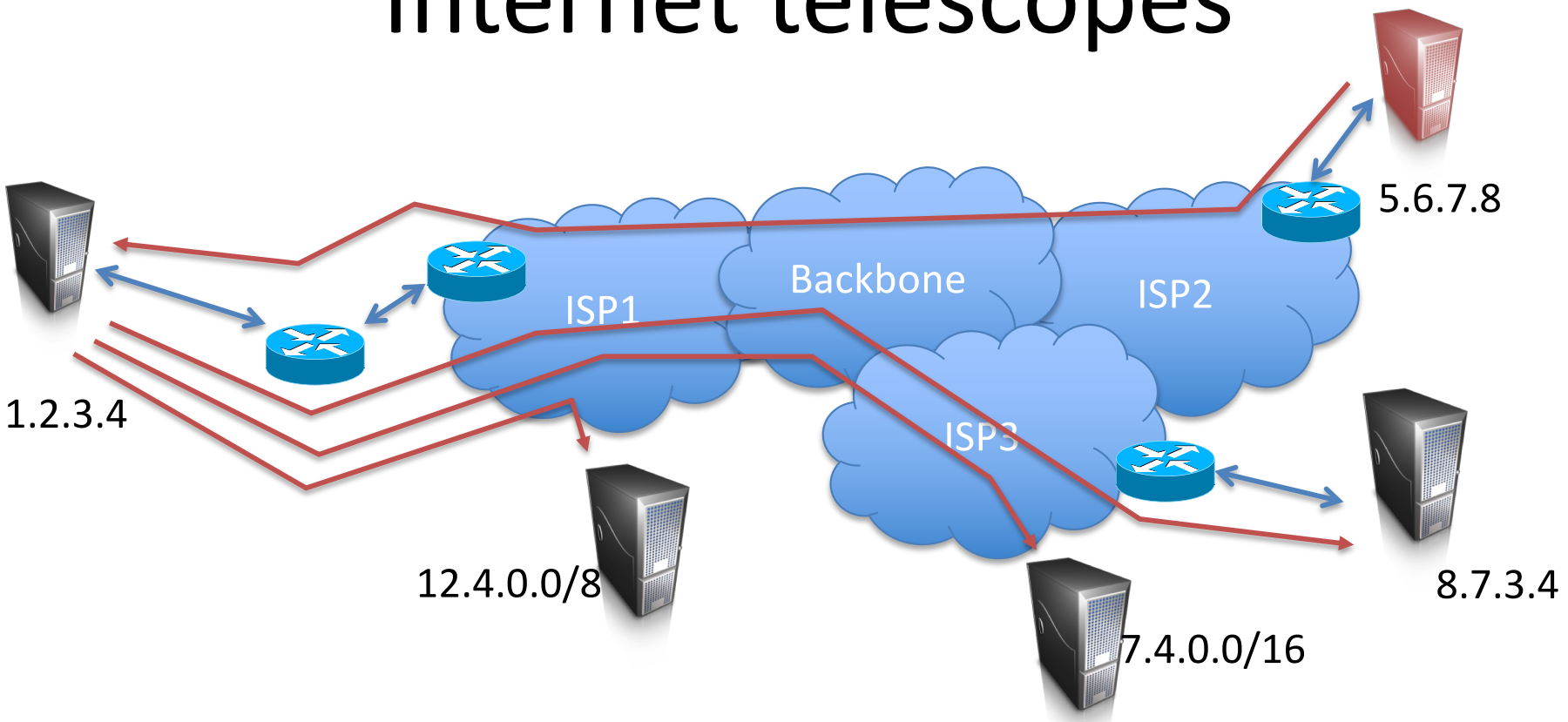
Types of responses to floods

Packet sent	Response from victim
TCP SYN (to open port)	TCP SYN/ACK
TCP SYN (to closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	no response
TCP NULL	TCP RST (ACK)
ICMP ECHO Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP pkt (to open port)	protocol dependent
UDP pkt (to closed port)	ICMP Port Unreach
...	...

Table 1: A sample of victim responses to typical attacks.

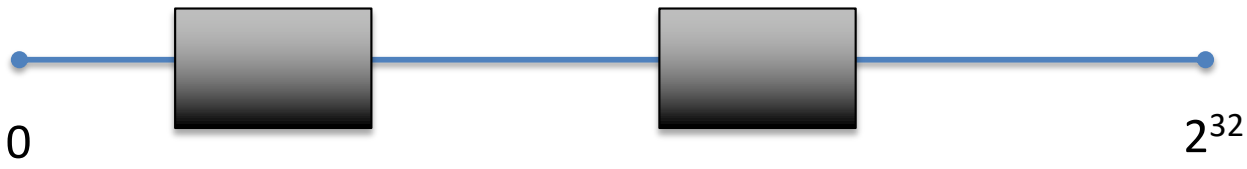
From Moore et al., “Inferring Internet Denial-of-Service Activity”

Internet telescopes



Setup some computers to watch traffic sent to darknets

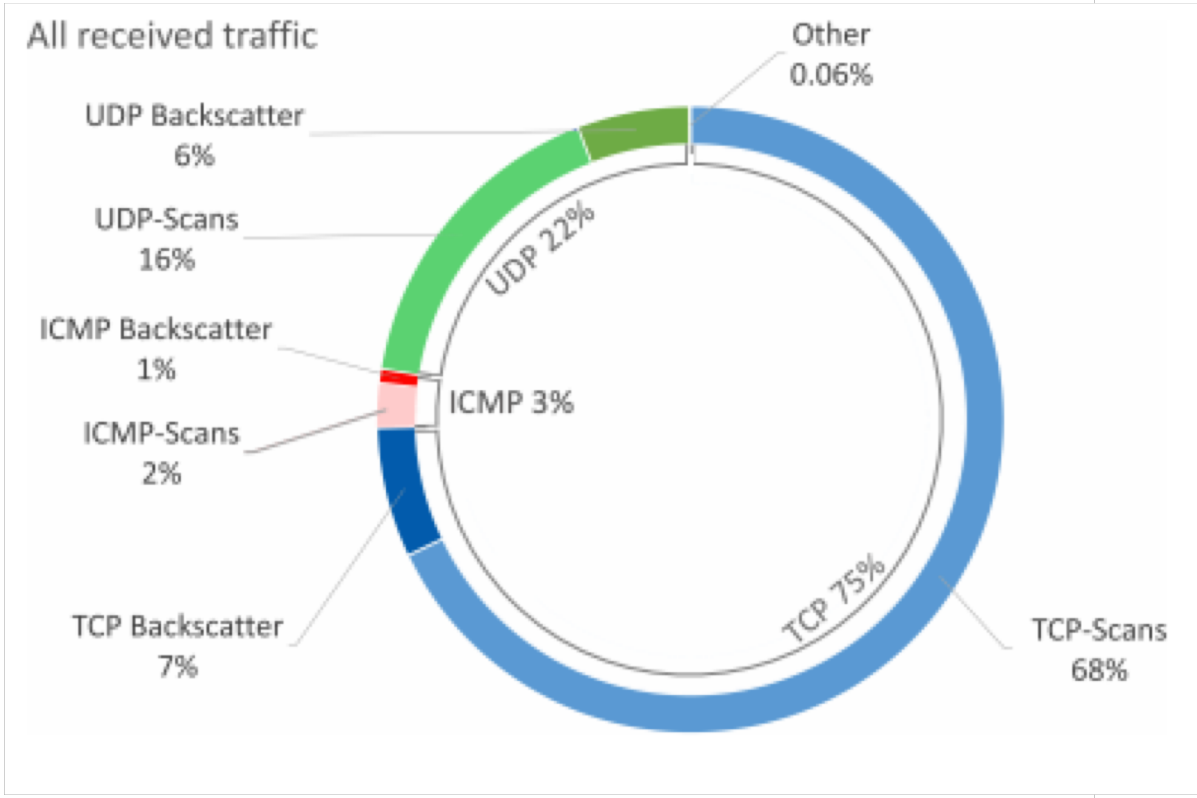
- Darknet = unused routable space

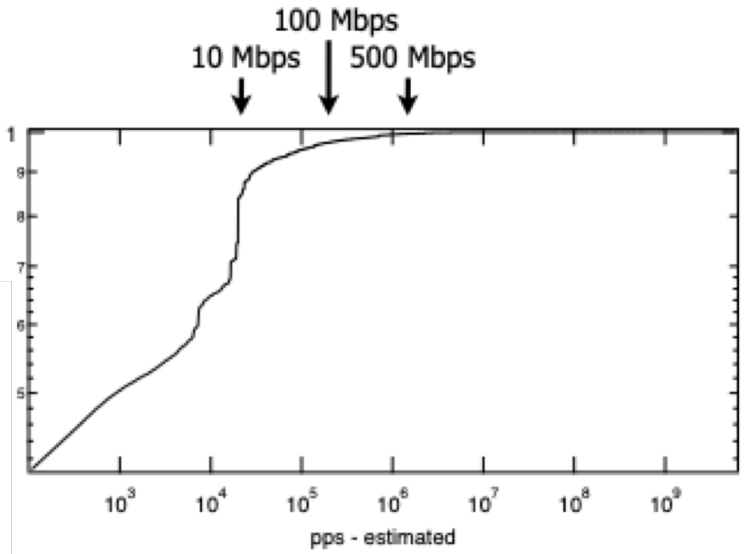


2001: 400 SYN attacks per week

2008: 4425 SYN attacks per 24 hours

Received traffic to idle machine (2017)





ıre 6: Cumulative density function of attack sizes.

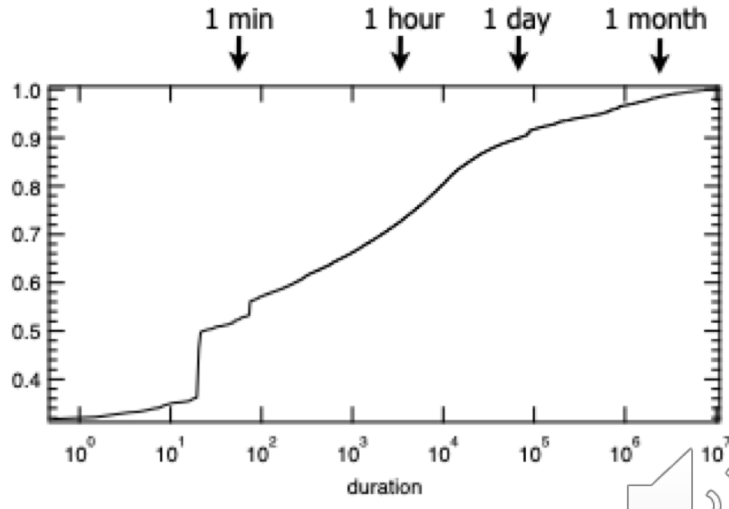
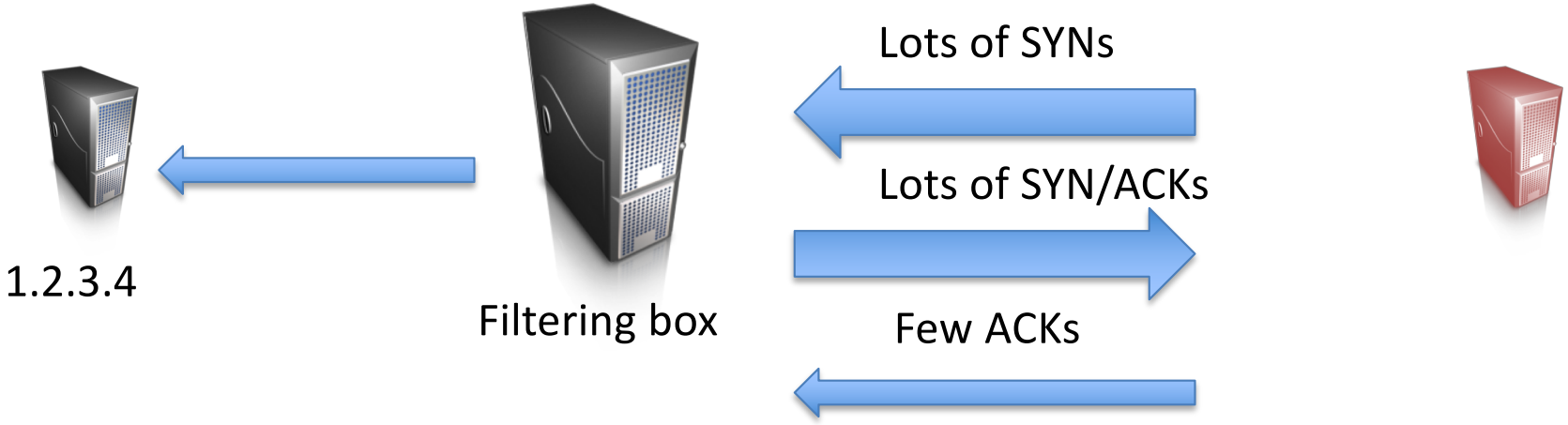


Figure 7: Cumulative density function of attack duration.

Preventing DoS: Akamai approach



Just need a beefy box to help with filtering.
Companies pay Prolexic to do it for them