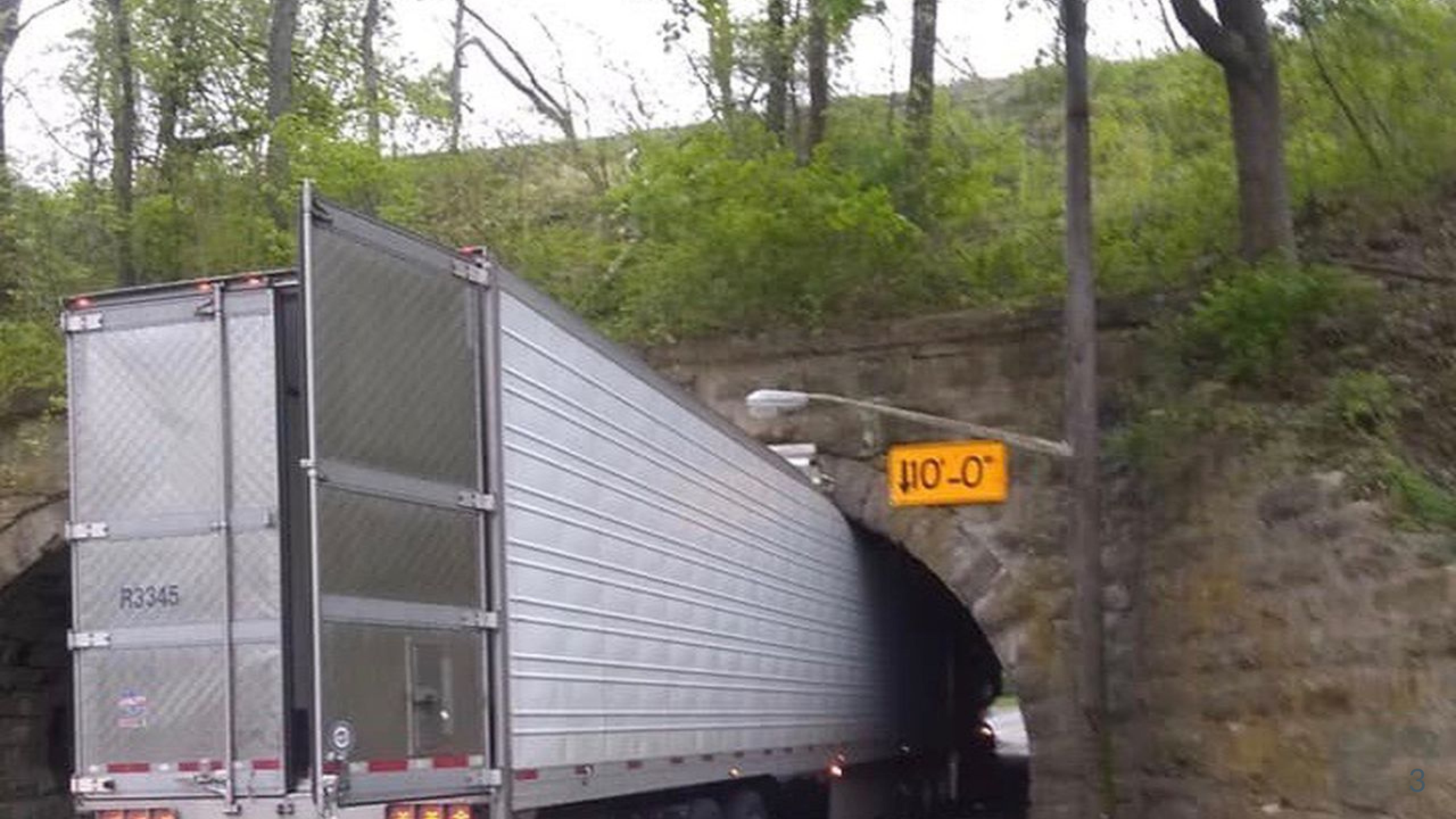
IP Fragmentation

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

Maximum Transmission Unit

The maximum transmission unit (MTU) is the size of the largest protocol data unit (PDU) that can be communicated in a single network layer transaction.

Or you can consider MTU as the "bandwidth" of a link.


↓10'-0"
R3345

Measure MTU of a Path

To use `ping` with the following parameters to ping a gateway or a destination host.

- `-M do`: Don't Fragment (DF) = 1
- `-s`: Size of the packet
- `-c`: Number of PING packets

Measure MTU of a Path

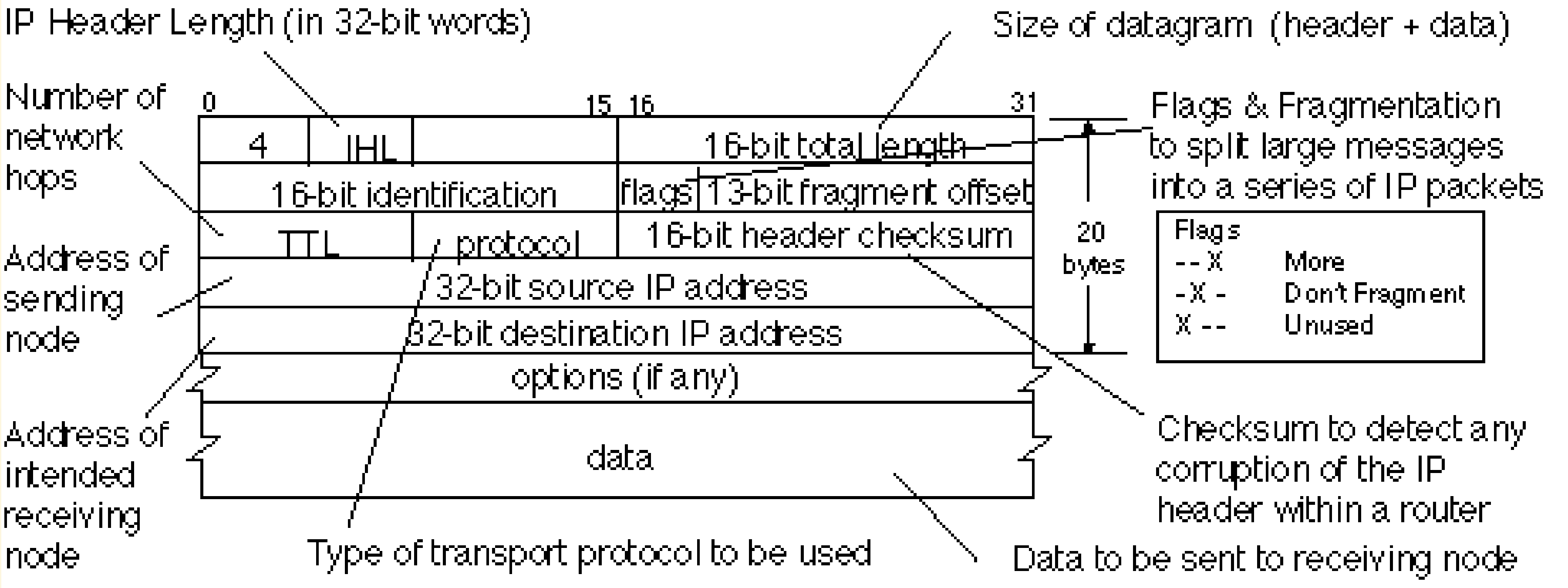
```
[jzhang@DESKTOP-DSVPHPI system32]$ping www.cnn.com -c 10 -M do -s 8000
PING cnn-tls.map.fastly.net (146.75.79.5) 8000(8028) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
```

```
[jzhang@DESKTOP-DSVPHPI system32]$ping www.cnn.com -c 10 -M do -s 1472
PING cnn-tls.map.fastly.net (146.75.79.5) 1472(1500) bytes of data.
1480 bytes from 146.75.79.5 (146.75.79.5): icmp_seq=1 ttl=54 time=28.0 ms
1480 bytes from 146.75.79.5 (146.75.79.5): icmp_seq=2 ttl=54 time=27.4 ms
1480 bytes from 146.75.79.5 (146.75.79.5): icmp_seq=3 ttl=54 time=26.9 ms
```

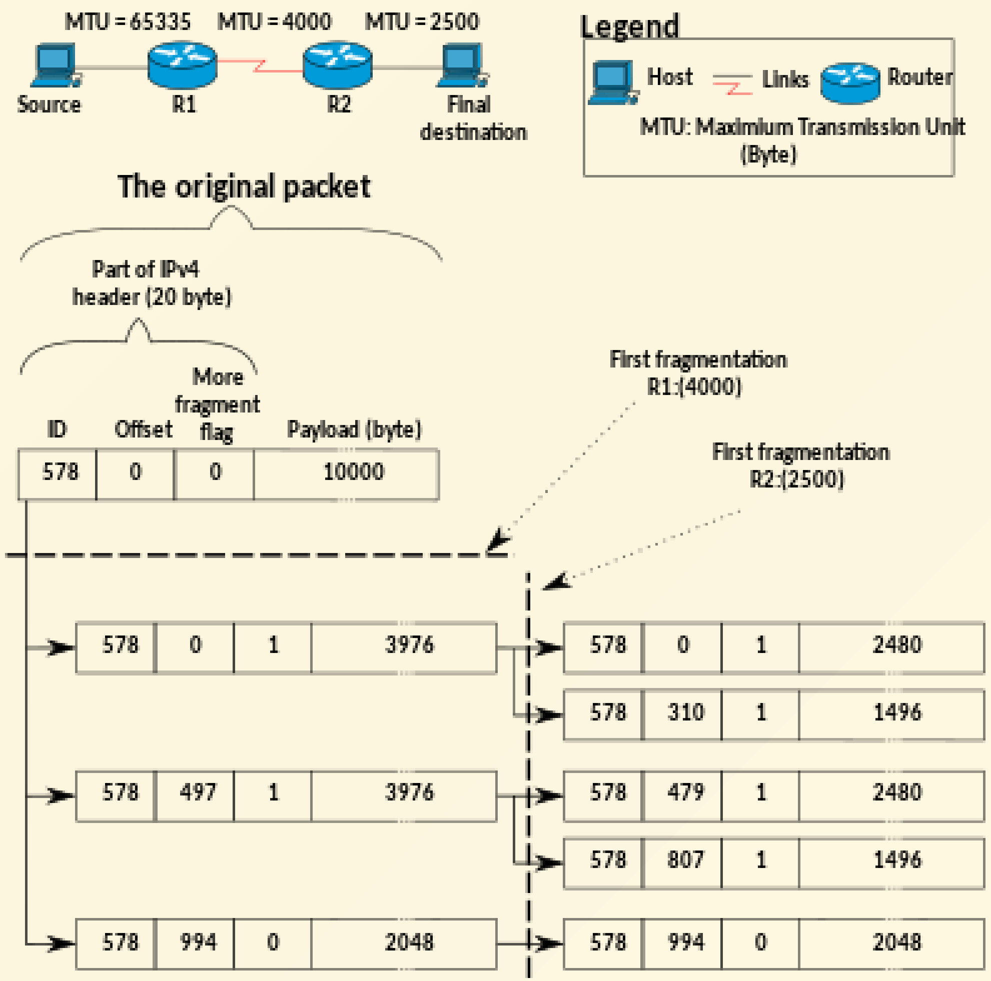
IP Fragmentation

IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size.

IP Fragmentation


IP Header Length (in 32-bit words)
Size of datagram (header + data)
Number of network hops
0
15 16
31
4
IHL
16-bit total length
16-bit identification
flags
13-bit fragment offset
TTL
protocol
16-bit header checksum
32-bit source IP address
32-bit destination IP address
options (if any)
data
20 bytes
Flags & Fragmentation to split large messages into a series of IP packets
Flags
- - X More
- X - Don't Fragment
X - - Unused
Address of sending node
Address of intended receiving node
Checksum to detect any corruption of the IP header within a router
Type of transport protocol to be used
Data to be sent to receiving node

An Example of IPv4 Fragmentation


MTU = 65335
MTU = 4000
MTU = 2500
Source
R1
R2
Final destination
Legend
Host
Links
Router
MTU: Maximium Transmission Unit (Byte)
The original packet
Part of IPv4 header (20 byte)
First fragmentation R1:(4000)
First fragmentation R2:(2500)

ID	Offset	More fragment flag	Payload (byte)
578	0	0	10000

ID	Offset	More fragment flag	Payload (byte)
578	0	1	3976
578	497	1	3976
578	994	0	2048

ID	Offset	More fragment flag	Payload (byte)
578	0	1	2480
578	310	1	1496
578	479	1	2480
578	807	1	1496
578	994	0	2048

Lab

Trace

A Few Questions

- Who does fragmentation?
  - A router can fragment a packet into multiple fragments if the packet size exceeds the link's MTU.
  - A sender can do it even if the packet size is smaller than the link's MTU. So the attacker can do it too.

A Few Questions

Who will de-fragmentation the fragments?

- The end host. This is a classic case of the end-to-end design principle of the Internet.

Why does not a router reassemble fragments?

- Needs to be stateful: too expensive for core routers.
- Fragments may traverse through different paths.

Security Concerns

Evading Network-Based Intrusion Detection Systems

- An attacker can split an IP packet that carries malicious content into a few fragments to disrupt the matching with a detection "signature". IDS can solve it by reassembling fragments, which is very expensive.

Security Concerns

Evading Network-Based Intrusion Detection Systems

- An attacker can create overlapping fragments, for example [fragment1-offset-0: be], [fragment1-offset-2: good], and [fragment1-offset-2: evil]. Then the IDS cannot decide whether the receiver will see "be good" or "be evil" unless it knows how the receiver uses it.

Security Concerns

State-Holding Attack

An attacker can send some fragments without sending other fragments. The receiver will need to hold received fragments for a long time, aiming at waiting for other fragments.