Network Layer: Attacks and Countermeasures

CYBR371: System and Network Security, (2024/T1)

Arman Khouzani, Mohammad Nekooei

Slides modified from "Masood Mansoori"

20 March, 2024

Victoria University of Wellington – School of Engineering and Computer Science

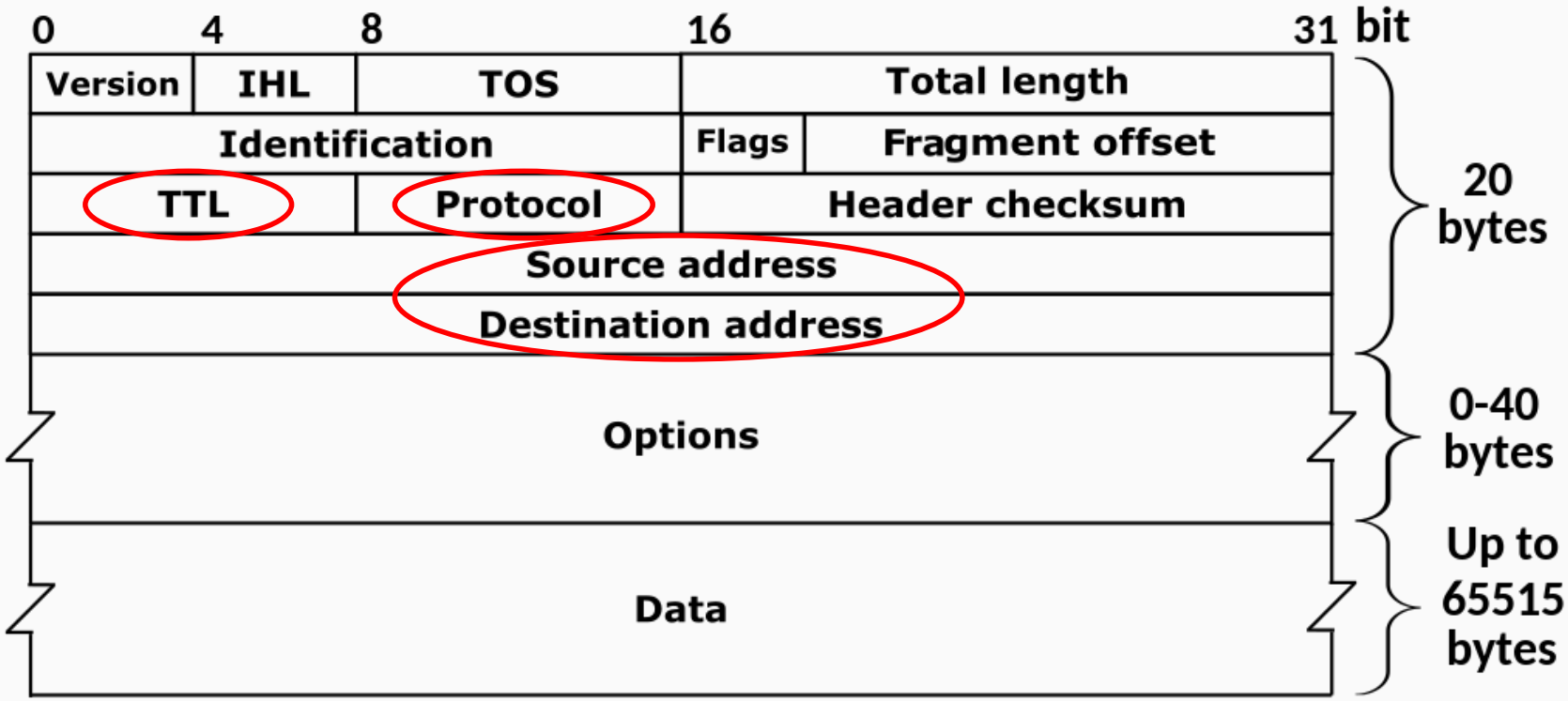

IP

Network Layer - IP Protocol

Basic functions:

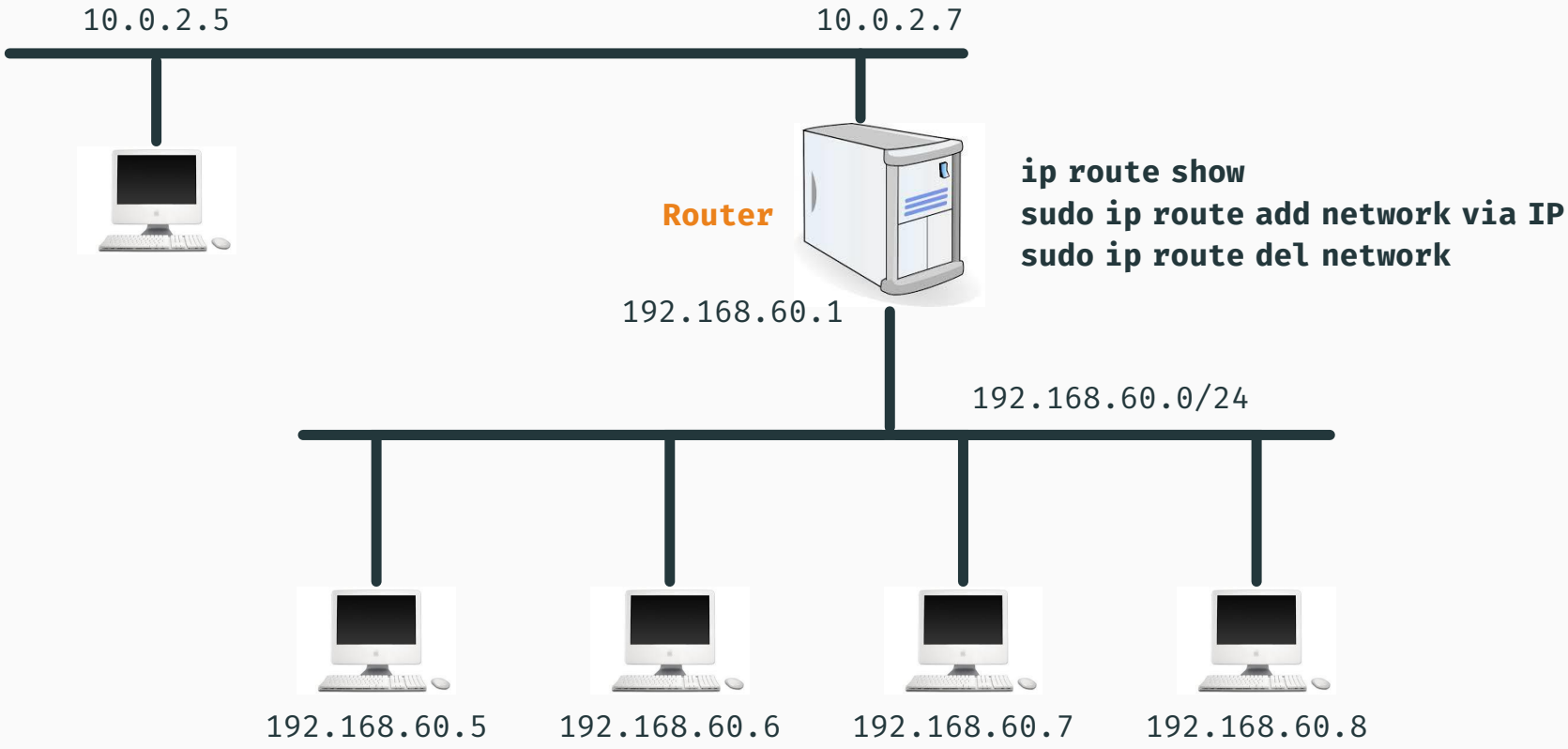
- Routing: figuring out which of the available interfaces should be used to forward an incoming packet.
- Passing packets to the transport layer at the destination host.
- Proving error detection and diagnostic capability
  - only for the IP header, not the payload!
  - IP is “best effort”

IP Header


0
4
8
16
31
bit
Version
IHL
TOS
Total length
Identification
Flags
Fragment offset
TTL
Protocol
Header checksum
Source address
Destination address
20 bytes
Options
0-40 bytes
Data
Up to 65515 bytes

Routing

Both routers and network hosts have routing tables that help direct traffic.



Packet Spoofing with Scapy

Constructing packet at **10.0.2.5**:

```
>>> a = IP(src='192.168.60.5', dst ='192.168.60.8')
>>> b = UDP(sport='1234', dport ='1020')
>>> c = "Hello World"
>>> pkt = a/b/c
>>> send(pkt, verbose =0)
```

So a machine outside our network is impersonating as a machine within the network.

- **Question:** where does the response go?
- *Hint:* The Internet operates via destination-based routing.

Can this be prevented?

How to Prevent IP Spoofing

At **Switches**:

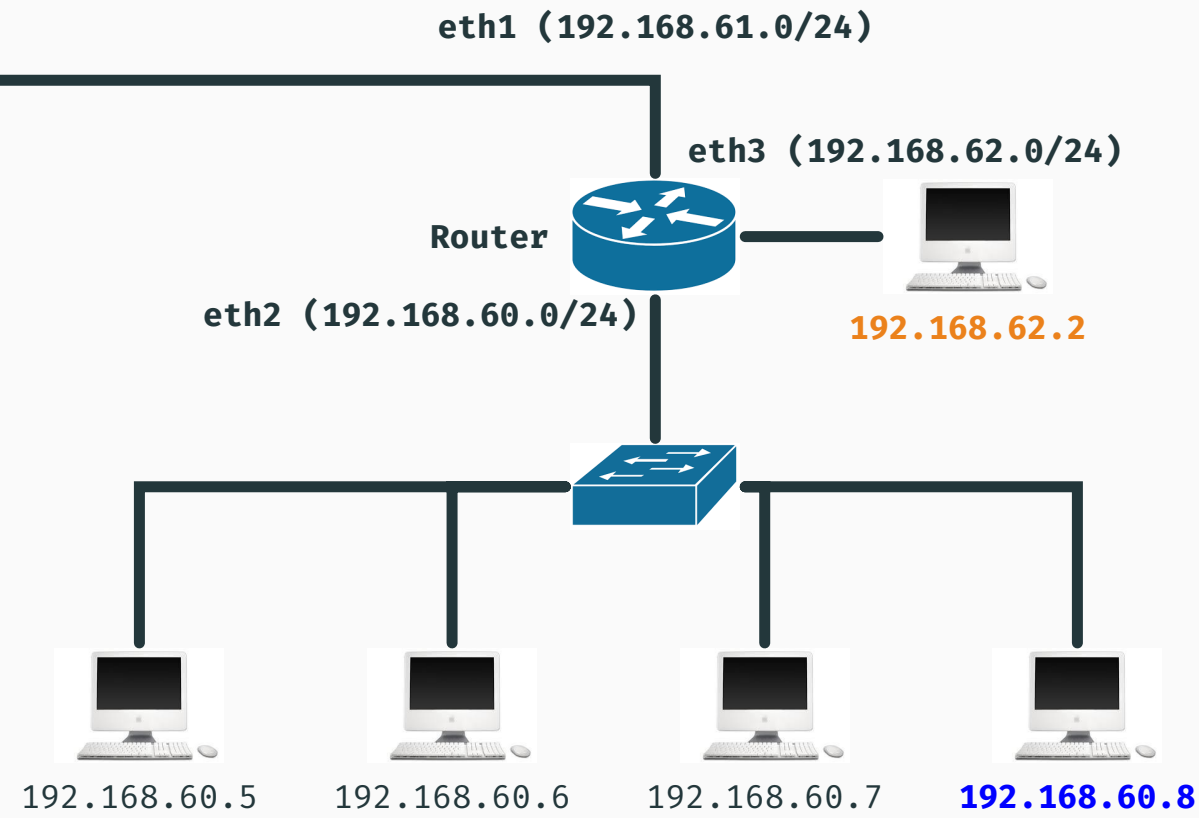
- IP Source Guard: checks the IP address, MAC address, VLAN and interface of each packet against entries stored in the DHCP snooping database.
  - If it does not match a valid entry, the packet is discarded.

At **Routers**:

- (Reverse) Path filtering: When a packet is received, check that:
  - the source ip address is routable; and
  - the route for the source IP points to the interface on which the packet was received.

  otherwise, discard the packet.

Reverse Path Filtering



Spoofed crafted packet from attacker
Source: **192.168.62.2**
Destination: **192.168.60.8**
Interface: **eth1**

Spoofed packet Reply
Source: **192.168.60.8**
Destination: **192.168.62.2**
Interface: **eth3**

ICMP

ICMP

TCP/IP Layers	Protocols
Application	HTTP, DNS, BGP, DNS, NTP
Transport	UDP, TCP
Internet	IP, **ICMP**
Network Interface	Ethernet, ARP

ICMP Messages

Internet Control Message Protocol (ICMP) used to assist with troubleshooting communication problems

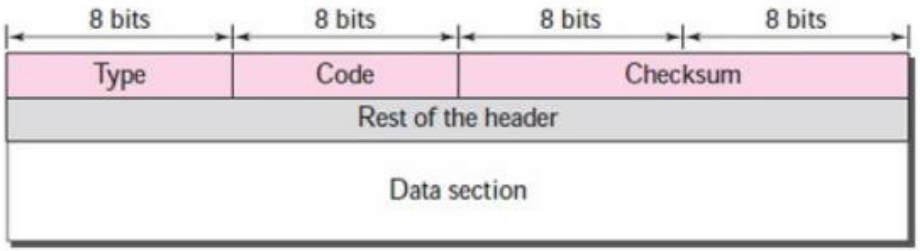
- Ping command uses ICMP to check whether a remote host has connectivity.

Processed at the network layer of the OSI model.

Firewalls or packet filters can be configured to accept or deny certain ICMP packets through the network.

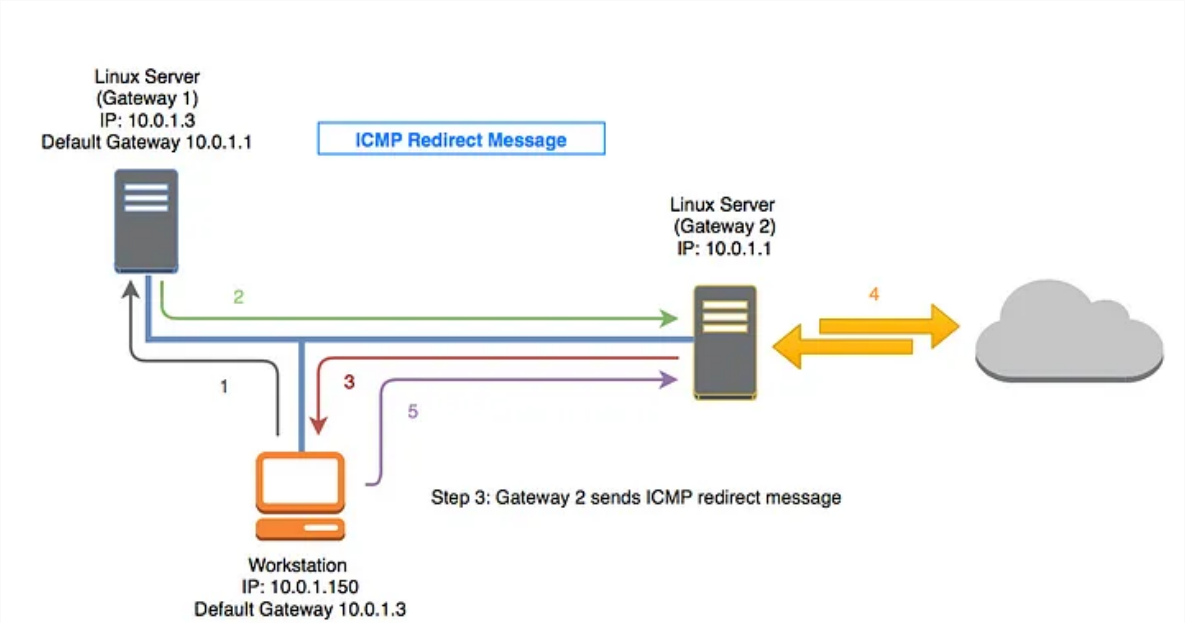
- Some ICMP packets could be used as part of an attack.

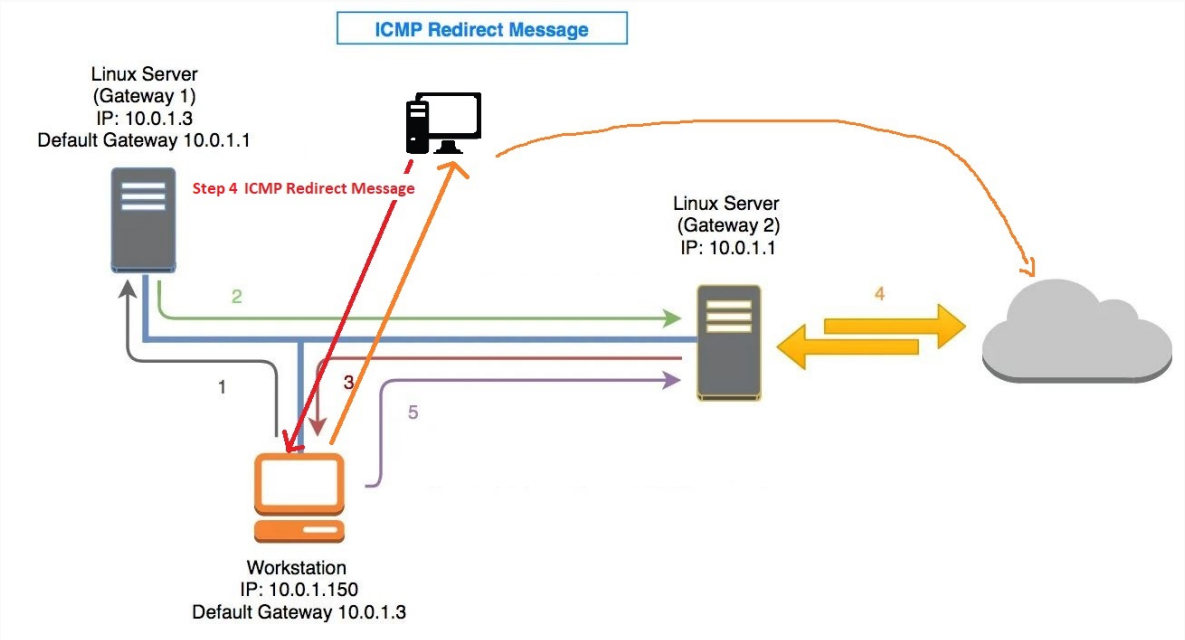
ICMP Header



ICMP type	Name	ICMP type	Name
0	Echo Reply	17	Address Mask Request
3	Destination Unreachable	18	Address Mask Reply
4	Source Quench	30	Traceroute
5	Redirect	31	Datagram Conversion Error
6	Alternate Host Address	32	Mobile Host Redirect
8	Echo	33	IPv6 Where-Are-You
9	Router Advertisement	34	IPv6 I-Am-Here
10	Router Selection	35	Mobile Registration Request
11	Time Exceeded	36	Mobile Registration Reply
12	Parameter Problem	37	Domain Name Request
13	Timestamp	38	Domain Name Reply
14	Timestamp Reply	39	SKIP
15	Information Request	40	Photuris
16	Information Reply	1–2, 7, 19–29, 41–252	Unassigned or Reserved

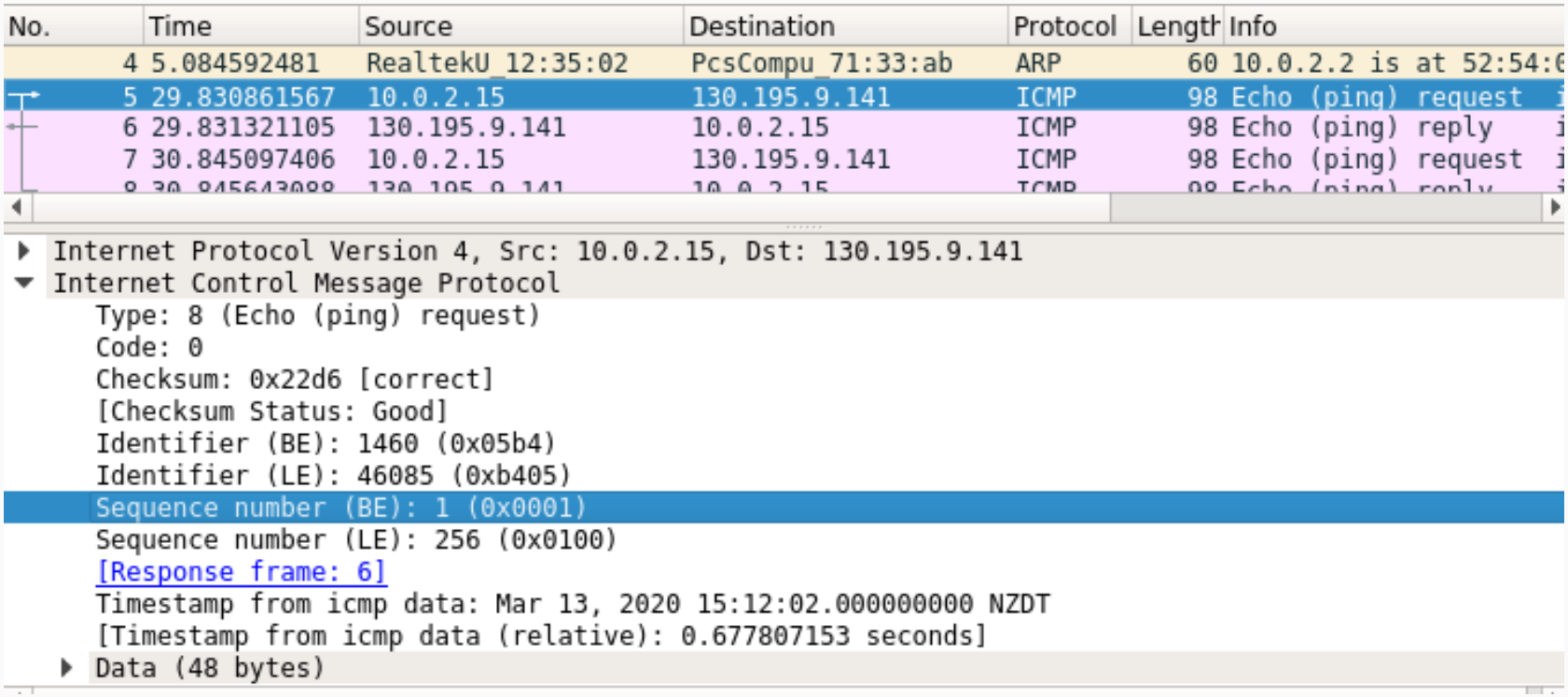
ICMP Redirect Attack





ICMP (Ping) Flood Attacks

- ICMP echo-request (`type 8`) and echo-reply (`type 0`).
- Ping network devices for:
  - Health
  - Connectivity
- ICMP echo-reply requires resources and bandwidth.



ICMP (Ping) Flood Mitigation

- Drop ICMP messages on the router
  - Can result in disabling network activities that use ICMP messages.
    - e.g. ICMP redirect: Used by a router to inform the host of a better gateway for a destination.
- Whitelisting: Expose your network to authorised entities only.

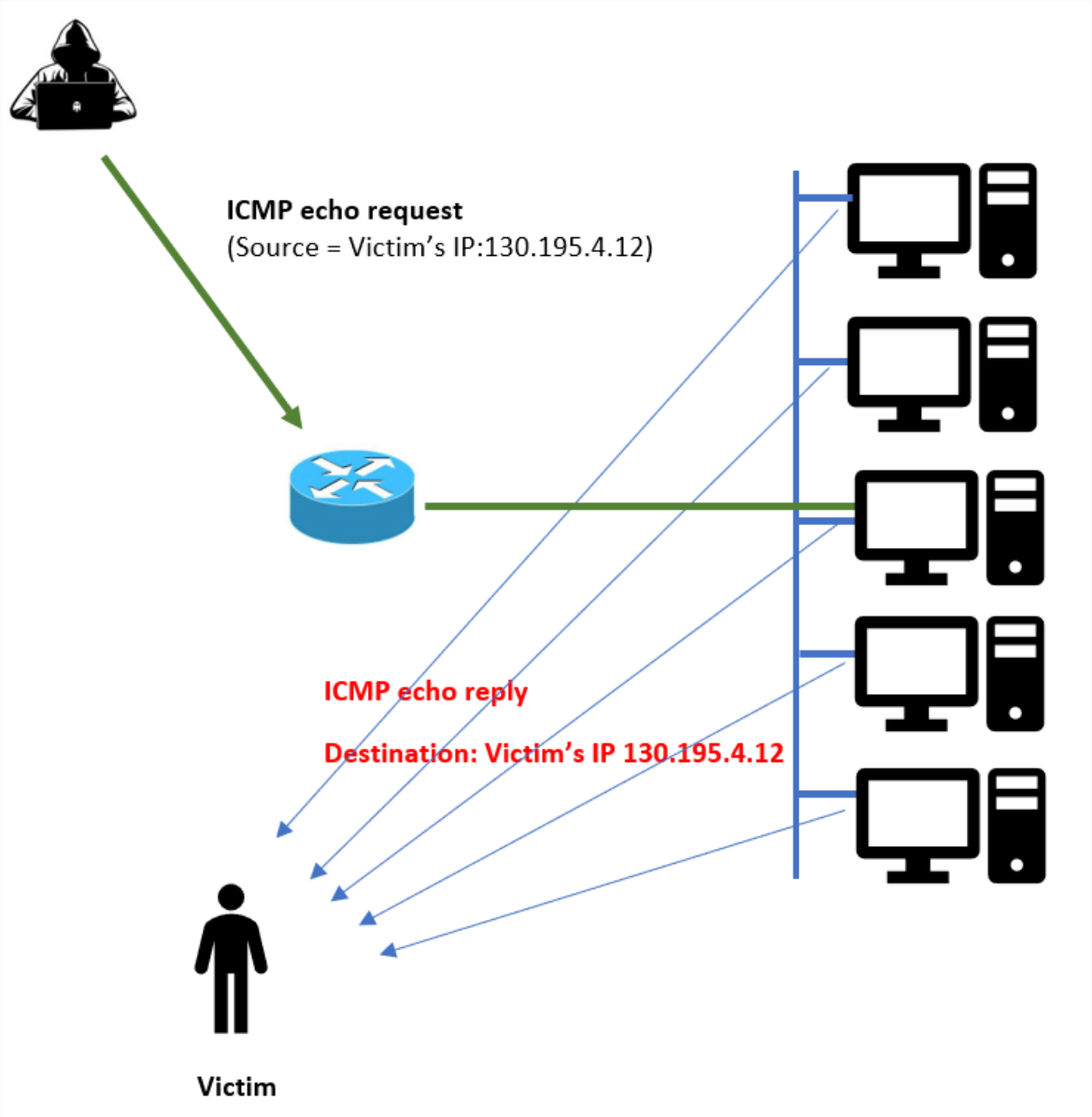
ICMP Smurf Attack

Normally ICMP echo request is sent => echo reply sent back

In a smurf attack:

1. Spoof the source address of the ICMP packet.
2. Send a packet to broadcast address of a network/to all computers on that network.
    - If intermediary device accepts broadcast packet, the packet is broadcast to all computers in the network.
3. Results in congestion at the victim.

ICMP Smurf Attack



ICMP Smurf Attack Mitigation

- Drop the traffic with invalid source IP address for segment
    - Router or firewall level
- Filters on L3 devices to not reply for broadcast address.
    - What are L3 devices?

ICMP Reconnaissance Attack

- Reconnaissance means, an inspection or exploration of an area.
- Reconnaissance of a network is performed for the following reasons:
  - To understand the environment of the target network.
  - Gather information about the target, to plan the attack approach.
  - Fingerprint the environment using right techniques & tools for the subsequent attack phases.

ICMP Reconnaissance Attack

Involves target discovery by sending ICMP messages:

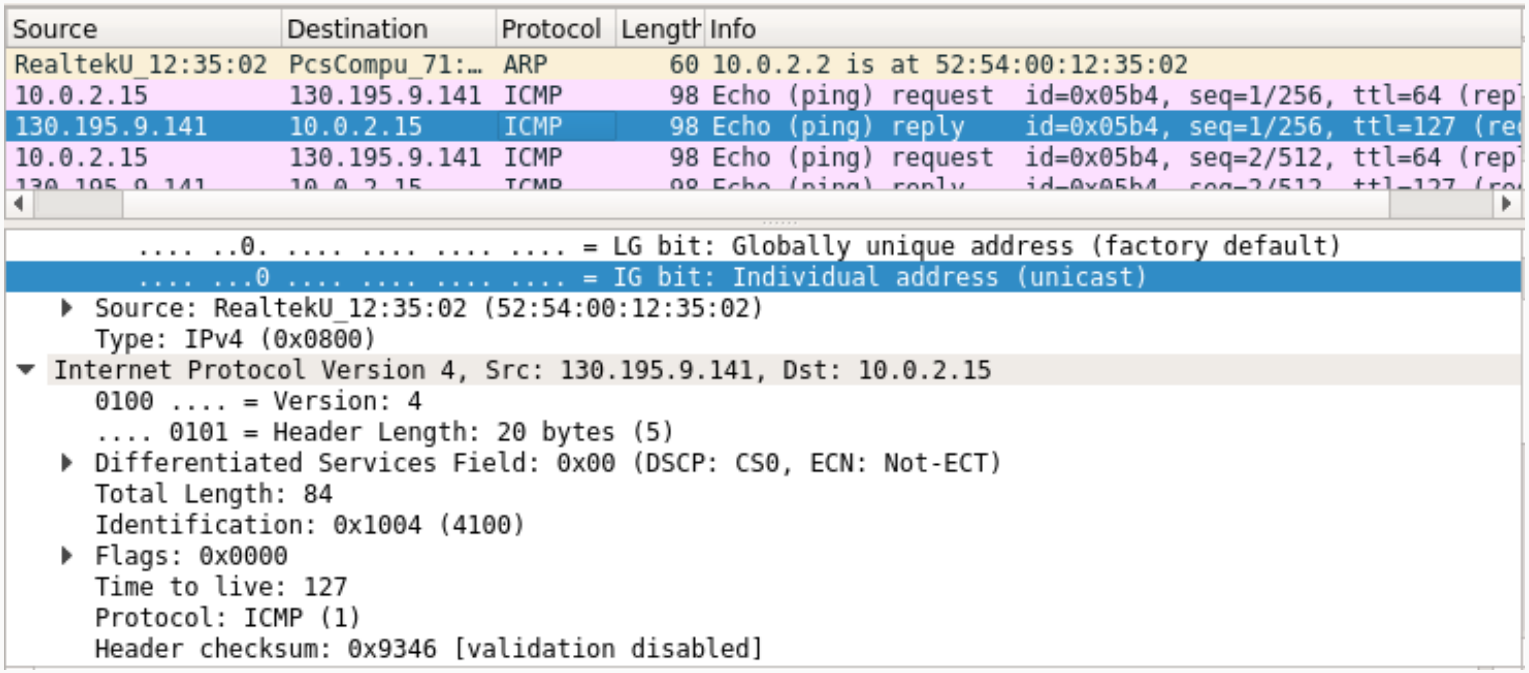
- Identifying hosts and valid IP addresses (ICMP Sweep): send a series of ICMP request packets to the target network range, analyse the ICMP replies to detect live hosts for further attacks
- Open ports detection
- Network topology detection
- OS Fingerprinting
- ACL detection

ICMP – Open Port Detection

- Different types of scanners are freely available
- Packets may be sent without any payload to each specified protocol on the target system
- The protocol is not used/Port is closed:
  - If an ICMP Protocol Unreachable error message is received.

ICMP OS Detection

- ICMP echo-request and echo-reply is used
- Check TTL value in ICMP Reply packet for OS signatures
  - If 128 then it is a Windows machine,
  - If TTL value of 64 then it is a Linux-based machine.



Packet Fragmentation Vulnerabilities

- Packet Fragmentation: Packet fragmentation is a legitimate process which can happen at either the source or the intermediary routers
- In IPv4 a router that receives a network packet larger than the next hop's MTU (Maximum Transmission Unit) has two options:
  - Drop the packet if the `Don't Fragment (DF)` flag bit is set in the packet's header and send an ICMP message which indicates the condition fragmentation needed, or,
  - Fragment the packet and send it over the link with a smaller MTU.

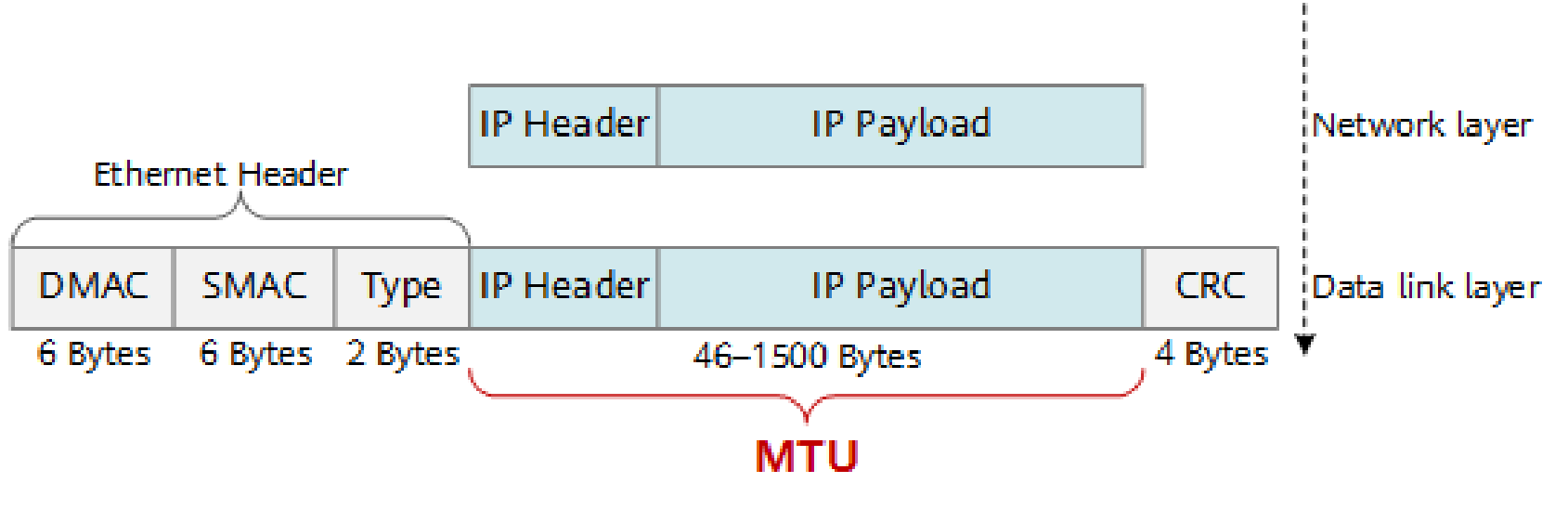
Maximum Transmission Unit (MTU)

The largest data packet that a networked device will accept.

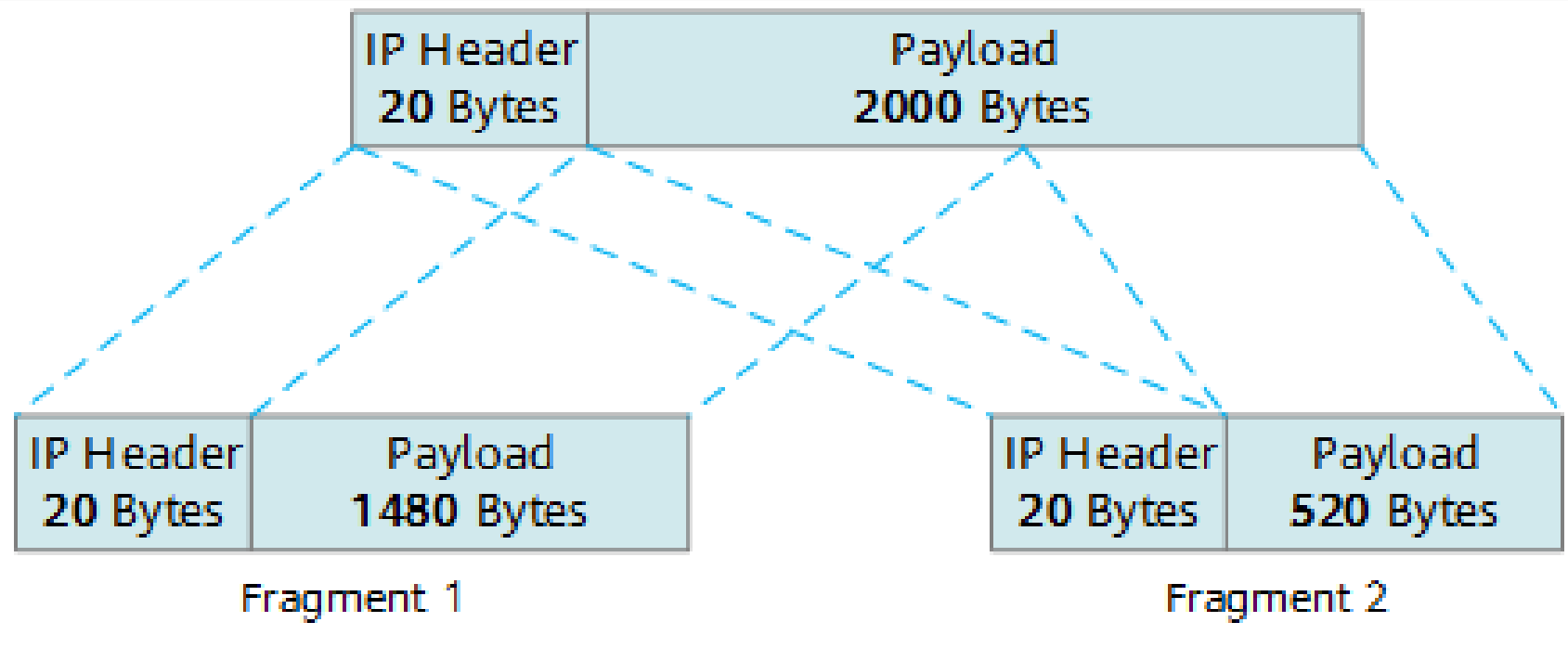
Larger packets are chopped and fragmented (network layer)

Routers will drop (packets > MTU)

MTU is derived from Ethernet frame size (max 1518 bytes (18 bytes for the ethernet header))



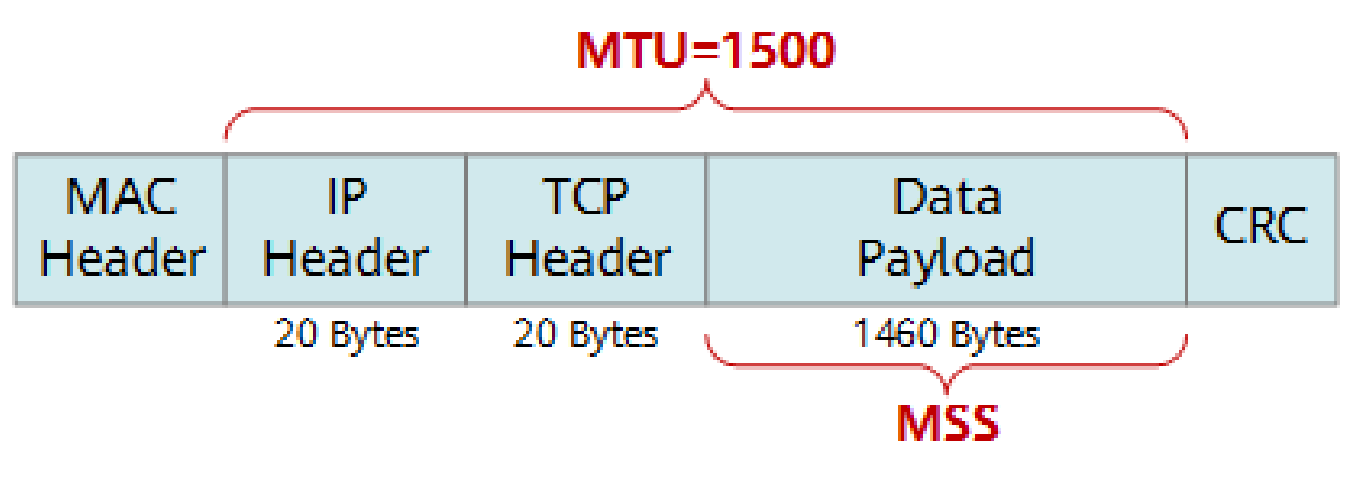
MTU and fragmentation



Ref: https://info.support.huawei.com/info-finder/encyclopedia/en/MTU.html.

TCP's MSS

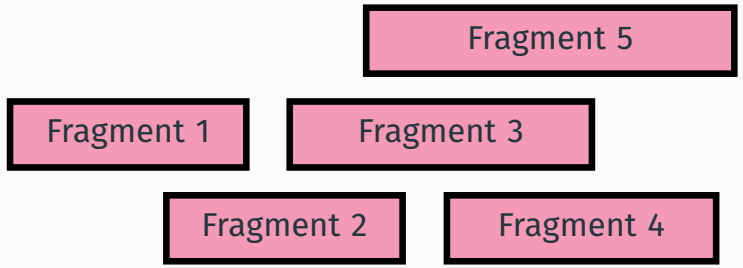
- A parameter in TCP header's options field which specifies the maximum size of packets that can be sent over a network.
- Several headers are appended to packets during transmission, indicating the source and destination of the packet. The non-header section of a packet, commonly known as the payload, is measured by MSS



Packet Fragmentation Vulnerabilities

1. What if we create a very large size packet (of size more than 65536-1), fragment it and send it to the destination:
   - buffer Overflow → Ping of Death Attack
2. What if we break packets into fragments such that they overlap:
   - Manipulate offset and payload size → Teardrop Attack

Legitimate fragmentation.



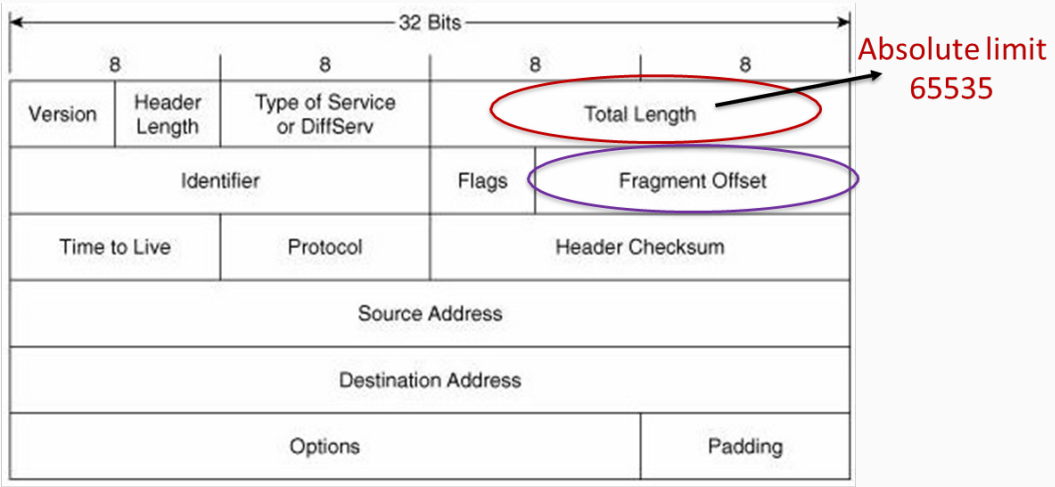
Malicious fragmentation.

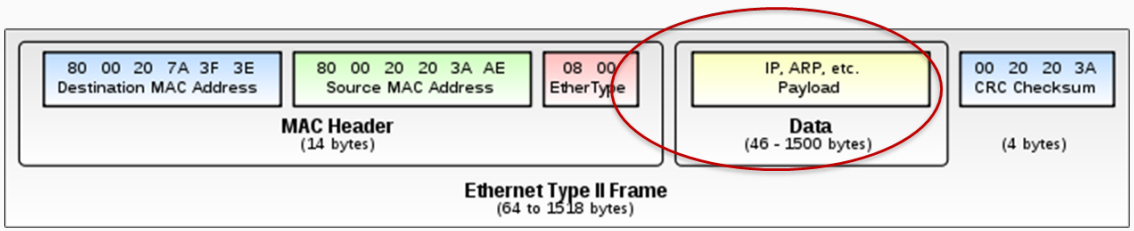
ICMP Ping of ☠ DEATH ☠

- ICMP echo packets are usually small
  - Maximum allowable packet size of 65,535 bytes
  - Violates IP protocol if larger
- Break the packet into smaller allowable size
  - Causing overflow when reassembled
  - Causing the target machine to freeze or crash
  - Not common now but works on old operating systems
  - Easy to do!

ICMP Teardrop Attack

- Uses overlapped fragmented packet.
- IP header contains three fields (of many):
  1. Do not fragment bit, 0x80
  2. Fragment bit 0x40
  3. offset fragments = states the starting position of each fragment, Multiple of 8 Bytes





ICMP Teardrop Attack

ICMP Teardrop Attack process:

1. Send large number of packets to target machine with overlapped offset values
2. Reassemble at the target
3. Packets overlap and cause fragmentation reassembly bug and cannot be reassembled → DoS

How to prevent them?

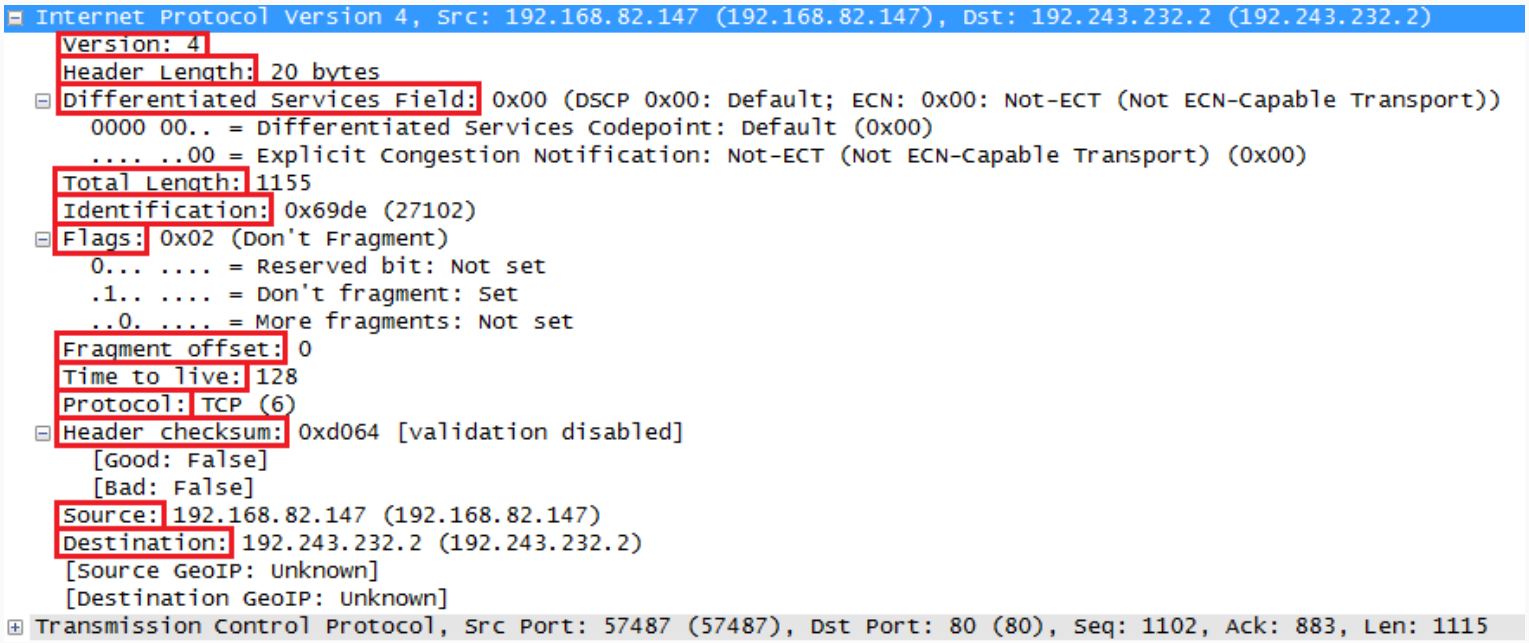
Check incoming packets' frame alignment and discard improperly formatted packets.

IP Null Attack

Legitimate IPv4 packets should contain information on which transport protocol is being used.

An attacker can set the value to zero

- Can bypass detection
- The target now has to assign resources to know what to do with the packets and where to forward it to



Next: Transport Layer (L4) Security (UDP, TCP)