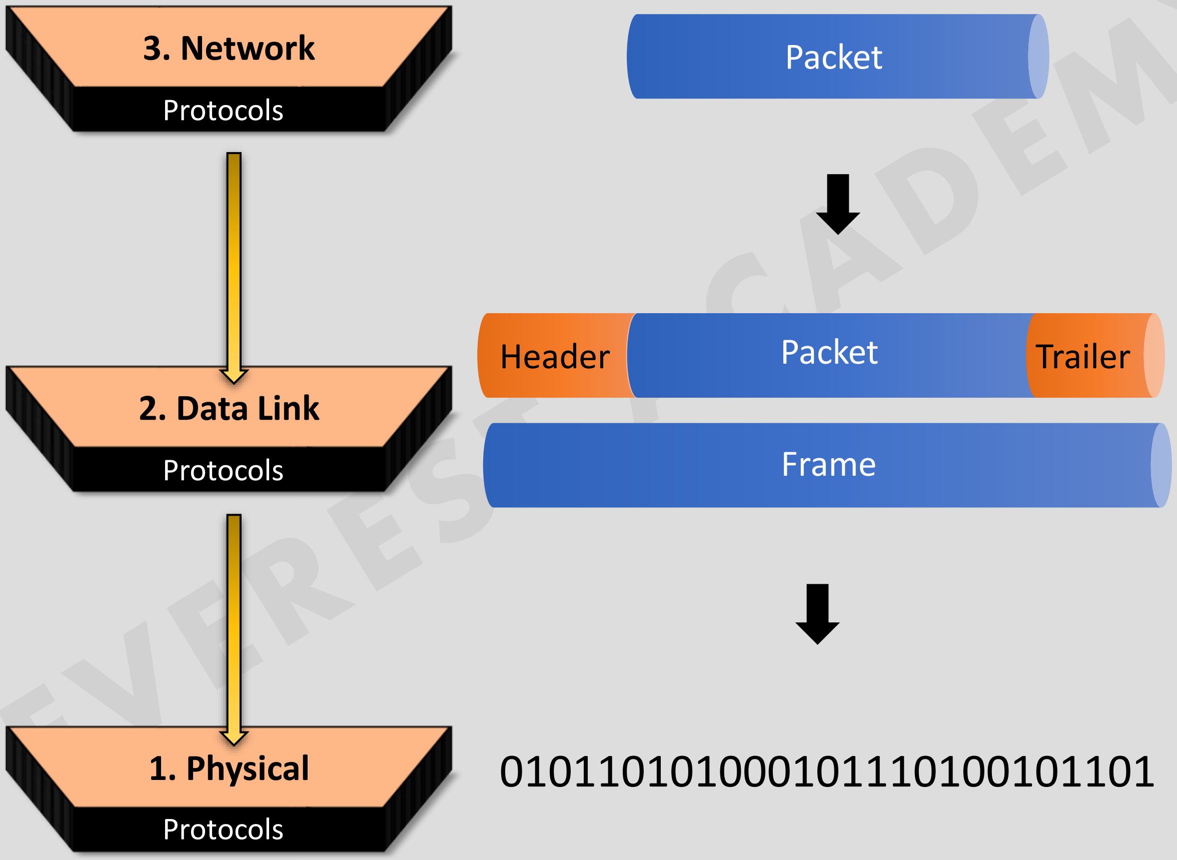
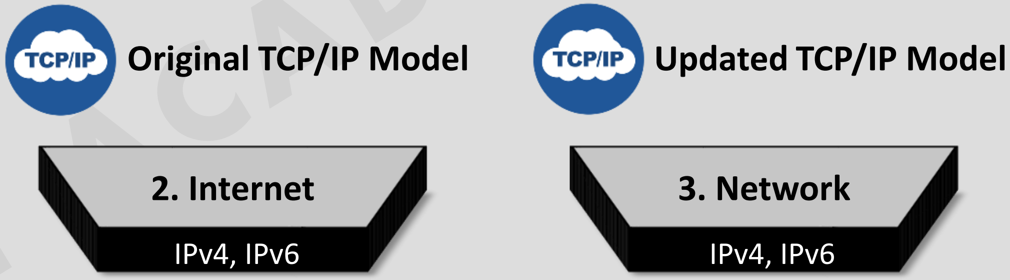
Internet Protocol Version 4 (IPv4)



Internet Protocol Version 4 (IPv4)

- **Internet Protocol version 4 (IPv4)** is the fourth version of the Internet Protocol (IP). It is one of the core protocols in the Internet .

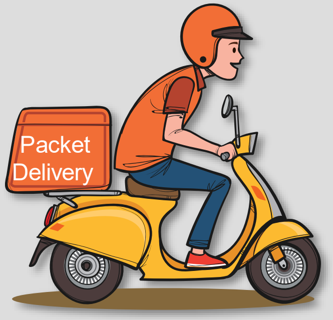
- **The Internet Protocol** is the protocol that defines and enables internetworking at the Internet Layer or the Network Layer



- **IPv4** uses a logical addressing system (IPv4 addressing) to performs routing or forwarding packets between different networks.

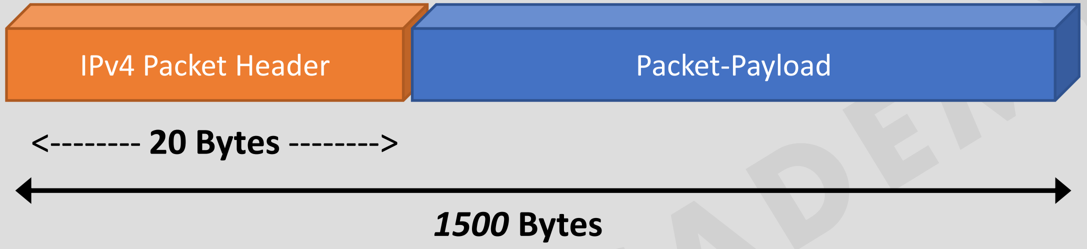
200 . 150 . 175 . 116

- **IPv4** is a connectionless protocol, operates on a best effort delivery model and does not guarantee of packets delivery or proper sequencing.

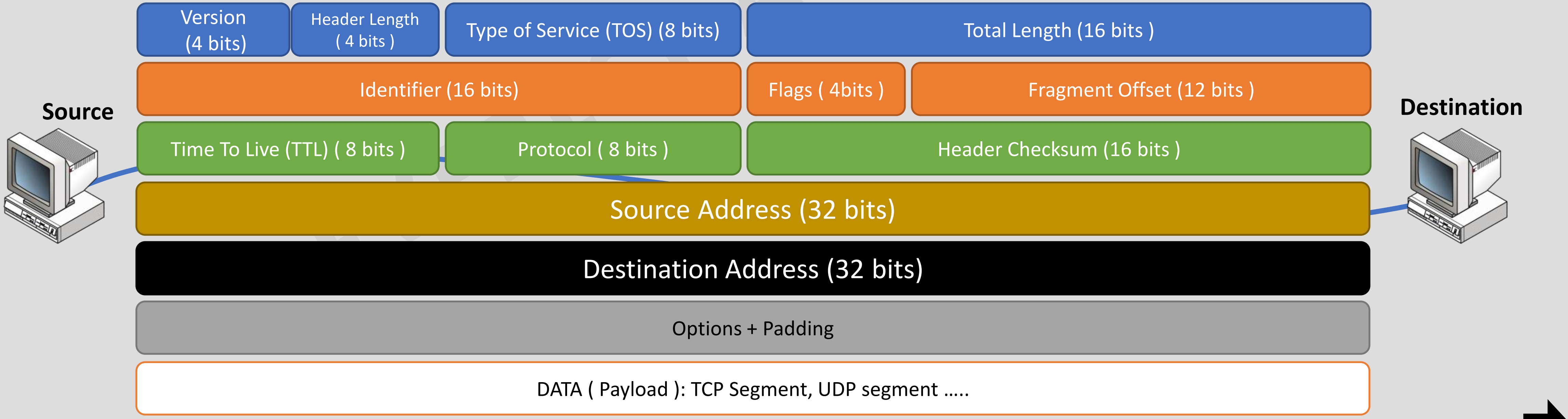


IPv4 Packet

- **An IP packet** is composed of a **header** and **payload**. **The header** consists of fixed and optional fields. **The payload** appears immediately after the header. An IP Packet is often carried as the payload inside an **Ethernet frame**.



4 + 4 + 8 + 16 + 16 + 4 + 12 + 8 + 8 + 16 + 32 + 32 = 160 bits = 20 Bytes or Octets or 5 Words



Version (4 bits) | Header Length (4 bits) | Type of Service (TOS) (8 bits) | Total Length (16 bits)

Identifier (16 bits) | Flags (4bits) | Fragment Offset (12 bits)

Time To Live (TTL) (8 bits) | Protocol (8 bits) | Header Checksum (16 bits)

Source Address (32 bits)

Destination Address (32 bits)

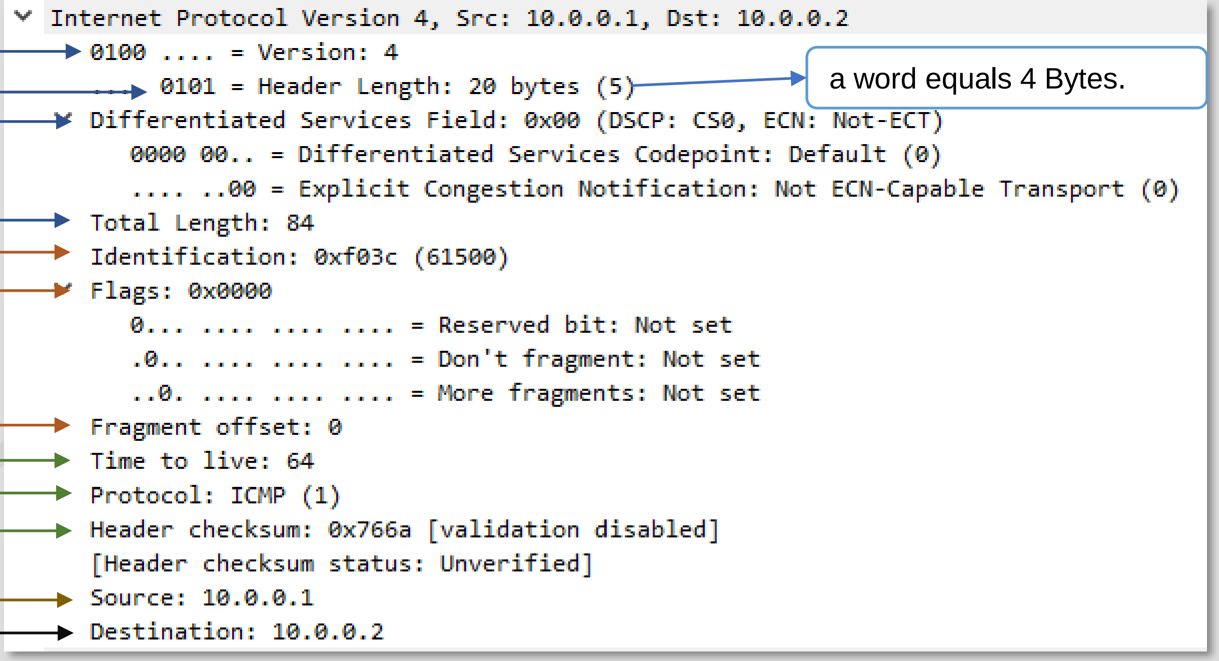
Options + Padding

DATA (Payload): TCP Segment, UDP segment .....

IPv4 Packet

- Version (4 bits)
- Header Length (4 bits)
- Type of Service (TOS) (8 bits)
- Total Length (16 bits)
- Identifier (16 bits)
- Flags (4bits)
- Fragment Offset (12 bits)
- Time To Live (TTL) (8 bits)
- Protocol (8 bits)
- Header Checksum (16 bits)
- Source Address (32 bits)
- Destination Address (32 bits)

IPv4 Packet



```
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0xf03c (61500)
    Flags: 0x0000
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x766a [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.1
    Destination: 10.0.0.2
```

a word equals 4 Bytes.

IPv4 Packet

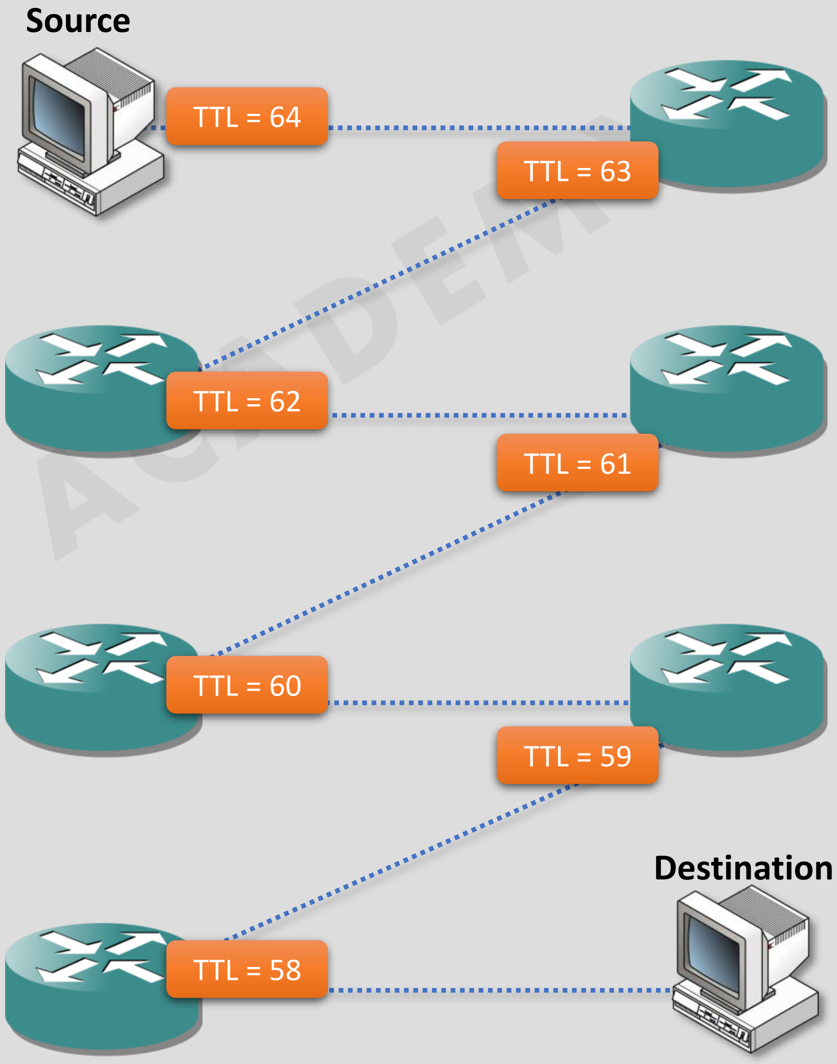
Version (4 bits)	IP version number, this is always equal to 4.
Header Length (4 bits)	Length of the IP header
Type of Service (TOS) (8 bits)	Defines how the IP network should treat the packet.
Total Length (16 bits)	Length of the IP packet, including the **header** and encapsulated **data** in Byte.
Identifier (16 bits)	Identifies the packet component if the packet has been fragmented.
Flags (4bits)	Is set if the packet is a fragment
Fragment Offset (12 bits)	Defines information about the packet if it is a fragment.
Time To Live (TTL) (8 bits)	Sets the number of hops the packet is allowed to traverse.
Protocol (8 bits)	Identifies the protocol of upper layer (such as TCP, UDP, ICMP, OSPF, etc.)
Header Checksum (16 bits)	Checksum on just the IP header fields.
Source Address (32 bits)	IP address of the source device.
Destination Address (32 bits)	IP address of the destination device.

Time To Live (TTL)

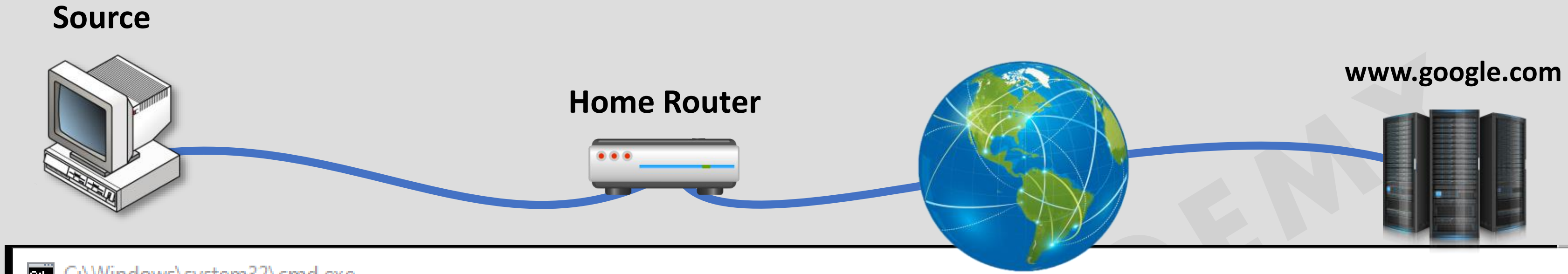
- **The TTL field** is set by the sender of the packet, and reduced by every router on the route to its destination. If the TTL field reaches zero before the packet arrives at its destination, then the datagram is discarded.

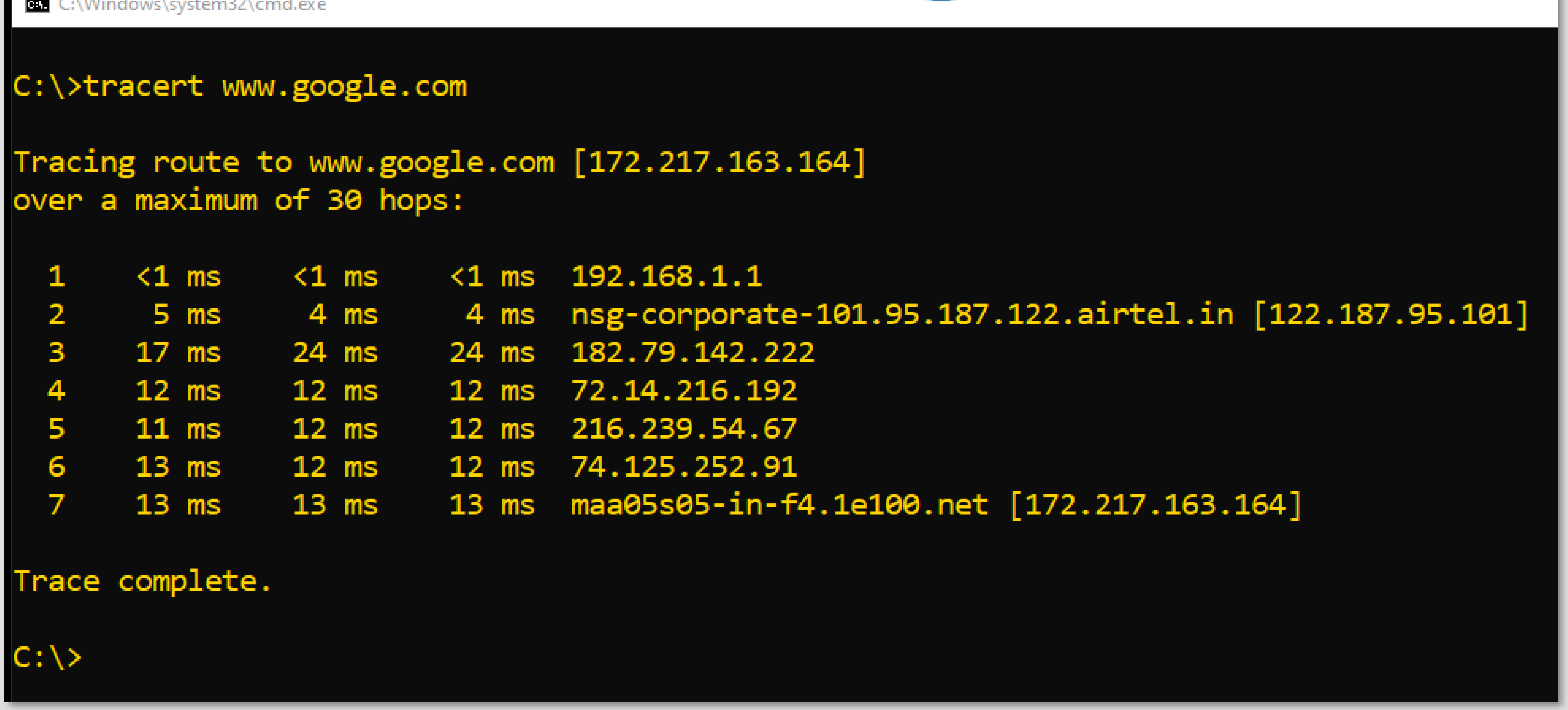
- **The purpose of the TTL field** is to avoid a situation in which an undeliverable packet keeps circulating on an Internet system.

- **The maximum TTL value** is 255, the maximum value of a single octet. A recommended initial value is 64.



Tracert (Traceroute) Tool

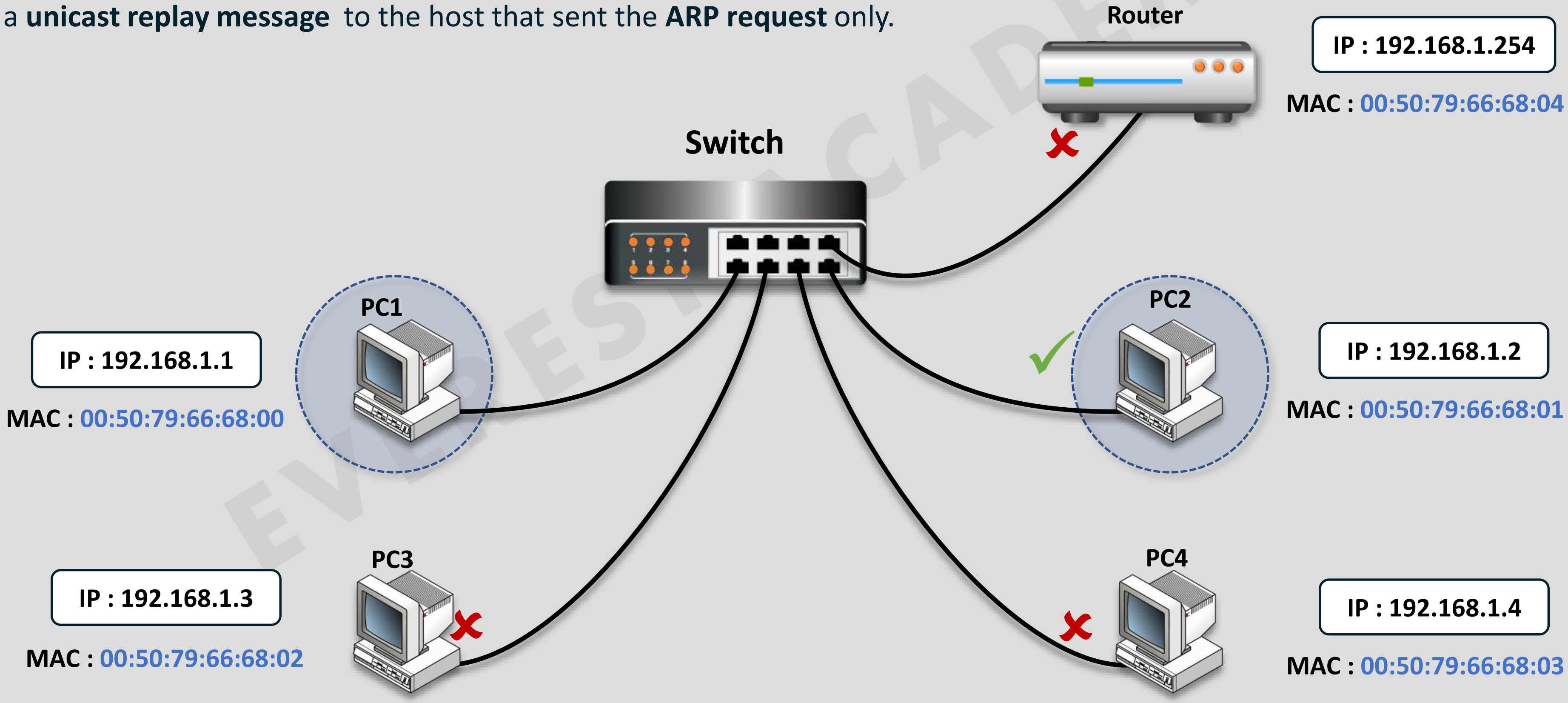




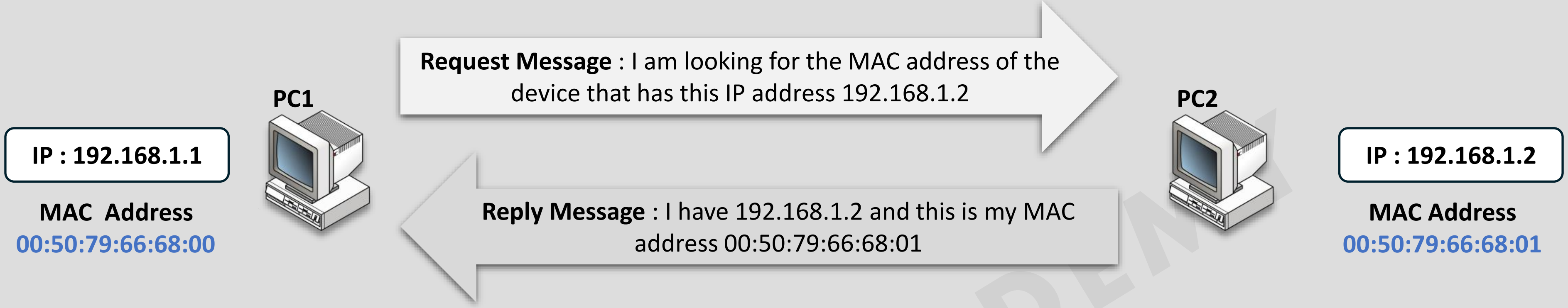
```
C:\>tracert www.google.com

Tracing route to www.google.com [172.217.163.164]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     5 ms     4 ms     4 ms  nsg-corporate-101.95.187.122.airtel.in [122.187.95.101]
  3    17 ms    24 ms    24 ms  182.79.142.222
  4    12 ms    12 ms    12 ms  72.14.216.192
  5    11 ms    12 ms    12 ms  216.239.54.67
  6    13 ms    12 ms    12 ms  74.125.252.91
  7    13 ms    13 ms    13 ms  maa05s05-in-f4.1e100.net [172.217.163.164]

Trace complete.

C:\>
```

Address Resolution Protocol (ARP)

- **Address Resolution Protocol (ARP)** is a network protocol used to find the hardware (MAC) address of a host from an IP address on the same LAN.
- **ARP** is used on **Ethernet LANs** because hosts that want to communicate with each other need to know their respective MAC addresses.
- **ARP** sends a **broadcast request message** to the Layer 2 broadcast address of **FF:FF:FF:FF:FF:FF.**
- **ARP** sends a **unicast replay message** to the host that sent the **ARP request** only.



Address Resolution Protocol (ARP)



PC1

IP : 192.168.1.1

MAC Address
00:50:79:66:68:00

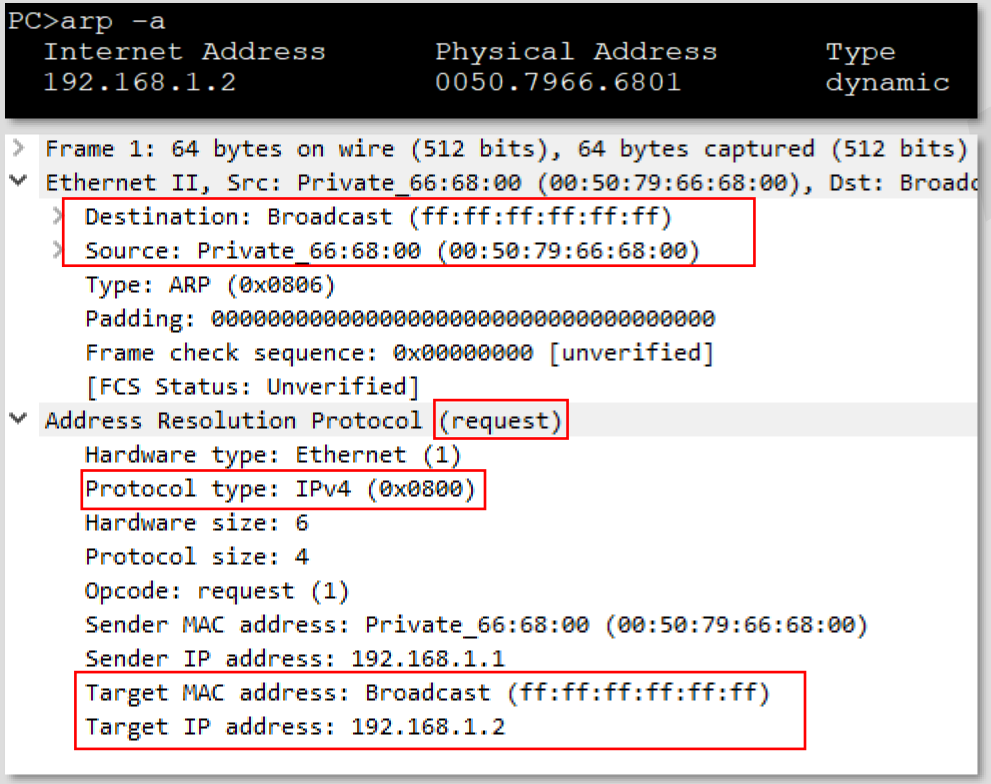
Request Message : I am looking for the MAC address of the device that has this IP address 192.168.1.2

Reply Message : I have 192.168.1.2 and this is my MAC address 00:50:79:66:68:01

PC2

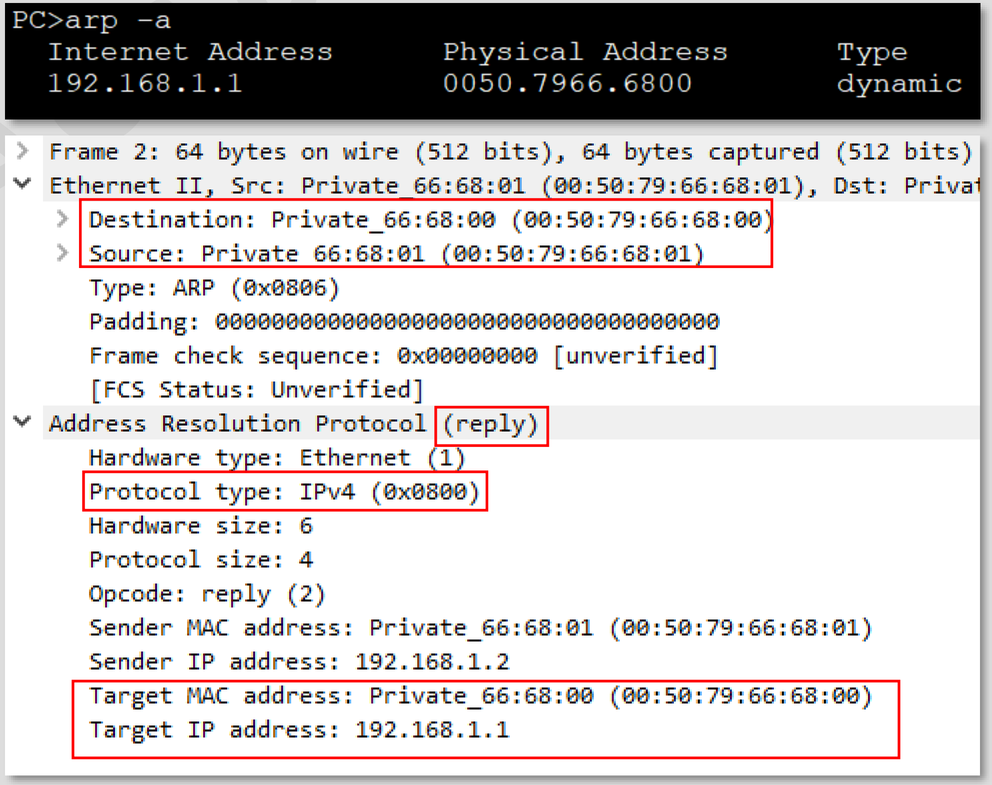
IP : 192.168.1.2

MAC Address
00:50:79:66:68:01



```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0050.7966.6801        dynamic
```

```
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadc
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Private_66:68:00 (00:50:79:66:68:00)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
    Sender IP address: 192.168.1.1
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.1.2
```



```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0050.7966.6800        dynamic
```

```
> Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v Ethernet II, Src: Private 66:68:01 (00:50:79:66:68:01), Dst: Privat
  > Destination: Private_66:68:00 (00:50:79:66:68:00)
  > Source: Private 66:68:01 (00:50:79:66:68:01)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
    Sender IP address: 192.168.1.2
    Target MAC address: Private_66:68:00 (00:50:79:66:68:00)
    Target IP address: 192.168.1.1
```

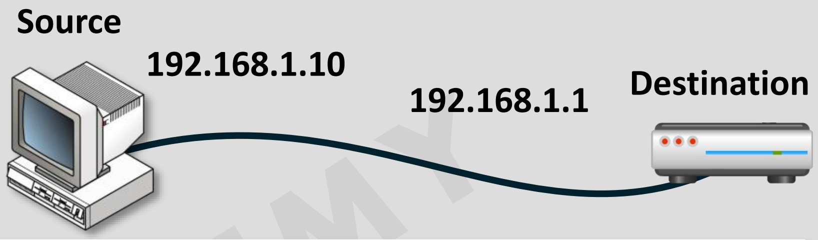
Internet Control Message Protocol (ICMP)

- **Internet Control Message Protocol (ICMP)** is a supporting protocol used by a network device to check connectivity with another device.

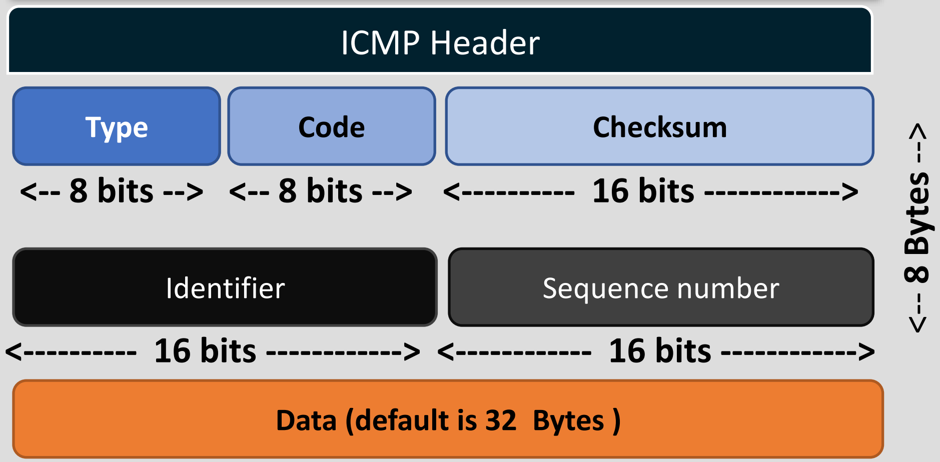
- **ICMP** sends messages that are typically used for diagnostic or control purposes or generated in response to errors in IP operations.

- **ICMP** errors are directed to the source IP address of the originating packet.

- Common network utilities that use ICMP messages are **Traceroute** or **Tracert** and **Ping** (**Packet internet groper**).



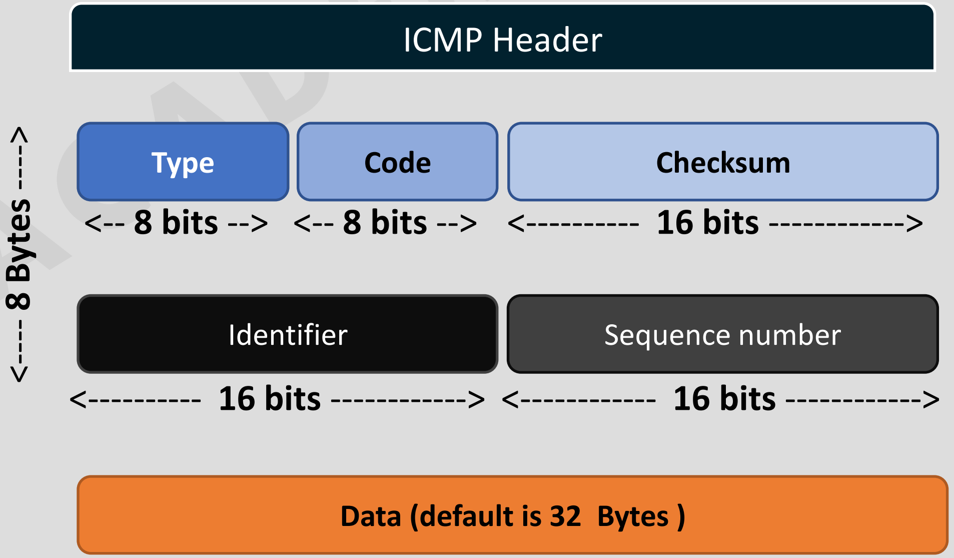
```
C:\>ping -n 1 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


ICMP Header
Type
Code
Checksum
<-- 8 bits -->
<-- 8 bits -->
<---------- 16 bits ------------>
Identifier
Sequence number
<---------- 16 bits ------------>
<------------ 16 bits ------------>
<-- 8 Bytes -->
Data (default is 32 Bytes)

Different Types of ICMP Messages

ICMP Message Types

Type	Codes	Description
0/8	0	Echo Reply/Echo Request
3	0-15	Destination Unreachable
4	0	Source Quench
5	0-3	Redirect
9/10	0	Router Advertisement
11	0-1	Time Exceeded
12	0	Parameter Problem
13/14	0	Timestamp Request/Timestamp Reply
17/18	0	Address Mask Request/Address Mask Reply



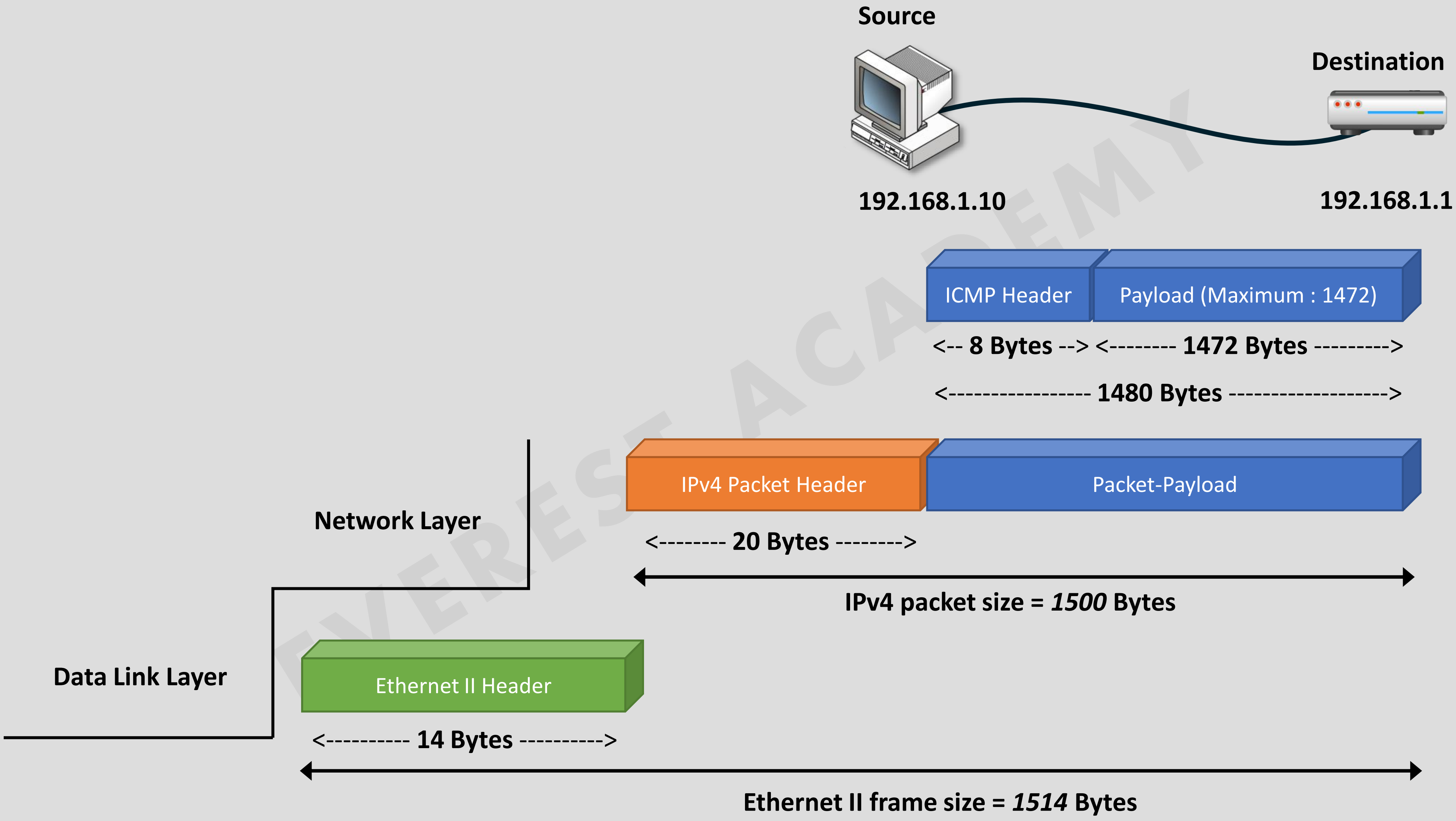
ICMP Header

Type	Code	Checksum
<-- 8 bits -->	<-- 8 bits -->	<---------- 16 bits ------------>

Identifier	Sequence number
<---------- 16 bits ------------>	<------------ 16 bits ------------>

Data (default is 32 Bytes)

ICMP Messages Encapsulation



Source

Destination

192.168.1.10

192.168.1.1

ICMP Header

Payload (Maximum : 1472)

<-- 8 Bytes --> <-------- 1472 Bytes --------->

<---------------- 1480 Bytes ----------------->

IPv4 Packet Header

Packet-Payload

Network Layer

<-------- 20 Bytes -------->

IPv4 packet size = *1500* Bytes

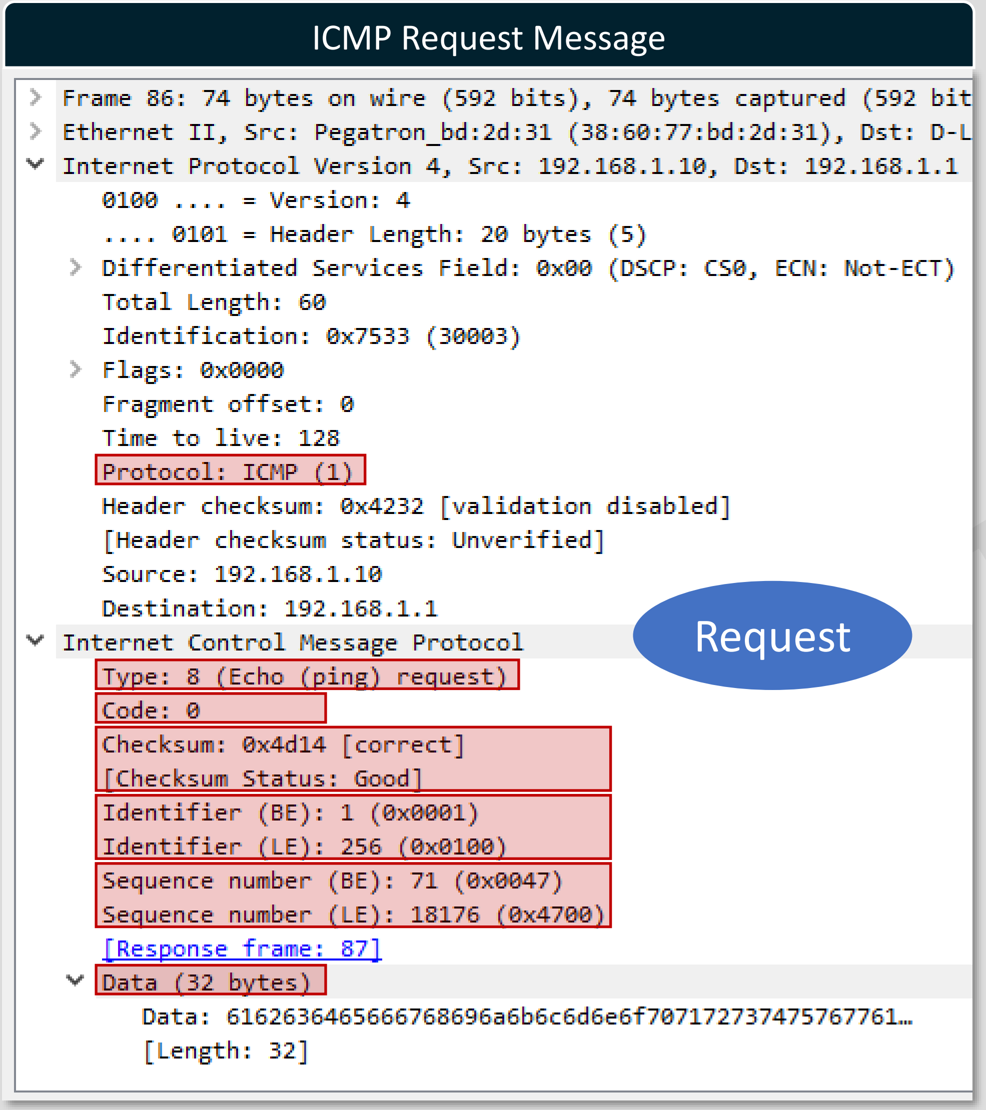
Data Link Layer

Ethernet II Header

<---------- 14 Bytes ---------->

Ethernet II frame size = *1514* Bytes

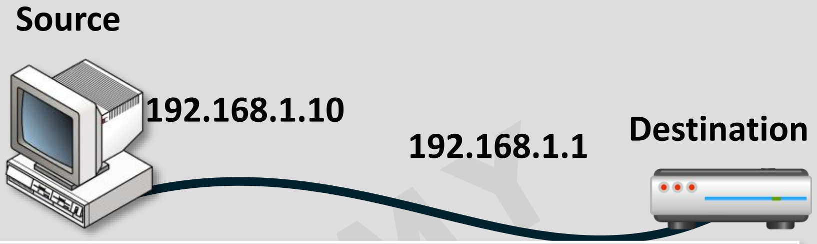
Ping Tool (Request Message)



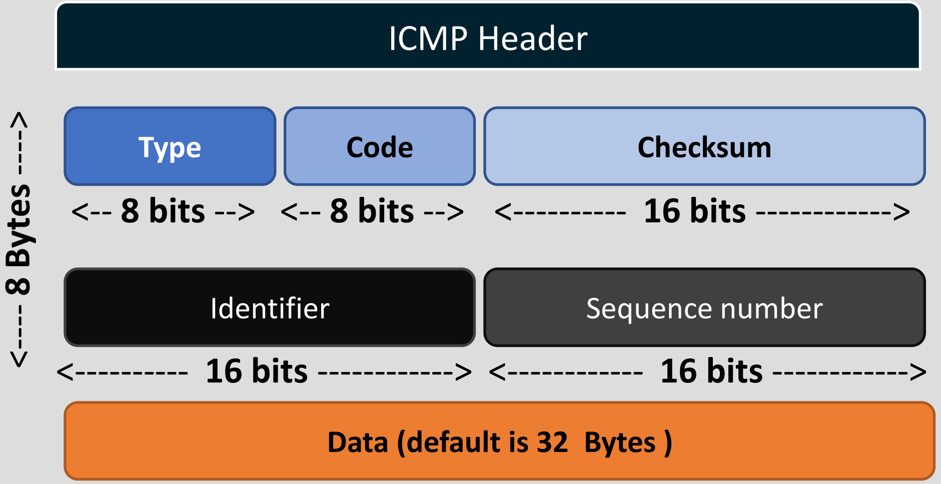
ICMP Request Message

```
> Frame 86: 74 bytes on wire (592 bits), 74 bytes captured (592 bit
> Ethernet II, Src: Pegatron_bd:2d:31 (38:60:77:bd:2d:31), Dst: D-L
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x4232 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.10
    Destination: 192.168.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d14 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Response frame: 87]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616…
      [Length: 32]
```

Request



```
C:\>ping -n 1 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.1.1:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



ICMP Header

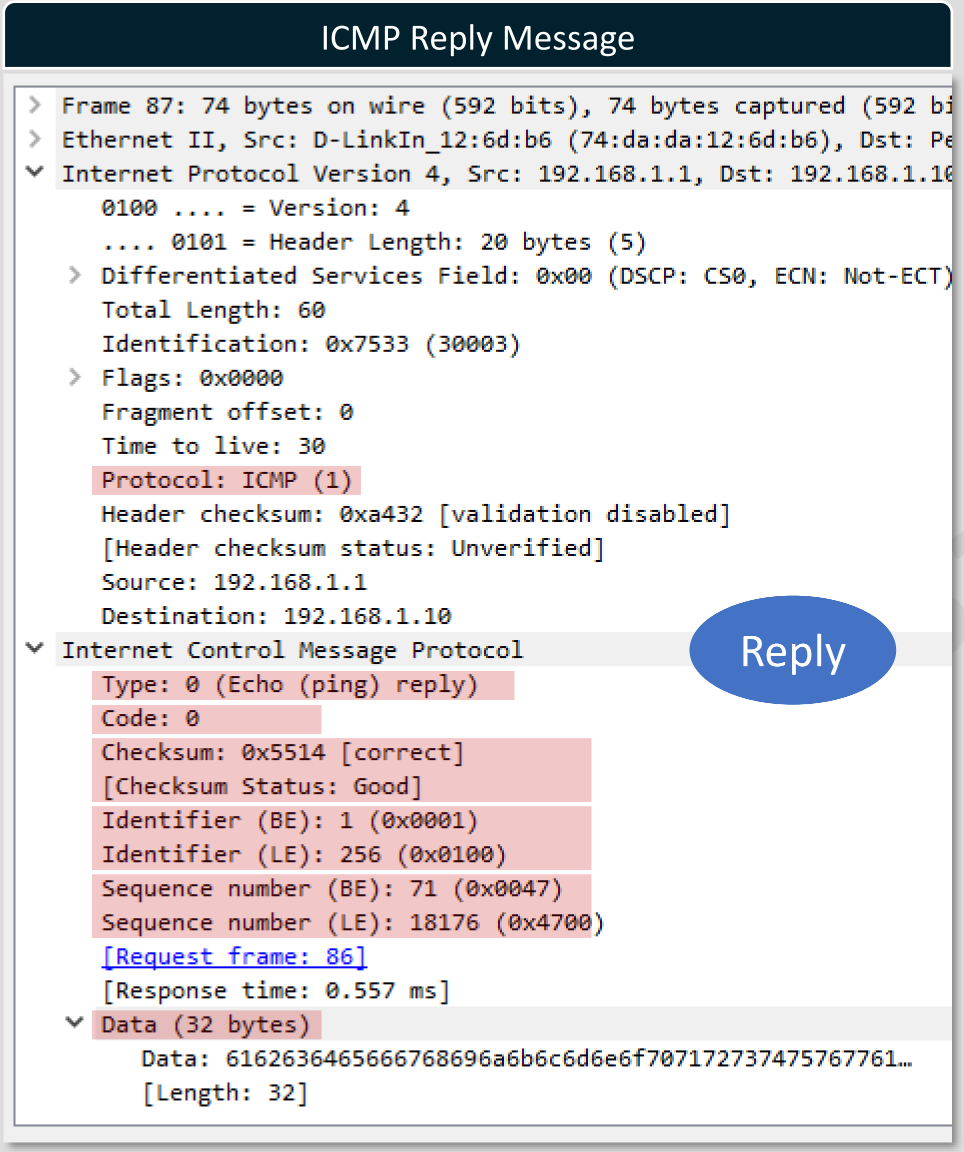
<--- 8 Bytes --->

Type	Code	Checksum
<-- 8 bits -->	<-- 8 bits -->	<---------- 16 bits ------------>

Identifier	Sequence number
<---------- 16 bits ------------>	<------------ 16 bits ------------>

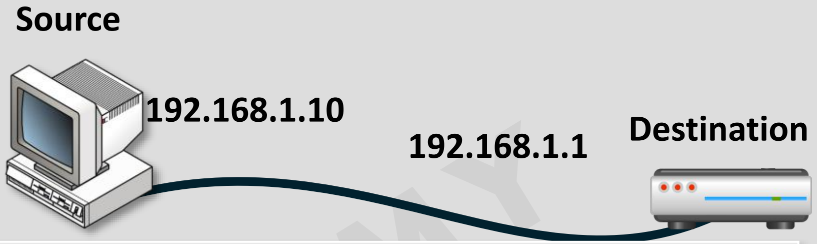
Data (default is 32 Bytes)

Ping Tool (Reply Message)

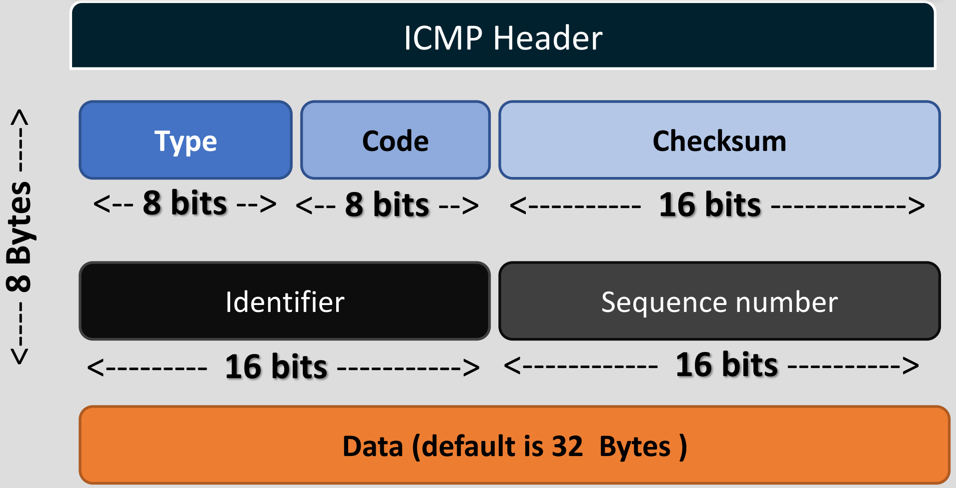


ICMP Reply Message

```
> Frame 87: 74 bytes on wire (592 bits), 74 bytes captured (592 bi
> Ethernet II, Src: D-LinkIn_12:6d:b6 (74:da:da:12:6d:b6), Dst: Pe
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 30
    Protocol: ICMP (1)
    Header checksum: 0xa432 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.10
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5514 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Request frame: 86]
    [Response time: 0.557 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761…
      [Length: 32]
```



```
C:\>ping -n 1 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.1.1:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



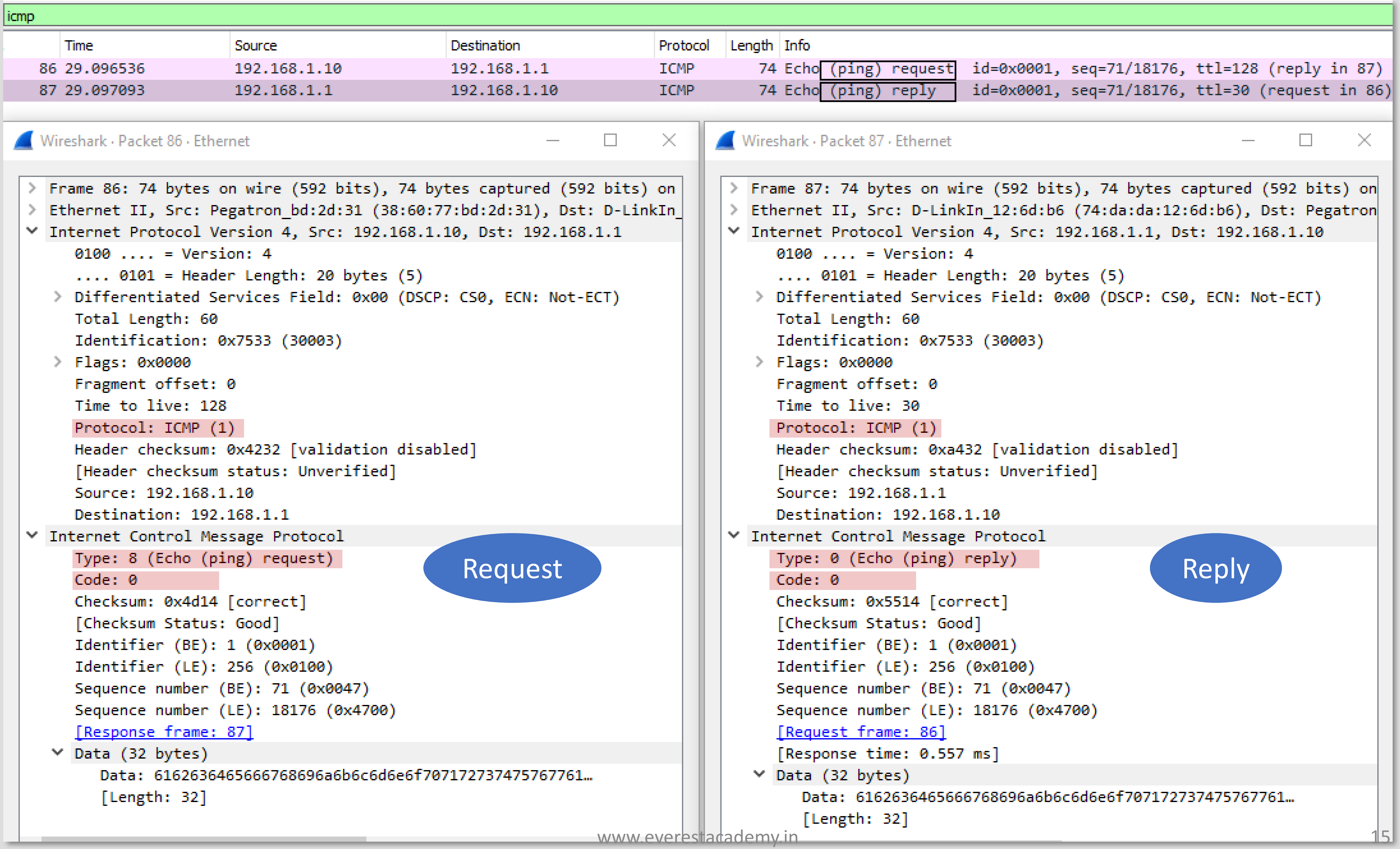
ICMP Header

<-------- 8 Bytes -------->

Type	Code	Checksum
<-- 8 bits -->	<-- 8 bits -->	<---------- 16 bits ------------>

Identifier	Sequence number
<--------- 16 bits ----------->	<------------ 16 bits ---------->

Data (default is 32 Bytes)



```
icmp

     Time          Source         Destination    Protocol  Length Info
  86 29.096536     192.168.1.10   192.168.1.1    ICMP        74 Echo (ping) request  id=0x0001, seq=71/18176, ttl=128 (reply in 87)
  87 29.097093     192.168.1.1    192.168.1.10   ICMP        74 Echo (ping) reply    id=0x0001, seq=71/18176, ttl=30 (request in 86)
```

Wireshark · Packet 86 · Ethernet

```
> Frame 86: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: Pegatron_bd:2d:31 (38:60:77:bd:2d:31), Dst: D-LinkIn_
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x4232 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.10
    Destination: 192.168.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d14 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Response frame: 87]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616…
      [Length: 32]
```

Request

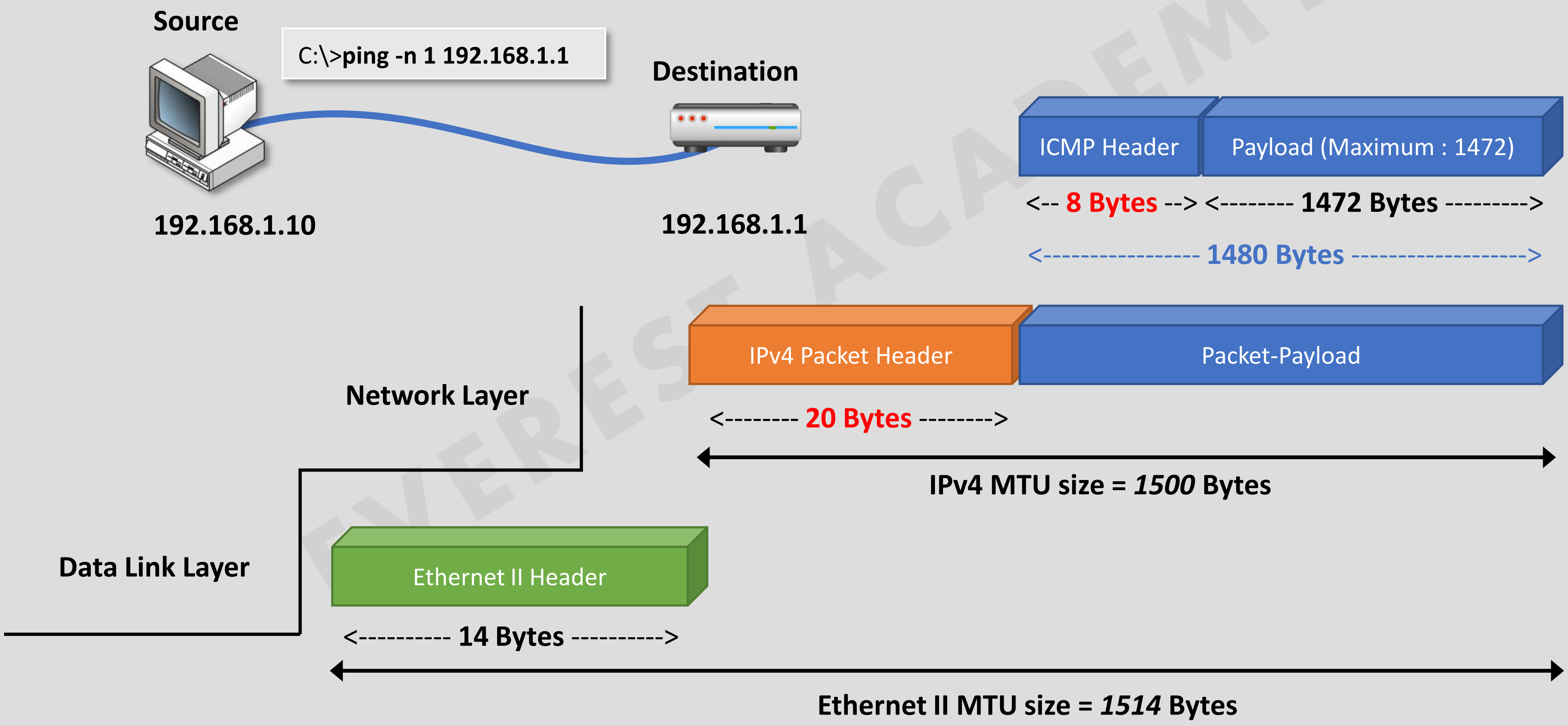
Wireshark · Packet 87 · Ethernet

```
> Frame 87: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: D-LinkIn_12:6d:b6 (74:da:da:12:6d:b6), Dst: Pegatron
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 30
    Protocol: ICMP (1)
    Header checksum: 0xa432 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.10
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5514 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Request frame: 86]
    [Response time: 0.557 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616…
      [Length: 32]
```

Reply

Maximum Transmission Unit (MTU)

- **A maximum transmission unit (MTU)** is the largest size of a packet that can be transmitted as a single entity in a network connection.



Source

```
C:\>ping -n 1 192.168.1.1
```

Destination

192.168.1.10

192.168.1.1

ICMP Header | Payload (Maximum : 1472)

<-- 8 Bytes --> <-------- 1472 Bytes --------->

<---------------- 1480 Bytes ------------------>

Network Layer

IPv4 Packet Header | Packet-Payload

<-------- 20 Bytes -------->

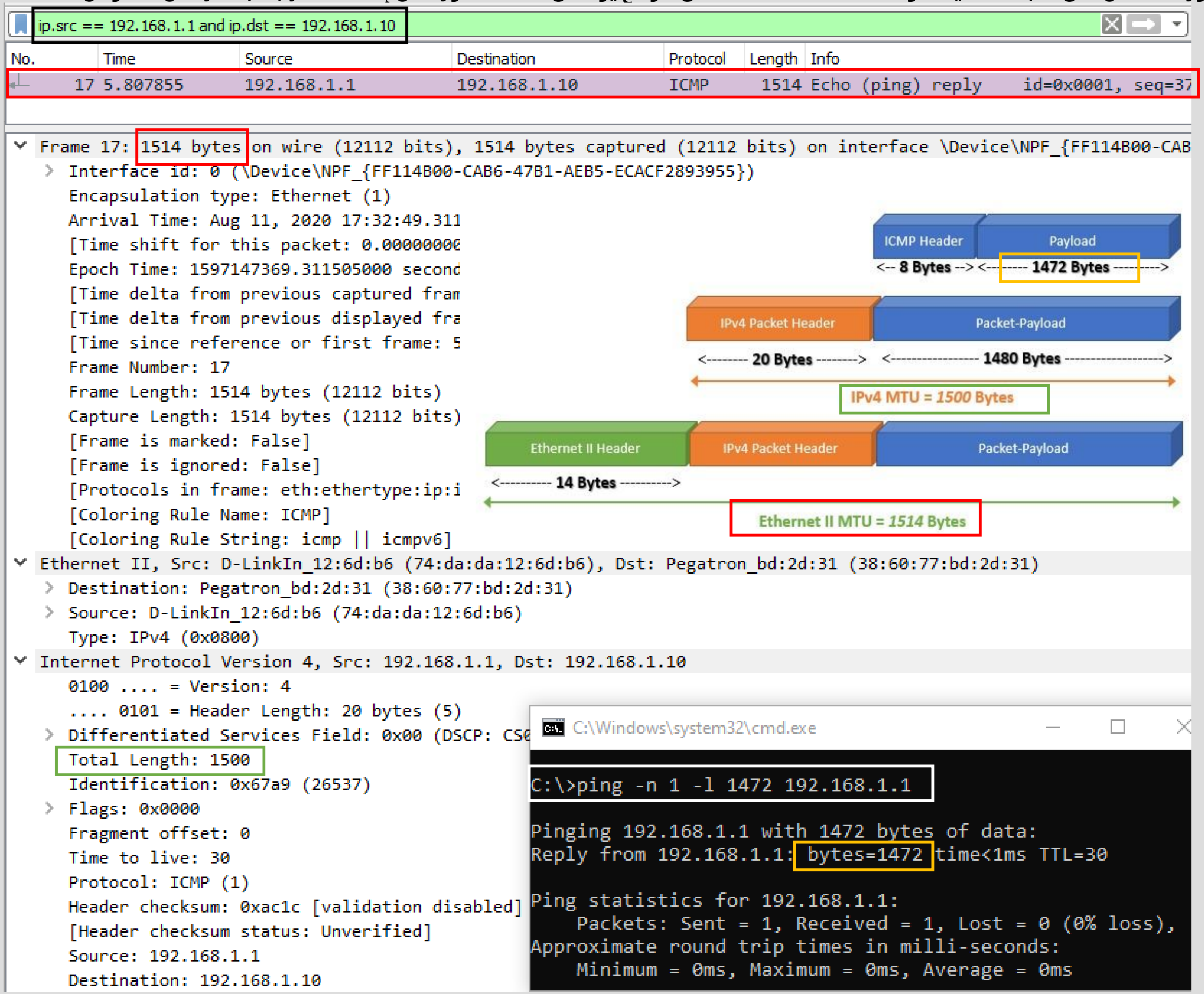
IPv4 MTU size = *1500* Bytes

Data Link Layer

Ethernet II Header

<---------- 14 Bytes ---------->

Ethernet II MTU size = *1514* Bytes



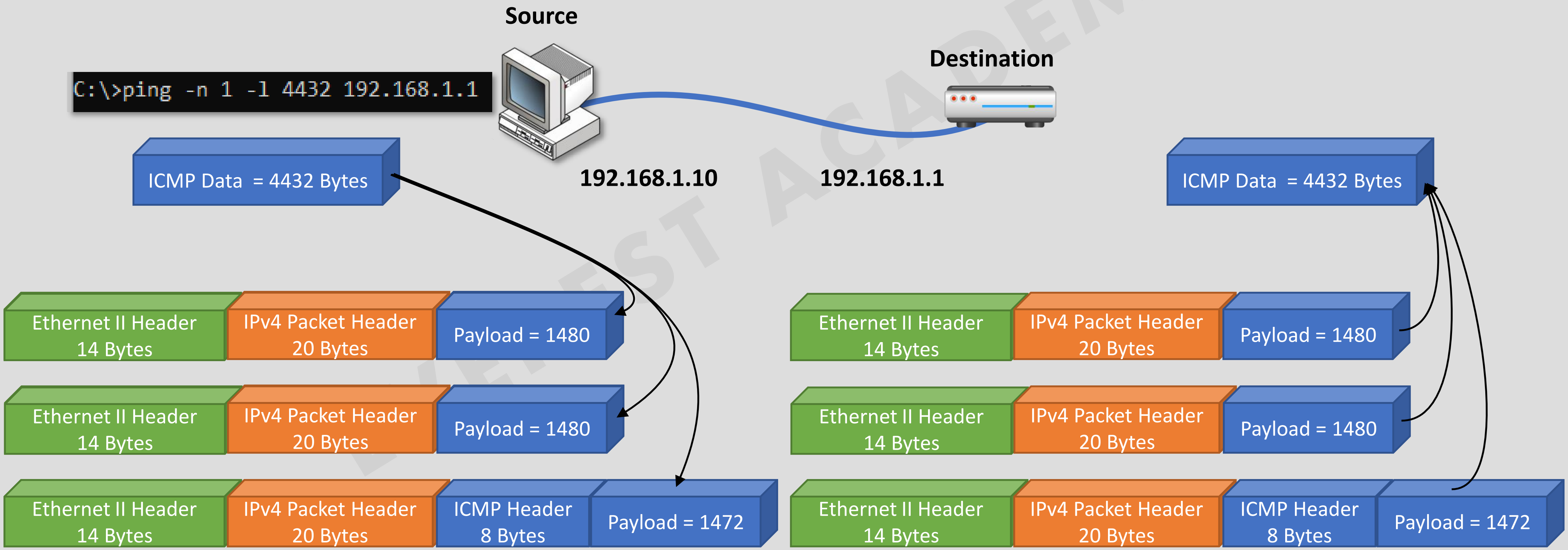
```
ip.src == 192.168.1.1 and ip.dst == 192.168.1.10

No.        Time          Source           Destination      Protocol  Length  Info
        17 5.807855      192.168.1.1      192.168.1.10     ICMP      1514 Echo (ping) reply    id=0x0001, seq=37

Frame 17: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{FF114B00-CAB
  > Interface id: 0 (\Device\NPF_{FF114B00-CAB6-47B1-AEB5-ECACF2893955})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 11, 2020 17:32:49.311
    [Time shift for this packet: 0.00000000
    Epoch Time: 1597147369.311505000 second
    [Time delta from previous captured fram
    [Time delta from previous displayed fra
    [Time since reference or first frame: 5
    Frame Number: 17
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:i
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: D-LinkIn_12:6d:b6 (74:da:da:12:6d:b6), Dst: Pegatron_bd:2d:31 (38:60:77:bd:2d:31)
  > Destination: Pegatron_bd:2d:31 (38:60:77:bd:2d:31)
  > Source: D-LinkIn_12:6d:b6 (74:da:da:12:6d:b6)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0
    Total Length: 1500
    Identification: 0x67a9 (26537)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 30
    Protocol: ICMP (1)
    Header checksum: 0xac1c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.10
```

ICMP Header
Payload
<-- 8 Bytes --> <------- 1472 Bytes ---------->
IPv4 Packet Header
Packet-Payload
<-------- 20 Bytes --------> <---------------- 1480 Bytes ------------------>
IPv4 MTU = 1500 Bytes
Ethernet II Header
IPv4 Packet Header
Packet-Payload
<---------- 14 Bytes ---------->
Ethernet II MTU = 1514 Bytes
C:\Windows\system32\cmd.exe

```
C:\>ping -n 1 -l 1472 192.168.1.1

Pinging 192.168.1.1 with 1472 bytes of data:
Reply from 192.168.1.1: bytes=1472 time<1ms TTL=30

Ping statistics for 192.168.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

IPv4 Fragmentation

- **IPv4 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. The fragments are reassembled by the receiving host.

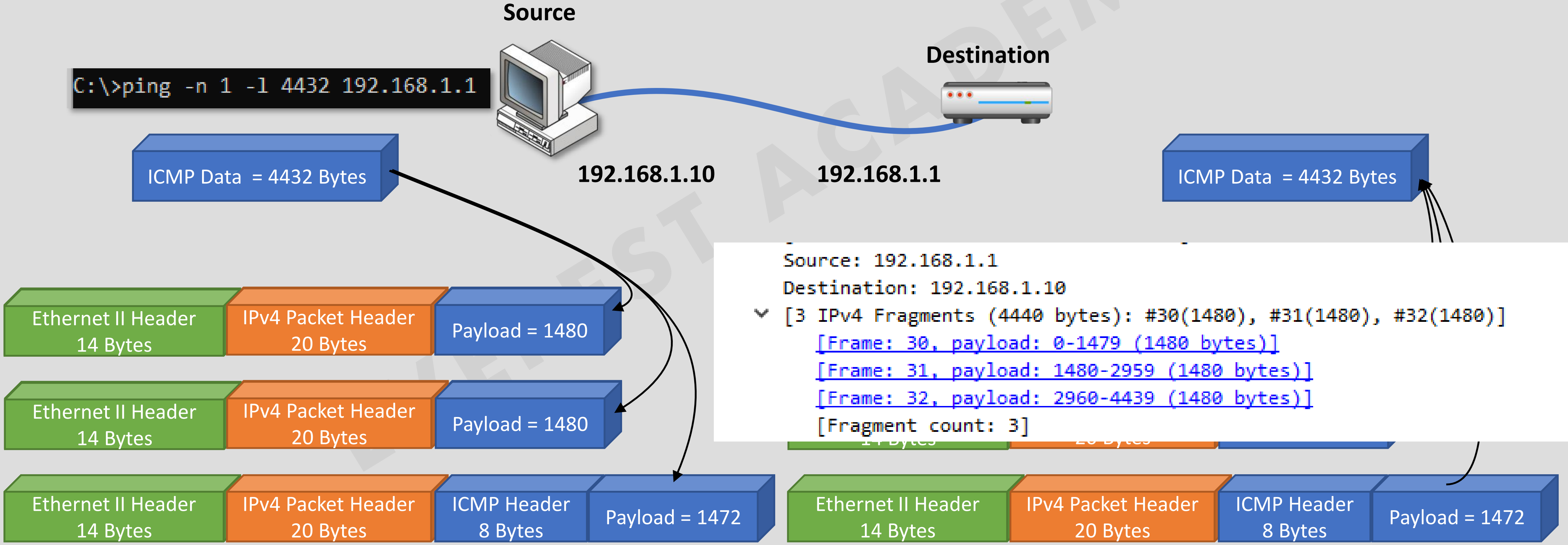


```
C:\>ping -n 1 -l 4432 192.168.1.1
```

Source
Destination
192.168.1.10
192.168.1.1
ICMP Data = 4432 Bytes
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
ICMP Header 8 Bytes
Payload = 1472
ICMP Data = 4432 Bytes
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
ICMP Header 8 Bytes
Payload = 1472

IPv4 Fragmentation

- **IPv4 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. The fragments are reassembled by the receiving host.

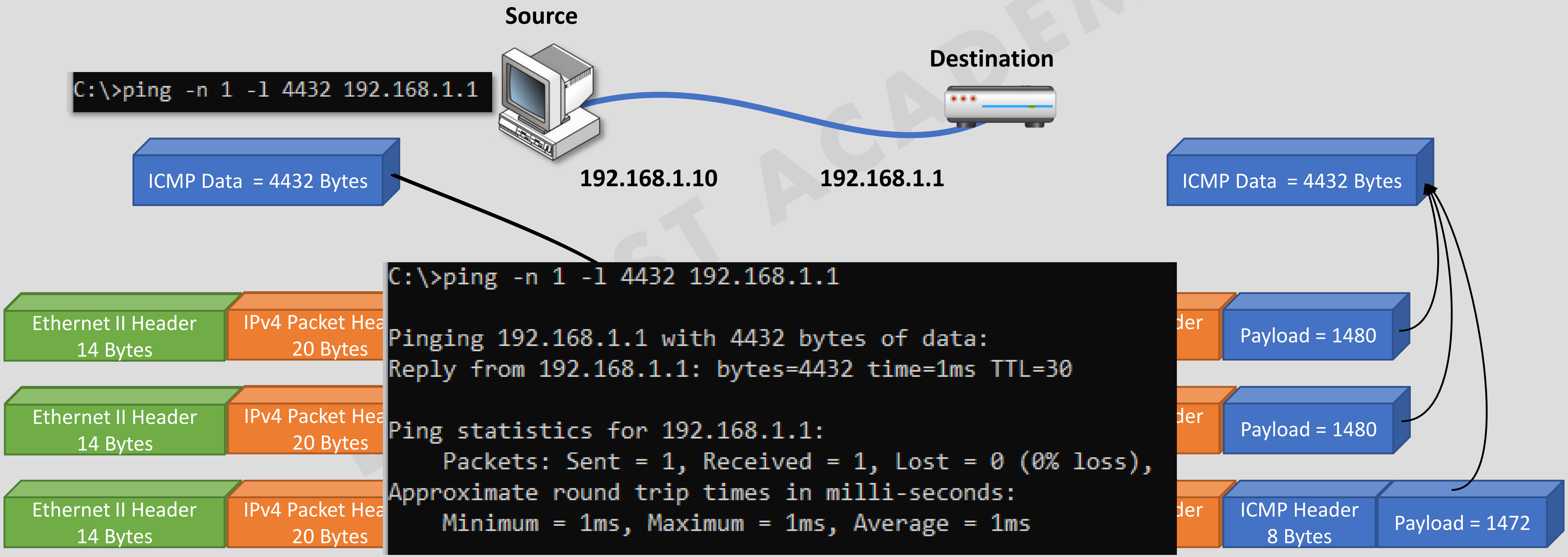

Source
Destination
192.168.1.10
192.168.1.1
ICMP Data = 4432 Bytes
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
Payload = 1480
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
ICMP Header 8 Bytes
Payload = 1472
ICMP Data = 4432 Bytes
14 Bytes
20 Bytes
Ethernet II Header 14 Bytes
IPv4 Packet Header 20 Bytes
ICMP Header 8 Bytes
Payload = 1472

```
C:\>ping -n 1 -l 4432 192.168.1.1
```

```
Source: 192.168.1.1
Destination: 192.168.1.10
[3 IPv4 Fragments (4440 bytes): #30(1480), #31(1480), #32(1480)]
    [Frame: 30, payload: 0-1479 (1480 bytes)]
    [Frame: 31, payload: 1480-2959 (1480 bytes)]
    [Frame: 32, payload: 2960-4439 (1480 bytes)]
    [Fragment count: 3]
```

IPv4 Fragmentation

- **IPv4 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. The fragments are reassembled by the receiving host.



```
C:\>ping -n 1 -l 4432 192.168.1.1
```

```
C:\>ping -n 1 -l 4432 192.168.1.1

Pinging 192.168.1.1 with 4432 bytes of data:
Reply from 192.168.1.1: bytes=4432 time=1ms TTL=30

Ping statistics for 192.168.1.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```