SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

CMPT 479/980: Systems and Network Security

Spring 2020

Network Analysis – Part 1

Instructor: Khaled Diab

Goal

- Analyze network traffic for different goals.

- Useful for:
  - Intrusion Analyst: dissect network traffic to study intrusions
  - Forensic Investigator: check the extent of a malware infection
  - Attackers: understand their victim networks!

Outline

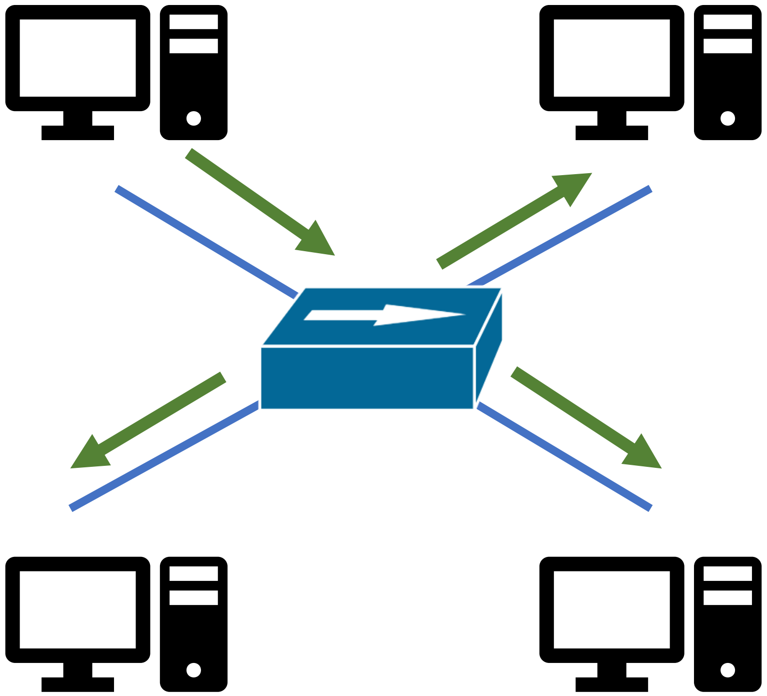
- Network Hardware
- Packets
    - Dissecting Packets
    - Sample of Network Protocols
        - ARP and ICMP
- Capturing packets
    - Packet Sniffing
        - Sniffer deployment
        - Tools: Wireshare
- Network-level operations:
    - Network Recon
    - Traffic Manipulation
        - Spoofing

Network Hardware

A quick review

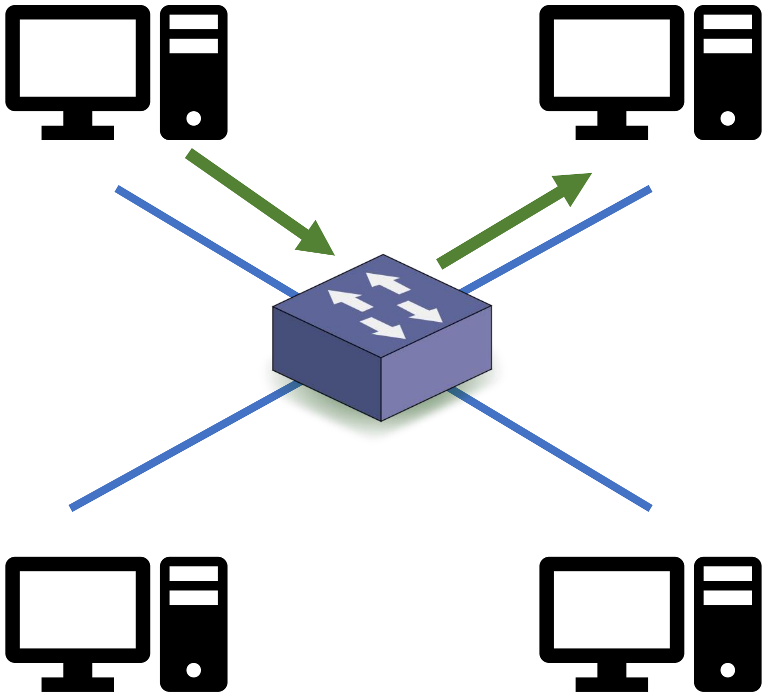
Hub

- L1 device
- Repeats the traffic on one port to other ports (i.e., broadcast)
- Usages:
  - Mirror traffic for analysis
  - Making multiple network devices act as one segment
- Obsolete and rarely deployed in modern networks



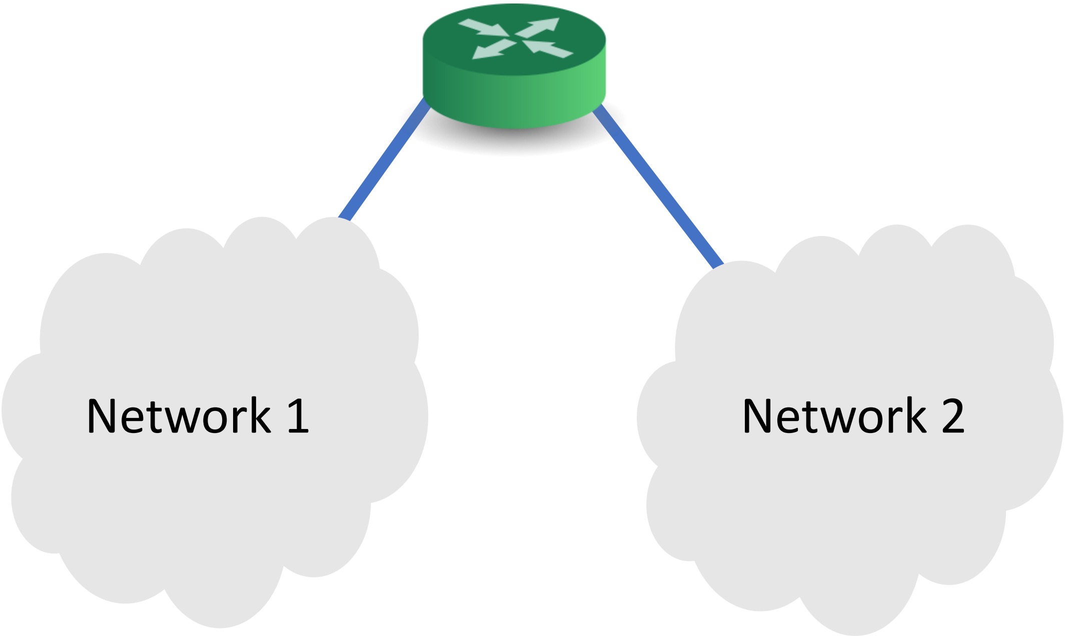
Ethernet Switch

- L2 device
- Decides outgoing port based on dst MAC
- Maintains a mapping between MAC address and outgoing ports
  - Using a CAM table
- Modern switches become smarter
  - Programmable and bare-metal



Router

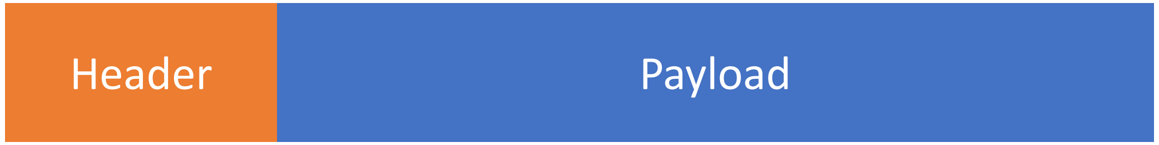
- L3 device
- Forwards packets based on IP address
  - How?



Dissecting Packets

Recall: Packet Switching

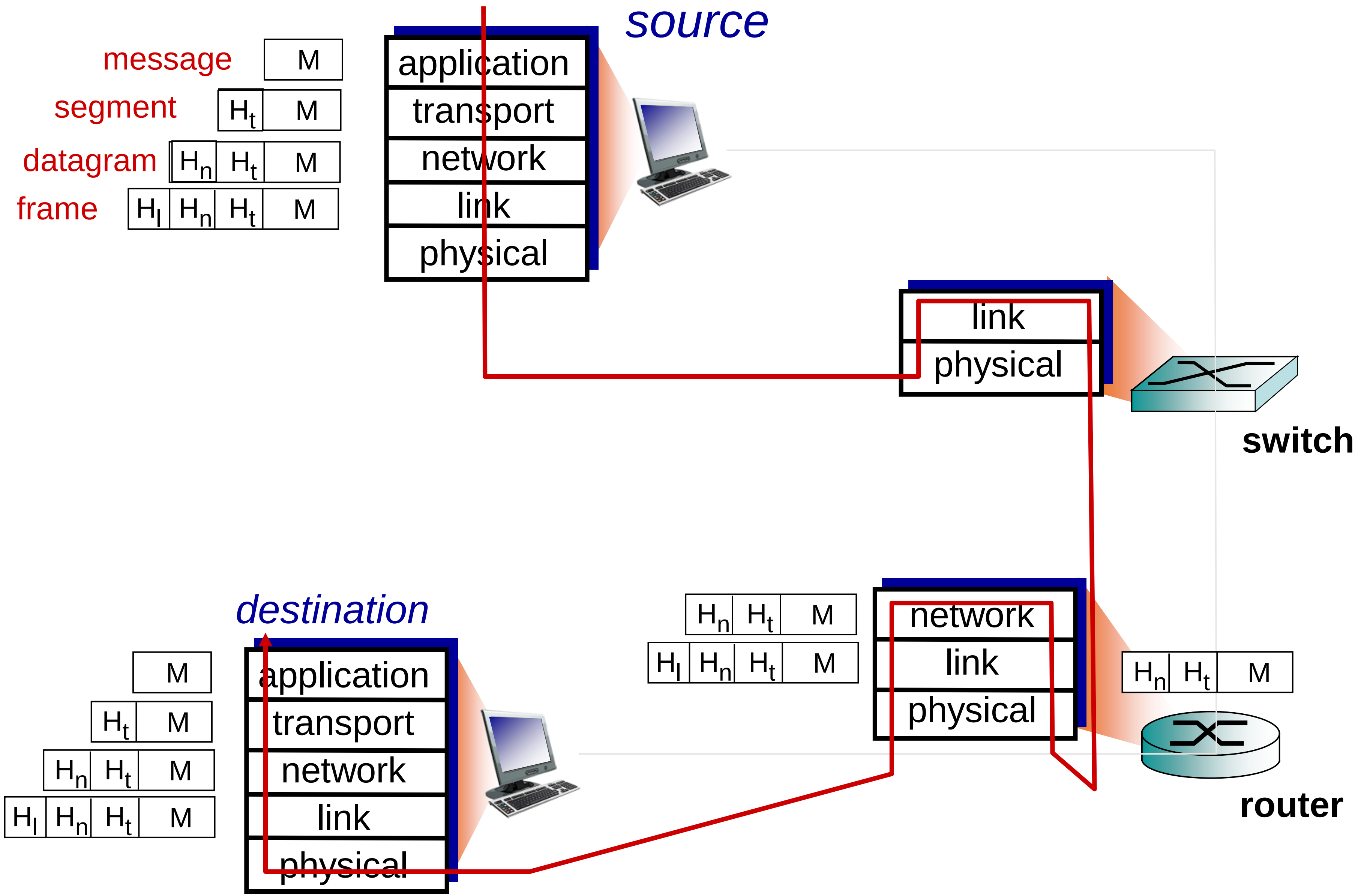
- Packet Switching: Hosts break application-layer messages into packets
  - Forward packets from one router to the next, across links on path from source to destination
  - Each packet is transmitted at full link capacity (no reservation)
- The header of each packet carries necessary information
  - Routers examine the header and make forwarding decisions



Header

Payload

Recall: Encapsulation



Packet Representation

- Packet is a sequence of bytes
  - Formatted based on the rules of protocols
  - Multiple fields, each has a specific value

- Binary representation:
  - Sequence of 0’s and 1’s
  - E.g.,
    ```
    100010100000000000000000011110001010000110110110000000000
    00000010000000000000011100111110001110
    ```
  - Hard to read

Packet Representation

- Hex representation
- Uses numbers 0–9 and letters a–f
- A byte is represented using two characters
  - E.g., 2a is one byte
- In a byte, a nibble has 4 bits
  - 4 bits represent a character from 0—f

20 bytes

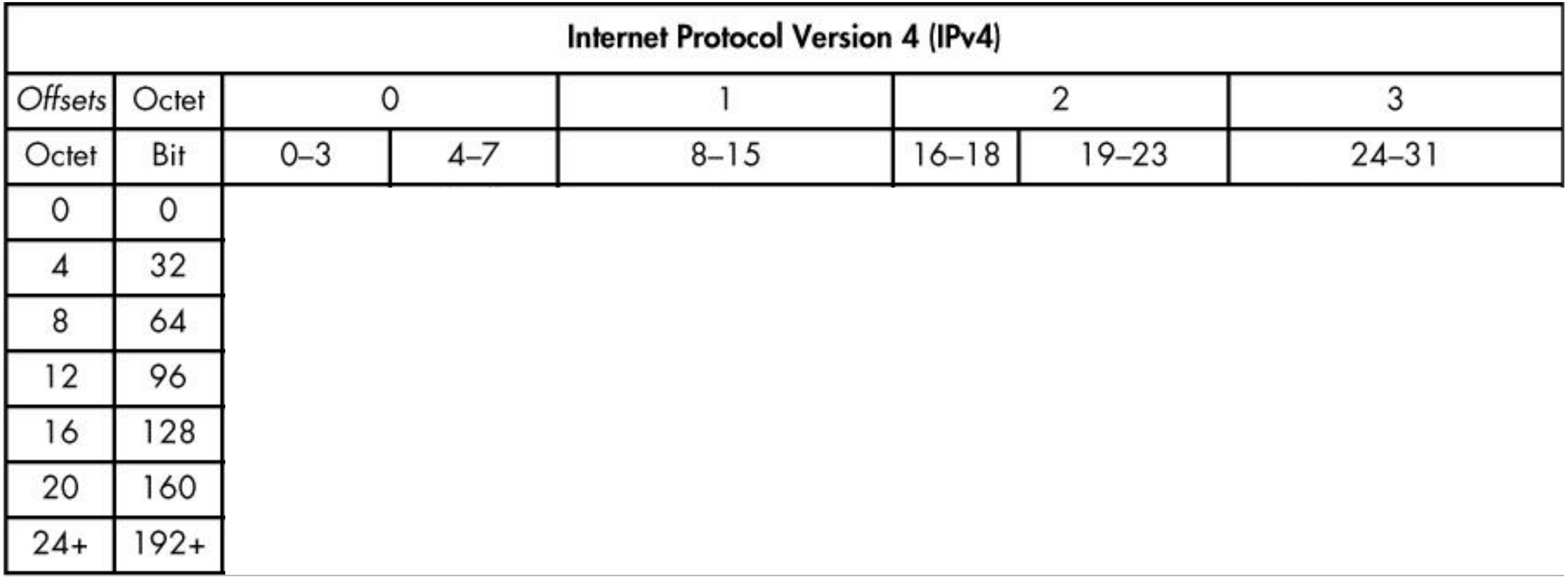
2 bytes

```
4500 003c 50db 0000 8001 cf8e 0a00 0048
0808 0808
```

What is this protocol? What is missing information?

Packet Diagram

- A graphical representation of a packet
  - Allows analysts to map bytes to fields
  - Often based on protocol’s RFC

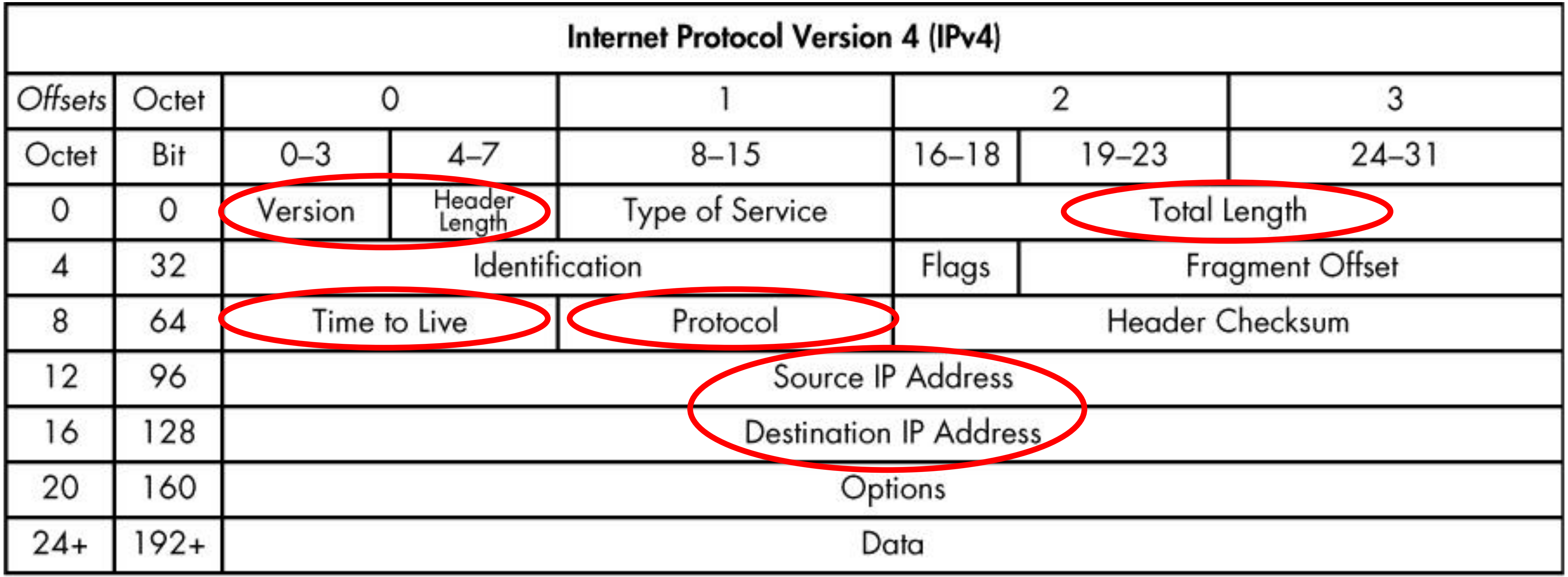


Internet Protocol Version 4 (IPv4)

Offsets	Octet	0		1	2		3
Octet	Bit	0–3	4–7	8–15	16–18	19–23	24–31
0	0						
4	32						
8	64						
12	96						
16	128						
20	160						
24+	192+						

Packet Diagram

- A graphical representation of a packet
  - Allows analysts to map bytes to fields
  - Often based on protocol's RFC

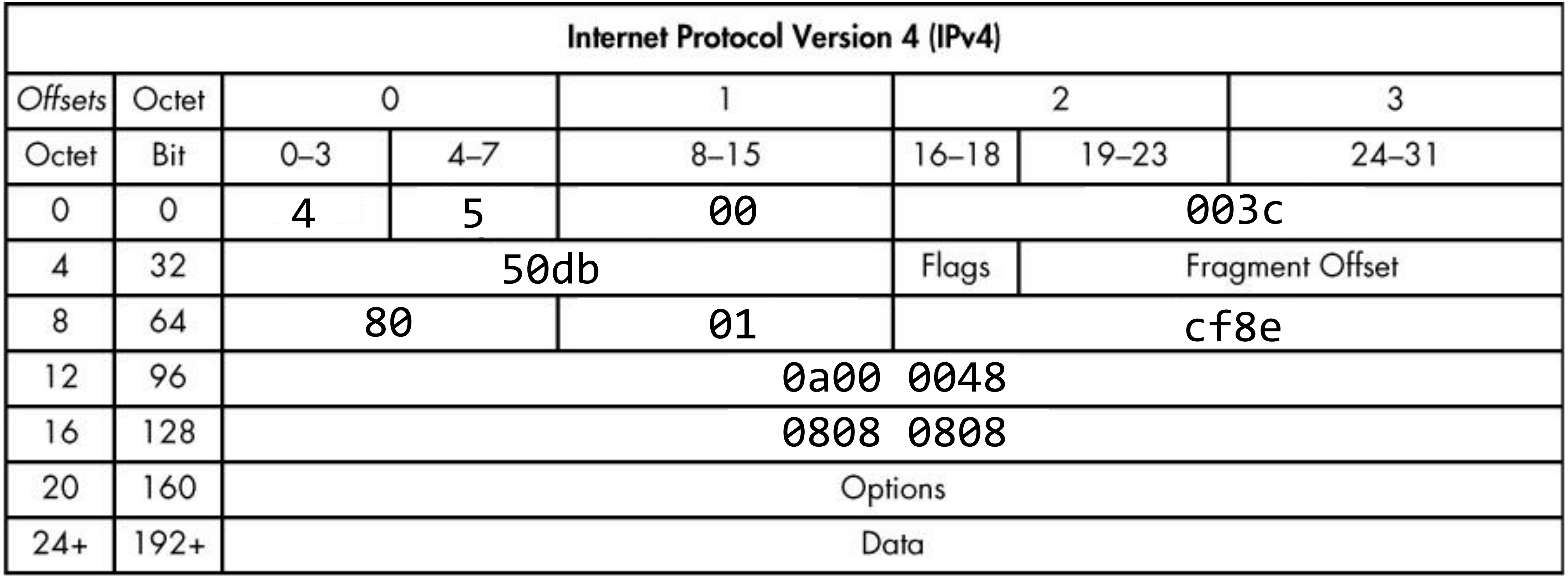


Internet Protocol Version 4 (IPv4)

Offsets	Octet	0		1	2		3
Octet	Bit	0–3	4–7	8–15	16–18	19–23	24–31
0	0	Version	Header Length	Type of Service	Total Length		
4	32	Identification			Flags	Fragment Offset	
8	64	Time to Live		Protocol	Header Checksum		
12	96	Source IP Address					
16	128	Destination IP Address					
20	160	Options					
24+	192+	Data					

Packet Diagram

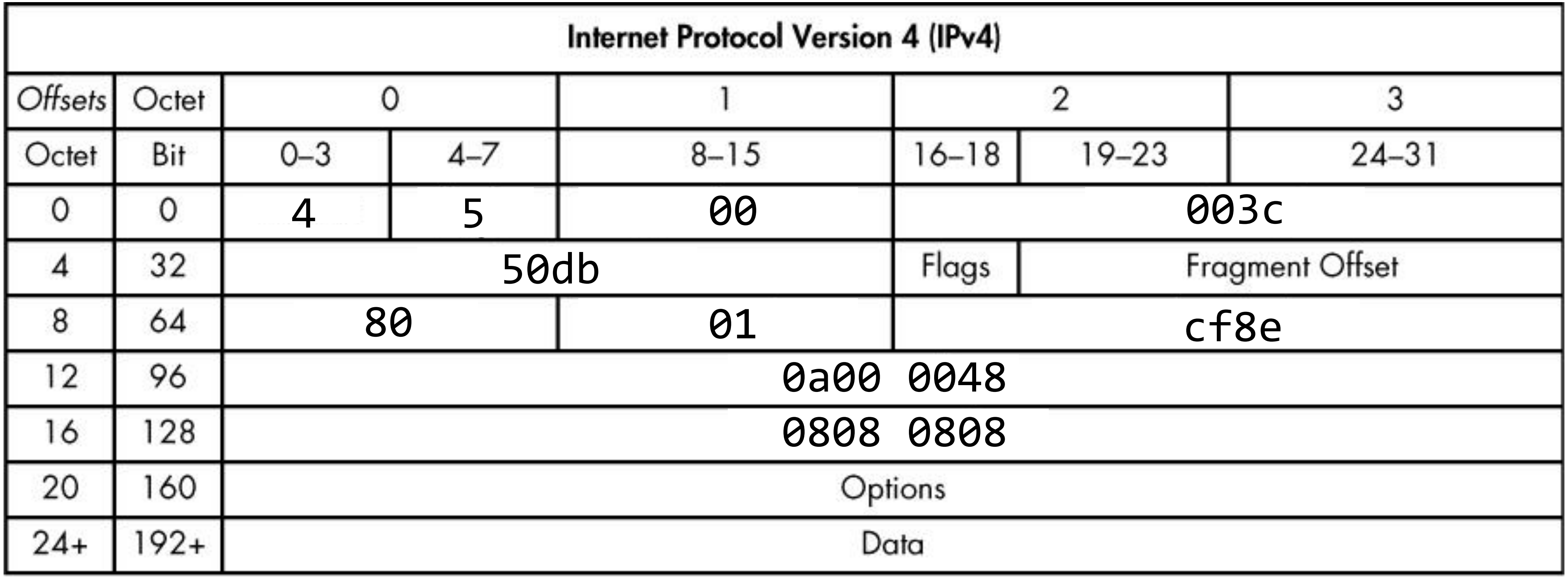
```
4500 003c 50db 0000 8001 cf8e 0a00 0048
0808 0808
```



Internet Protocol Version 4 (IPv4)							
Offsets	Octet	0		1	2		3
Octet	Bit	0–3	4–7	8–15	16–18	19–23	24–31
0	0	4	5	00	003c		
4	32	50db			Flags	Fragment Offset	
8	64	80		01	cf8e		
12	96	0a00 0048					
16	128	0808 0808					
20	160	Options					
24+	192+	Data					

Packet Diagram

- Protocol is 0x01. What is this protocol?
- Check IP protocol numbers.



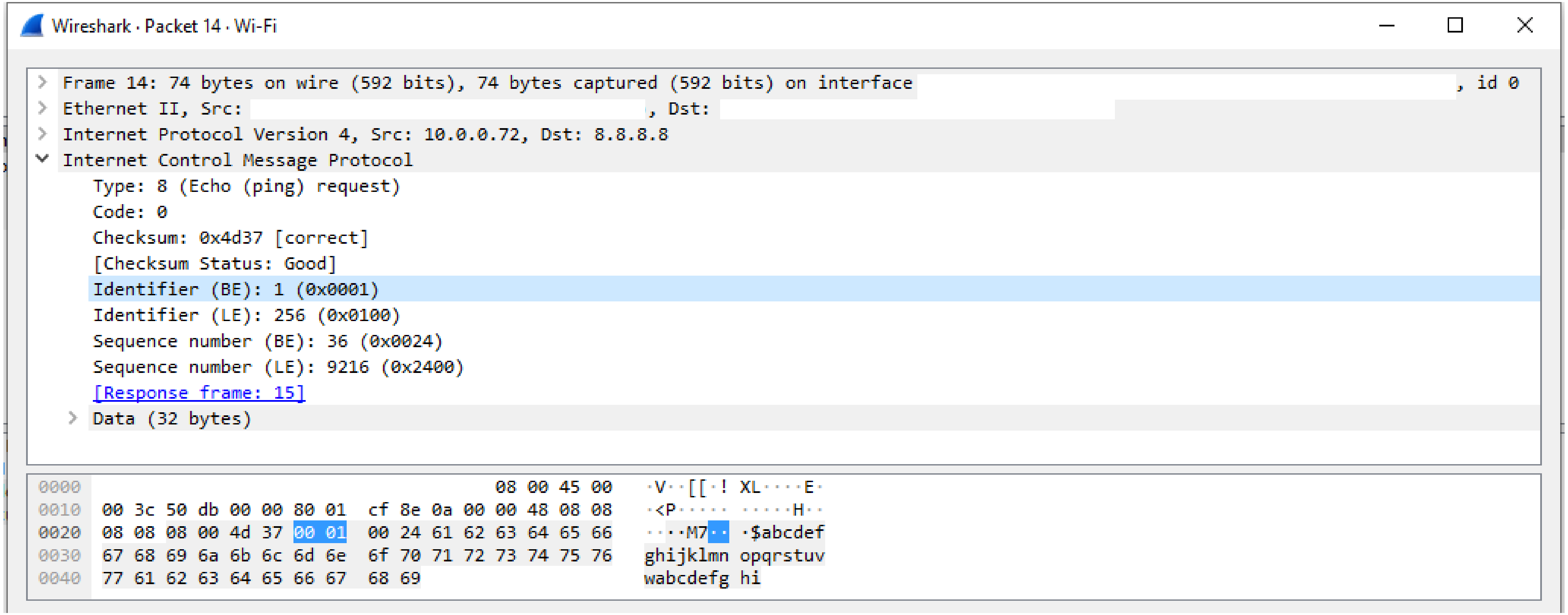
Internet Protocol Version 4 (IPv4)							
Offsets	Octet	0		1	2		3
Octet	Bit	0–3	4–7	8–15	16–18	19–23	24–31
0	0	4	5	00	003c		
4	32	50db			Flags	Fragment Offset	
8	64	80		01	cf8e		
12	96	0a00 0048					
16	128	0808 0808					
20	160	Options					
24+	192+	Data					

IP Protocol Numbers: Examples

Protocol Number (Hex)	Protocol
`0x01`	ICMP
`0x06`	TCP
`0x11`	UDP
`0x29`	IPv6 (why?)
`0x2f`	GRE
`0x59`	OSPF

Tools for Dissecting Packets

- Various tools can be used to dissect and decode a packet



Wireshark · Packet 14 · Wi-Fi

```
> Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface [redacted], id 0
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: 10.0.0.72, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d37 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 36 (0x0024)
    Sequence number (LE): 9216 (0x2400)
    [Response frame: 15]
  > Data (32 bytes)
```

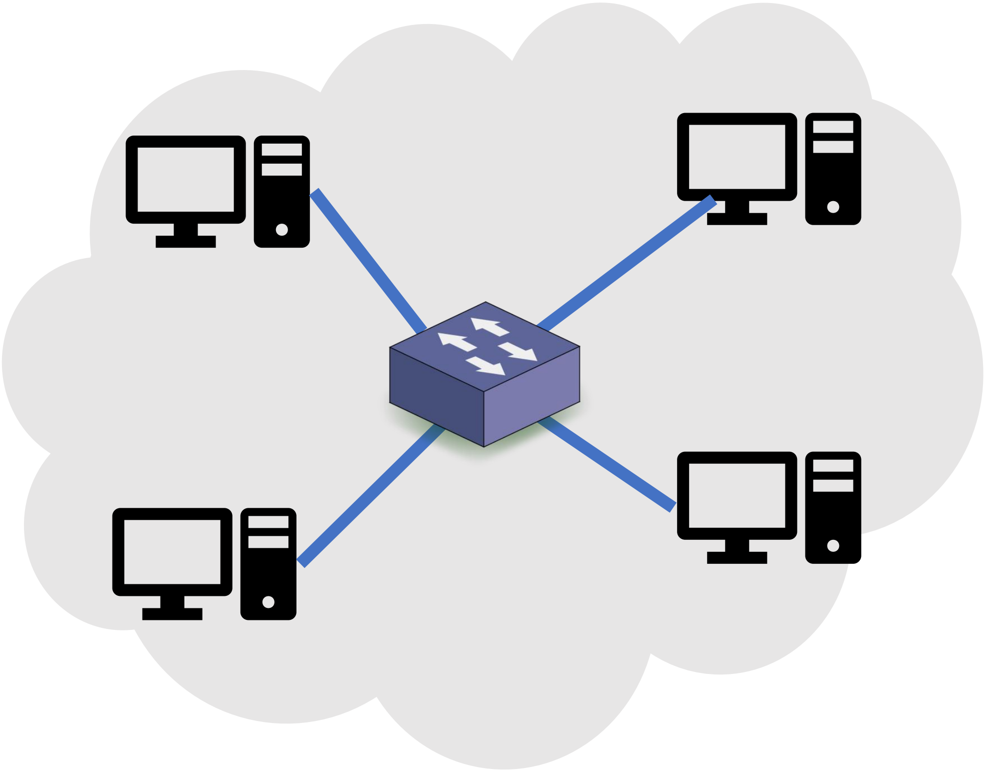
```
0000  [redacted]                          08 00 45 00   ·V··[[·! XL····E·
0010  00 3c 50 db 00 00 80 01  cf 8e 0a 00 00 48 08 08   ·<P····· ·····H··
0020  08 08 08 00 4d 37 00 01  00 24 61 62 63 64 65 66   ····M7·· ·$abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

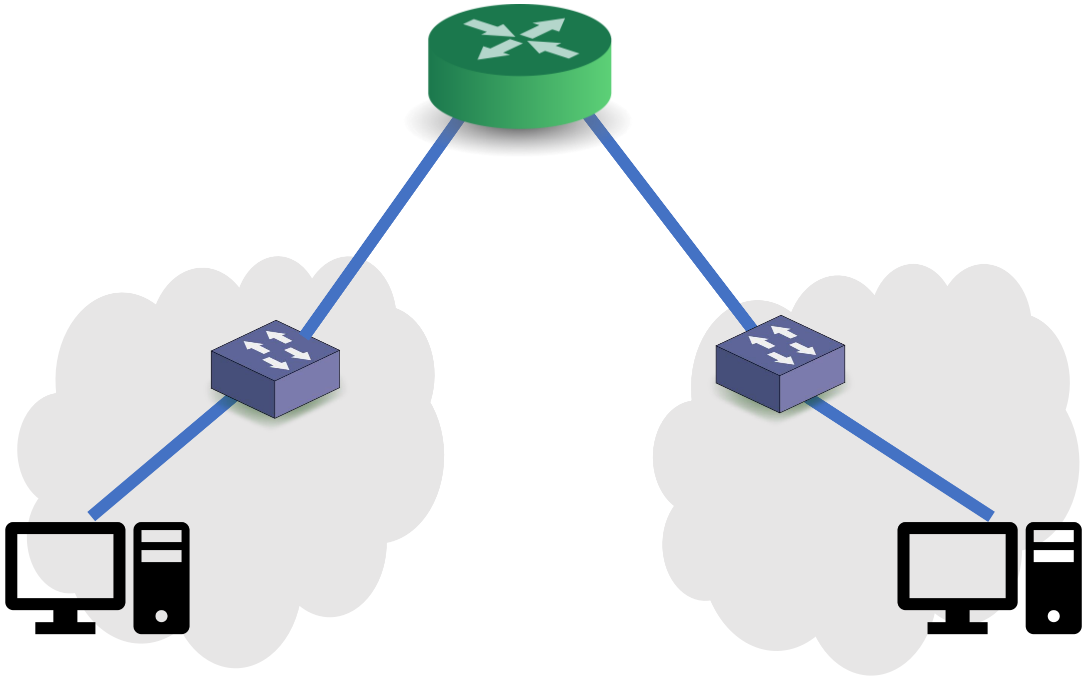
Sample of Network Protocols

ARP and ICMP

Address Resolution Protocol (ARP)

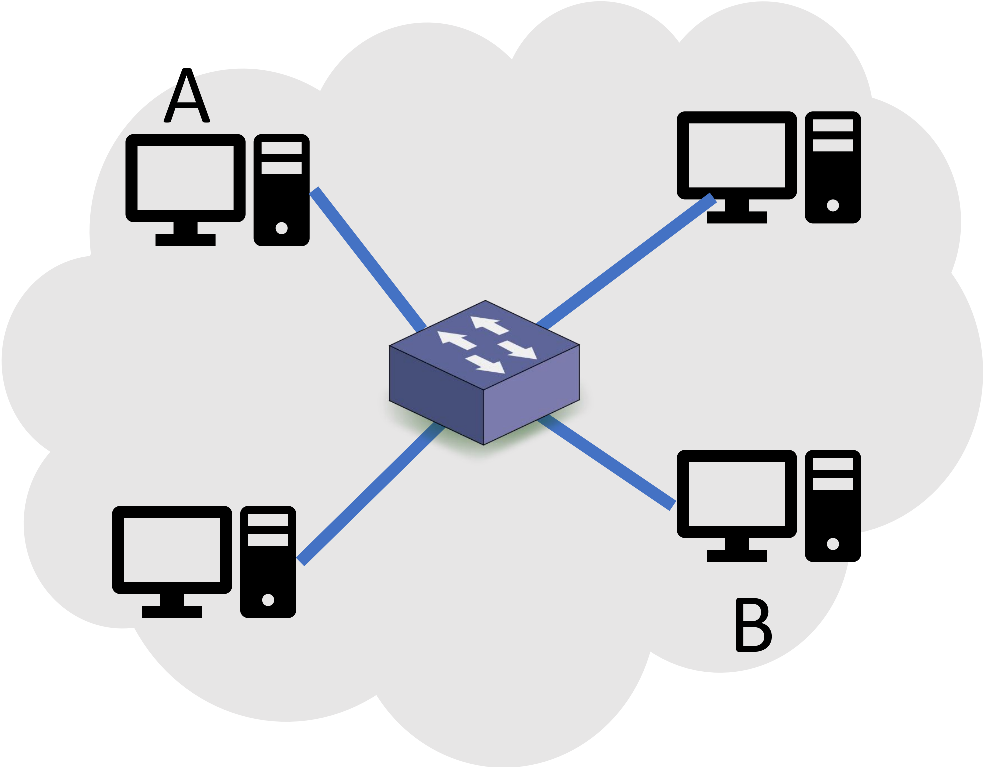
- Two types of addresses are used for communication:
  - Physical (e.g., MAC): within a single network
  - Logical (e.g., IP): among multiple networks, and indirectly connected devices





Address Resolution Protocol (ARP)

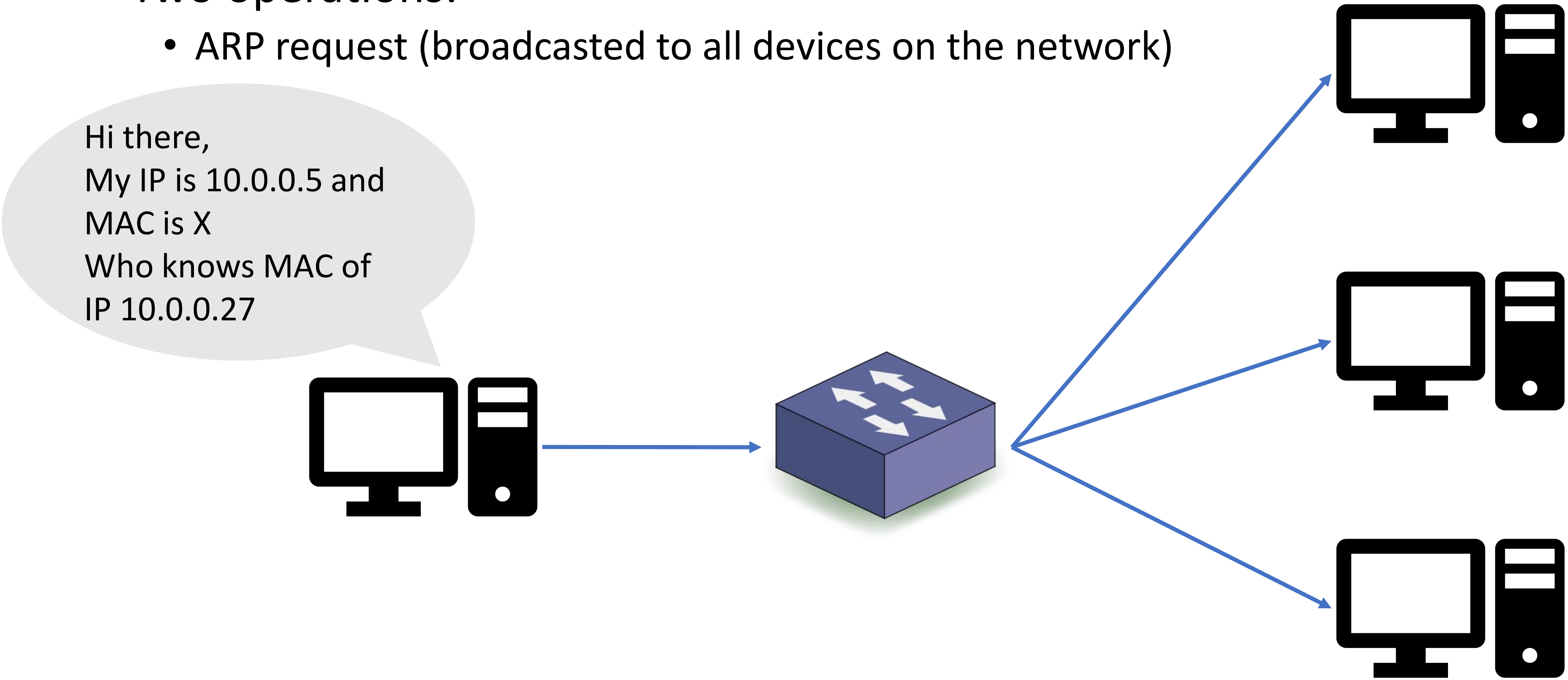
- Consider the case when:
  - an application at A communicates with an app at B
- Device A needs to fill fields L2—L5
  - It has all the information of L3—L5 (why?)
- However, device A does not know the physical address of device B
  - A field in L2 (dst MAC)



ARP (RFC 826): a protocol to map an IP address to MAC address

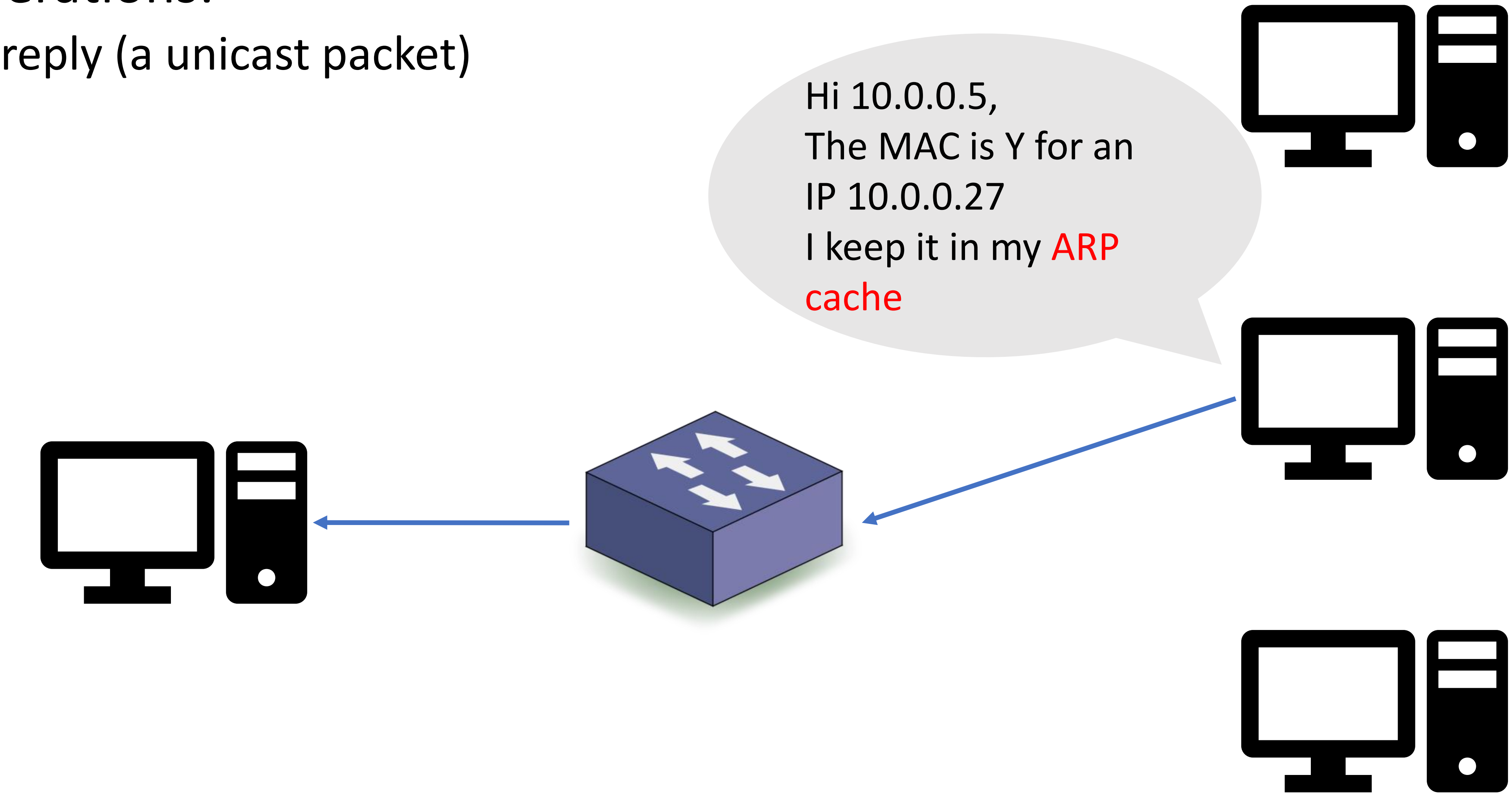
Address Resolution Protocol (ARP)

- Two operations:
  - ARP request (broadcasted to all devices on the network)

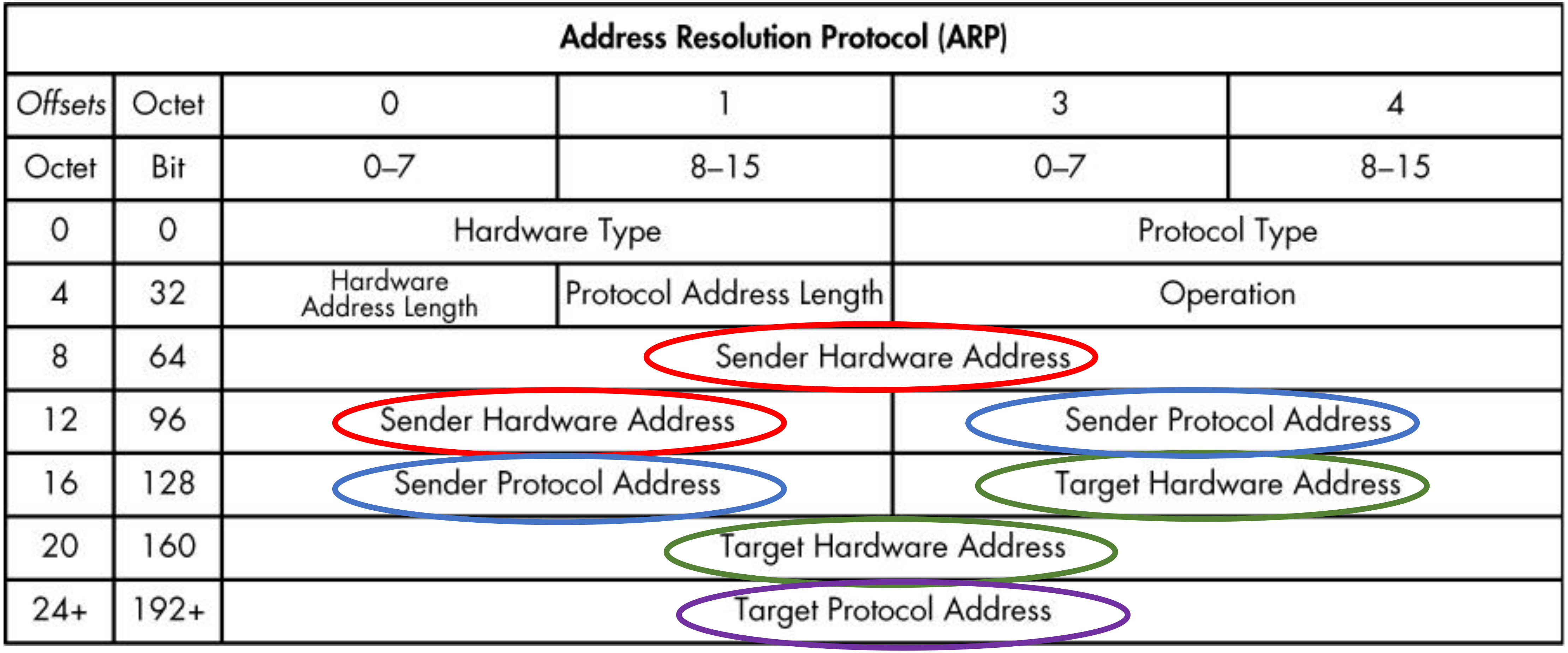


Address Resolution Protocol (ARP)

- Two operations:
  - ARP reply (a unicast packet)



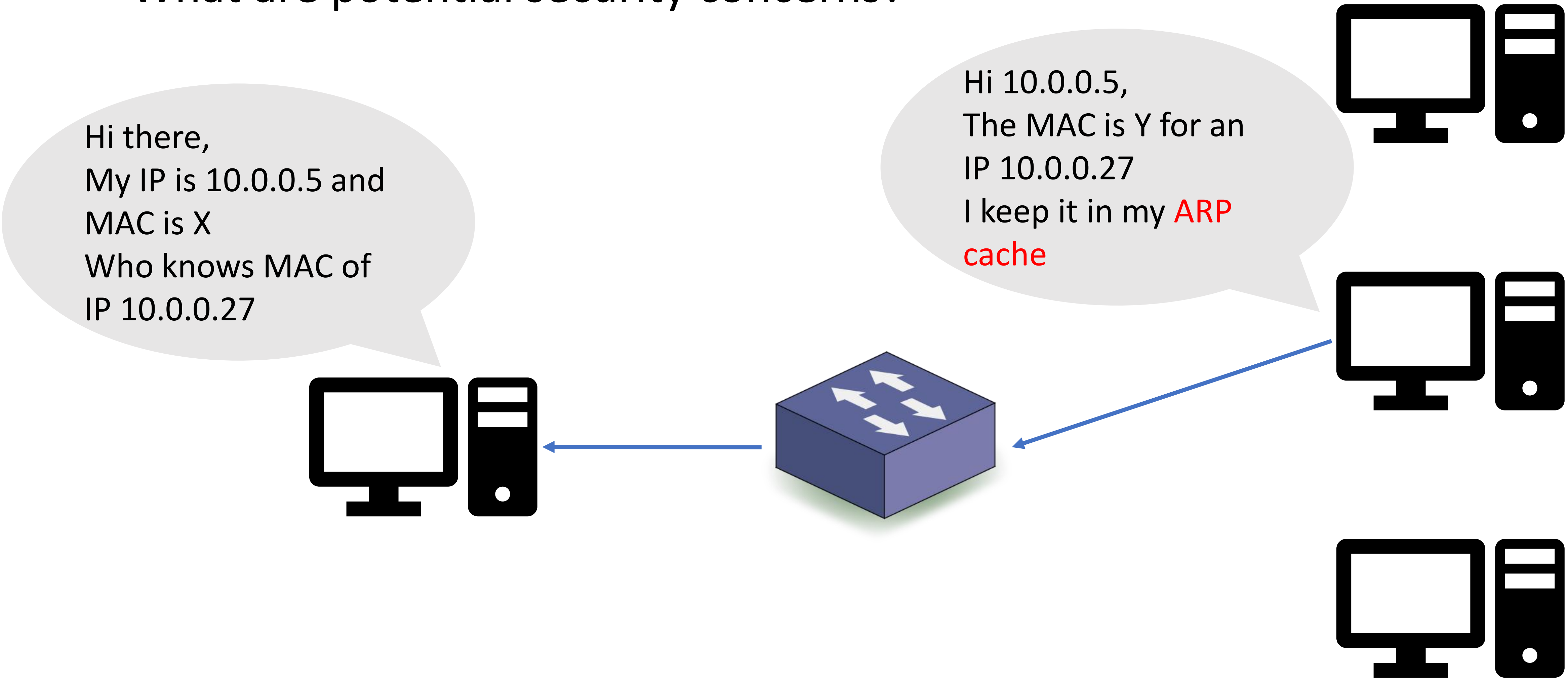
ARP Packet Structure



Address Resolution Protocol (ARP)					
Offsets	Octet	0	1	3	4
Octet	Bit	0–7	8–15	0–7	8–15
0	0	Hardware Type		Protocol Type	
4	32	Hardware Address Length	Protocol Address Length	Operation	
8	64	Sender Hardware Address			
12	96	Sender Hardware Address		Sender Protocol Address	
16	128	Sender Protocol Address		Target Hardware Address	
20	160	Target Hardware Address			
24+	192+	Target Protocol Address			

Address Resolution Protocol (ARP)

- What are potential security concerns?



Hi there,
My IP is 10.0.0.5 and
MAC is X
Who knows MAC of
IP 10.0.0.27

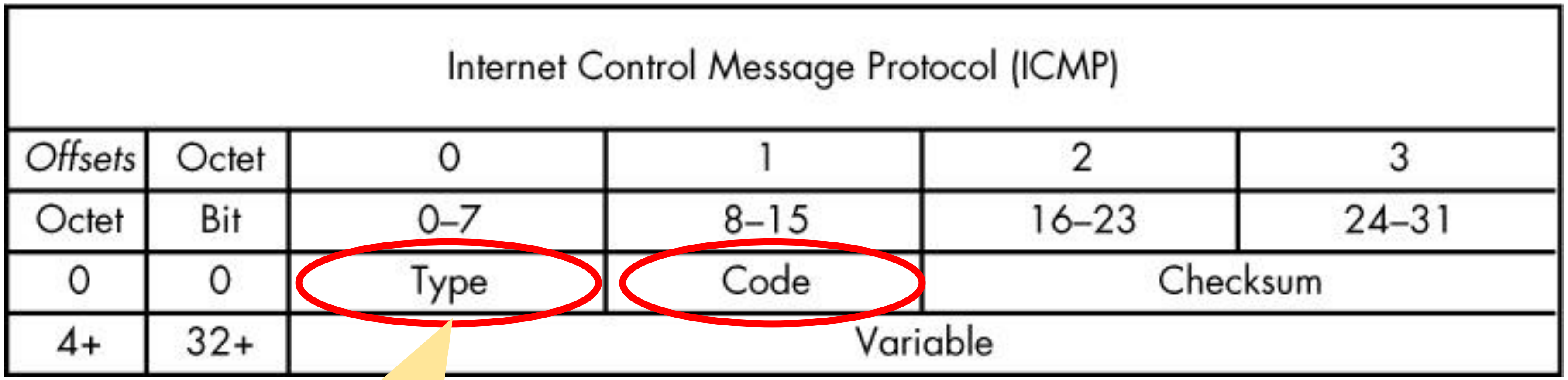
Hi 10.0.0.5,
The MAC is Y for an
IP 10.0.0.27
I keep it in my ARP
cache

Internet Control Message Protocol (ICMP)

- RFC 792
- A utility protocol of TCP/IP
- Provides information about availability of:
    - Devices, services, or routes on a TCP/IP network

- Popular utilities that use ICMP?

ICMP Packet Structure

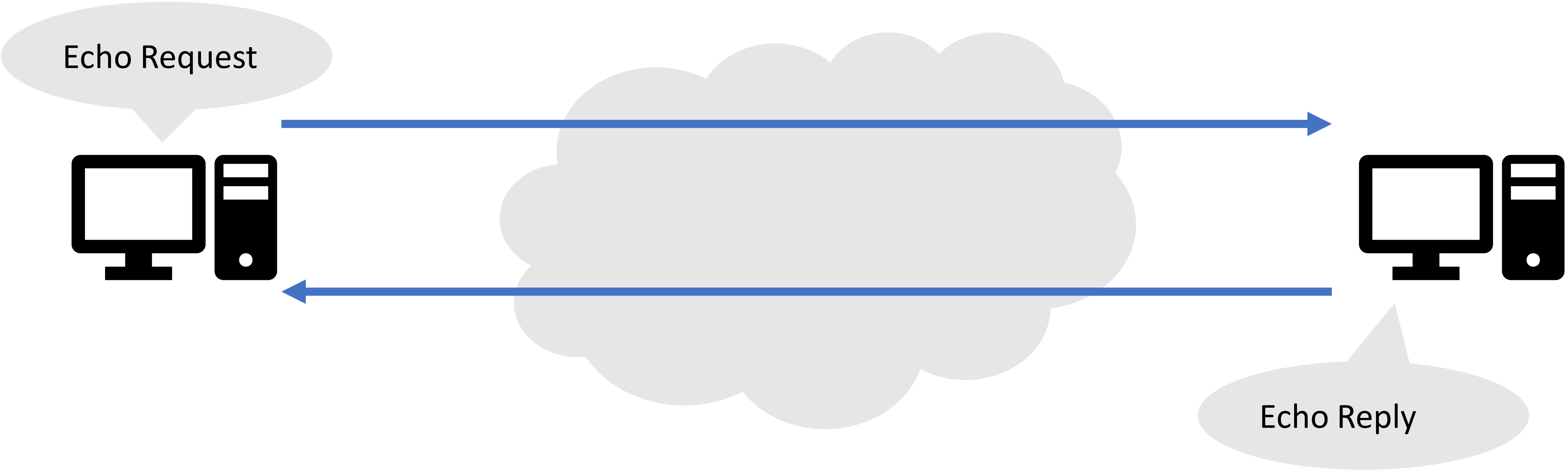


Internet Control Message Protocol (ICMP)					
Offsets	Octet	0	1	2	3
Octet	Bit	0–7	8–15	16–23	24–31
0	0	Type	Code	Checksum	
4+	32+	Variable			

0 : Echo Reply
8 : Echo Request
11: Time Exceeded

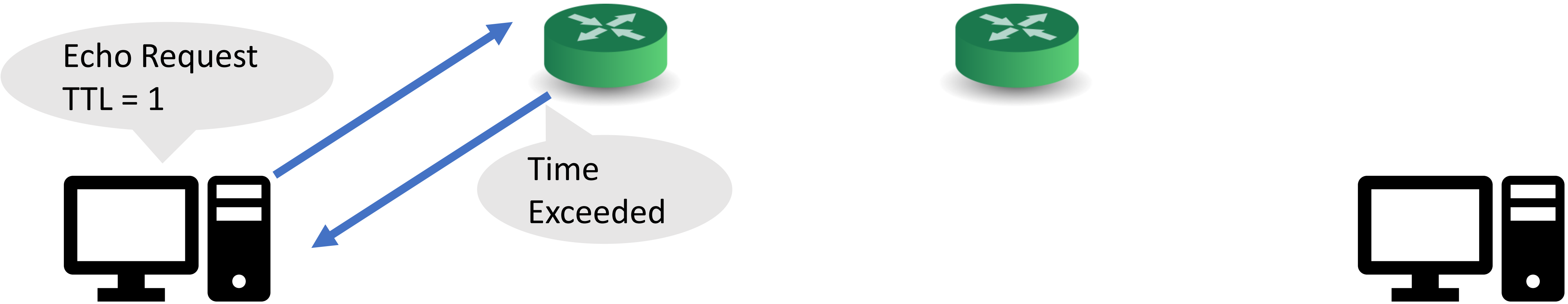
ICMP: `ping`

Often used to check availability



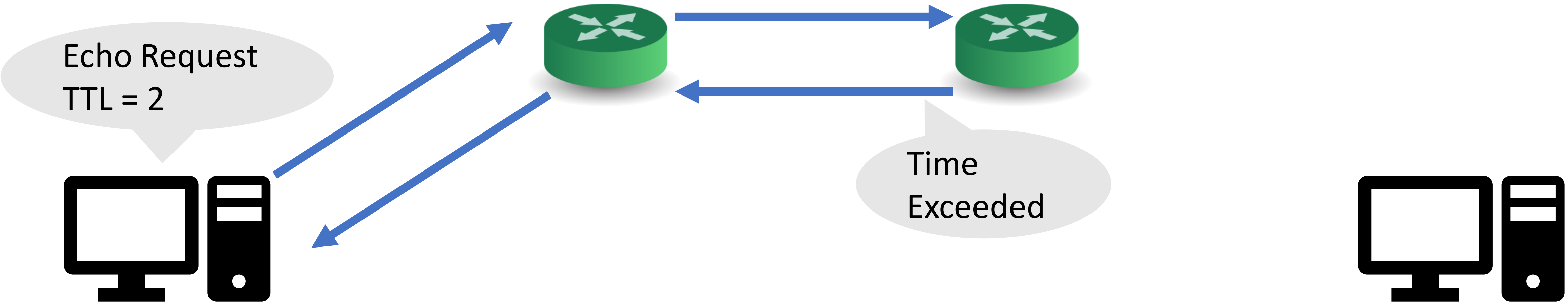
ICMP: `traceroute`

Build a path of routers from source to destination. How?



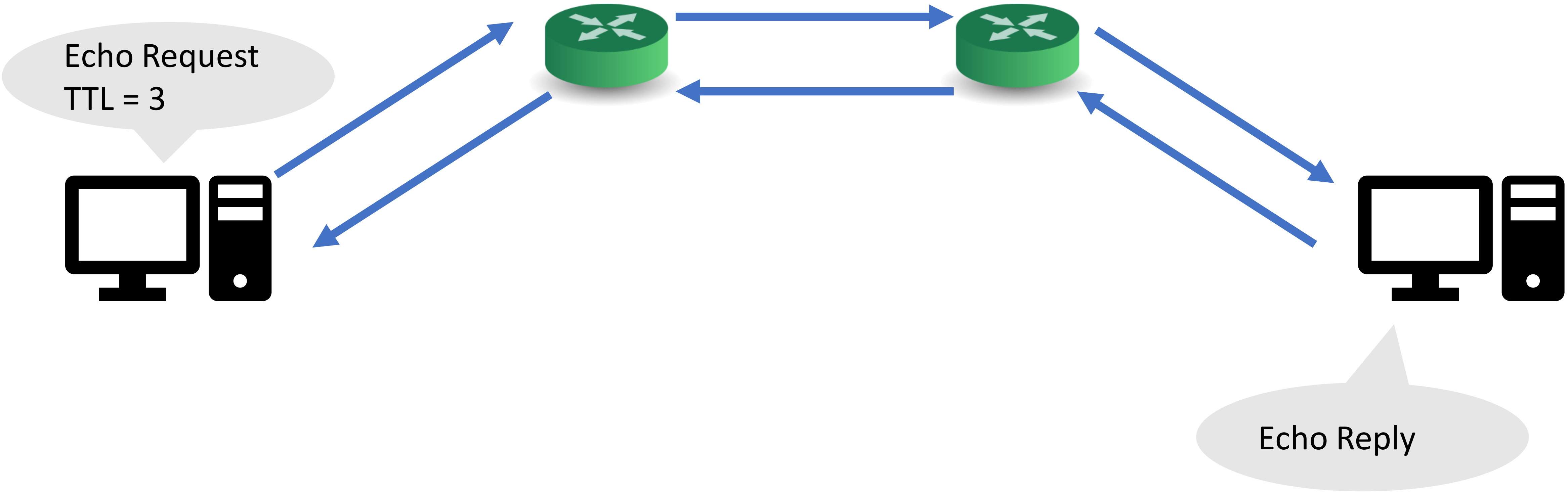
ICMP: `traceroute`

Build a path of routers from source to destination. How?



ICMP: `traceroute`

Build a path of routers from source to destination. How?



To do list

- Start using Wireshark
- Get familiar with packet diagrams and major protocols:
  - IP, ARP, ICMP, DNS, TCP, UDP

Next Lecture

- Packet Sniffing
- Packet Spoofing