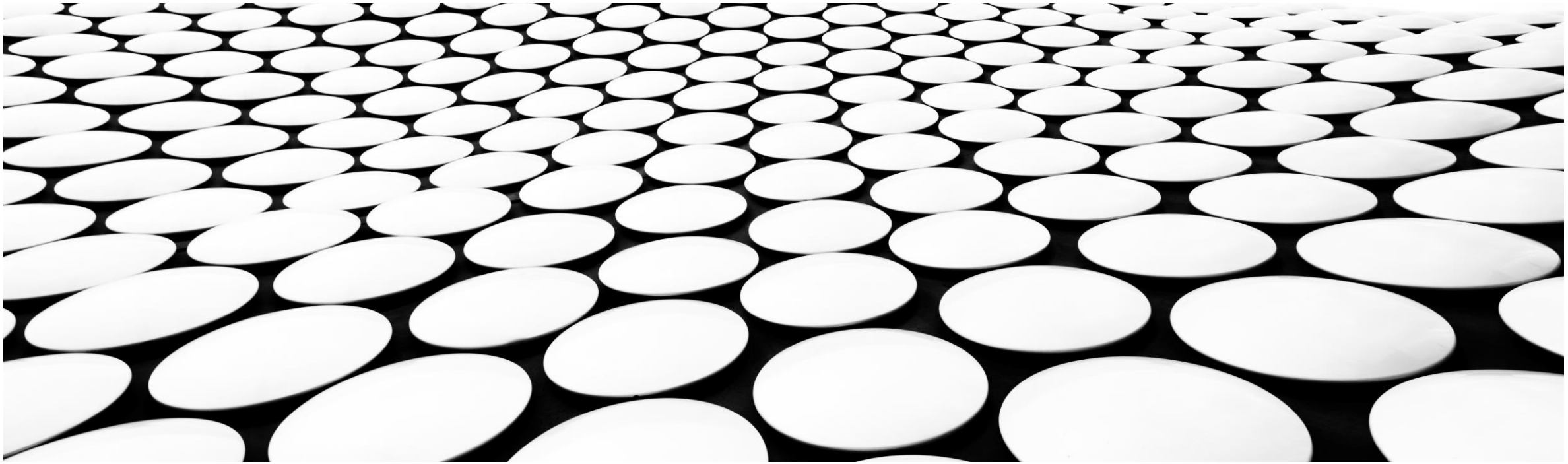
COMPUTER NETWORKS

INTERNETWORKING

HEMANT GHAYVAT, (hemant.ghayvat@lnu.se)

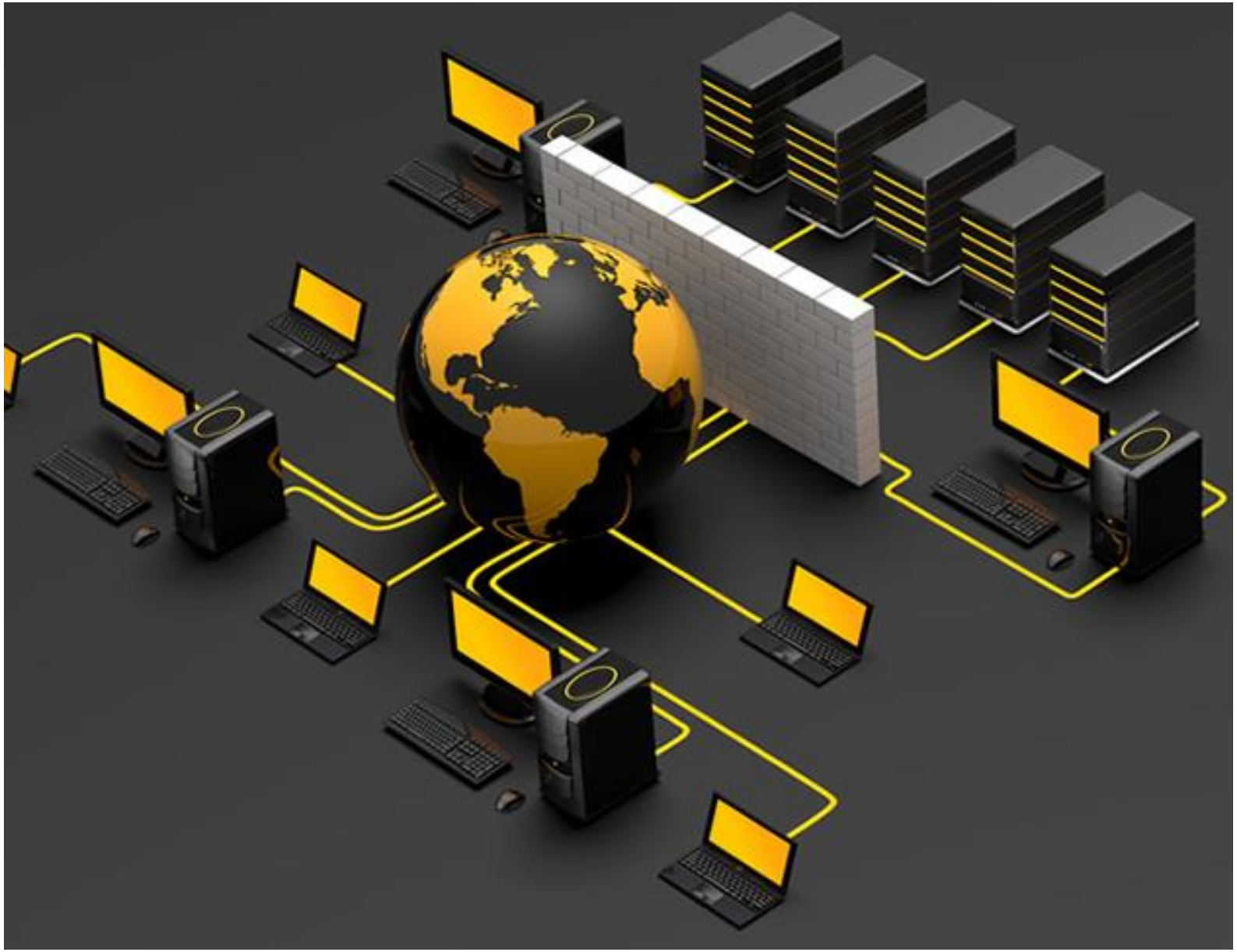


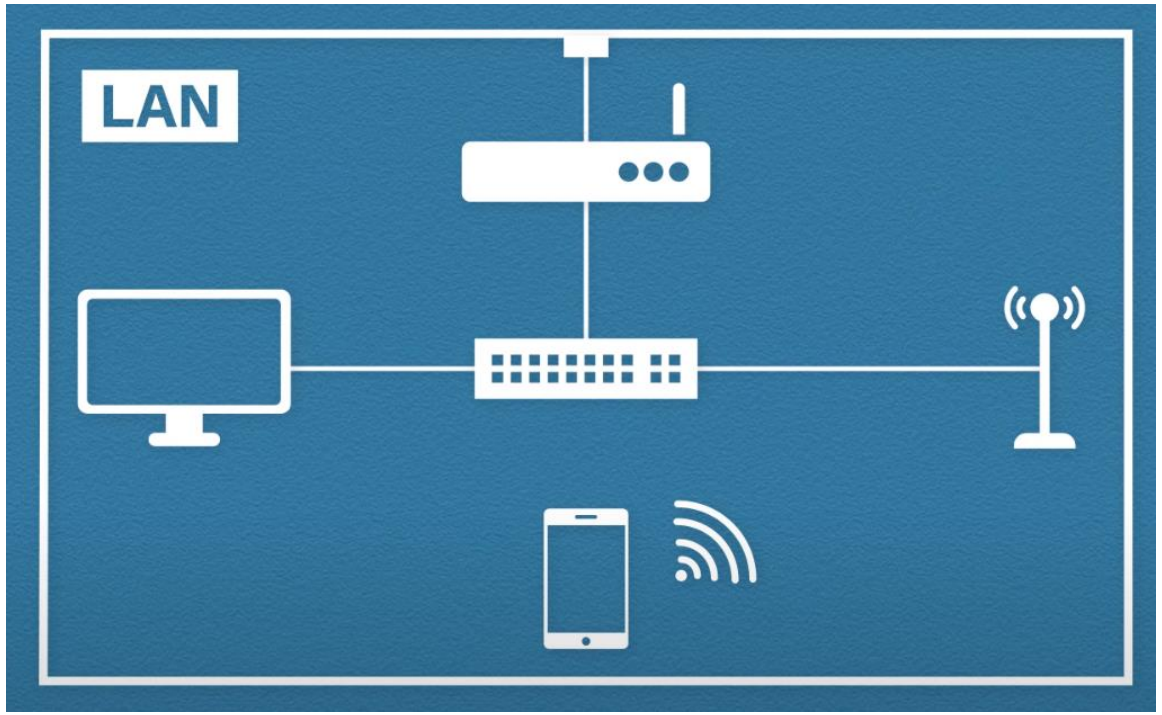
THIS WEEK

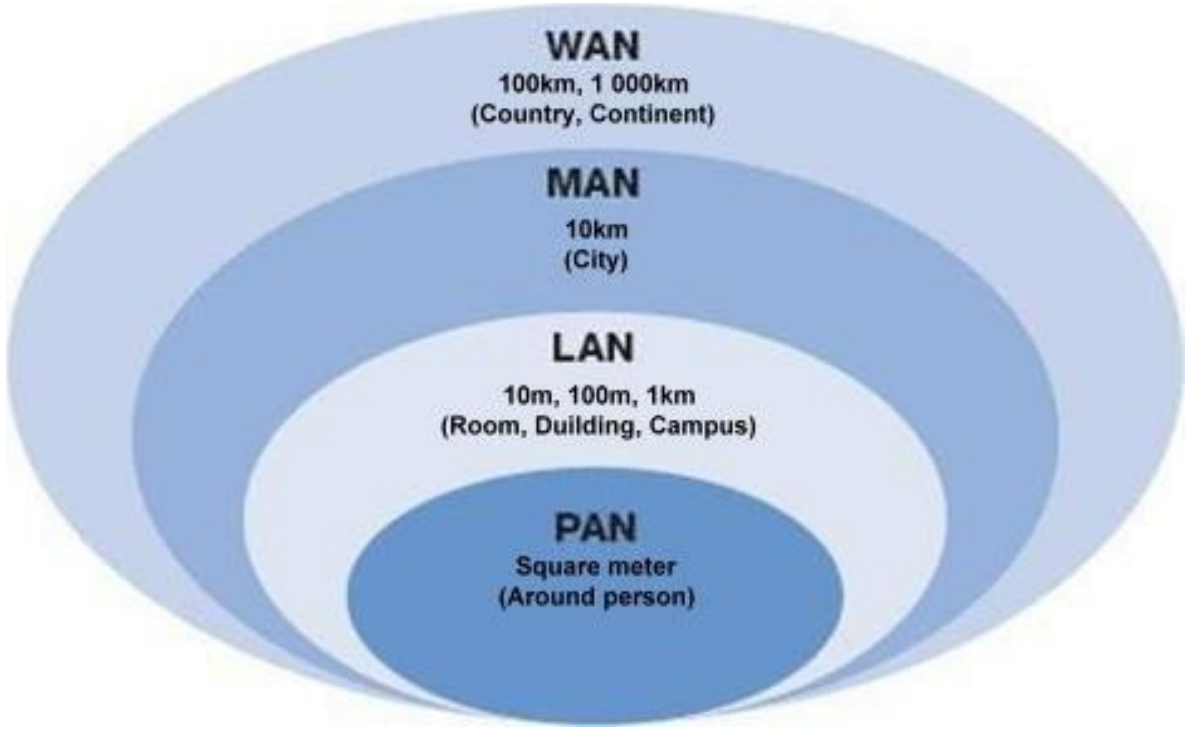
- Introduction to and motivation for internetworking
- Universal service
- Intranets and Internets
- Protocols and layers
- The Internet Protocol (v4 and v6)
- IP addressing, schemes and hierarchies
- Classless addressing
- Forwarding
- Best-effort delivery
- Fragmentation
- All references are over last slide

COMPUTER NETWORKING

- A system of interconnected things is the network
- Essentially a computer network is a group of computers (or other devices) interconnected, either by a cable or wirelessly via single technology





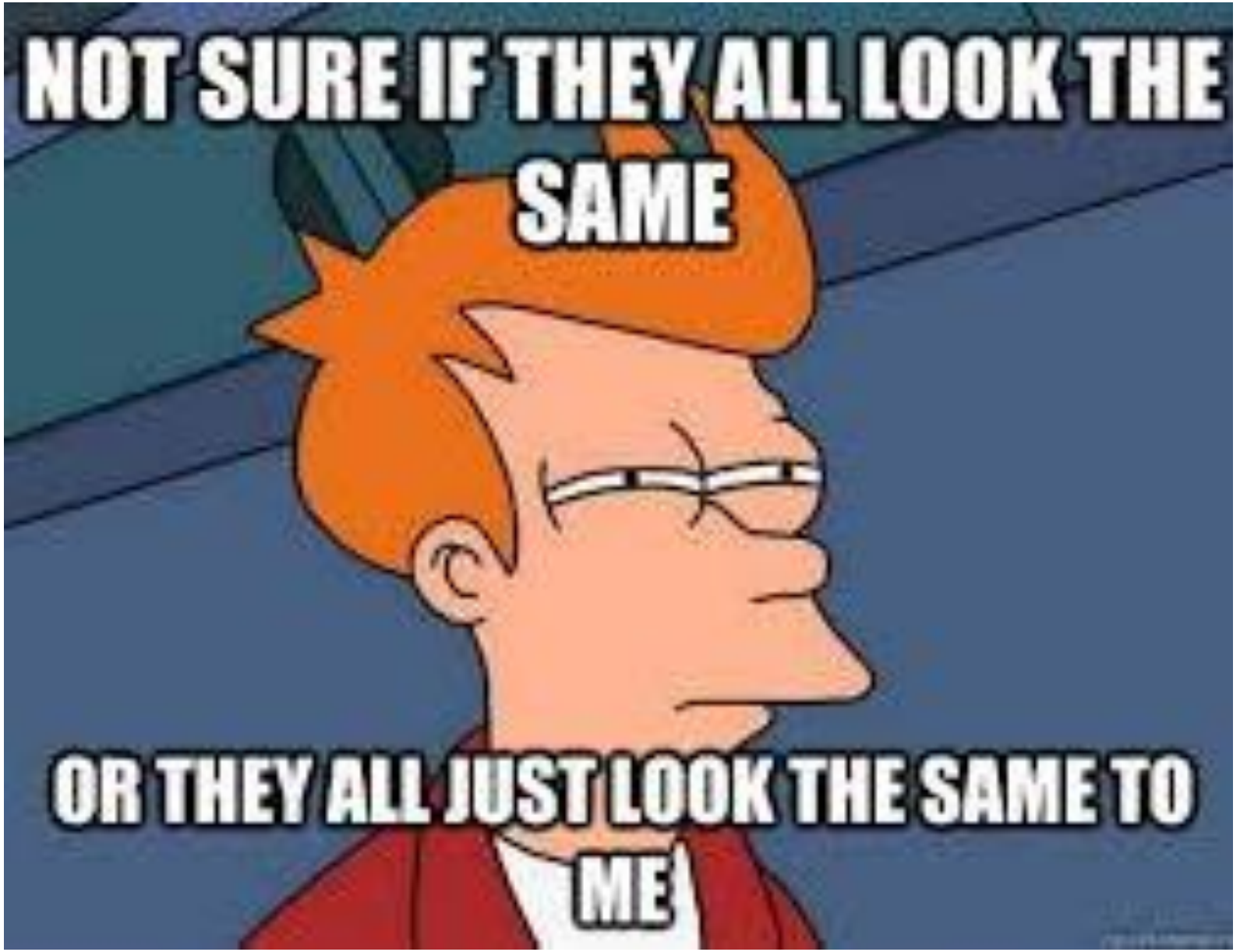


LAN, MAN AND WAN


WHY IS LAN FATER THAN OTHER TWO
??????

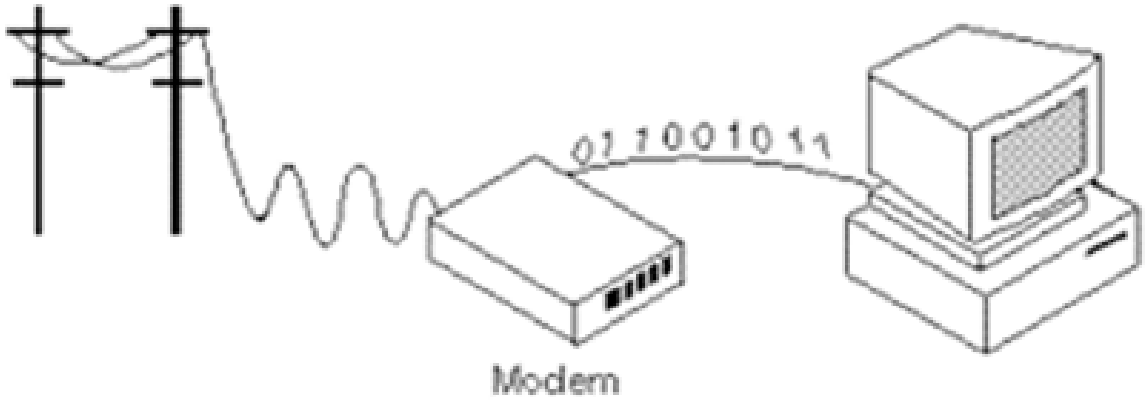
COMPUTER NETWORKING: MODEMS, ROUTERS, SWITCHES, & HUBS

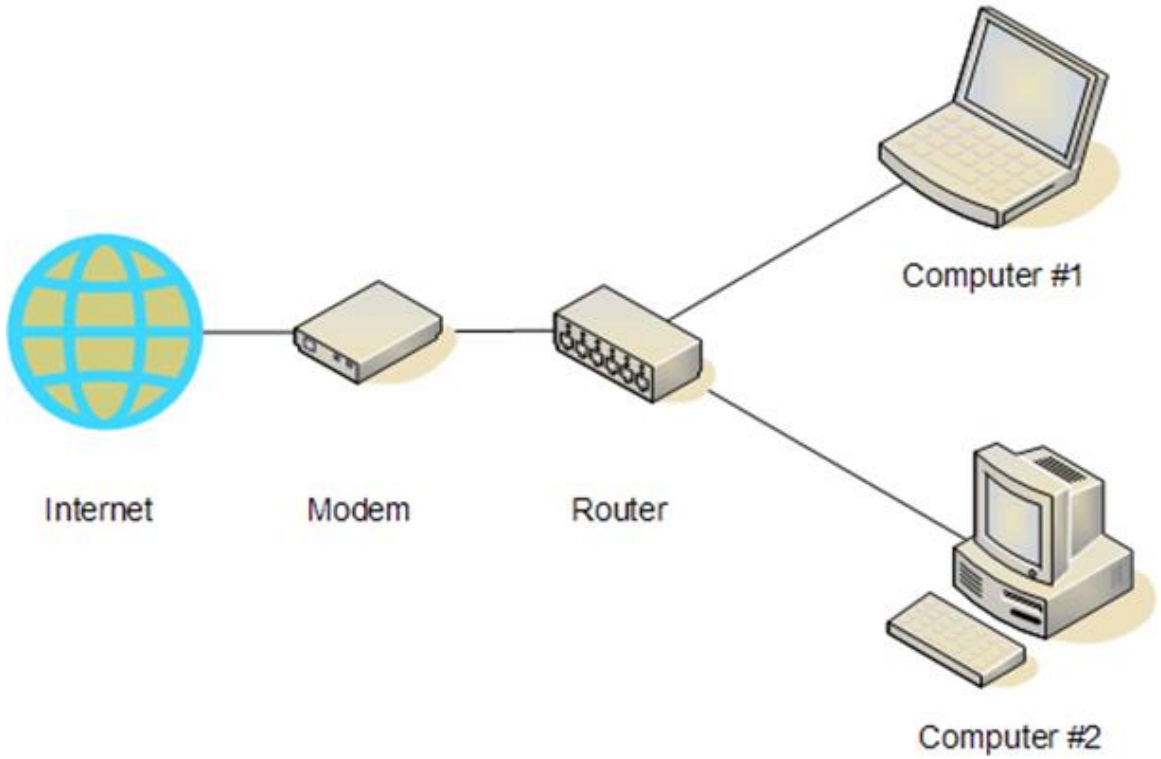
- Understanding Computer Networking could be highly challenging especially if it is your first time to delve into it. Computer networking is loaded with technical jargon, and devices that appear similar however perform very different functions. We will briefly go through a couple concepts and terminology that you will need to seamlessly understand the roles.



MODEM

- A modem is short for a **mo**dulator-**dem**odulator. Its function is to facilitate the transmission of data, by converting an **analogue signal to code** and **decoding digital information**. This means that it converts the telephone connection information into digital information for the computer to understand, and converts computer digits into analog waves so that it can be transmitted over telephone lines. It could be seen as the center for information collection from WAN, as it directly connects to the outside world.





ROUTER

- Routers pass the information provided by the modem and routes it to the devices in the network such as the home computers. The information transferred by a router can be directed to a specific device by its unique number or rather its IP address. As noted before each device in that network is labelled by an IP address that allows other devices to communicate with it.
- There are two ways to connect to a router:

- Wired: the device is connected by a wire directly to the router (or an attached switch)
- Wirelessly: the device is not connected with a wire but rather through WiFi.

SWITCH

- A switch connects two or more nodes in the same or different network. Unlike the router which labels through IP address, switches use MAC addresses to direct the data to its correct destination.
- A switch can be used connect multiple Network devices (such as a computer, laptop, printer etc.) to the Home LAN.

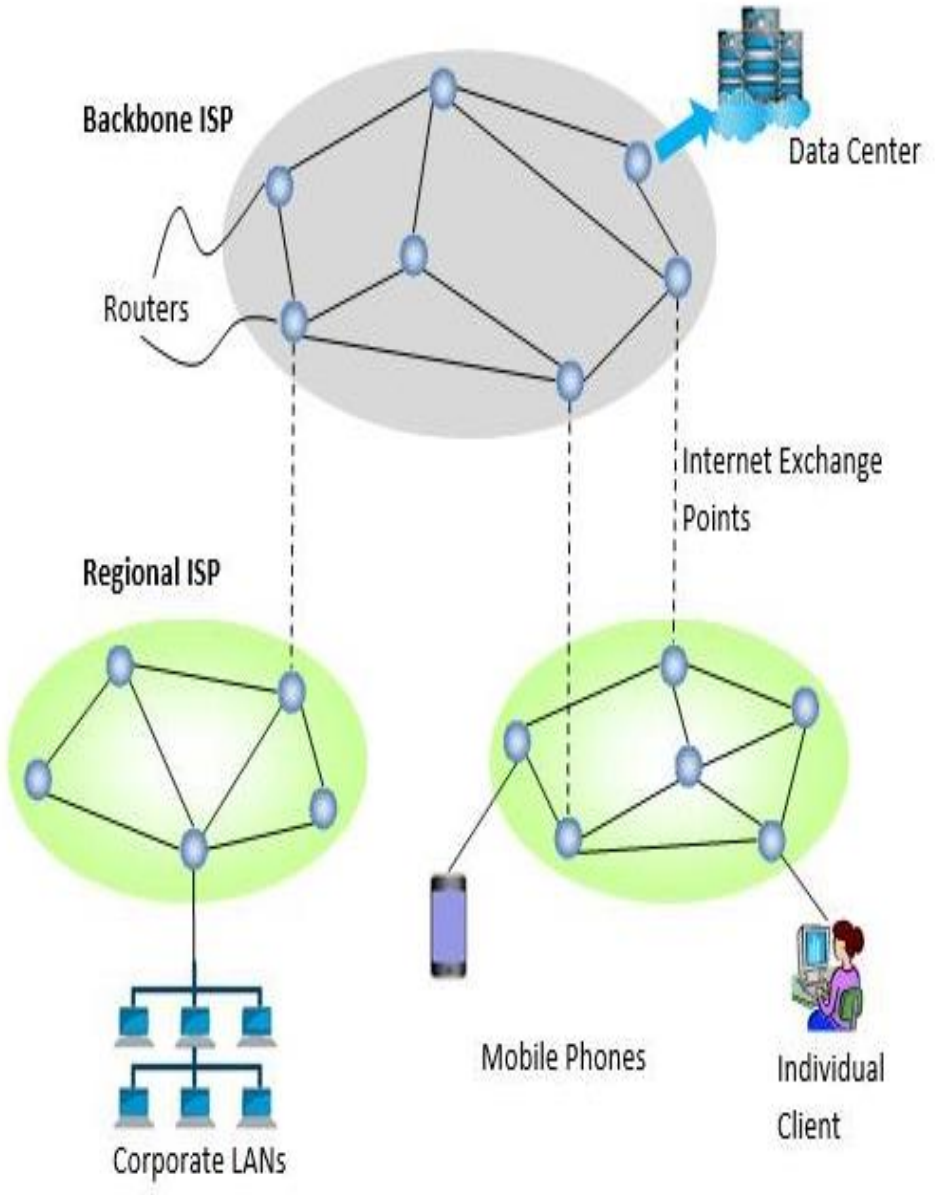
A typical router

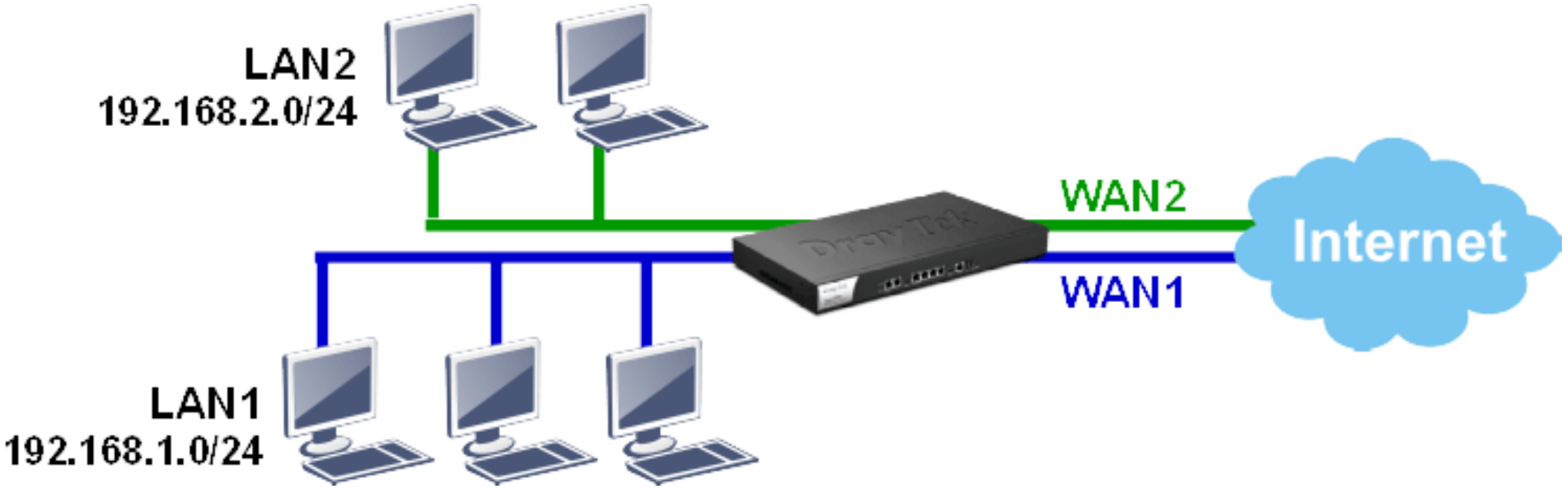
NETWORK HUB

- A hub is a device that allows several network devices to connect together to exchange data on a single network however, they have no management component. Network hubs are also known as repeaters. They are less ‘intelligent’ than switches. Unlike switches, which forward data to the intended devices, hubs merely send the data packets to all its ports. So as the name repeaters suggests, it only repeats the data from an incoming port to all the other devices; this leads to frequent collisions between packets.

INTERNET AND ISP

- A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
- The Internet is a global wide area network that connects computer systems across the world. It includes several high-bandwidth data lines that comprise the Internet "backbone." These lines are connected to major Internet hubs that distribute data to other locations, such as web servers and ISPs.
- **Internet service provider** (**ISP**), company that provides **Internet** connections and services to individuals and organizations.
- Just like the human backbone carries signals to many smaller nerves in the body, a network backbone carries data to smaller lines of transmission. A local backbone refers to the main network lines that connect several local area networks (LANs) together. The result is a wide area network (WAN) linked by a backbone connection.





WHY INTERNETWORKING

- What happens if LAN1 and LAN2 use completely different transmission technologies (e.g., Wifi and Ethernet)?
- No single networking technology is best for all needs!

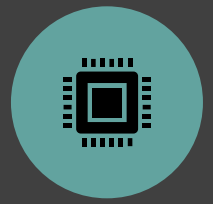
IMAGINE COMPUTER WORLD WITHOUT INTERNETWORKING

Each computer attached to a single network

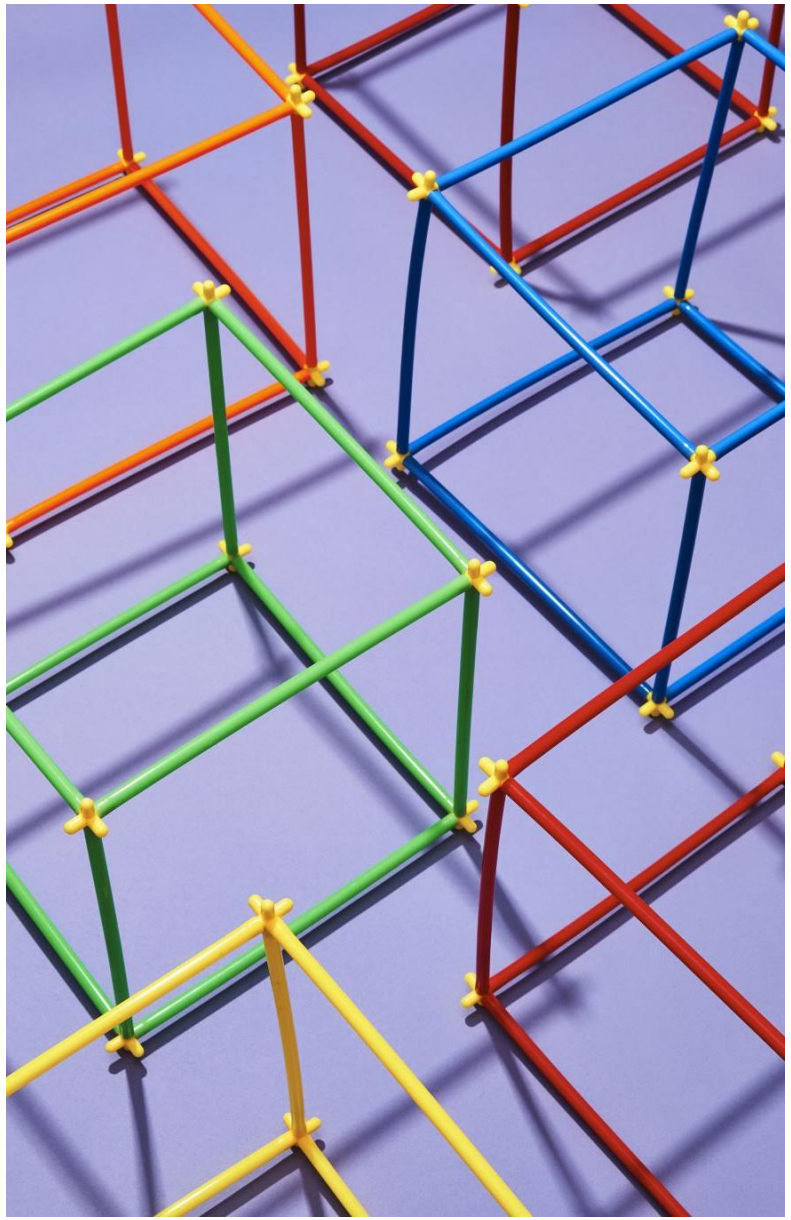
And employees had to choose a computer appropriate for each task

An employee was given access to multiple screens and keyboards

The employee was forced to move from one computer to another to send a message across the appropriate network



Users are neither satisfied nor productive when they must use a separate computer for each network



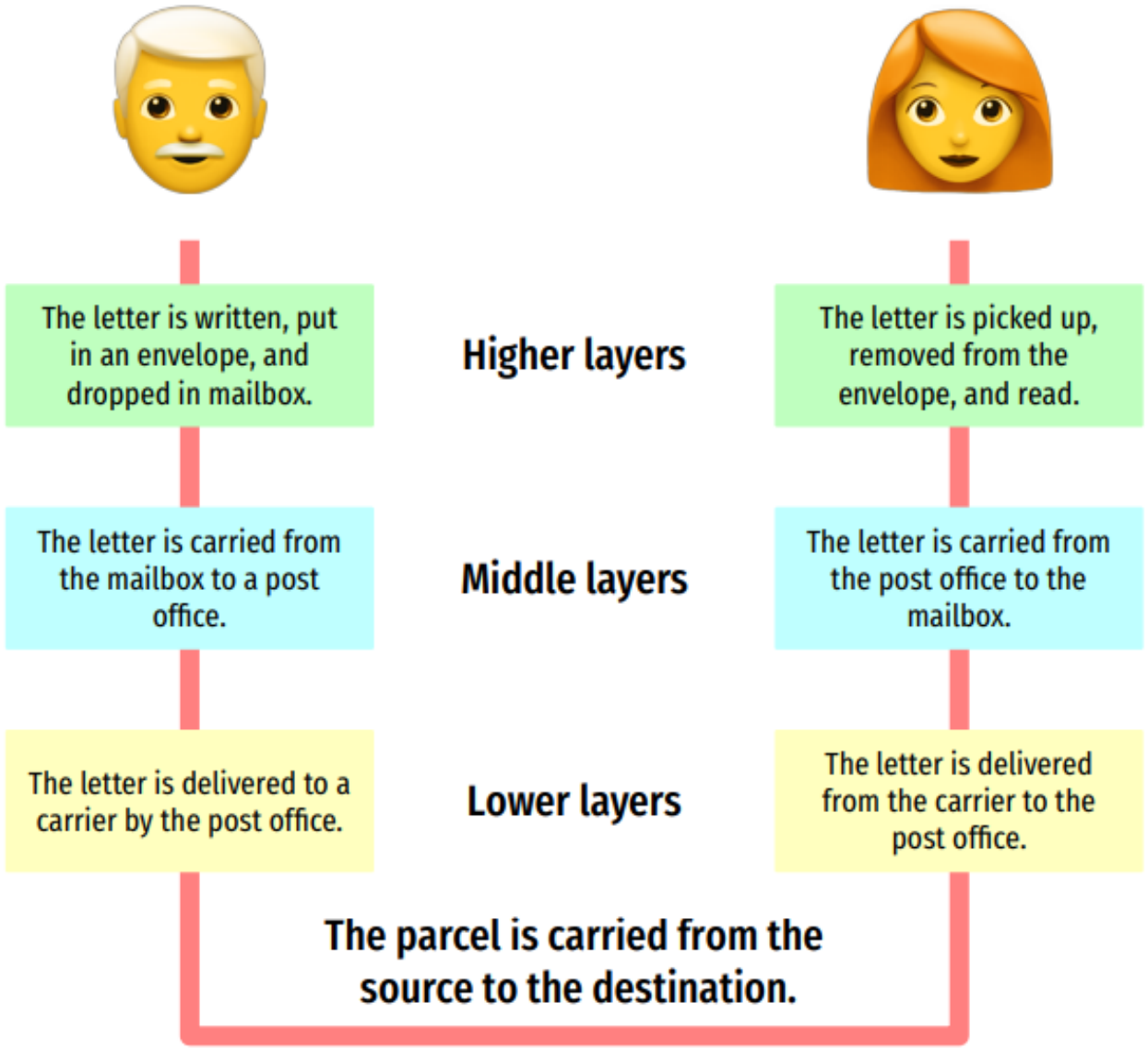
UNIVERSAL SERVICE

- Universal service means interconnecting networks employing different technologies.
- To provide universal service among all computers on an internet, routers must agree to forward information from a source on one network to a specified destination on another network.
- The task is complex because frame formats and addressing schemes used by the underlying networks can differ
- Telephones are acceptable and feasible for all as one telephone can connect any other telephone,

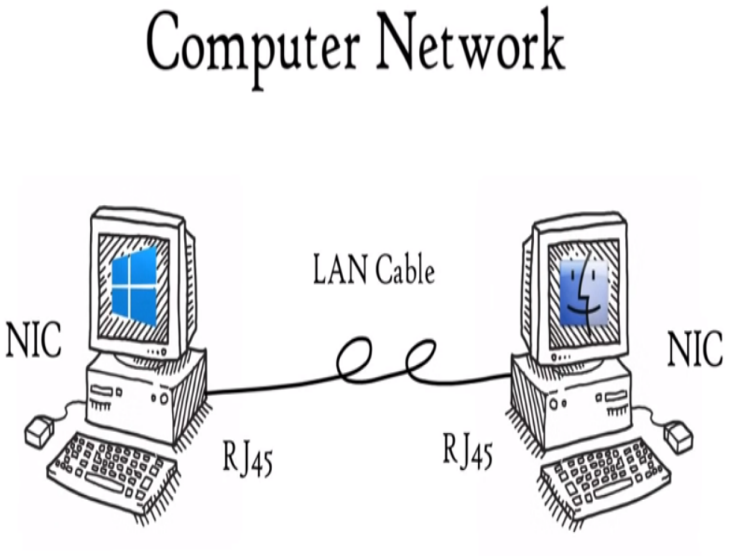
INTERNETWORKING

- Researchers have devised a scheme that provides universal service among heterogeneous networks, called internetworking.
- Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.
- A computer network is a set of different computers connected together using networking devices such as switches and hubs. To enable communication, each individual network node or segment is configured with similar protocol or communication logic, which usually is TCP/IP. When a network communicates with another network having the same or compatible communication procedures, it is known as Internetworking.

PROTOCOLS AND LAYERS?

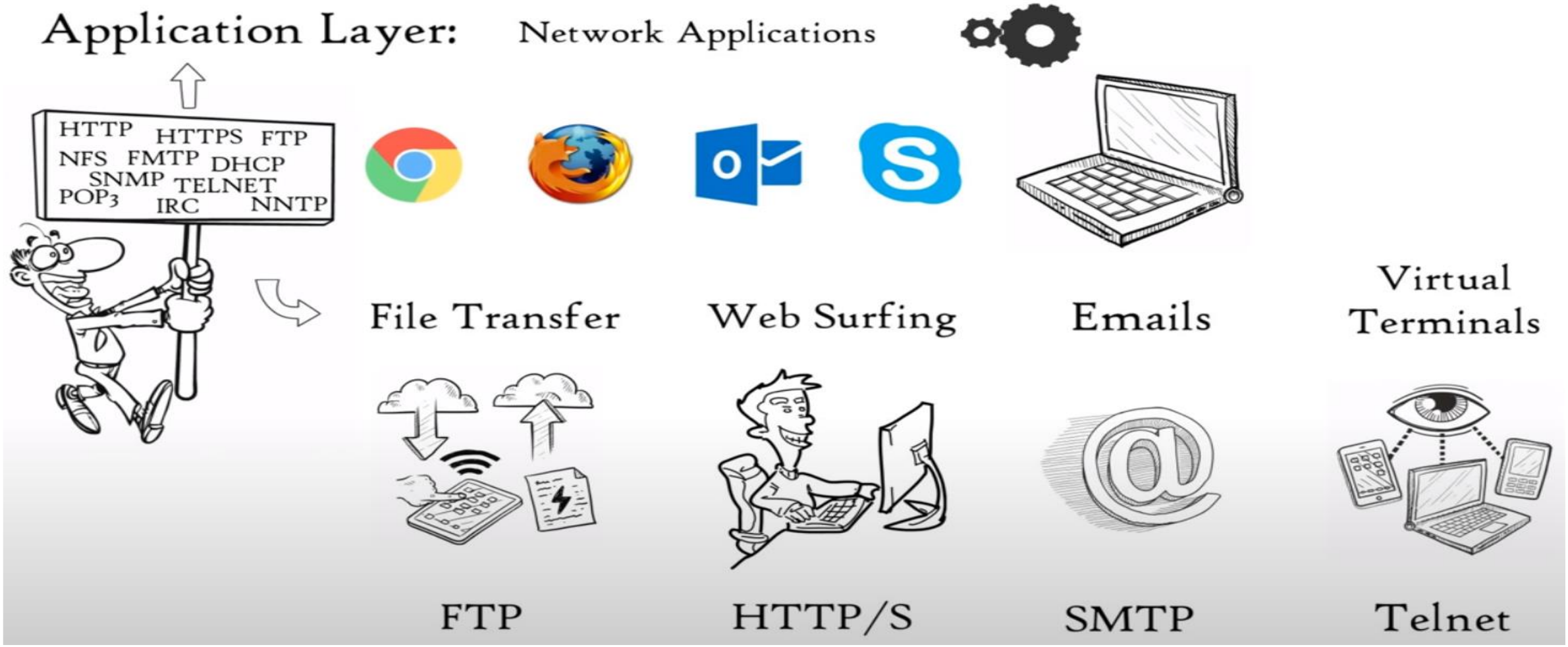


OSI MODEL (TOP DOWN) -84

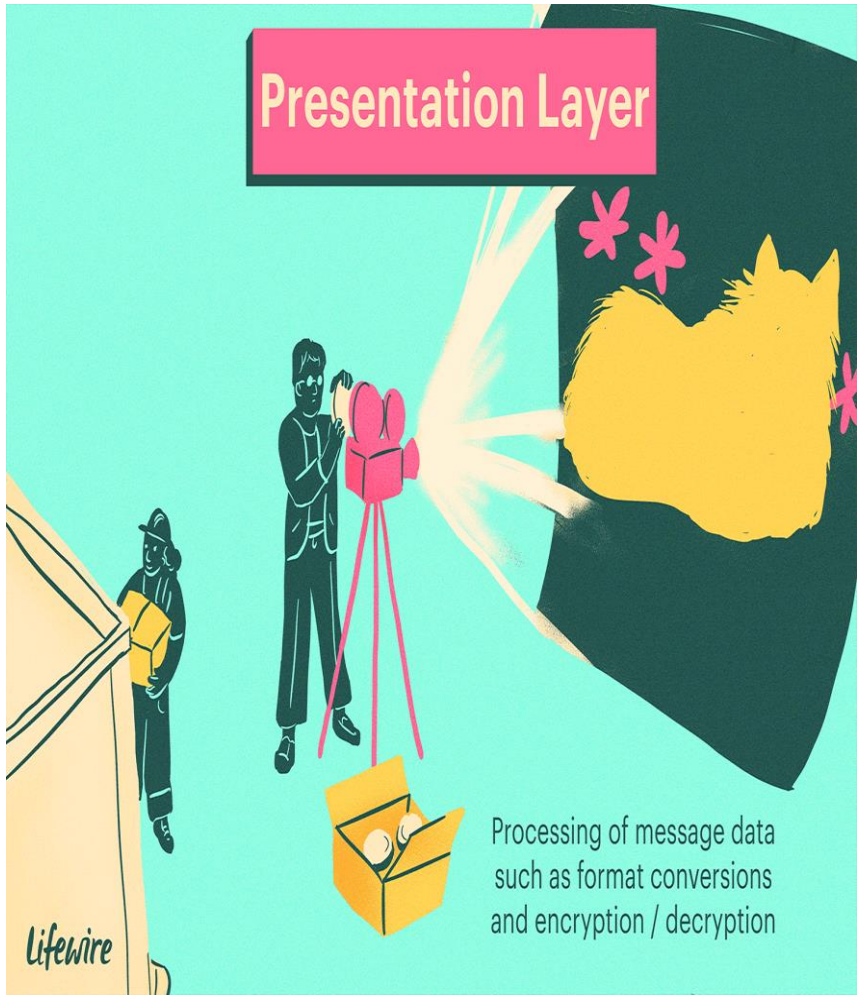


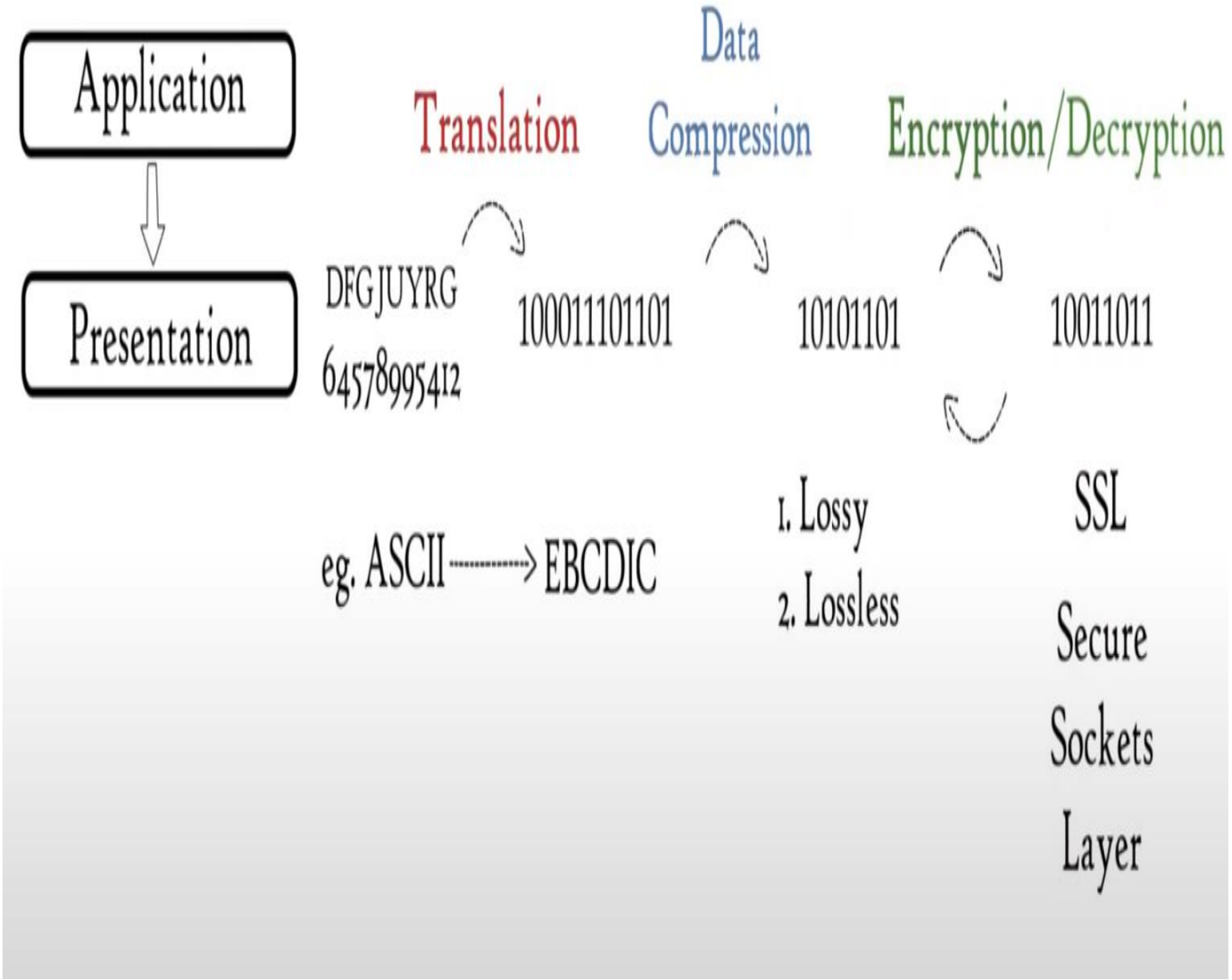
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

APPLICATION LAYER

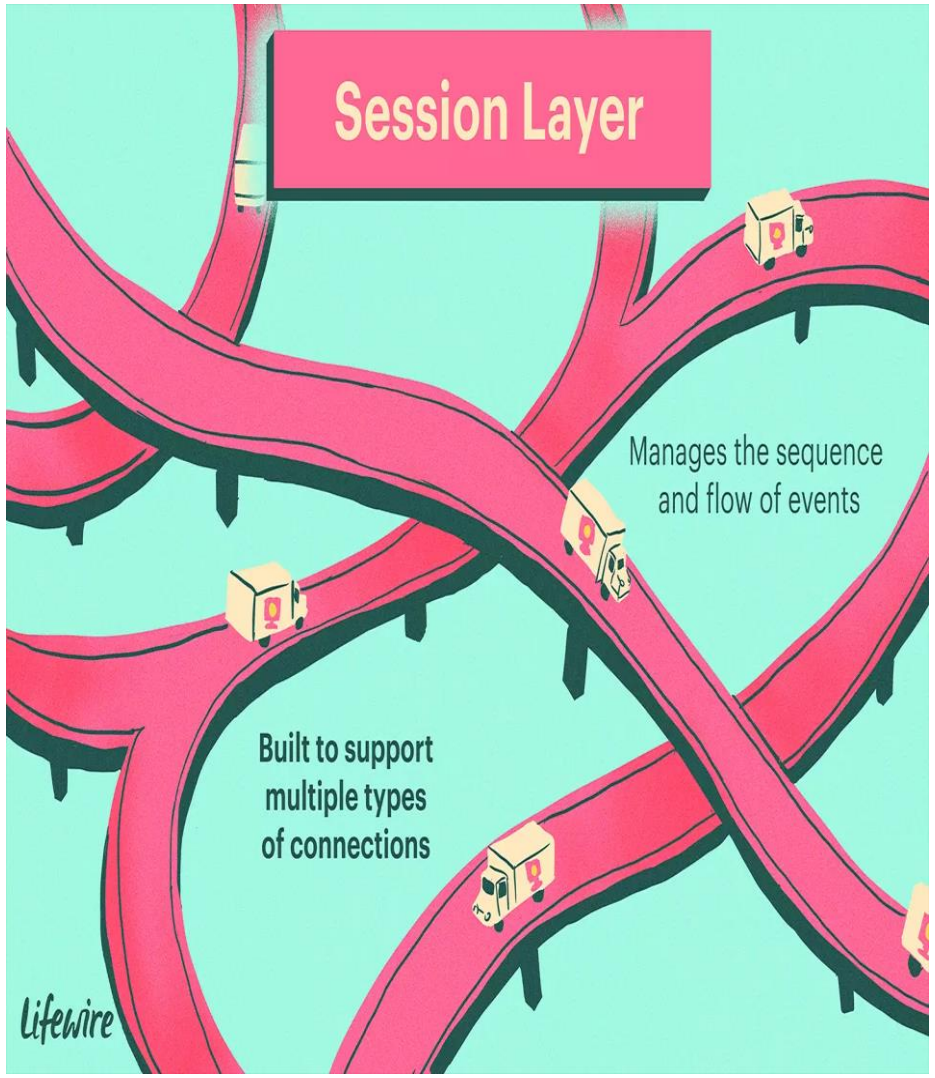


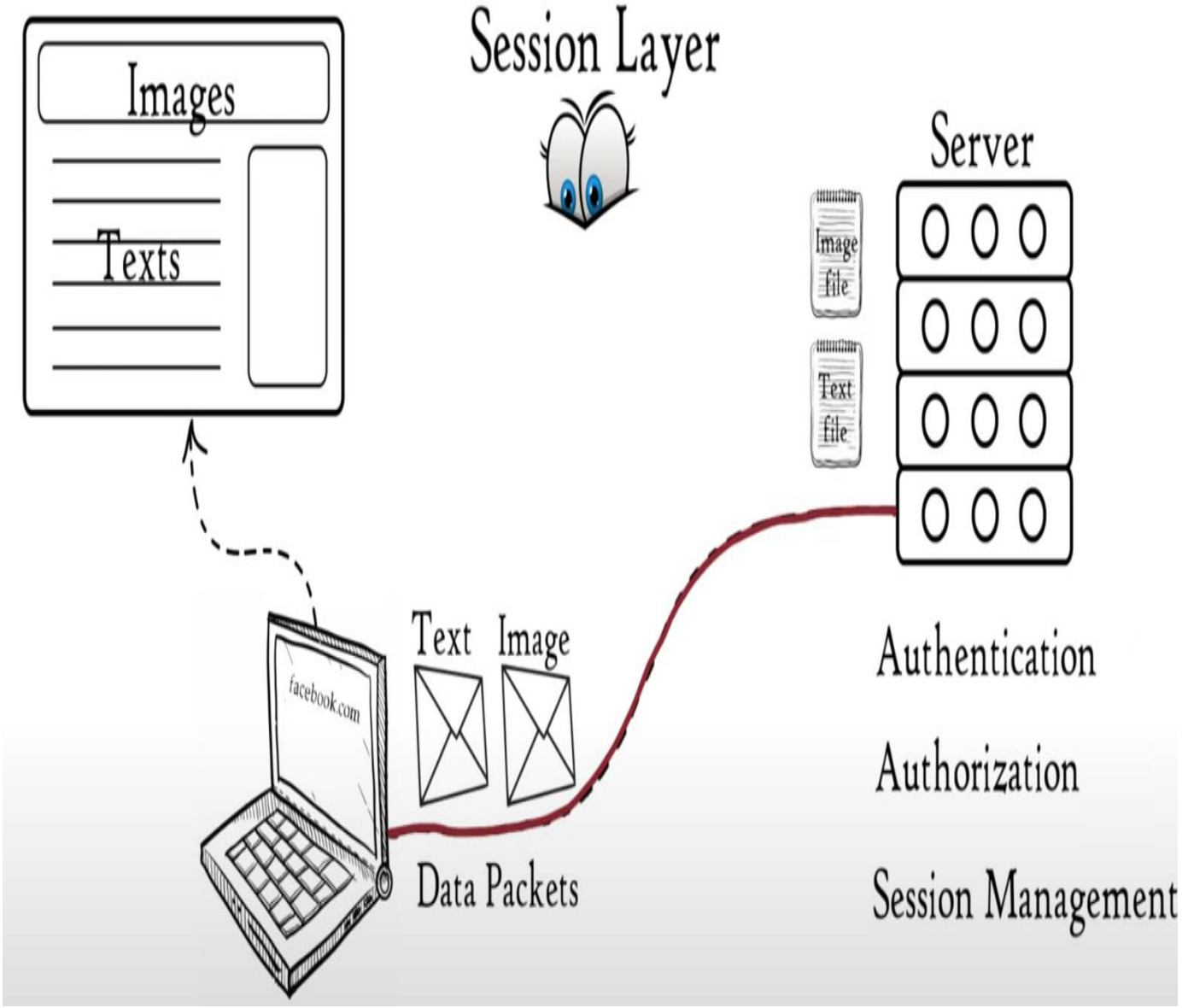
PRESENTATION LAYER



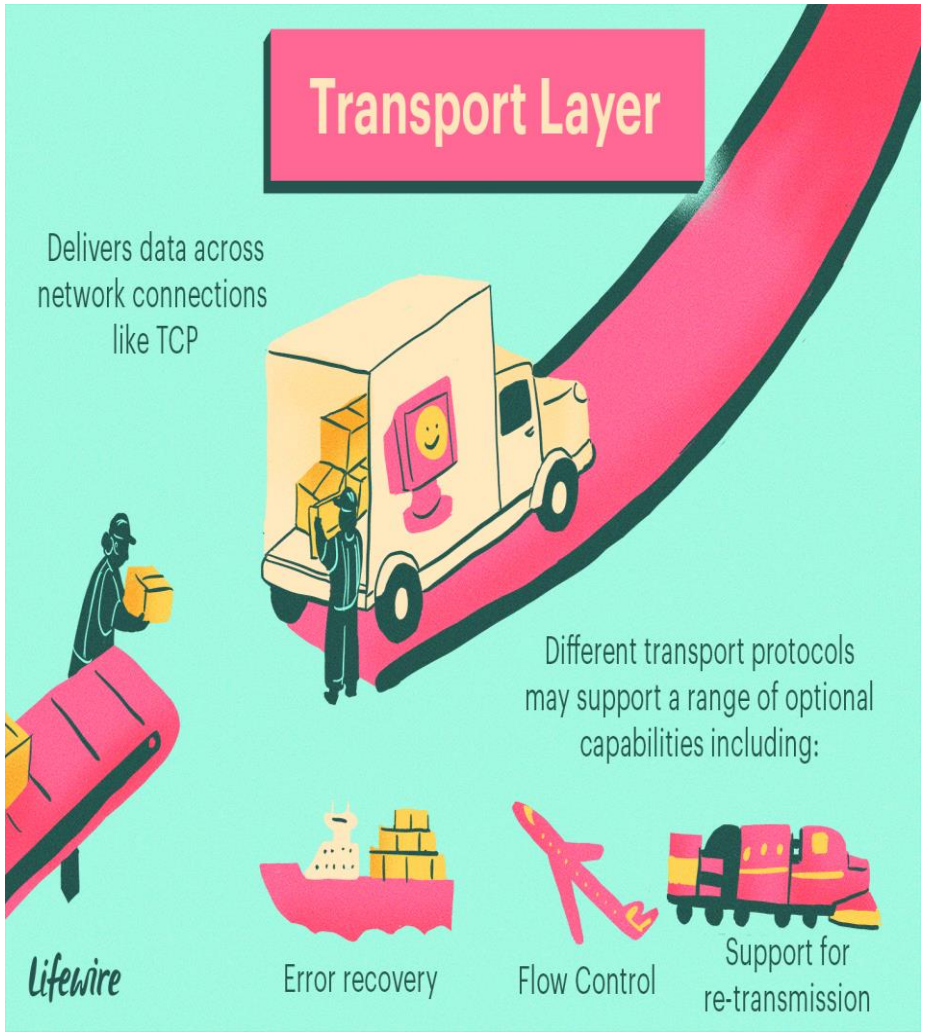


SESSION LAYER





TRANSPORT LAYER



Transport Layer

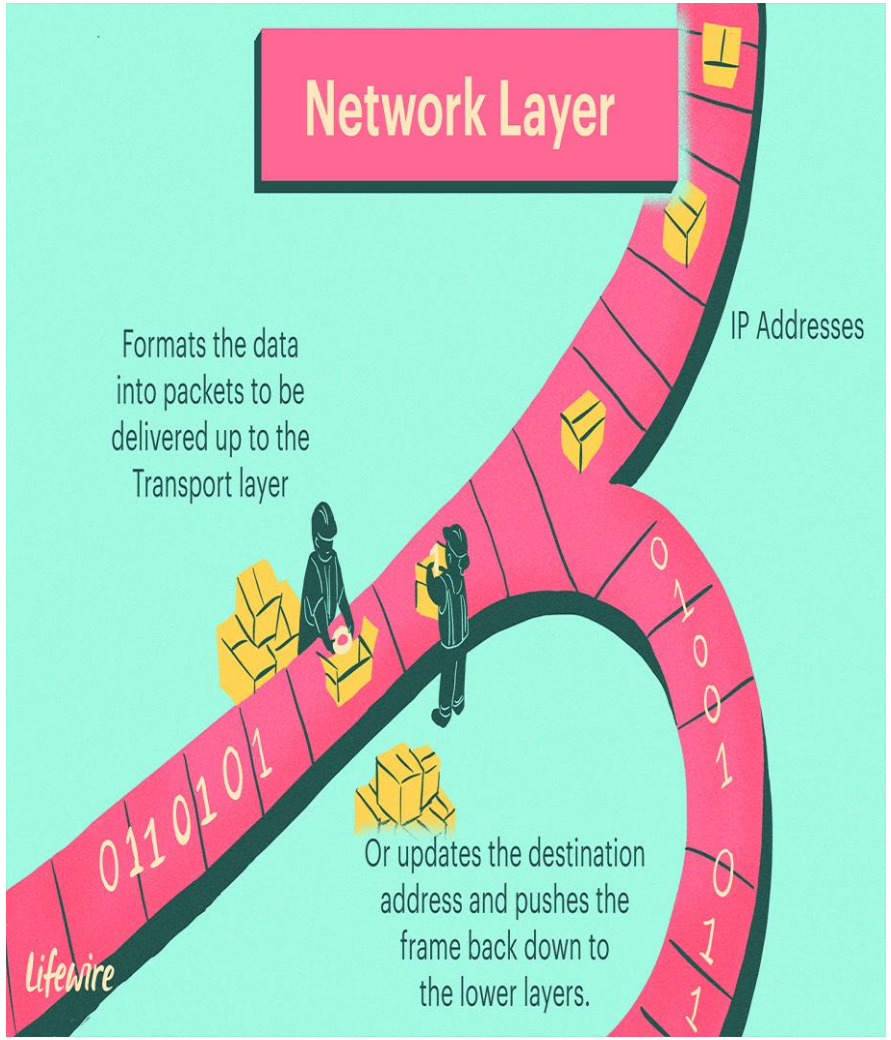
Segmentation

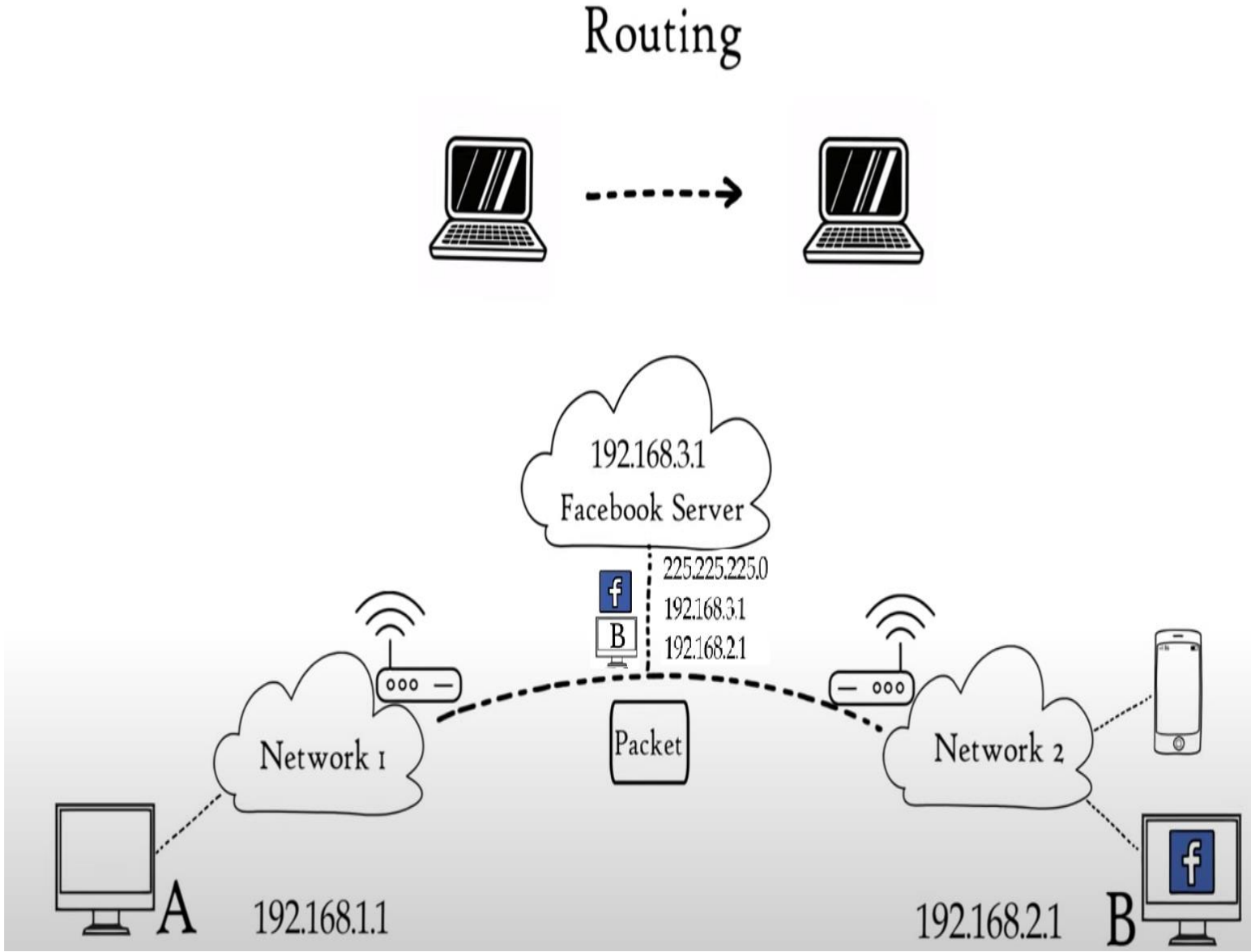
Flow Control

Error Control

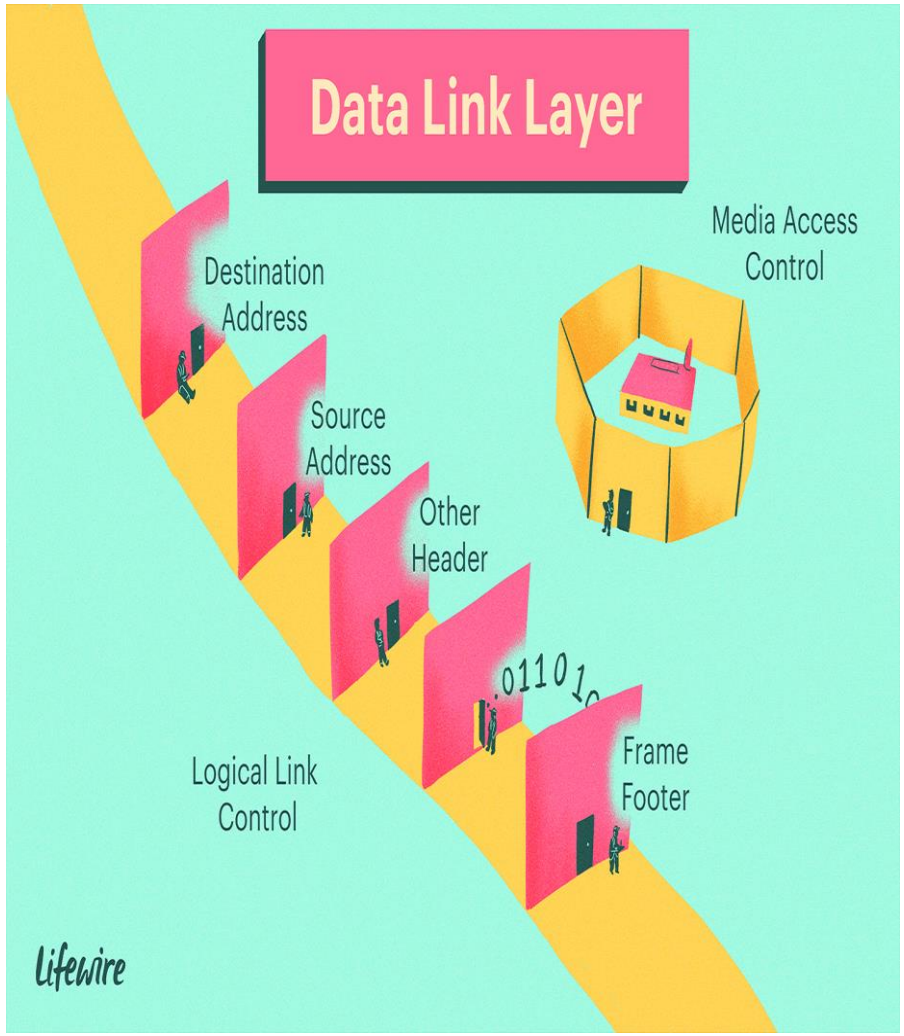
Connection and Connectionless Tx

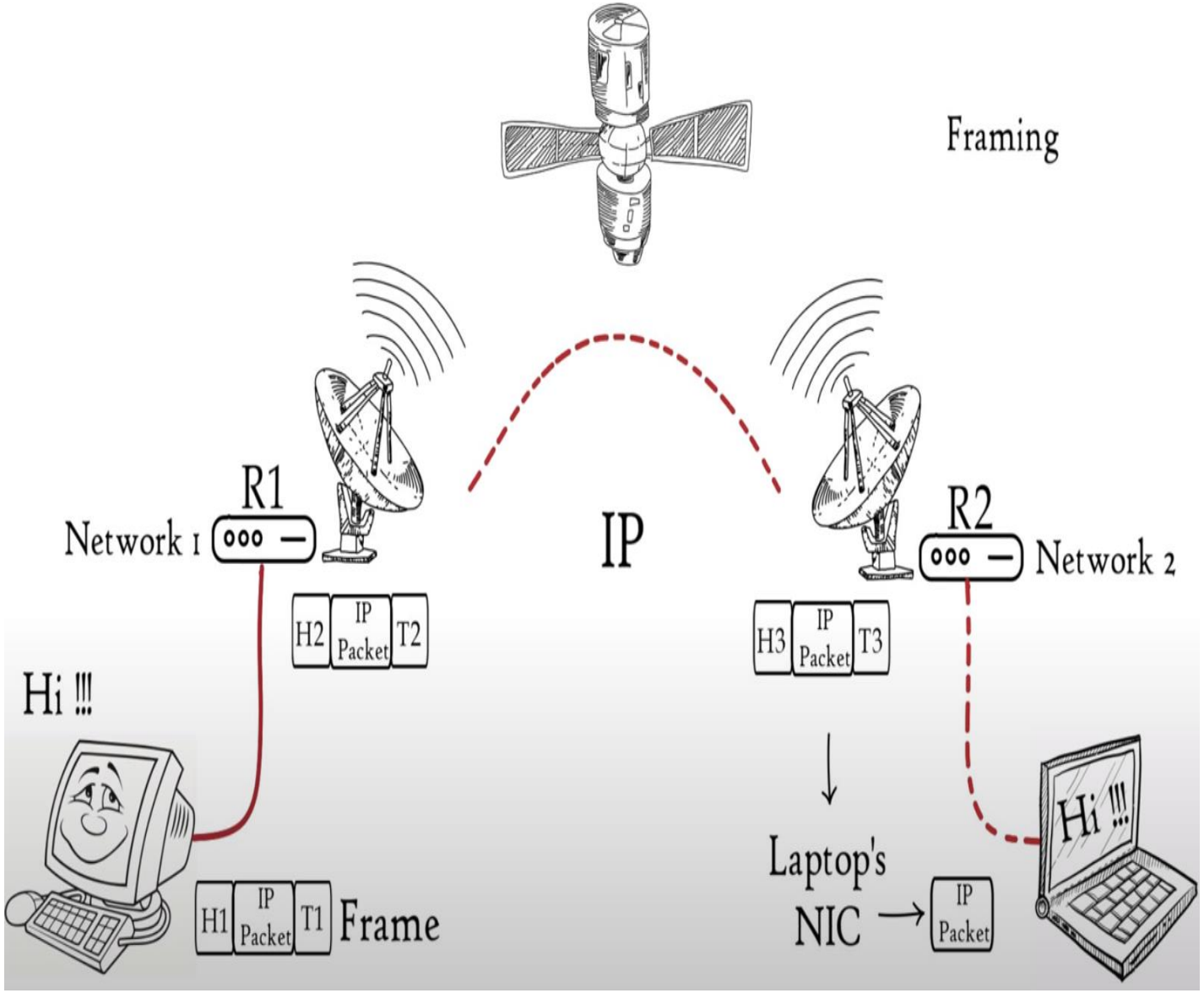
NETWORK LAYER



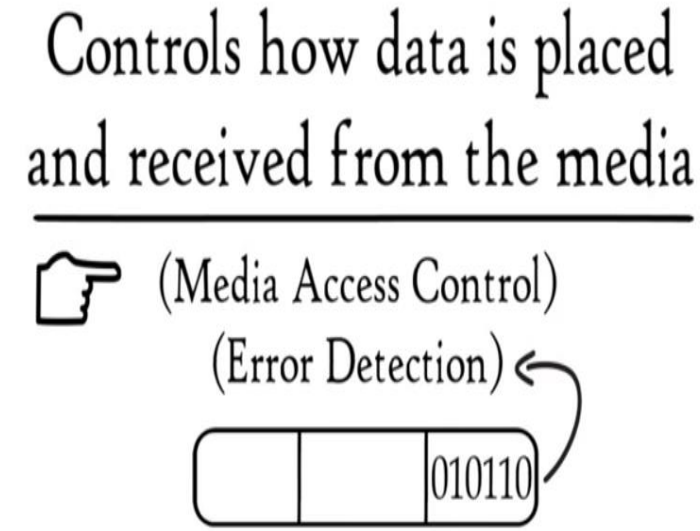


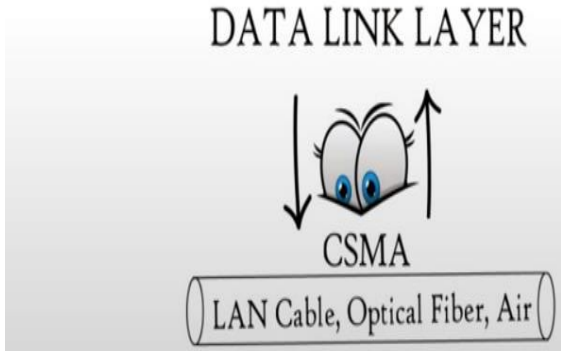
DATA LINK LAYER

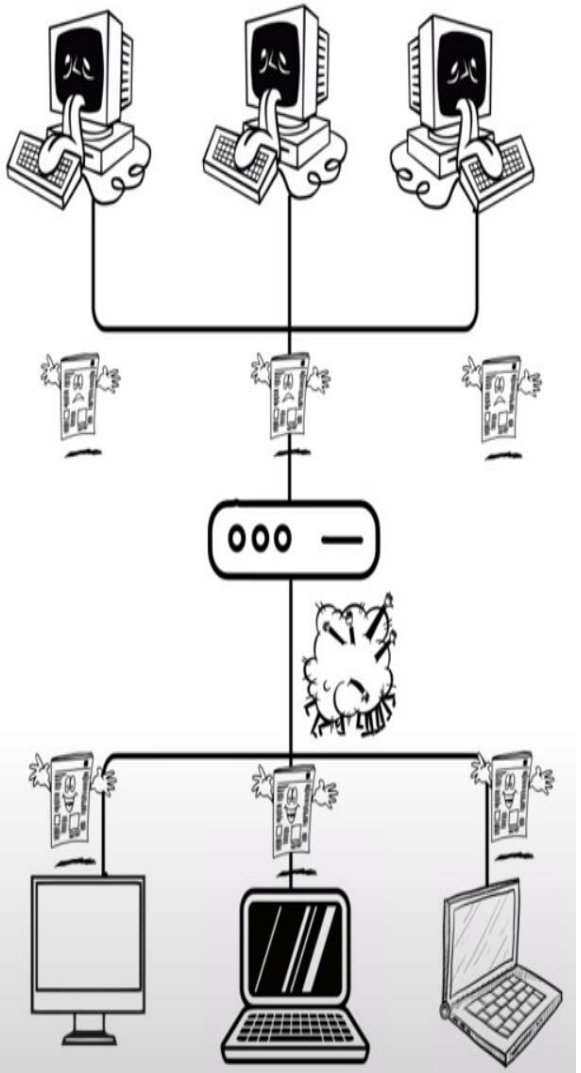




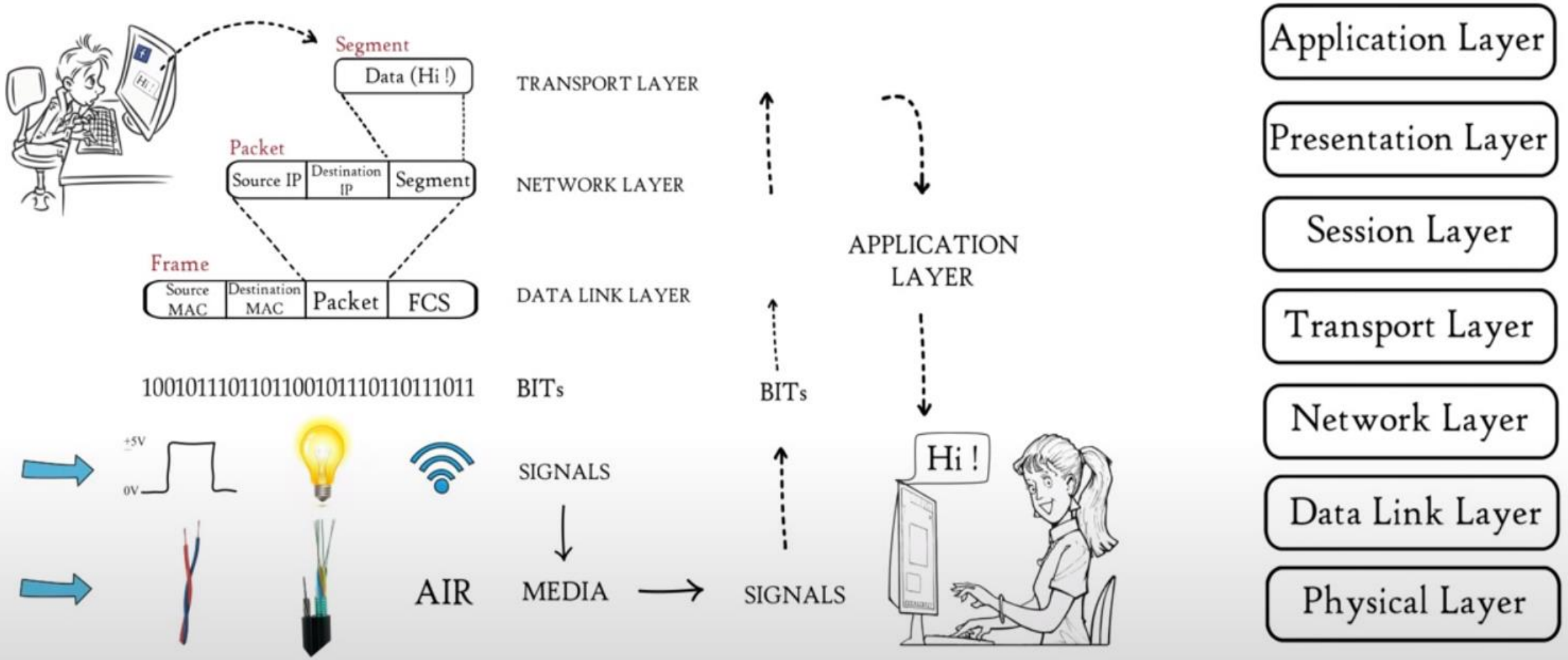
DATA LINK LAYER (MEDIA ACCESS CONTROL AND ERROR DETECTION)



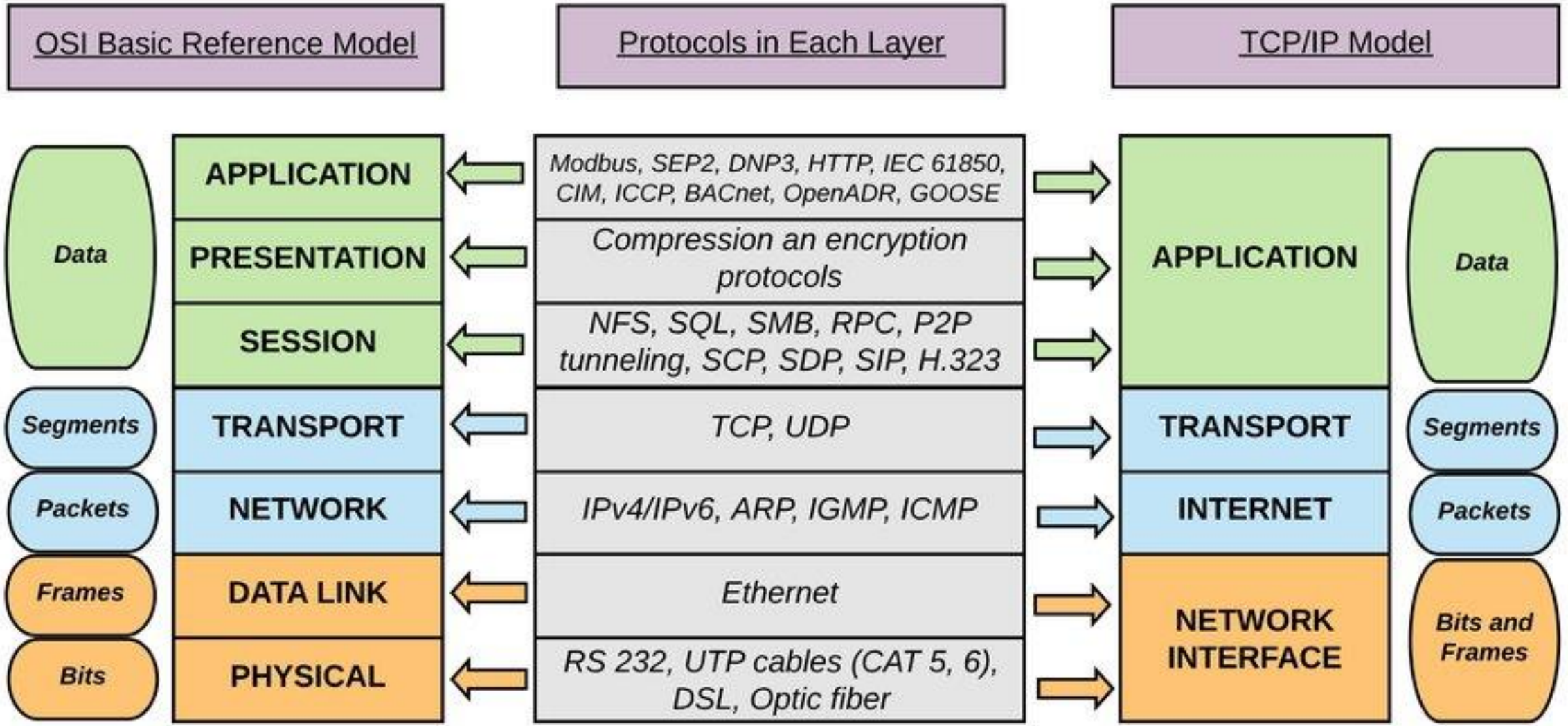




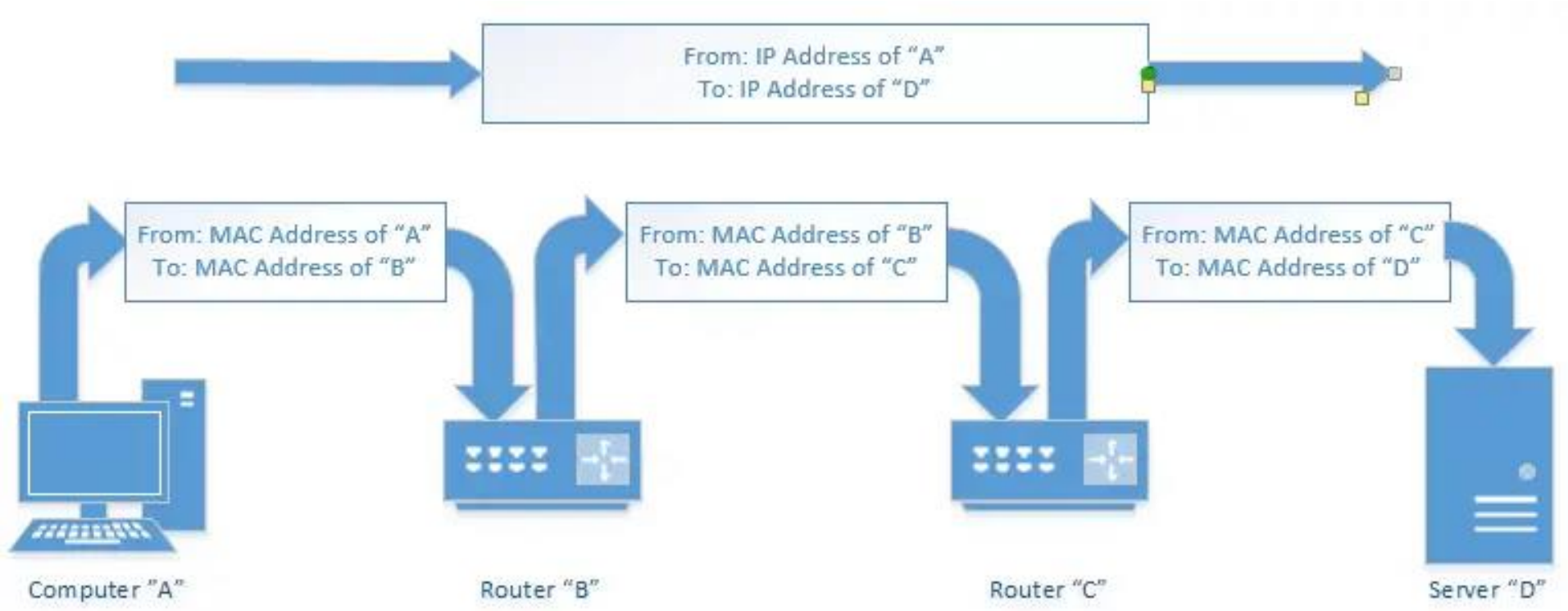
PHYSICAL LAYER



MAPPING TCP/IP MODEL-70 AND PROTOCOLS IN EACH LAYER WITH OSI MODEL



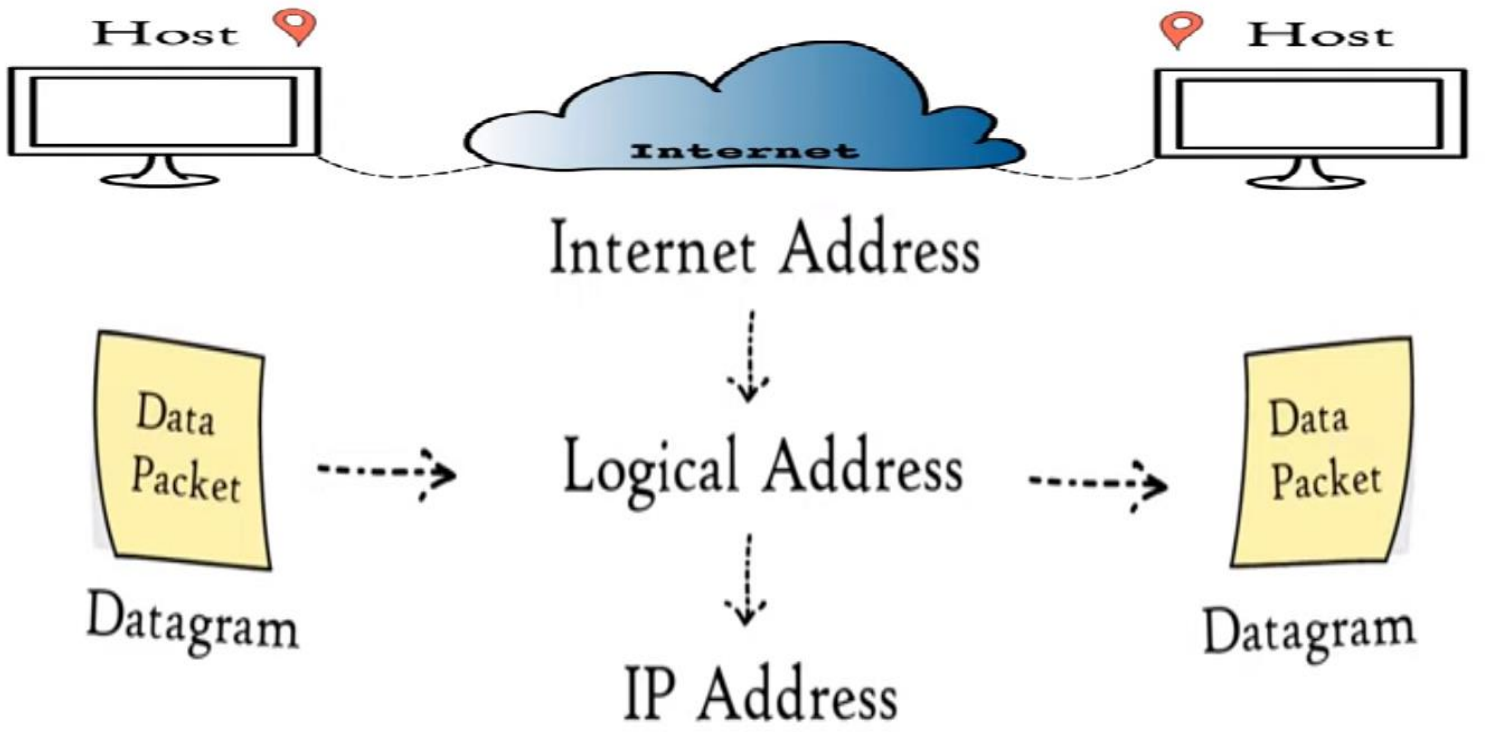
IP ADDRESS


From: IP Address of "A"
To: IP Address of "D"
From: MAC Address of "A"
To: MAC Address of "B"
From: MAC Address of "B"
To: MAC Address of "C"
From: MAC Address of "C"
To: MAC Address of "D"
Computer "A"
Router "B"
Router "C"
Server "D"

IP ADDRESS TYPES

- IPV4
- IPV6
- Dynamic and Static IP addresses

DATAGRAM



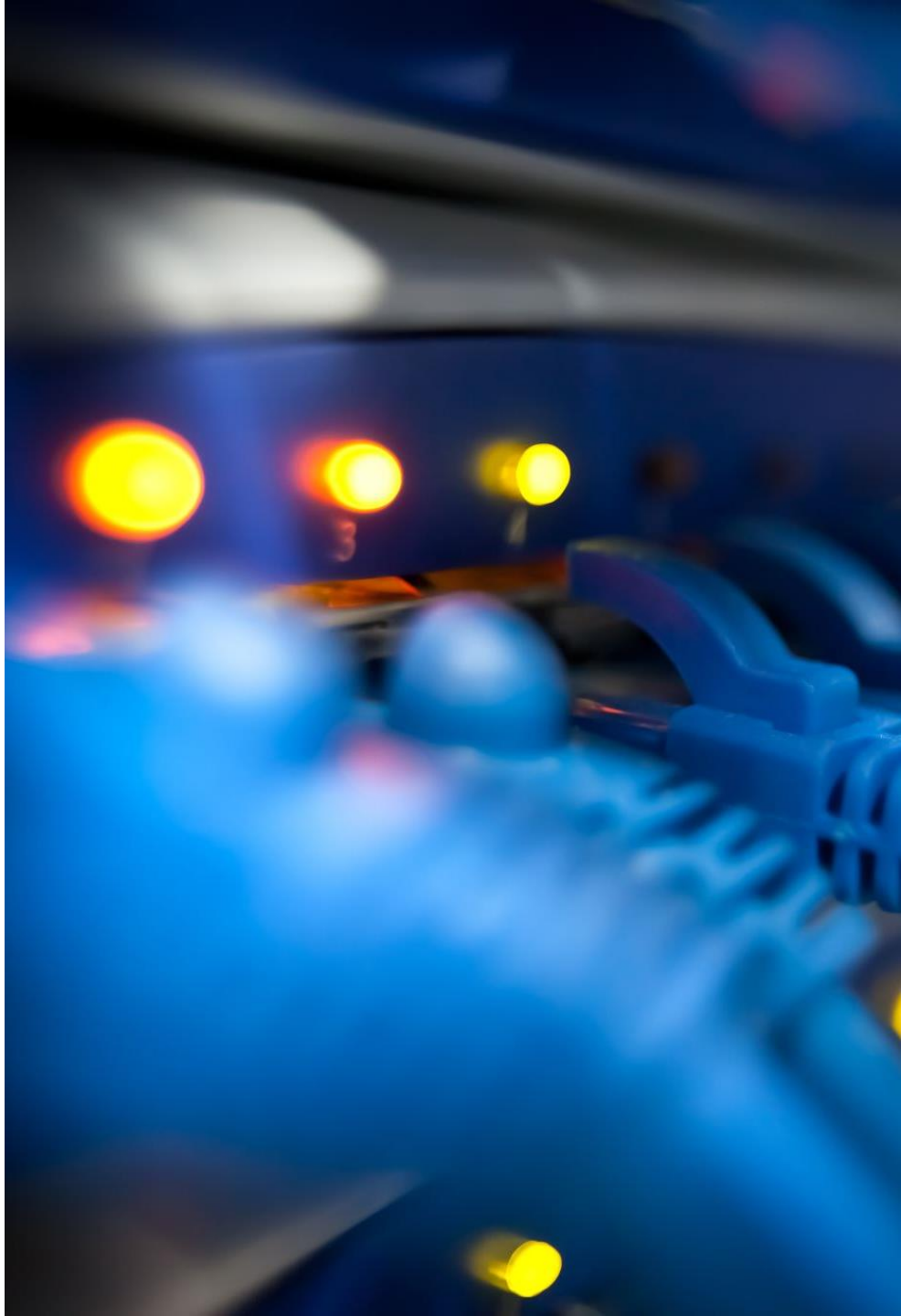
0100100111 ----> 10-bit

IPv4 address ----> 32-bit ----> 2^{32} addresses

IPv6 address ----> 128-bit ----> 2^{128} addresses

DATAGRAM PATHS

- A router reads the IP address, calculates the network portion of that IP address, looks up that value in its routing table and then sends the packet to the next router (or to the host if it is local).
- The destination field in the packet contains the destination address. The router uses its Mask to calculate the network address for the Next Hop (Router destination).
- The Mask is a set of bits which are ANDed with the destination address to produce the destination network address.



(a)

Destination	Next Hop
net 1	R_1
net 2	deliver direct
net 3	deliver direct
net 4	R_3

(b)

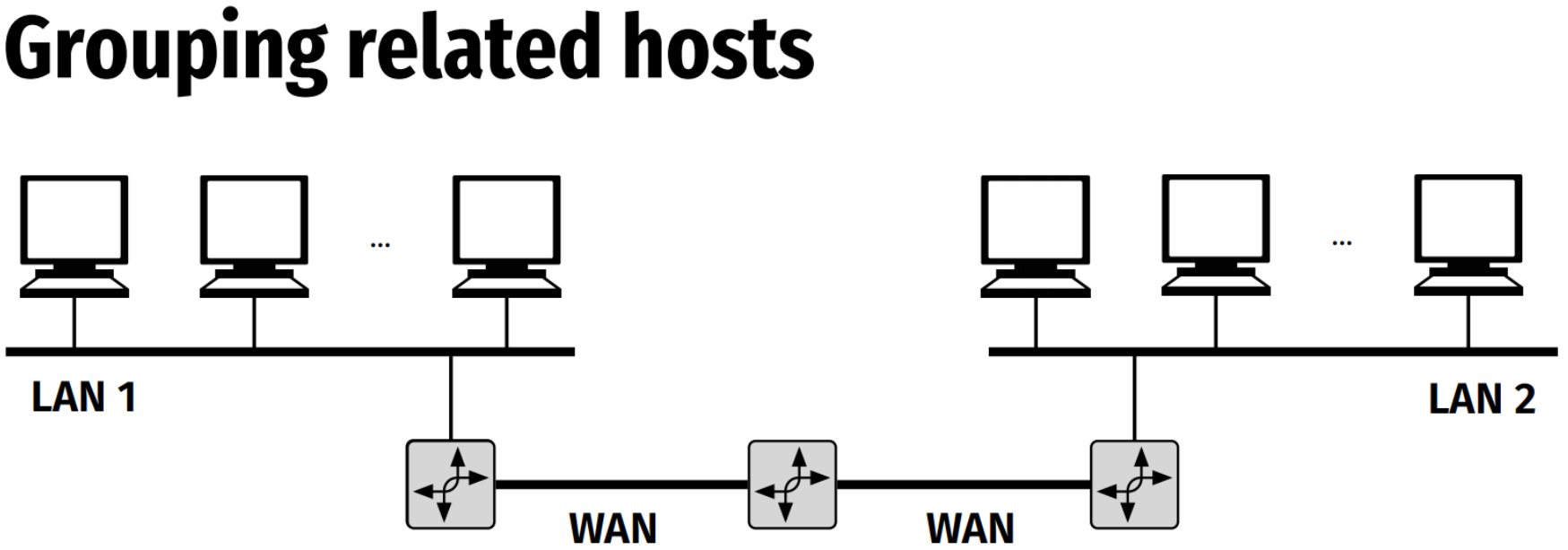
EXAMPLE FOR TO UNDERSTAND ROUTING VIA TABLE OF ROUTER R2

IP ADDRESS (IPV4)

- A unique 32-bit number
- Identifies an interface (on a host, on a router, …)
- Represented in dotted-quad notation (a.b.c.d)
  - » each quad is 8 bits or 1Byte (0-255 or 0x00-0xFF)
  - » e.g., 194.47.94.71

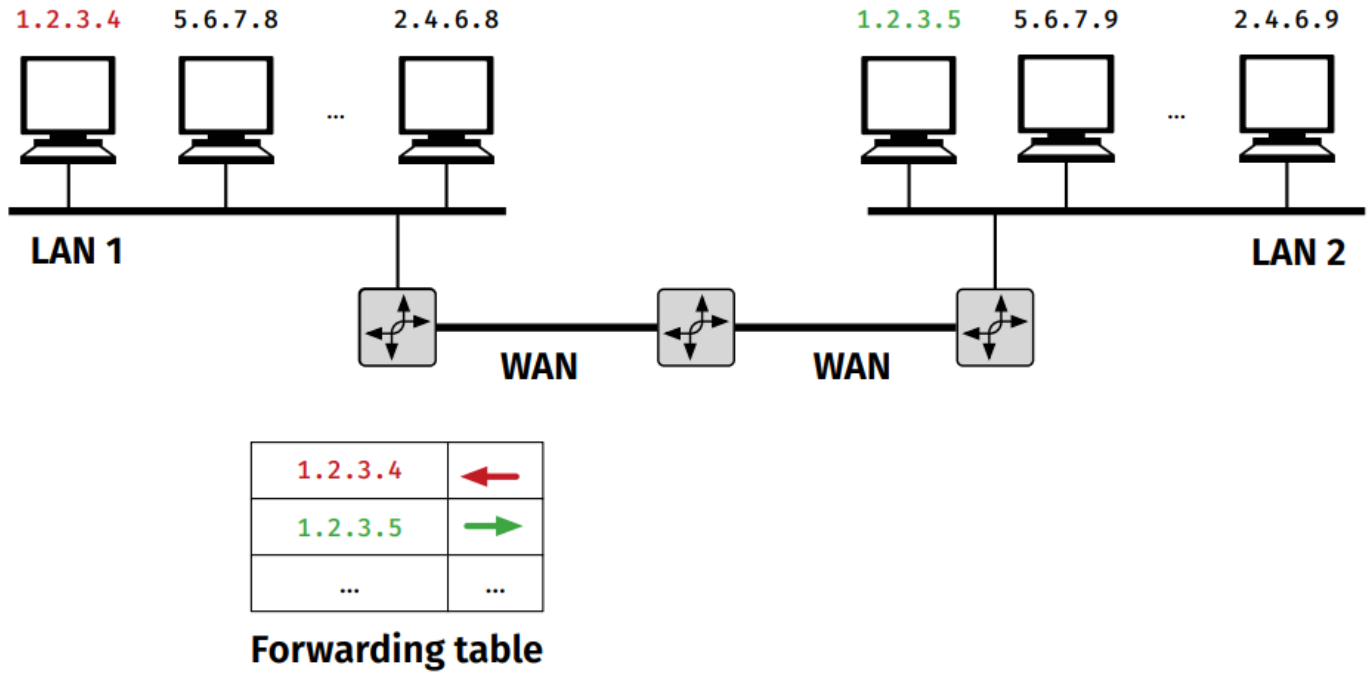
IP CONNECTS NETWORKS

- IP connects the networks not the hosts
- It addresses a network through connecting group of hosts instead of each host individually



SCALABILITY CHALLENGE

- Suppose hosts had arbitrary addresses. Then every router would need a lot of information to know how to direct packets toward every host.



SCALABILITY CHALLENGE

- Suppose hosts had arbitrary addresses. Then every router would need a lot of information to know how to direct packets toward every host. If we approximate:

» 32-bit IP address:

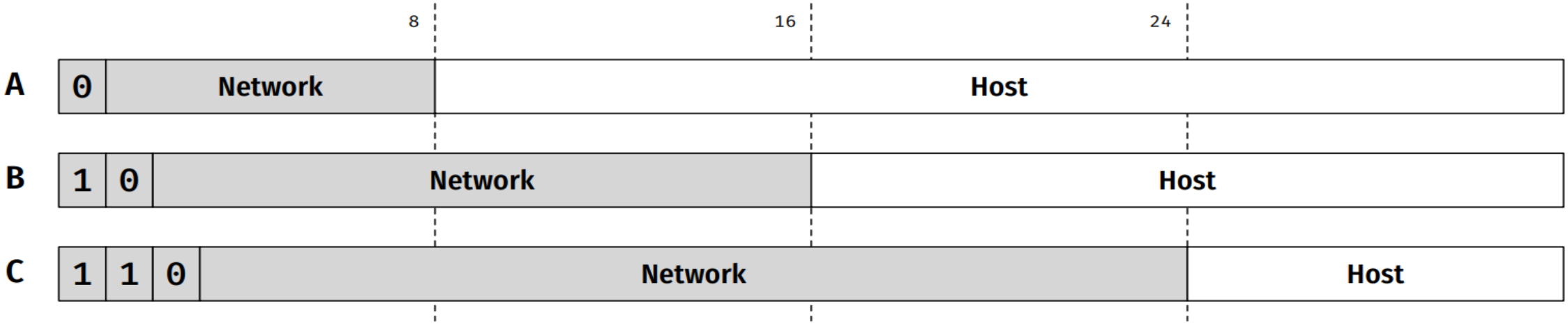
» 4.29 billion (232) possible addresses

» How much storage?

» Minimum: 4B address + 2B forwarding info per line

» Total: 24.58 GB just for forwarding table

CLASS-BASED ADDRESSING TO RESOLVE THE SCALABILITY ISSUE

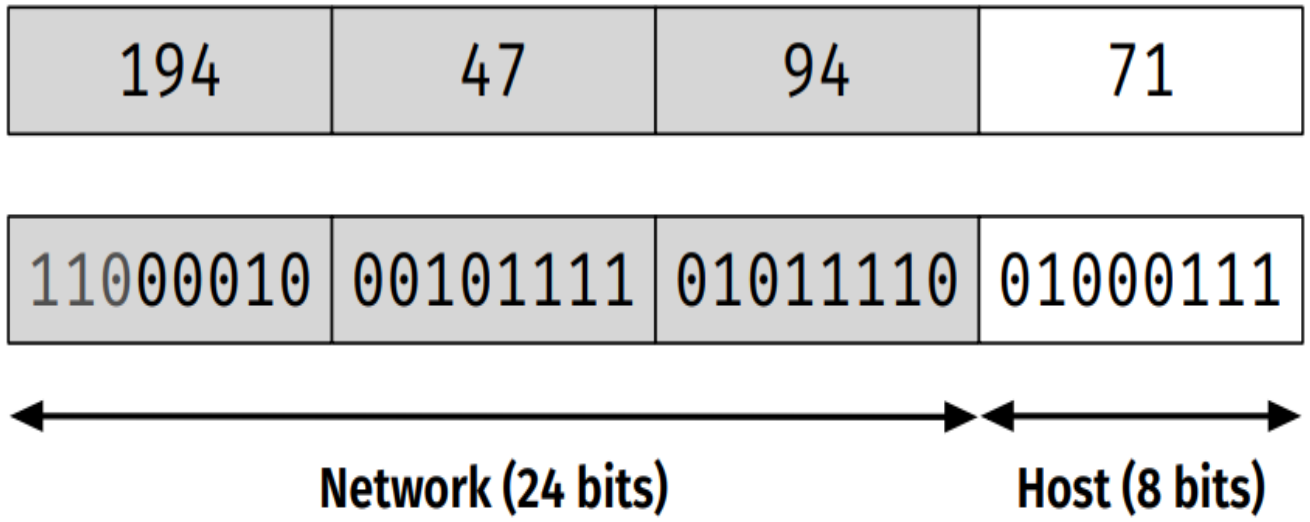


Class-based Addressing (RFC791) Address Formats:

High Order Bits	Format	Class
0	7 bits of net, 24 bits of host	a
10	14 bits of net, 16 bits of host	b
110	21 bits of net, 8 bits of host	c
111	escape to extended addressing mode	

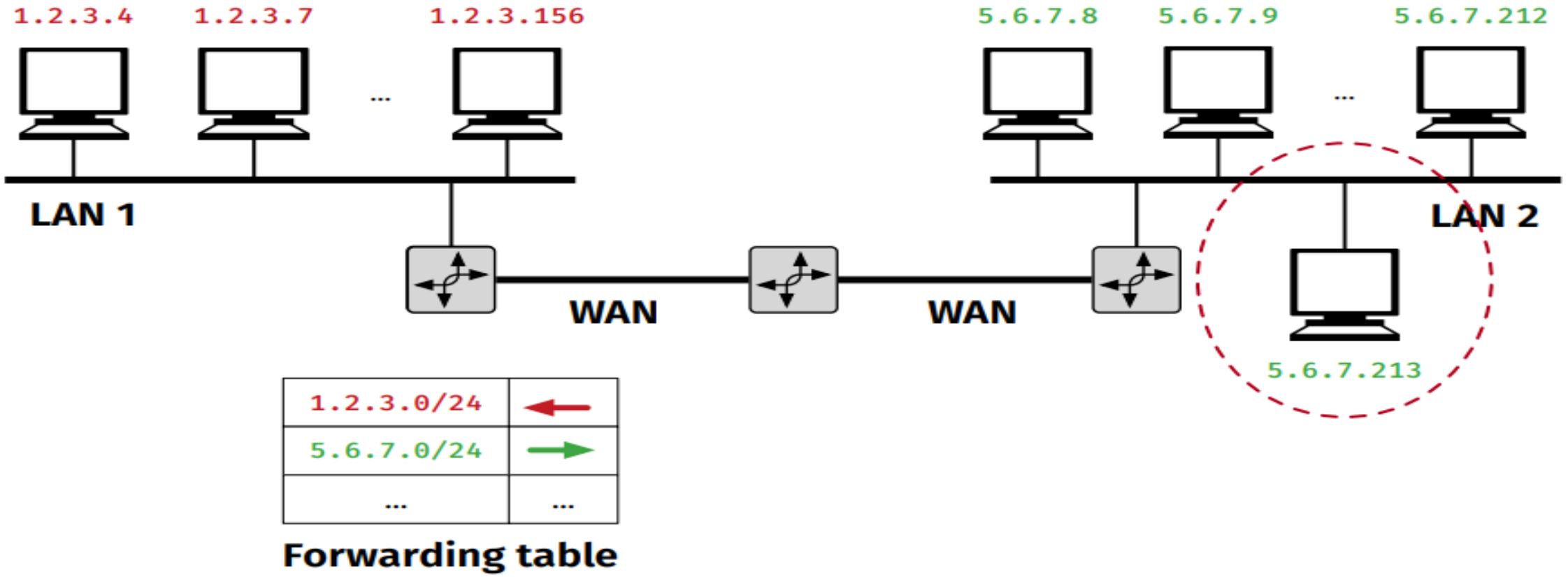
HIERARCHICAL ADDRESSING: IP PREFIXES

IP addresses can be divided into two parts: network (left) and host (right)



194.47.94.0/24 is a 24-bit prefix (class C) which covers 28 addresses (e.g., up to 255 hosts)

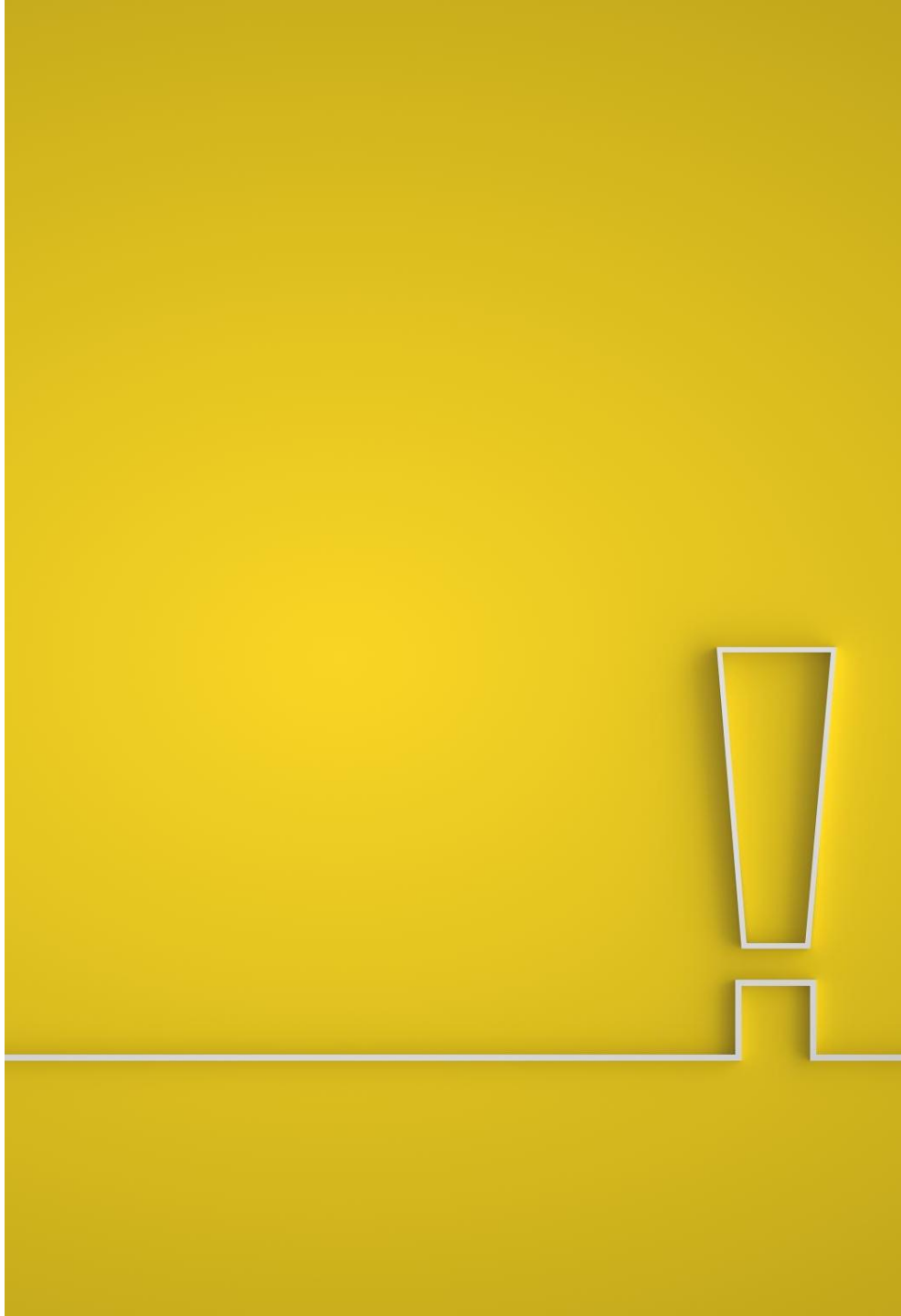
SCALABILITY IMPROVED



There is no need to update the routers. Adding a new host 5.6.7.213 on the right does not require a new forwarding-table entry.

IP ADDRESS PROBLEM (1991)

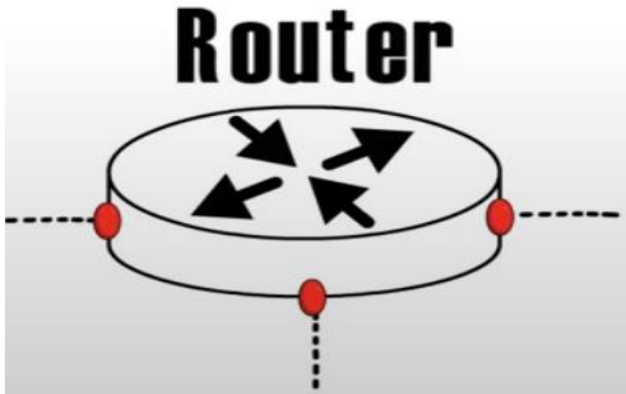
- Class A, B and C all ranges from 24 to 8 bits address, which is not sufficient for the bigger network



IP ADDRESS AND INTERFACE

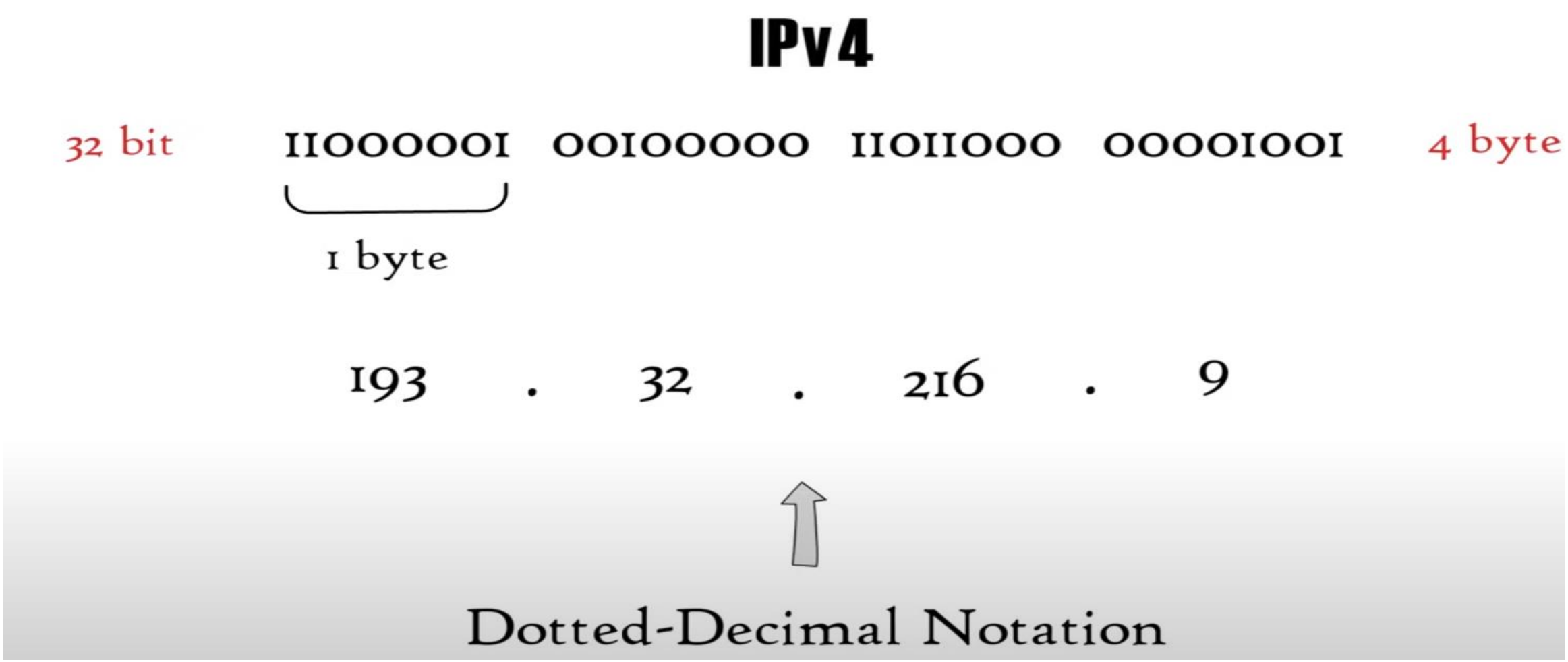
IP Datagrams

IP addresses ⇌ Interface

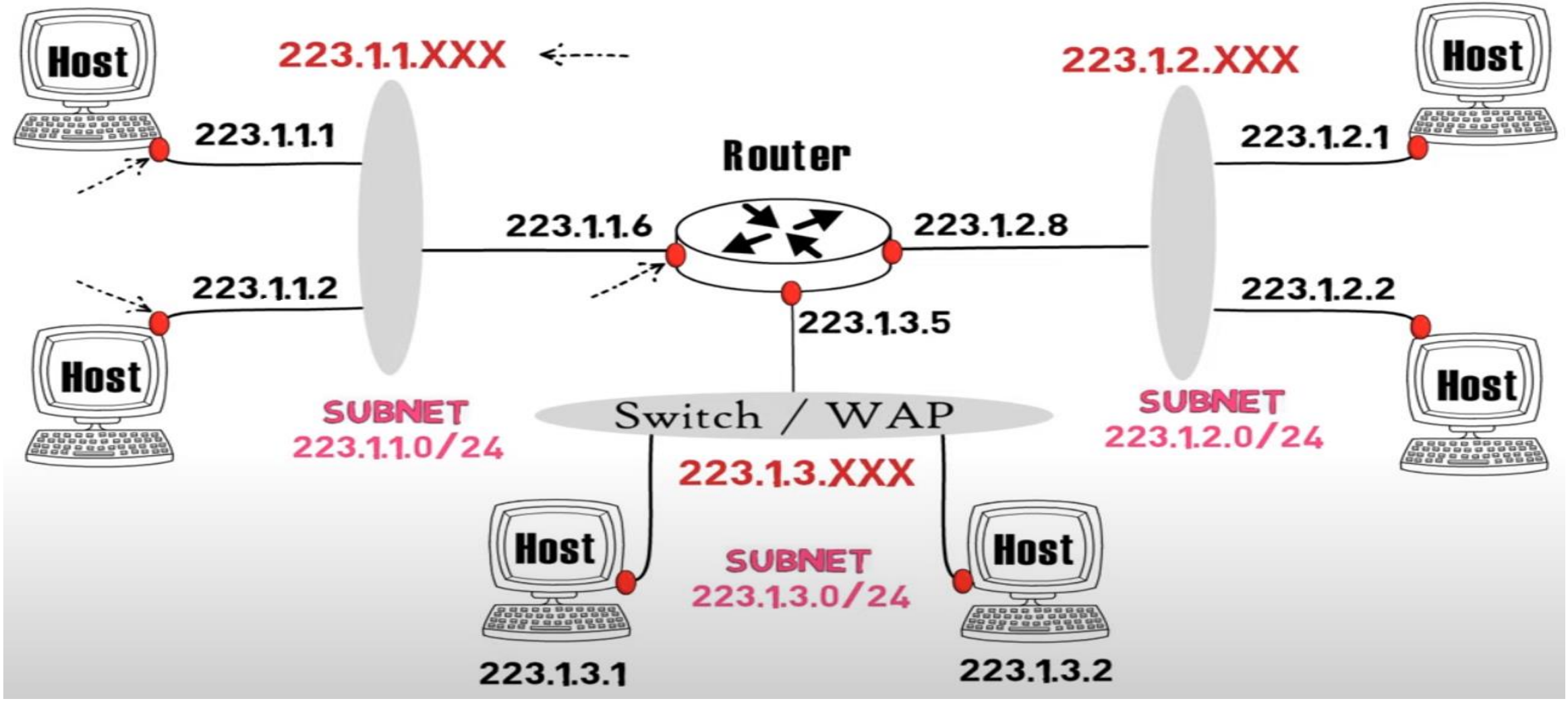


IP Datagrams

EXAMPLE OF IPV4 ADDRESSING



SUBNET AND SUBNET MASK



CLASSLESS INTERDOMAIN ROUTING (CIDR), OR CIDR ADDRESS ASSIGNMENT STRATEGY

Subnet Address : a.b.c.d/x

11001000 00010111 00010000 00000000

Network prefix

Organisation IP block — Binary form

200.23.16.0/20 — 11001000 00010111 00010000 00000000

X = 20

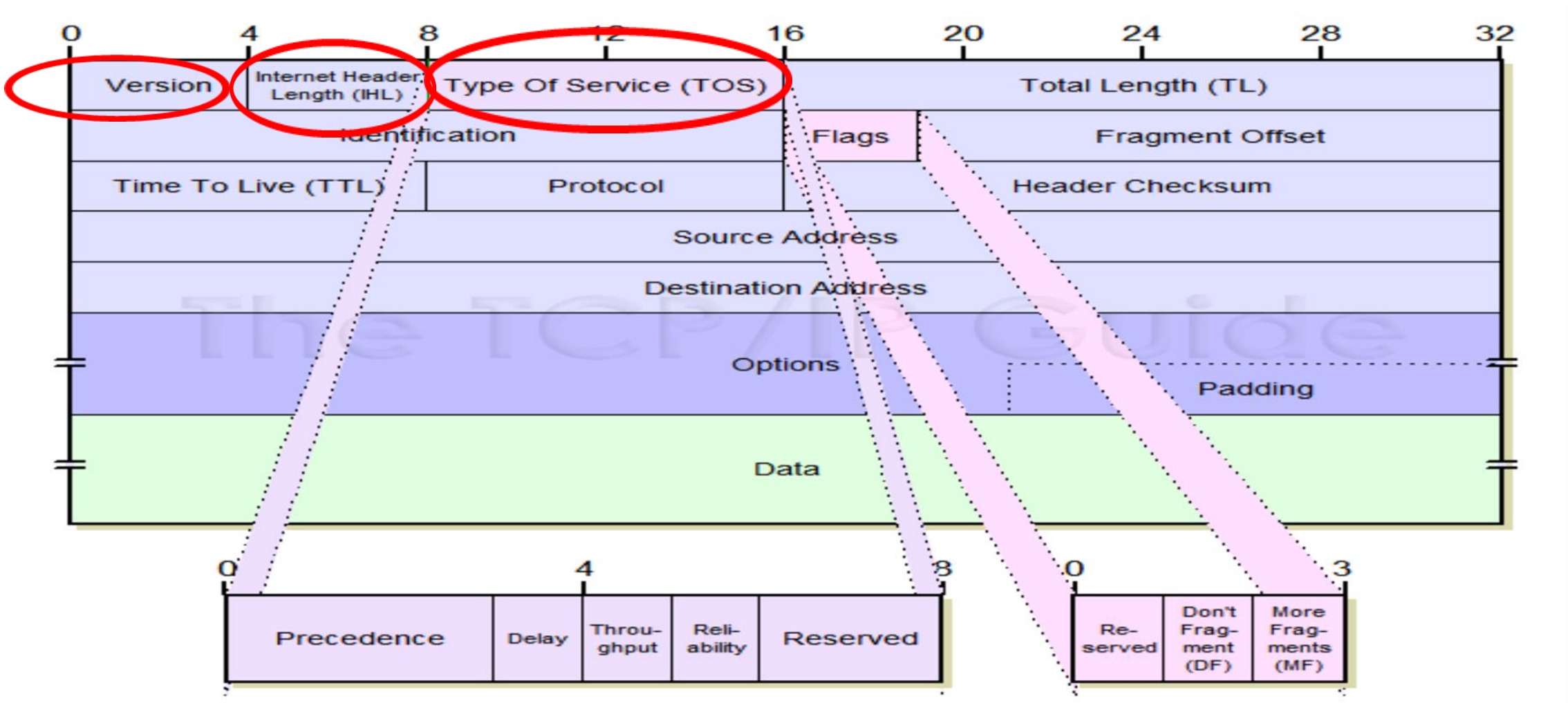
In this way an organization can create multiple subnets within the allocated IP address space.

CIDR EXAMPLE

Organisation IP block	Binary form
200.23.16.0/20	11001000 00010111 00010000 00000000
X = 20	

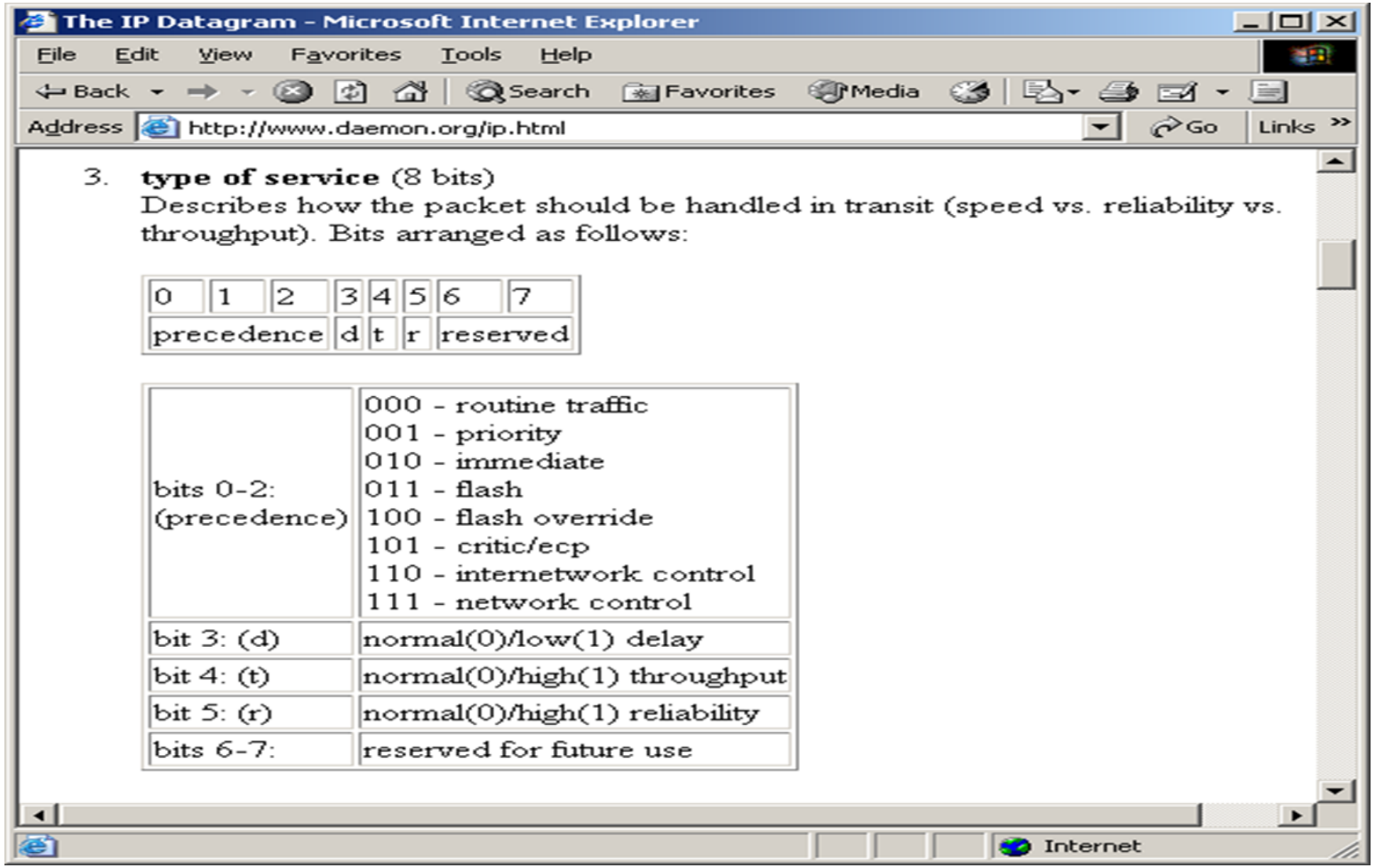
Subnet 0	200.23.16.0/23	11001000 00010111 00010000 00000000
Subnet 1	200.23.18.0/23	11001000 00010111 00010010 00000000
Subnet 2	200.23.20.0/23	11001000 00010111 00010100 00000000

VERSION, INTERNET HEADER LENGTH, AND TYPE OF SERVICE (TOS)



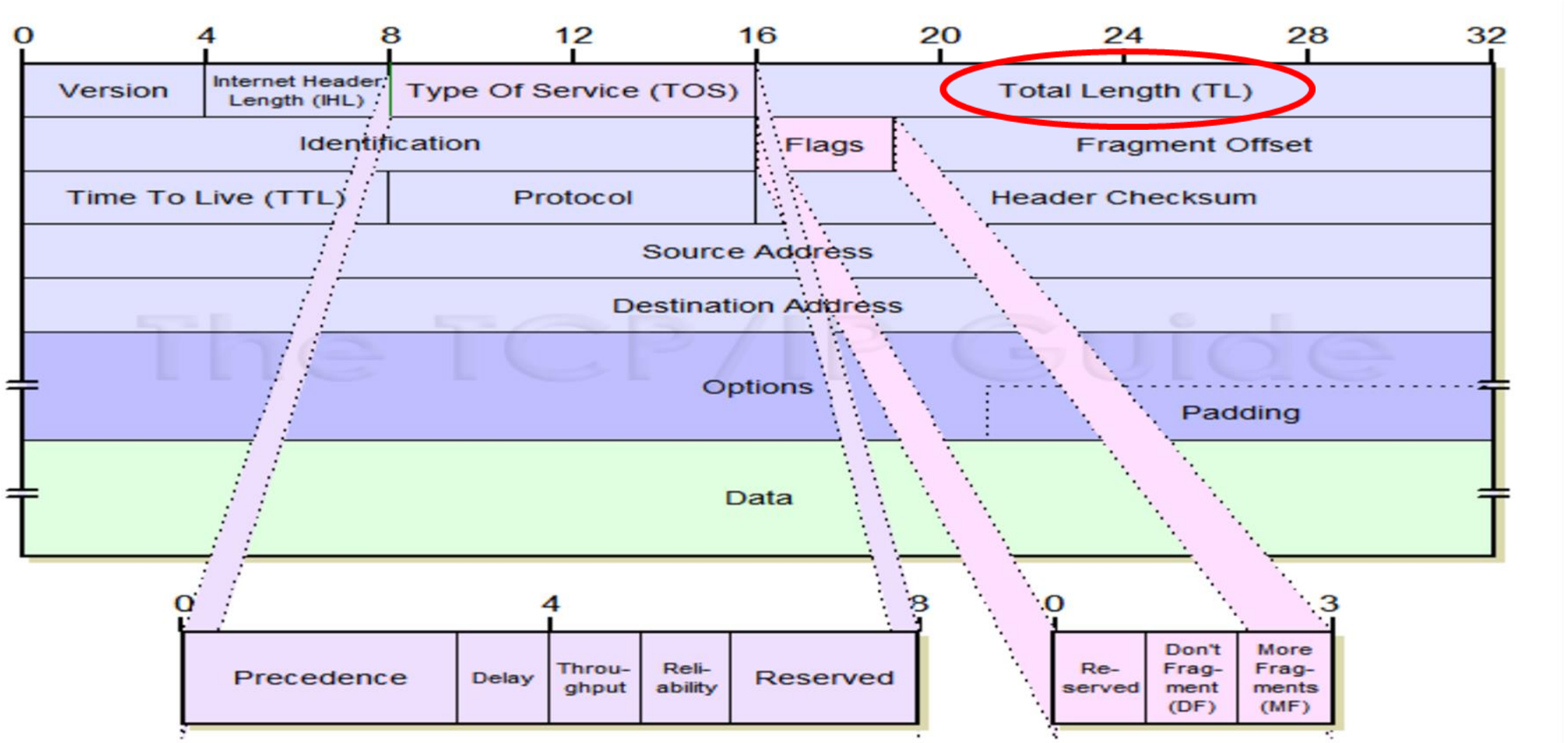
The size of the Header Length or the IHL field is 4 bits. You must multiply the value in this field by four to get the length of the IP header. For example, if the value in this field is 5, the length of the header is 5*4, which is 20 bytes.

TYPE OF SERVICE (TOS)



It was never widely used as originally defined, and its meaning has been subsequently redefined for use by a technique called Differentiated Services (DS).

TOTAL LENGTH (TL)



Total length of the datagram = Length of the header + Length of the data

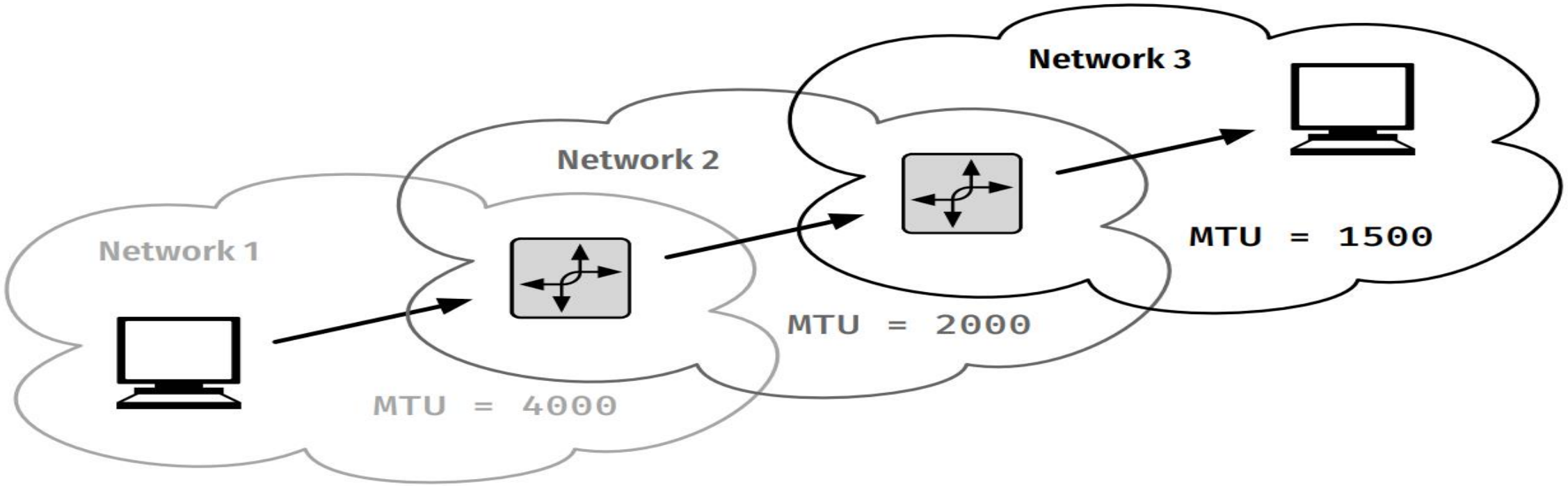
MTU

Every network has a Maximum Transmission Unit (MTU):

» Largest IP datagram that can be carried within a frame.

» Typically, 1500 bytes for Ethernet.

WHAT HAPPENS IF A PACKET TRAVERSE NETWORKS WITH DIFFERENT MTUS?



IP FRAGMENTATION

We do not know the MTUs of all intermediate networks in advance

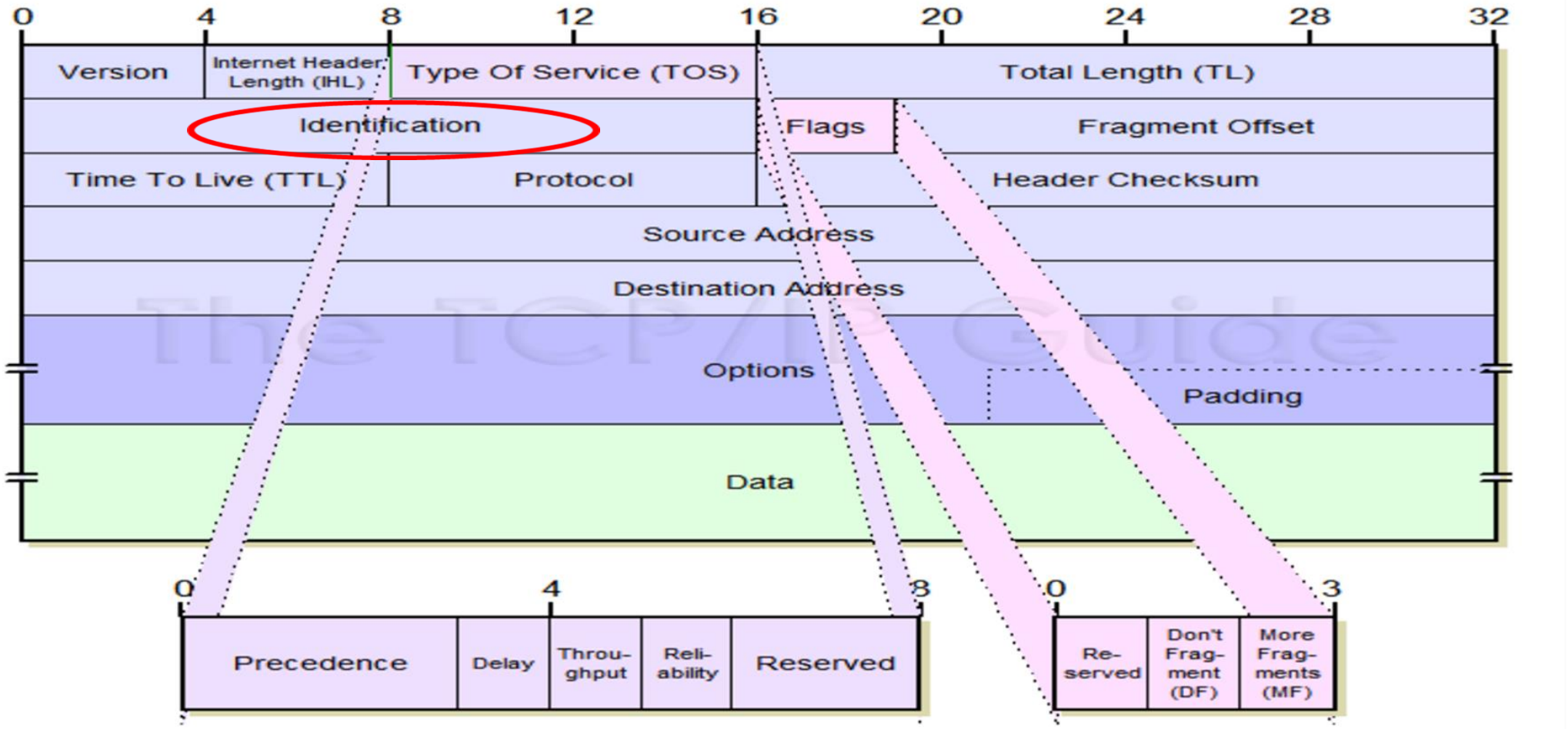
Applicable to the IP (v4)

» When the MTU is smaller than the packet, fragment it.

» Reassemble at destination.

» Drop the packet if a fragment is lost.

IDENTIFICATION



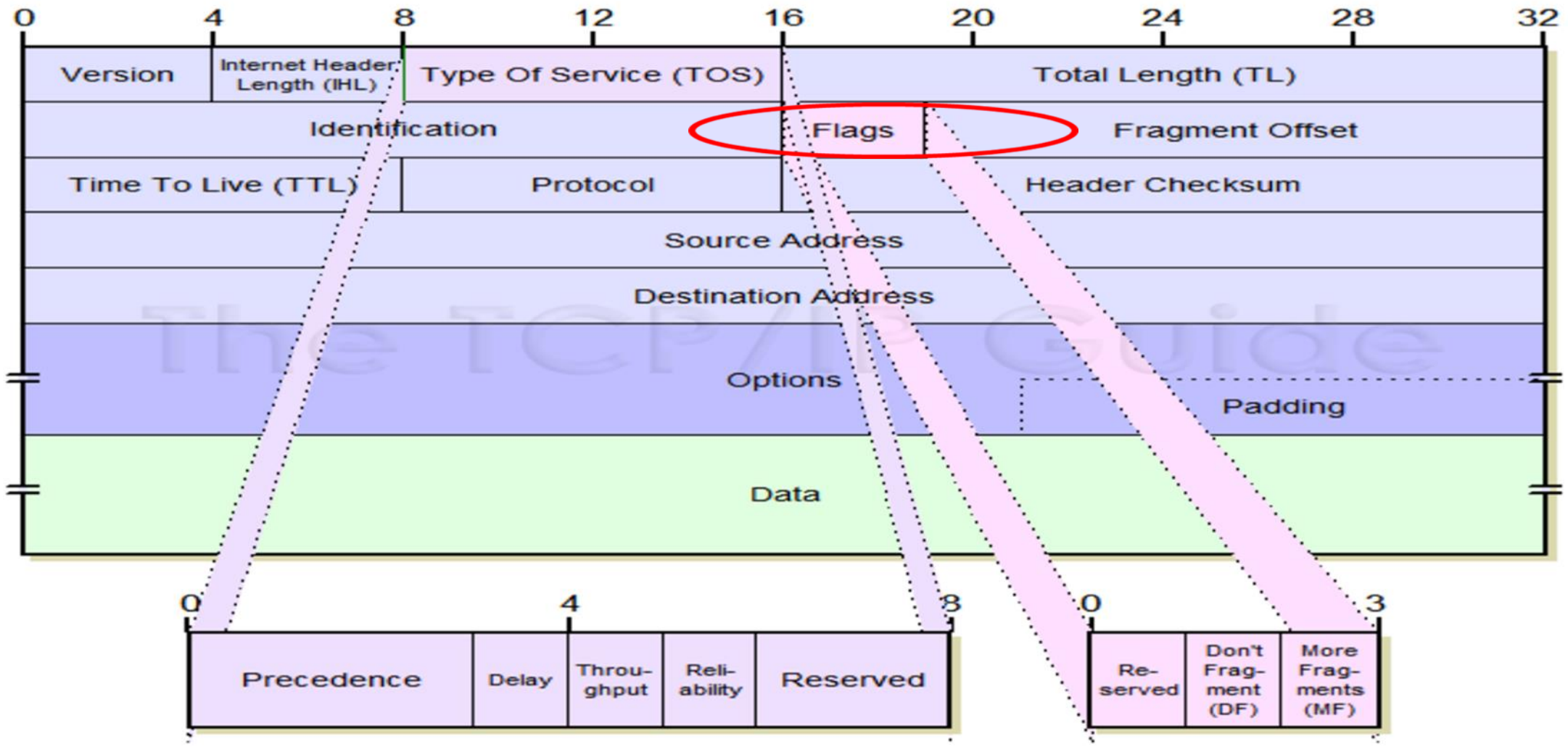
IDENTIFICATION

Uniquely identifies the datagram. Usually incremented by 1 each time a datagram is sent.

All fragments of a datagram contain the same identification value.

This allows the destination host to determine which fragment belongs to which datagram. This field is used by the recipient to reassemble messages without accidentally mixing fragments from different messages. This is needed because fragments may arrive from multiple messages mixed together, since IP datagrams can be received out of order from any device.

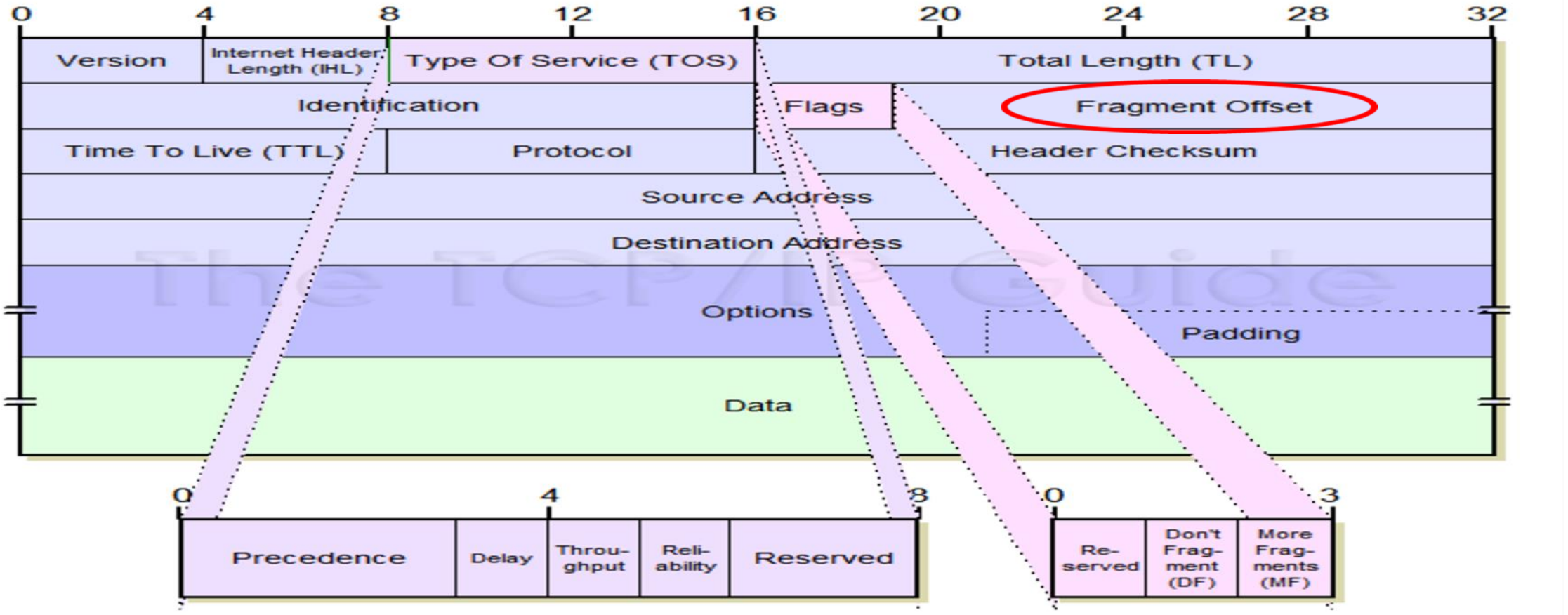
FLAGS


0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Throu-ghput
Reli-ability
Reserved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

FLAGS

Subfield Name	Size (bytes)	Description
Reserved	1/8 (1 bit)	***Reserved:*** Not used.
DF	1/8 (1 bit)	***Don't Fragment:*** When set to 1, specifies that the datagram should not be fragmented. Since the fragmentation process is generally "invisible" to higher layers, most protocols don't care about this and don't set this flag. It is, however, used for testing the maximum transmission unit (MTU) of a link.
MF	1/8 (1 bit)	***More Fragments:*** When set to 0, indicates the last fragment in a message; when set to 1, indicates that more fragments are yet to come in the fragmented message. If no fragmentation is used for a message, then of course there is only one "fragment" (the whole message), and this flag is 0. If fragmentation is used, all fragments but the last set this flag to 1 so the recipient knows when all fragments have been sent.

FRAGMENT OFFSET (13 BITS)

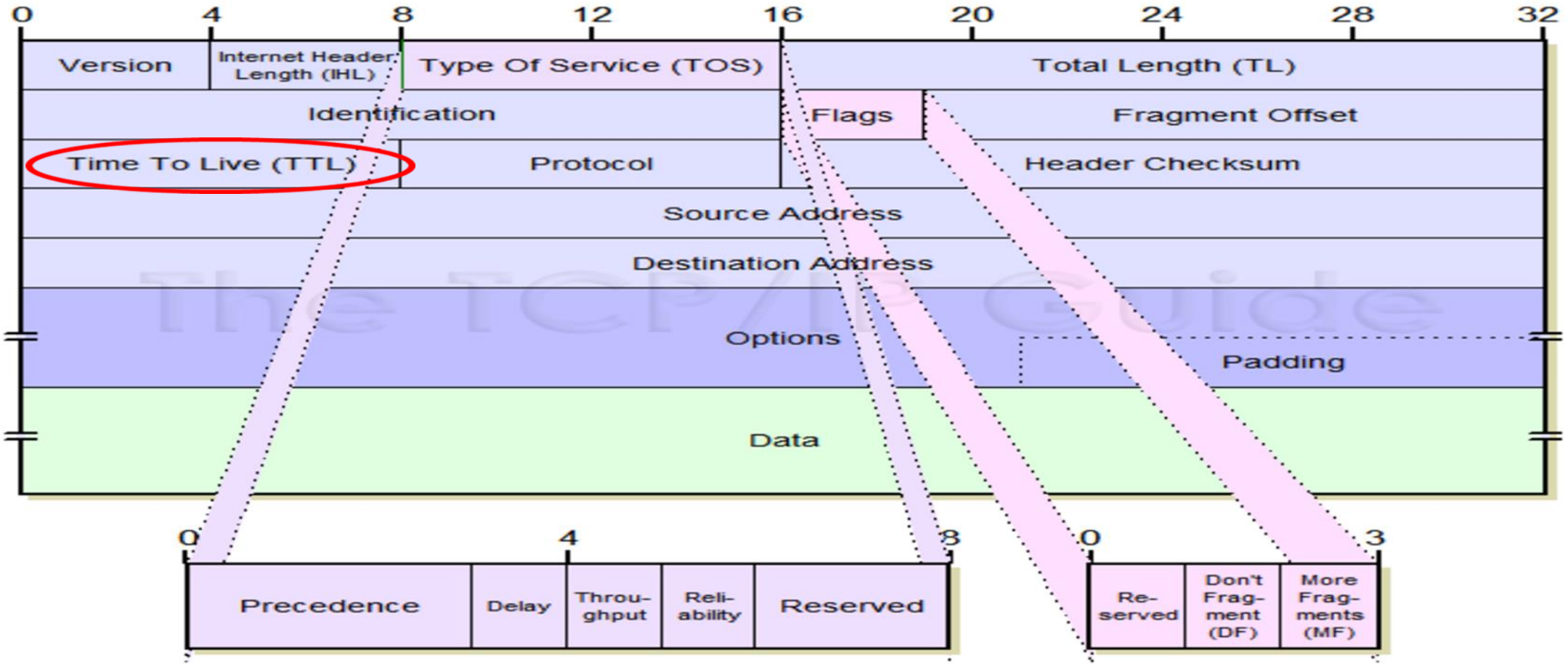


This field helps the destination device to place the fragments in the proper sequence to build the original packet

EXAMPLE FOR FRAGMENT OFFSET

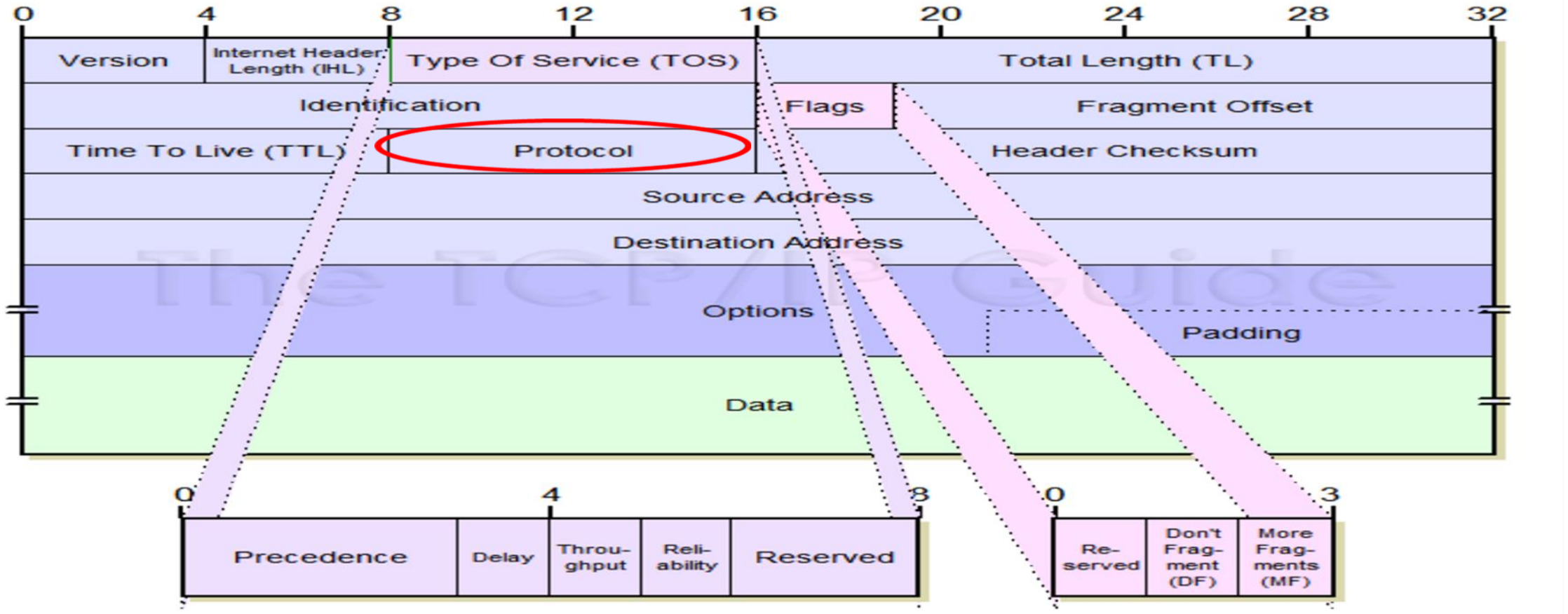
- Suppose we have a packet for 1700 bytes and IP header is 20 bytes to be transmitted over an MTU of 1500 bytes.
  - First fragment:
  - Fragment Offset: 0
  - ID : 1
  - MF = 1
  - DF = 0
  - Total Length : 1500 bytes
  - Data Payload = 1500 -20 bytes (IP header) = 1480 bytes
  - Second Fragment:
  - Fragment Offset: (Calculation = Previous fragment Offset + (Previous Fragment Data transmitted/8))= 0 + (1480/8) = 185
  - ID : 1
  - MF = 0
  - DF = 0
  - Data Payload = 220
  - Total Length: (Data payload plus IP header) 240 bytes

TIME TO LIVE

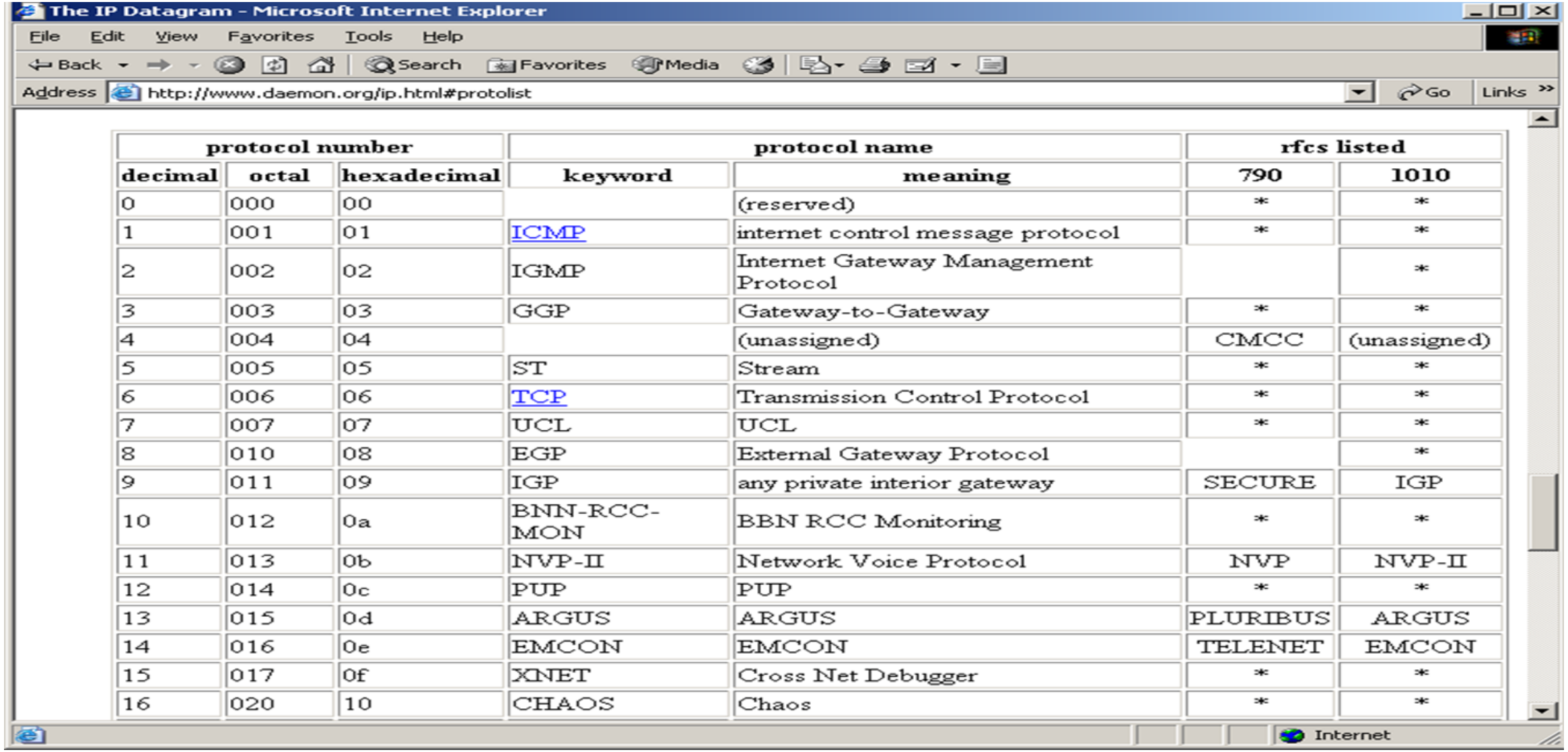


Time To Live (TTL): Short version: Specifies how long the datagram is allowed to “live” on the network, in terms of router hops. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

PROTOCOL

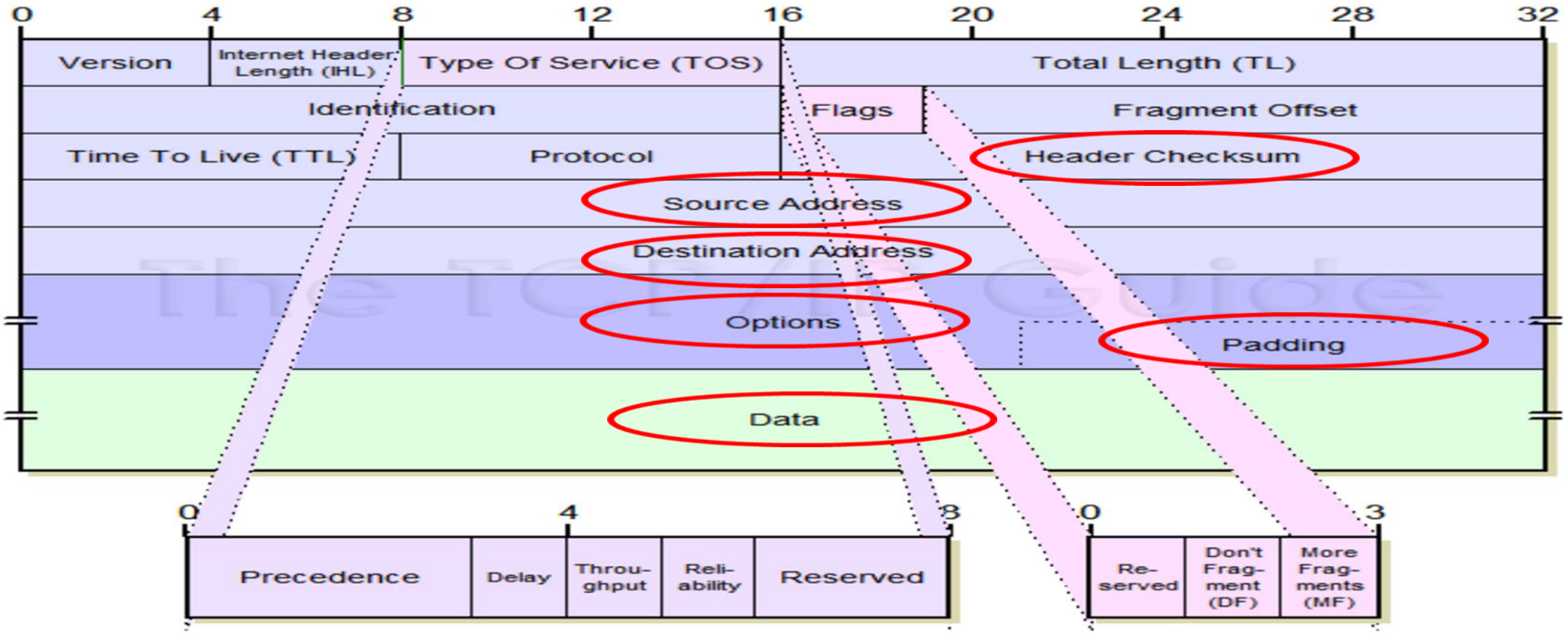

0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Throu-ghput
Reli-ability
Reserved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

PROTOCOL



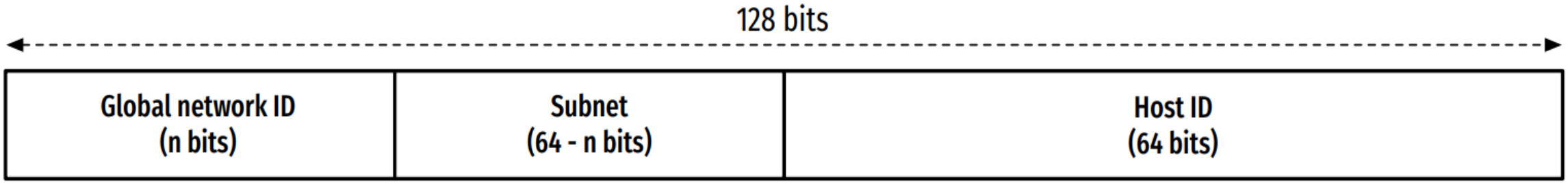
protocol number			protocol name		rfcs listed	
decimal	octal	hexadecimal	keyword	meaning	790	1010
0	000	00		(reserved)	*	*
1	001	01	ICMP	internet control message protocol	*	*
2	002	02	IGMP	Internet Gateway Management Protocol		*
3	003	03	GGP	Gateway-to-Gateway	*	*
4	004	04		(unassigned)	CMCC	(unassigned)
5	005	05	ST	Stream	*	*
6	006	06	TCP	Transmission Control Protocol	*	*
7	007	07	UCL	UCL	*	*
8	010	08	EGP	External Gateway Protocol		*
9	011	09	IGP	any private interior gateway	SECURE	IGP
10	012	0a	BNN-RCC-MON	BBN RCC Monitoring	*	*
11	013	0b	NVP-II	Network Voice Protocol	NVP	NVP-II
12	014	0c	PUP	PUP	*	*
13	015	0d	ARGUS	ARGUS	PLURIBUS	ARGUS
14	016	0e	EMCON	EMCON	TELENET	EMCON
15	017	0f	XNET	Cross Net Debugger	*	*
16	020	10	CHAOS	Chaos	*	*

HEADER CHECKSUM, SOURCE ADDRESS, DESTINATION ADDRESS, OPTIONS, PADDING AND DATA



IPV6 ADDRESSING AND ITS FIELD COMPONENTS

- Written as groups of 2B (four hexadecimal digits):
  - » fdd3:d79f:e4d8:f666:c0ab:1c29:b676:af96
- Leading zeros may be dropped, and up to one double colon substitution is permitted:
  - » 344d:9a03:0000:12c1:0000:0000:0fab:0001
  - » 344d:9a03:0:12c1:0:0:fab:1
  - » 344d:9a03:0:12c1::fab:1



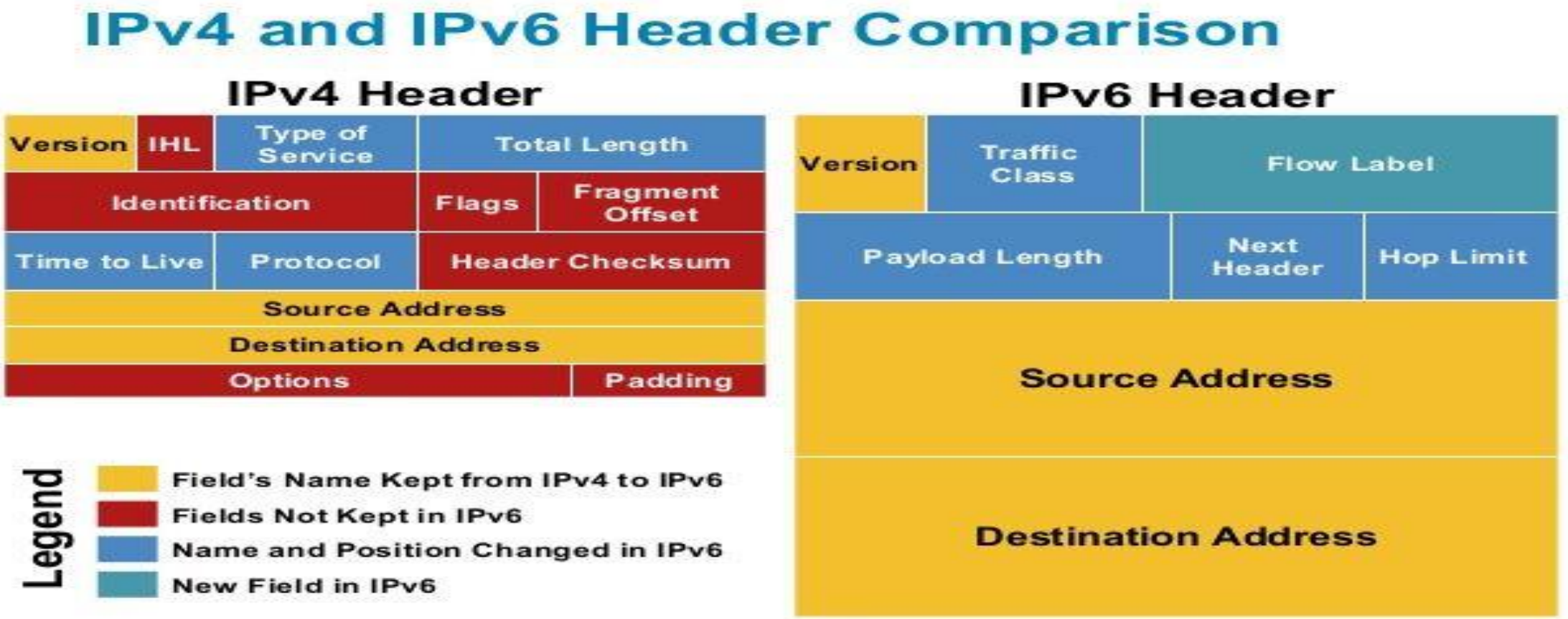
IPV6 ADDRESS TYPES

1. **Unicast addresses**: Used to provide one to one communication.
2. **Multicast addresses**: Used to provide one to many (group) communication. The prefix for multicast addresses is FF00::/8.
3. A**nycast addresses**: A special type of communication address in which a packet is delivered to the nearest of multiple interfaces

IPV4 VS IPV6

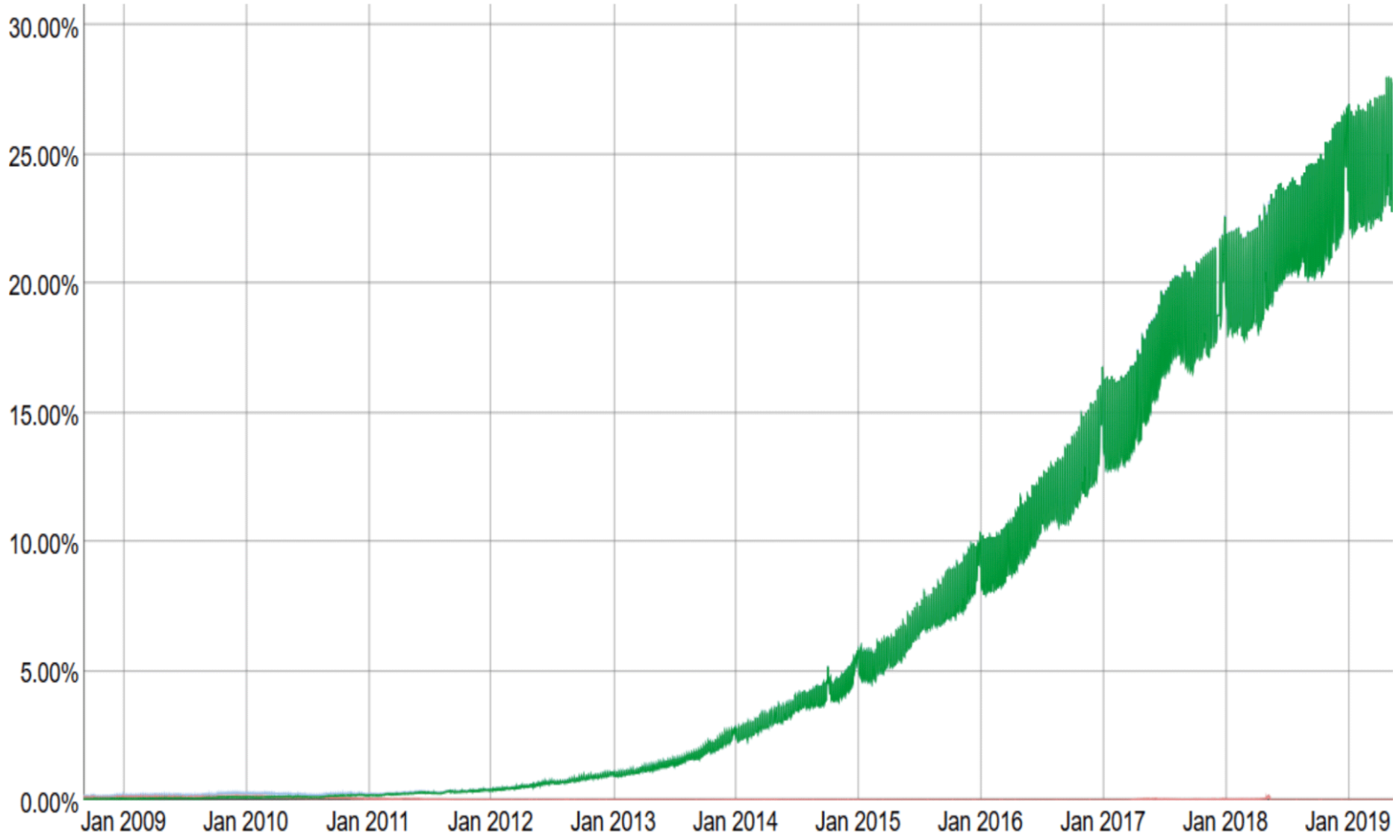
Feature	IPv4	IPv6
Address length	32-bits, divided in to 4 octets	128-bits, divided in to 8 blocks
Address format	Decimal (0-9)	Hexadecimal (0-9, A-F)
Separation of octets/blocks	By period (.)	By colon (:)
Total available addresses	4.3 billion	36 trillion
Local subnet group management	Internet Group Message Protocol (IGMP)	Multicast Listener Discovery (MLD)
Auto configuration	Does not support	Support
Type	Unicast, Multicast, and Broadcast	Unicast, Multicast, and Anycast
IP to MAC resolution	Broadcast (ARP)	Multicast Neighbor Solicitation
Network ID notation	Subnet mask and CIDR	Prefix notation
Example	192.168.1.100 255.255.255.0	2001:0123:aabb:ccdd::1/64

IPV6 HEADER


IPv4 and IPv6 Header Comparison
IPv4 Header
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Legend
Field's Name Kept from IPv4 to IPv6
Fields Not Kept in IPv6
Name and Position Changed in IPv6
New Field in IPv6

WHY IPV6 DEPLOYMENT AND ACCEPTANCE IS SLOW !

- Reason 1: It's bloody expensive
- Reason 2: Compatibility please!
- Reason 3: I will not do it if you don’t



Percentage of users that access Google over native IPv6.

CHALLENGES OF FRAGMENTATION

Fragments might arrive out-of-order and we do not know how much memory required until receive final fragment.

Some fragments may be duplicated, we should only keep one copy.

Some fragments may never arrive, after a while, give up the entire packet.

FRAGMENTATION AND REASSEMBLY CONCEPTS

Demonstrates many Internet concepts:

- a. Decentralized; every network can choose MTU
- b. Connectionless datagram protocol
  - Each (fragment of) packet contains full routing information.
  - Fragments can proceed independently and along different routes.

IPV6 AND FRAGMENTATION

- IPv6 routers never fragment packets. If they are too large, they will be dropped and Packet too Big will be signaled. This is similar to IPv4 Do not Fragment.
- End nodes are expected to do path MTU discovery to determine the maximum size.
- If there is a need to fragment, hosts can do end-to-end fragmentation using special headers.

References

- http://www.whatis.com
- http://www.webopedia.com
- Understanding Data Communications & Networks, Shay (1999)
- http://www.daemon.org/ip.html
- https://www.youtube.com/watch?v=OqsXzkXfwRw&t=1s&ab_channel=TechTerms

READING INSTRUCTIONS

- » Ch. 1-2
- » Ch. 20-22