Computer Network Protocols
Data Link Layer
Lesson -2

جامعة المستقبل
كلية الهندسة والتقنيات الهندسية
قسم هندسة تقنيات الحاسوب
المرحلة الرابعة

By

Dr. Layth Abdulkareem Hassnawi
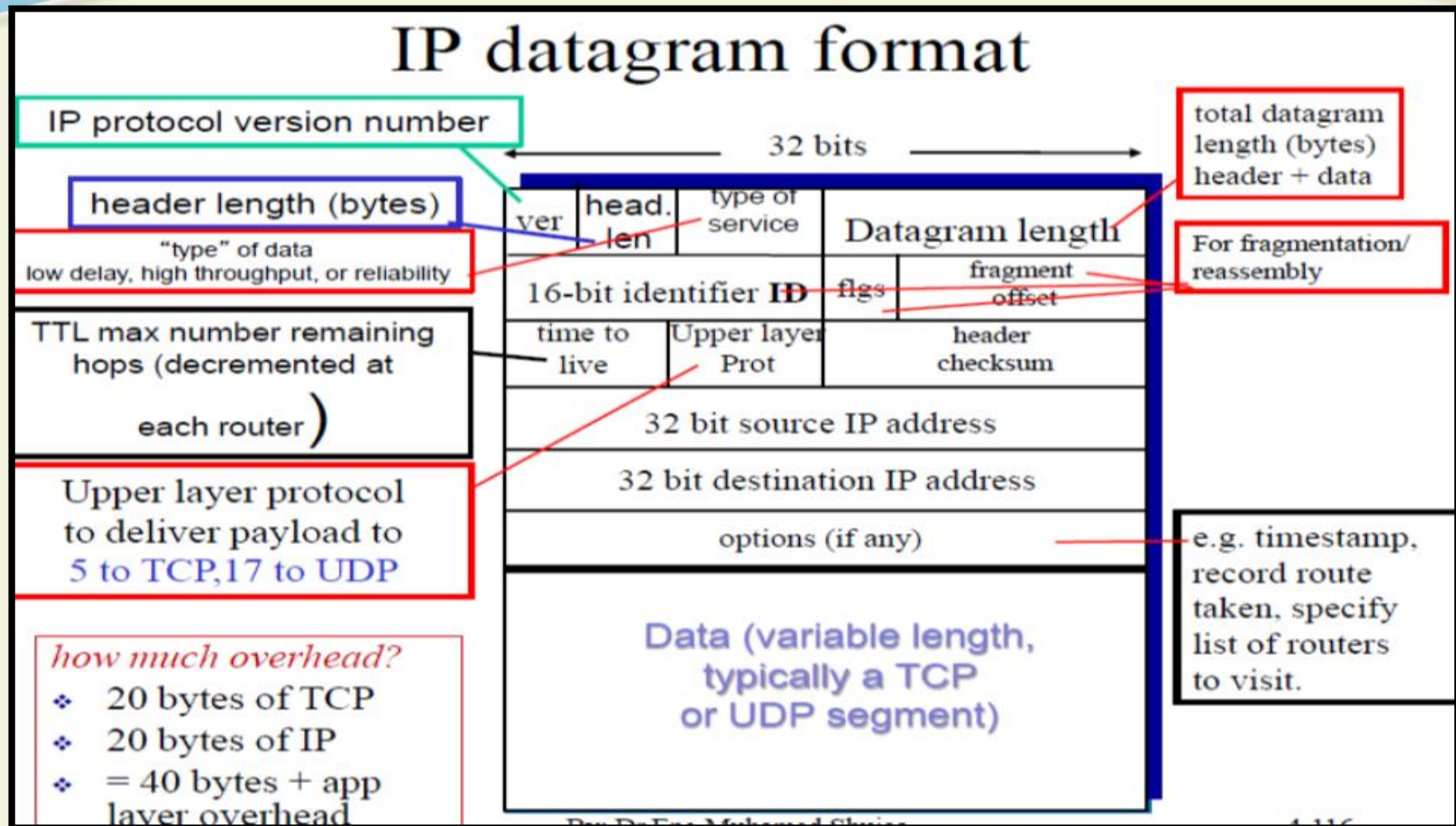
Layer 2 Tunneling Protocol (L2TP)

L2TP is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. The main features of L2TP protocol are:

- *Is an **extension of the Point-to-Point Tunneling Protocol (PPTP).***

- ***Used** by an Internet service provider (ISP) to **enable the operation of a virtual private network (VPN) over the Internet**.*

- *The goal of a Virtual Private Network (VPN) is to **provide private communications within the public Internet Infrastructure***

Why is there a need for VPN?

1. Internet has **insufficient security** mechanisms

2. IP packets are **not authenticated or encrypted**

3. Users with access to network **can read content of IP traffic**

IP Datagram Format

IP datagram format

IP protocol version number

header length (bytes)

"type" of data
low delay, high throughput, or reliability

TTL max number remaining hops (decremented at each router)

Upper layer protocol to deliver payload to 5 to TCP,17 to UDP

how much overhead?
- ❖ 20 bytes of TCP
- ❖ 20 bytes of IP
- ❖ = 40 bytes + app layer overhead

32 bits

ver	head. len	type of service	Datagram length
16-bit identifier **ID**		flgs	fragment offset
time to live	Upper layer Prot	header checksum	
32 bit source IP address			
32 bit destination IP address			
options (if any)			
Data (variable length, typically a TCP or UDP segment)			

total datagram length (bytes) header + data

For fragmentation/ reassembly

e.g. timestamp, record route taken, specify list of routers to visit.

Transition from IPV 4 to IPV 6

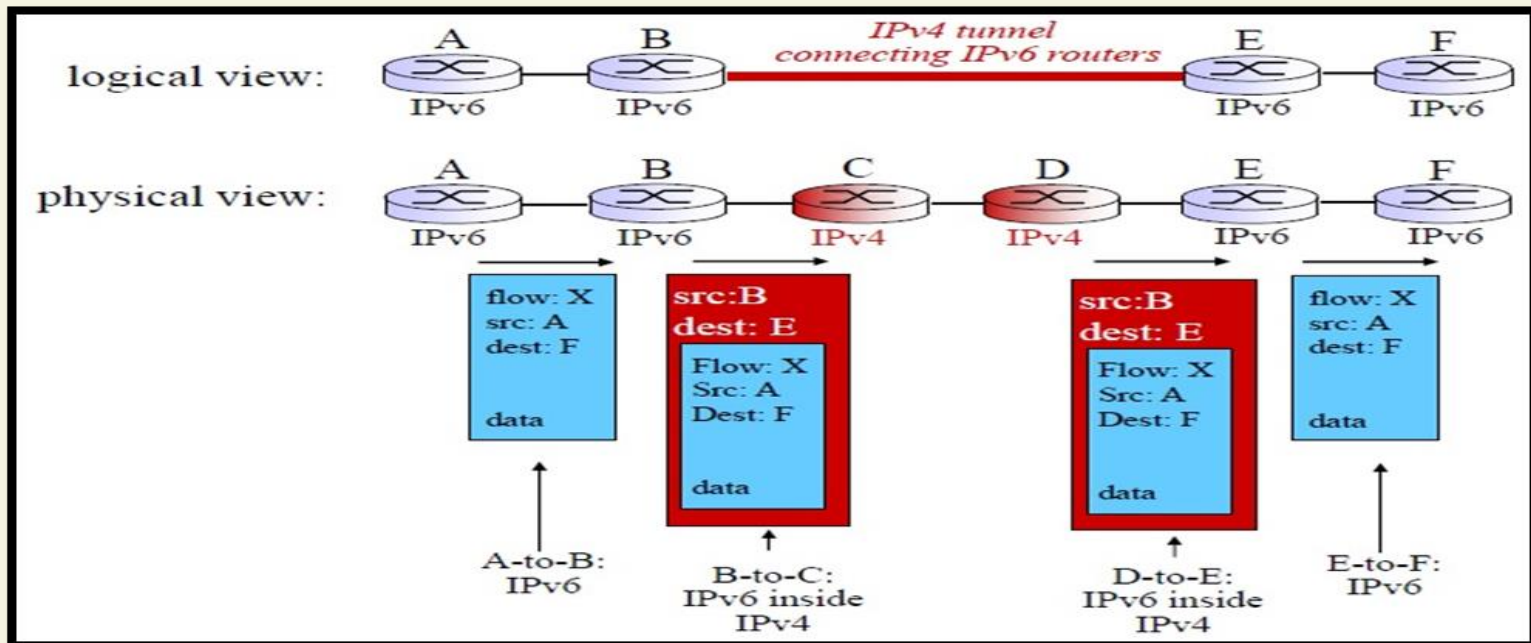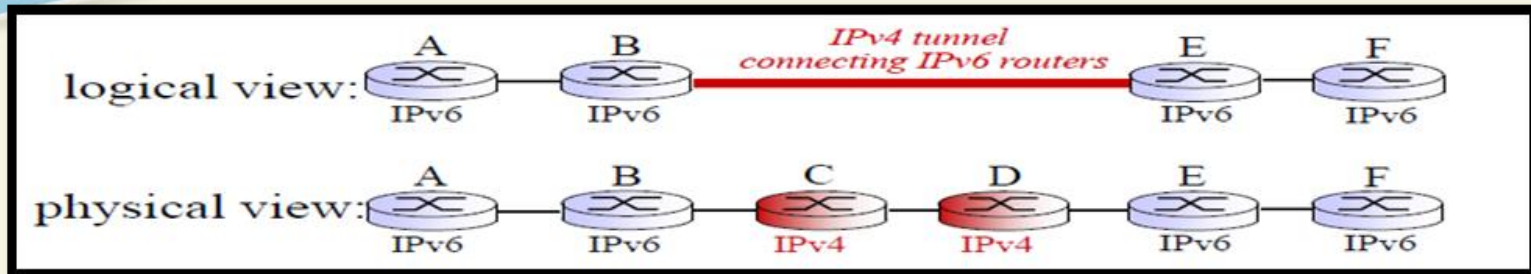**Not all routers can be upgraded simultaneously**

How will network operate with mixed IPv4 and IPv6 routers?

Answer: this can be done by Tunneling: IPv6 datagram carried as payload in IPv4 datagram among IPv4 routers
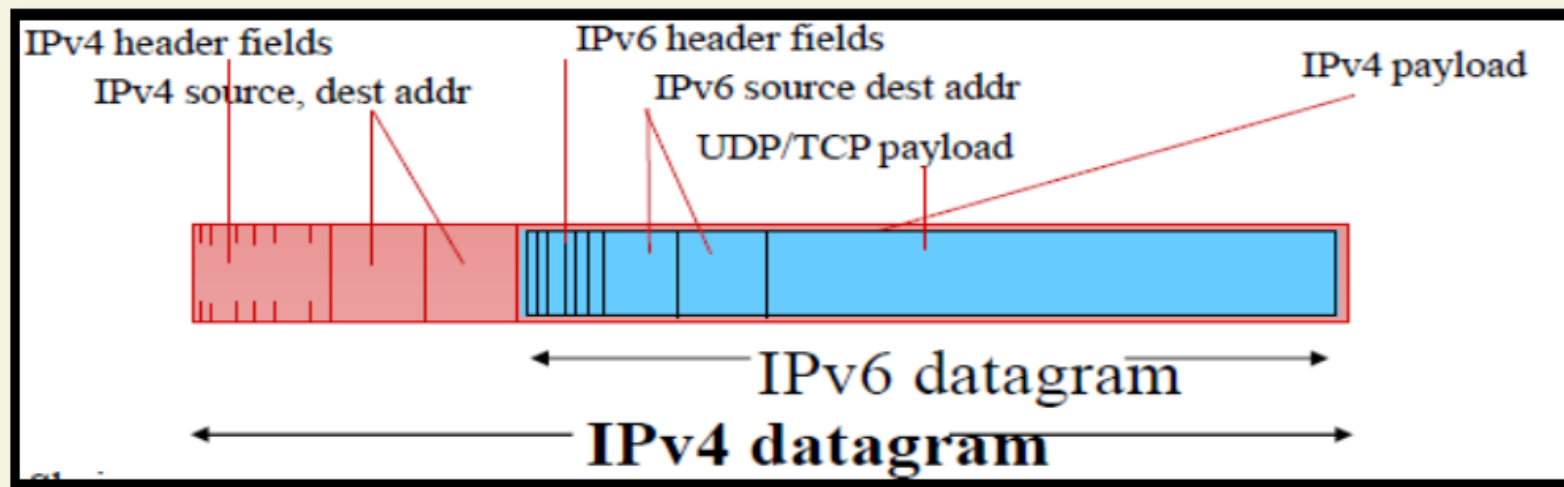
Transition from IPV 4 to IPV 6

Errors Detection and Correction

Networks must be able to **transfer data from one device to another with complete accuracy**. Data can be **corrupted during transmission**. For reliable communication, **errors must be detected and corrected**. Error detection is implemented either at the data link layer or the transport layer of the OSI model.
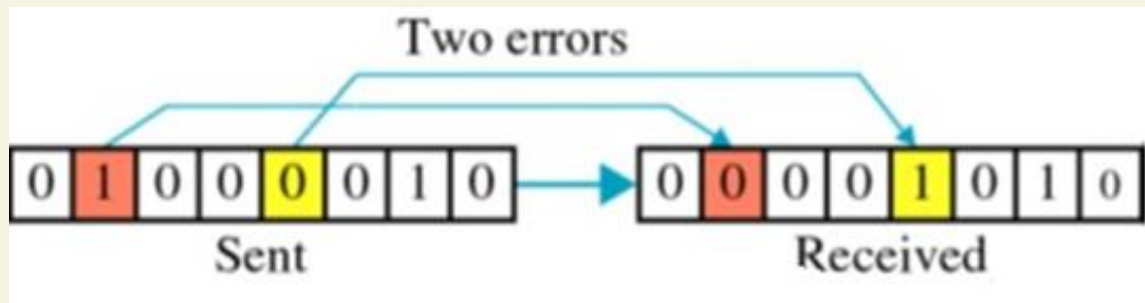
fppt.com

Types of Errors

*There are three types of error, these are:*

1. Single Bit Error
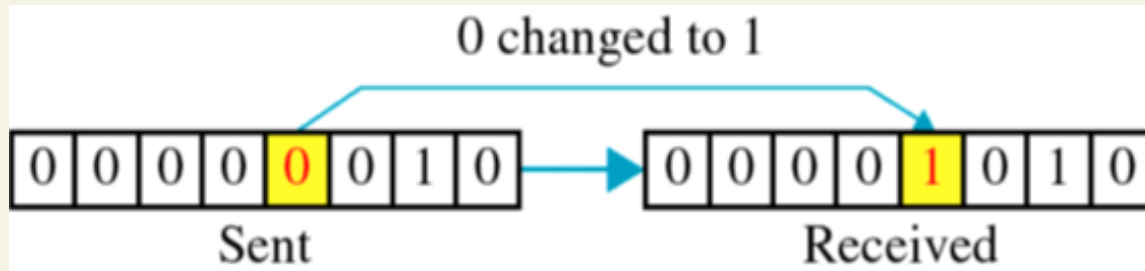
2. Multiple Error

Types of Errors

3. Burst Error: *means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1. Burst errors do not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.*
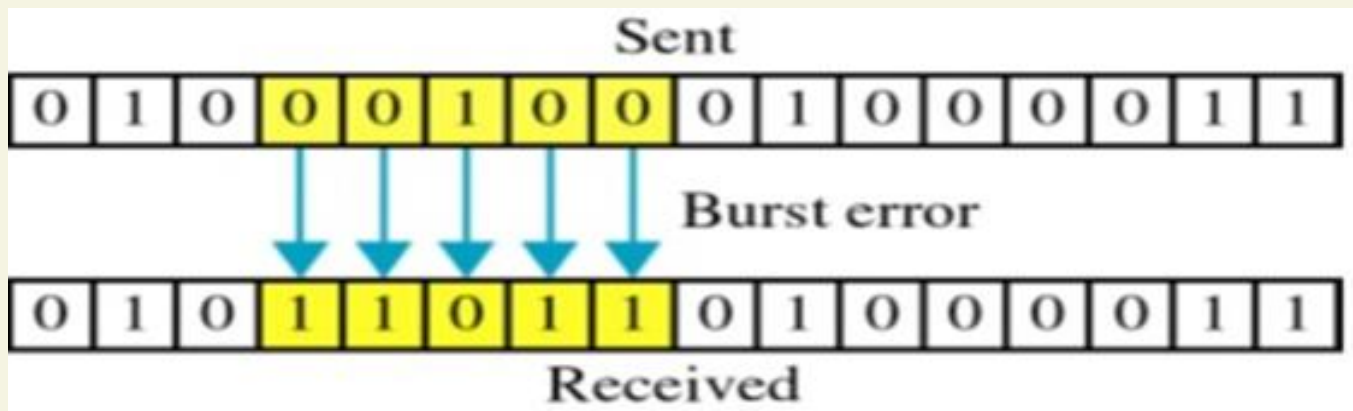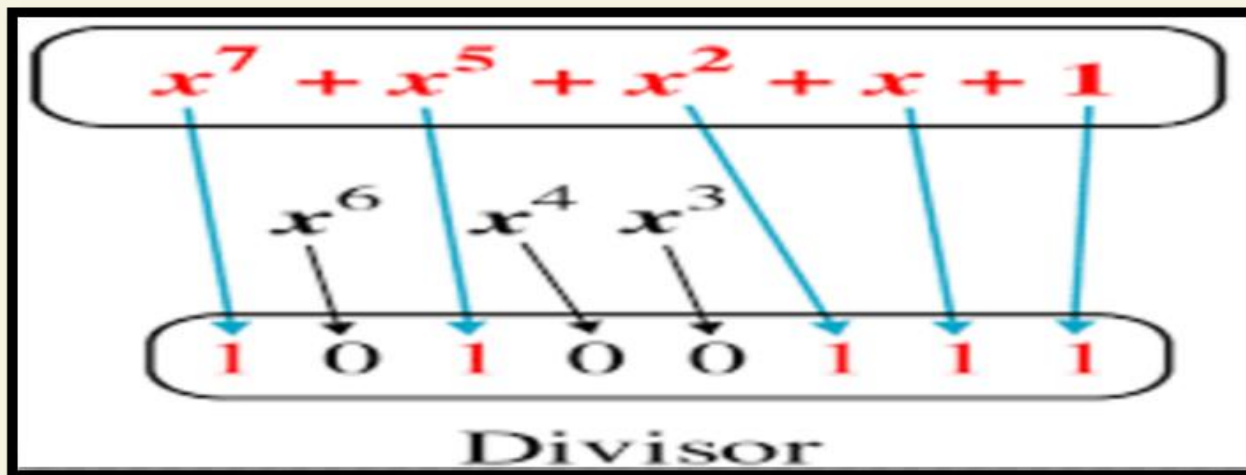
Polynomial Calculation

Byte representation is X^7 X^6 X^5 X^4 X^3 X^2 X^1 X^0

The rules of calculation according to byte representation are:

1. If you have number "1" alone just put 1 because $X^0=1$
2. Put "1" whenever you find x
3. Put zero whenever you didn't find x
4. All zeros to **LEFT** of number are neglected (~~000~~10001)

$$x^7 + x^5 + x^2 + x + 1$$

x^6 x^4 x^3

1   0   1   0   0   0   1   1   1

Divisor

fppt.com

Polynomial Calculation Examples

$$X^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$ it is represented in binary like this: **110110111**

Explanation:

$X^8 = 1$

$x^7 = 1$

$x^6 = 0$ because it is not there

$x^5 = 1$

$x^4 = 1$

$x^3 = 0$ because it is not there

$x^2 = 1$

$x = 1$ -> the rule says that whenever we have x alone, we put '1' because $x = x^1$

$1 = 1$ -> the rule says that whenever we have 1 alone, we put '1' because $1 = x^0$

End Of Lesson 2

Thanks For Listening