פרק 8

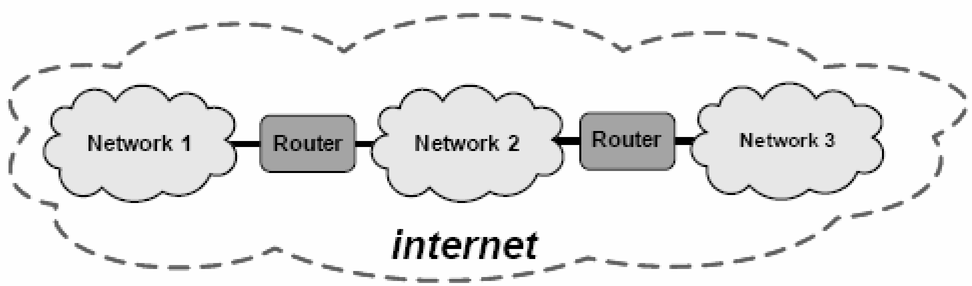
- הגדרות ועקרונות בסיסיים
- מודל השכבות
- משפחת הפרוטוקולים
- מאפייני פרוטוקול IP
- מיבנה פרוטוקול ה- IP
- כתובות IP
- IPV4 לעומת IPV6

הגדרות

- The term internet is short for “internetworking”
  - interconnection of networks with different network access mechanisms, addressing, different routing techniques, etc
- An internet
  - Collection of communications networks interconnected by layer 3 switches and/or routers
- IP (Internet Protocol)
  - Most widely used internetworking protocol
  - IP provides <u>connectionless</u> (datagram) service
  - Each packet treated separately
  - Network layer protocol

עקרונות בסיסיים

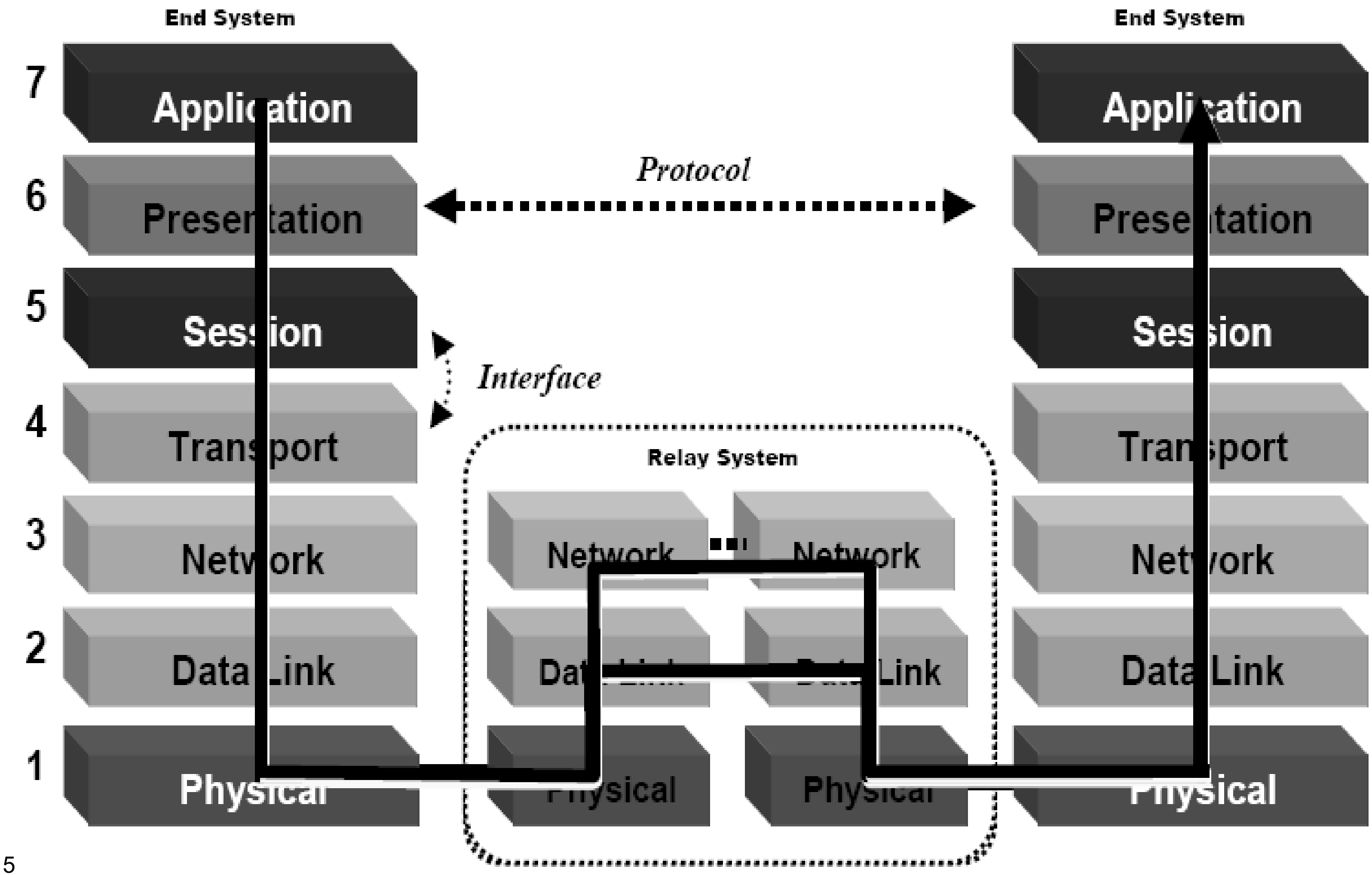
- TCP/IP protocol suite – also called “ **Internet Protocol Suite**” is named for two of its most important protocols:
  - Transmission Control Protocol (TCP)
  - Internet Protocol (IP)
- Goals:
  - build an interconnection of networks that provided **universal communication services**:
    - architecture of the physical networks is **hidden** from the user.
  - **interconnect** different physical networks to form what appears to the user to be one large network.
    - such a set of interconnected networks is called an ***internet***.



מודל 7 השכבות לפי OSI

7	**Application**	File xfers, e-mail, term. emulation, etc.
6	**Presentation**	Data formatting and encryption
5	**Session**	Setup & maintain application sessions
4	**Transport**	End-to-end reliable data delivery
3	**Network**	Route packets through an internetwork
2	**Data Link**	Data framing, error checking over link
	Physical	Define/transmit raw data over channel

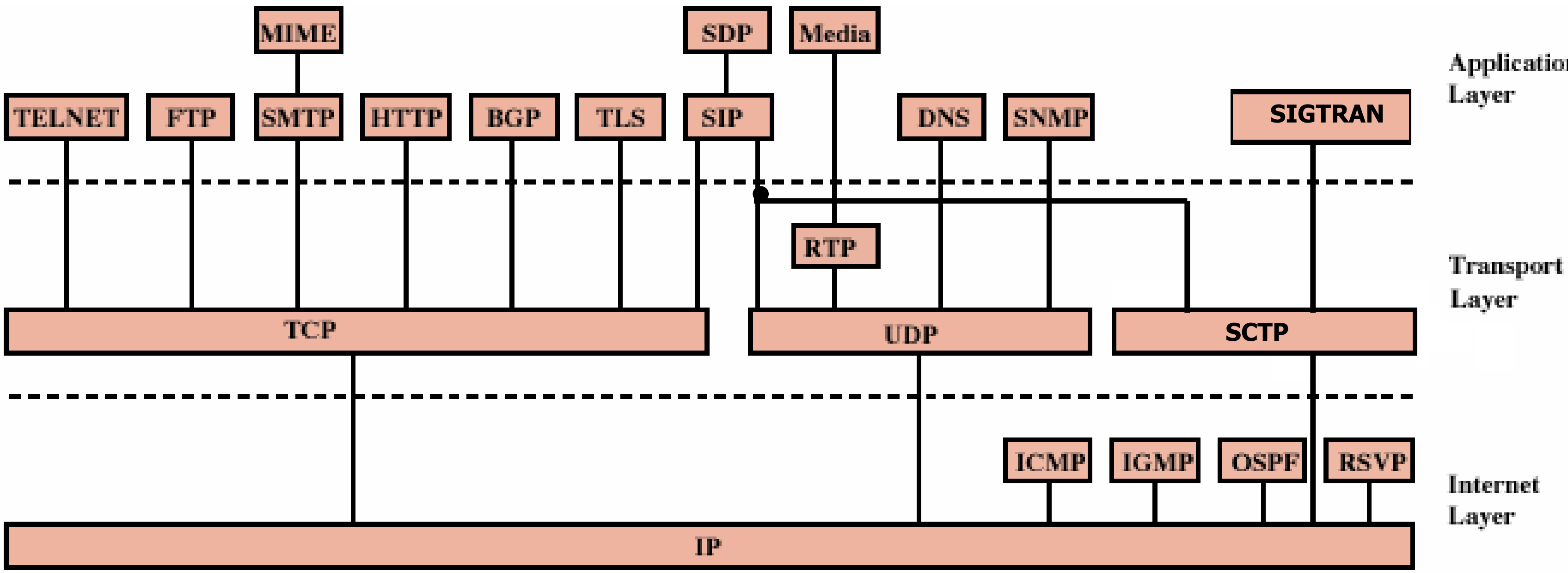
מודל 7 השכבות לפי OSI (המשך)



IP פרוטוקול

- IP stands for **Internet Protocol**
- A set of rules to send and receive messages at the Internet address level
- Computers must run IP to communicate across the internet
- IP forwards each packet based on a four byte destination address (the IP number) (e.g, 192.156.1.1)

משפחת הפרוטוקולים מעל IP



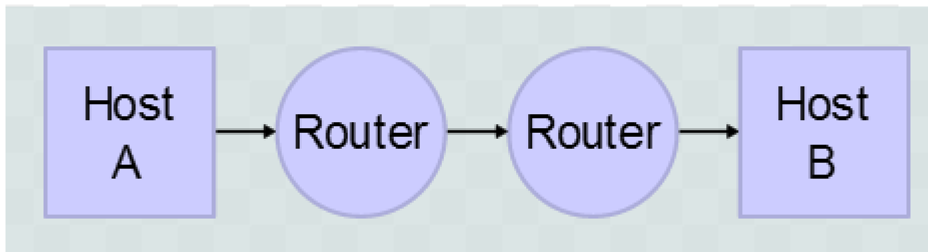
BGP	=	Border Gateway Protocol	RSVP	=	Resource ReSerVation Protocol
DNS	=	Domain Name System	RTP	=	Real-Time Transport Protocol
FTP	=	File Transfer Protocol	SDP	=	Session Description Protocol
HTTP	=	Hypertext Transfer Protocol	SIP	=	Session Initiation Protocol
ICMP	=	Internet Control Message Protocol	SMTP	=	Simple Mail Transfer Protocol
IGMP	=	Internet Group Management Protocol	SNMP	=	Simple Network Management Protocol
IP	=	Internet Protocol	TCP	=	Transmission Control Protocol
MIME	=	Multi-Purpose Internet Mail Extension	TLS	=	Transport Layer Security
OSPF	=	Open Shortest Path First	UDP	=	User Datagram Protocol

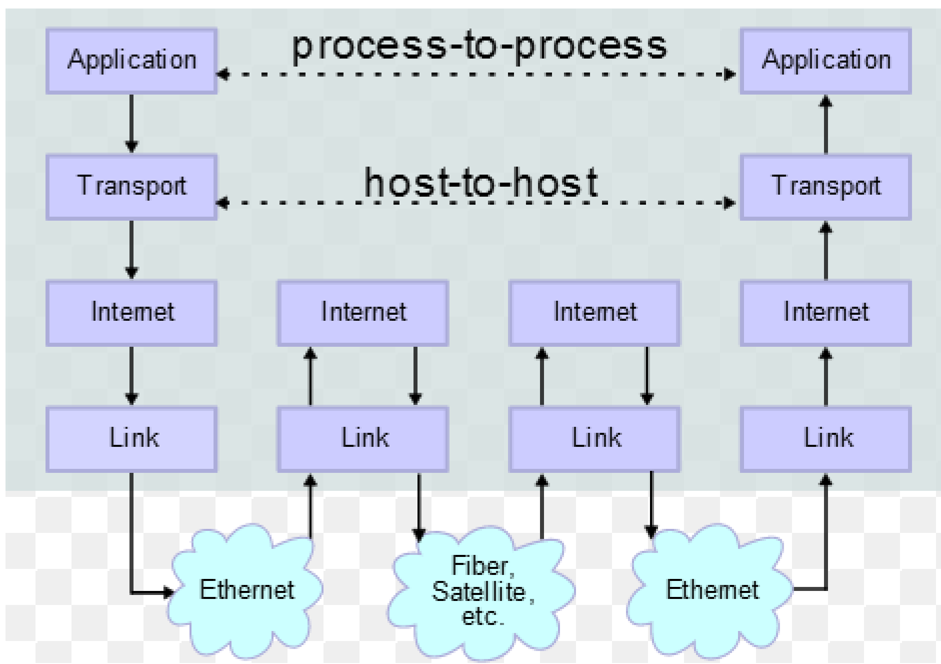
Connectionless Internetworking

- Advantages
  - Flexible and robust
    - In case of congestion or node failure, packets find their way easier than connection-oriented services
  - No unnecessary overhead for connection setup
  - Can work with different network types

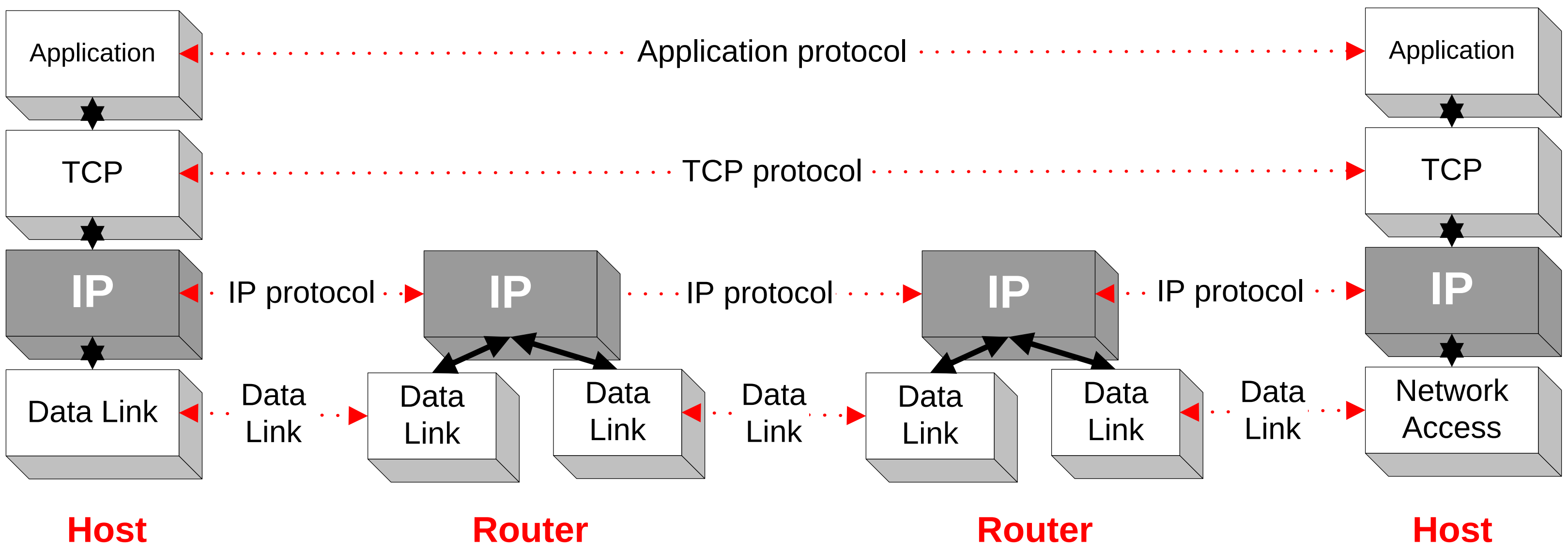
- Disadvantage: Unreliable
  - Not guaranteed delivery
  - Not guaranteed order of delivery
    - Packets can take different routes
  - Reliability is responsibility of next layer up (for example:TCP)

דוגמא לתקשורת IP (1)





דוגמא לתקשורת IP (2)

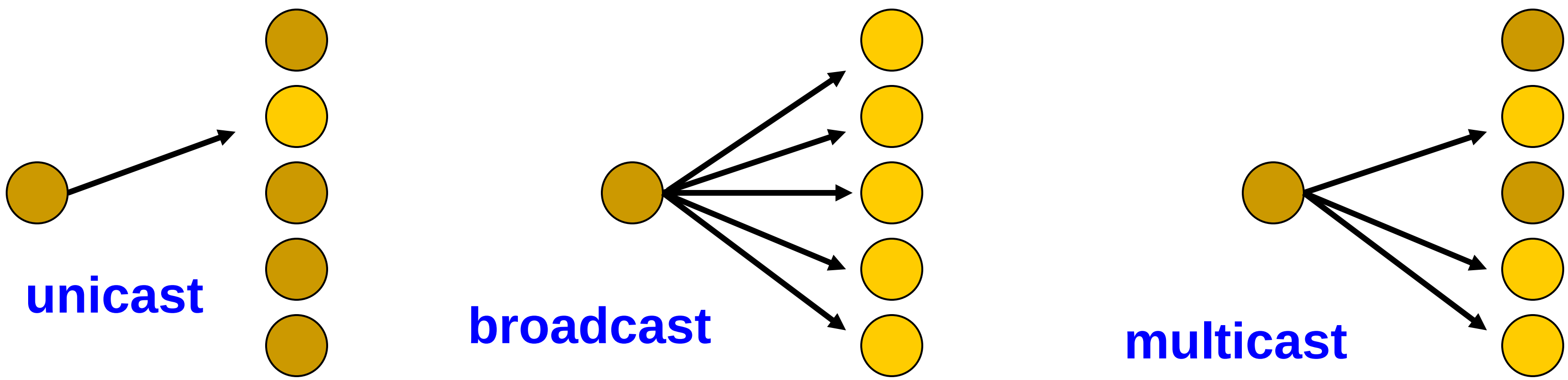


שירותי IP

- IP provides an unreliable connectionless best effort service (also called: “datagram service”)
  - Unreliable: IP does not make an attempt to recover lost packets
  - Connectionless: Each packet (“datagram”) is handled independently. IP is not aware that packets between hosts may be sent in a logical sequence
  - Best effort: IP does not make guarantees on the service (no throughput guarantee, no delay guarantee,…)
- Consequences
  - Higher layer protocols have to deal with losses or with duplicate packets
  - Packets may be delivered out-of-sequence

שירותי IP (המשך)

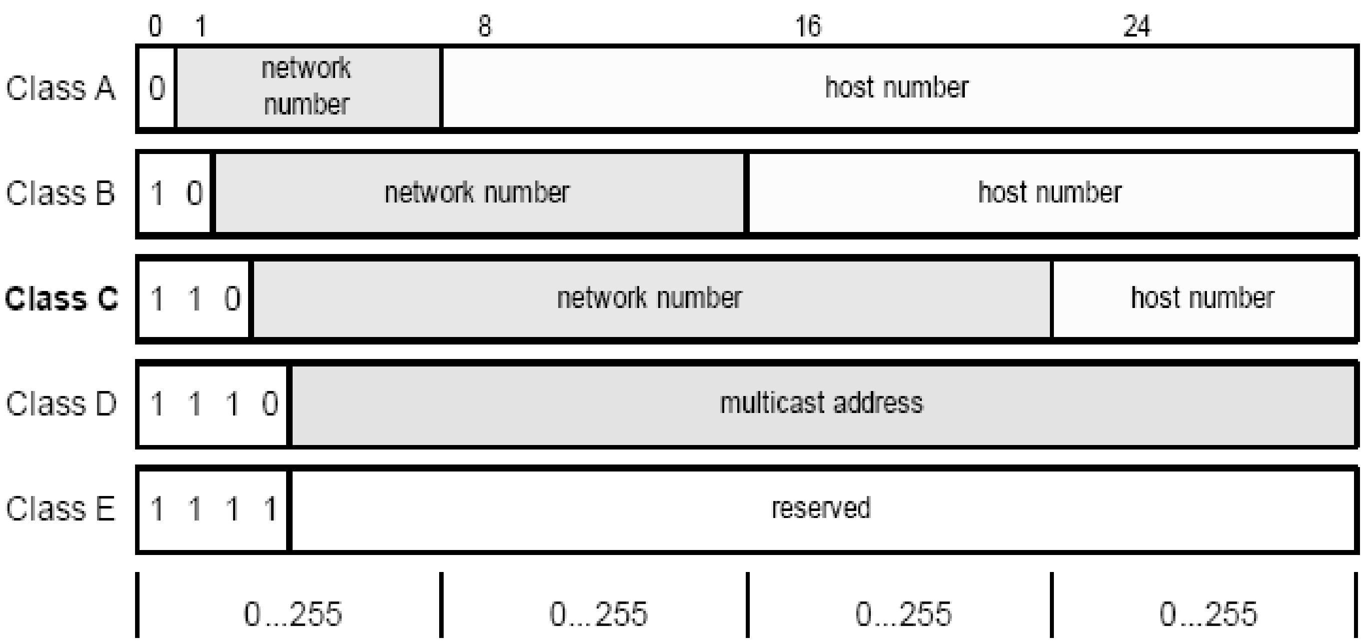
- IP supports the following services:
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-several (multicast)



- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)

מיבנה כתובות ה-IP

IP Address = <network number><host number>
Initially, 5 Classes of IP addresses where defined



מיבנה כתובות ה-IP (המשך)

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

מיבנה כתובות ה-IP (המשך)

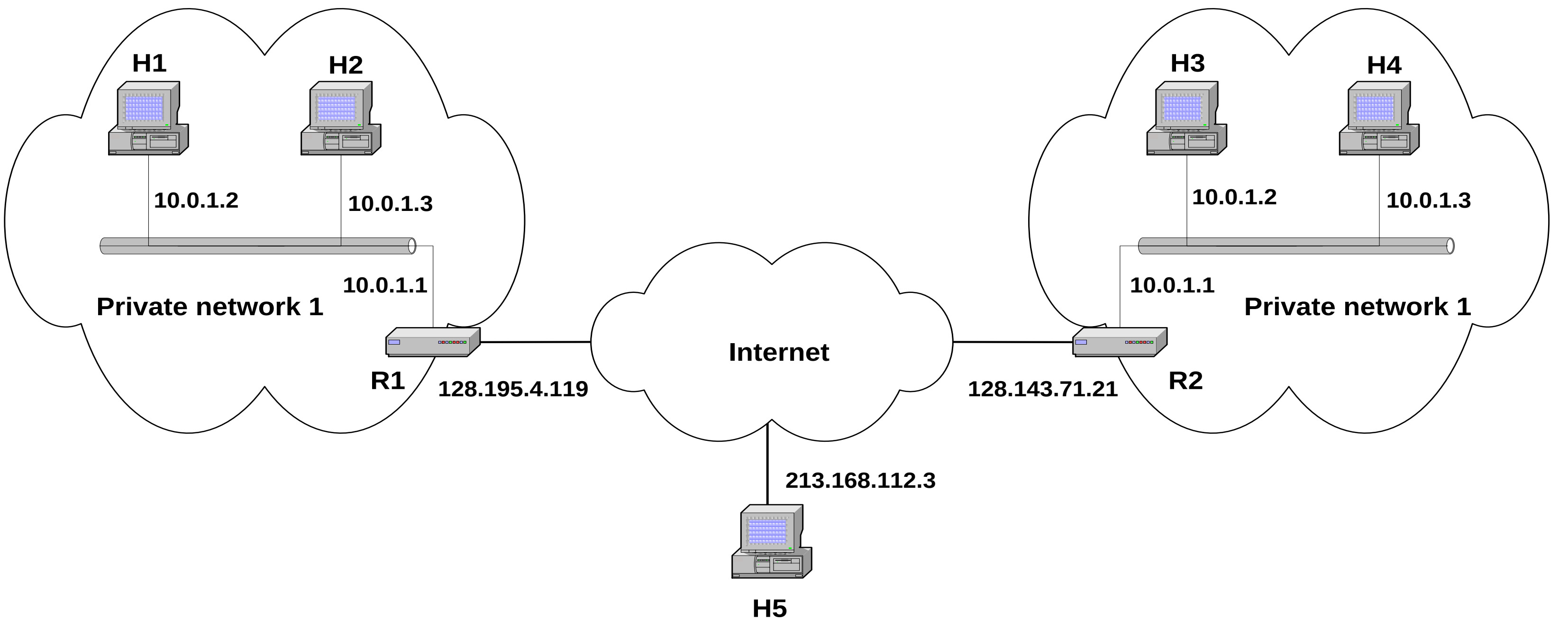
125.31.137.33

01111101 00011111 10001001 00100001

32 bits - Decimal Notation

Each node has at least one IP address on each one of its interfaces

כתובות פרטיות לעומת כתובות גלובליות



כתובות ברשתות פרטיות

- Private IP network is an IP network that is not Directly Connected to the Internet
- Not unique IP addresses
- Private networks address ranges
  - Class A: 10.0.0.0 – 10.255.255.255 **10.x.x.x**
  - Class B: 172.16.0.0 – 172.31.255.255 **172.16.x.x-172.31.x.x**
  - Class C: 192.168.0.0 – 192.168.255.255 **192.168.x.x**

Subnets and Subnet Masks

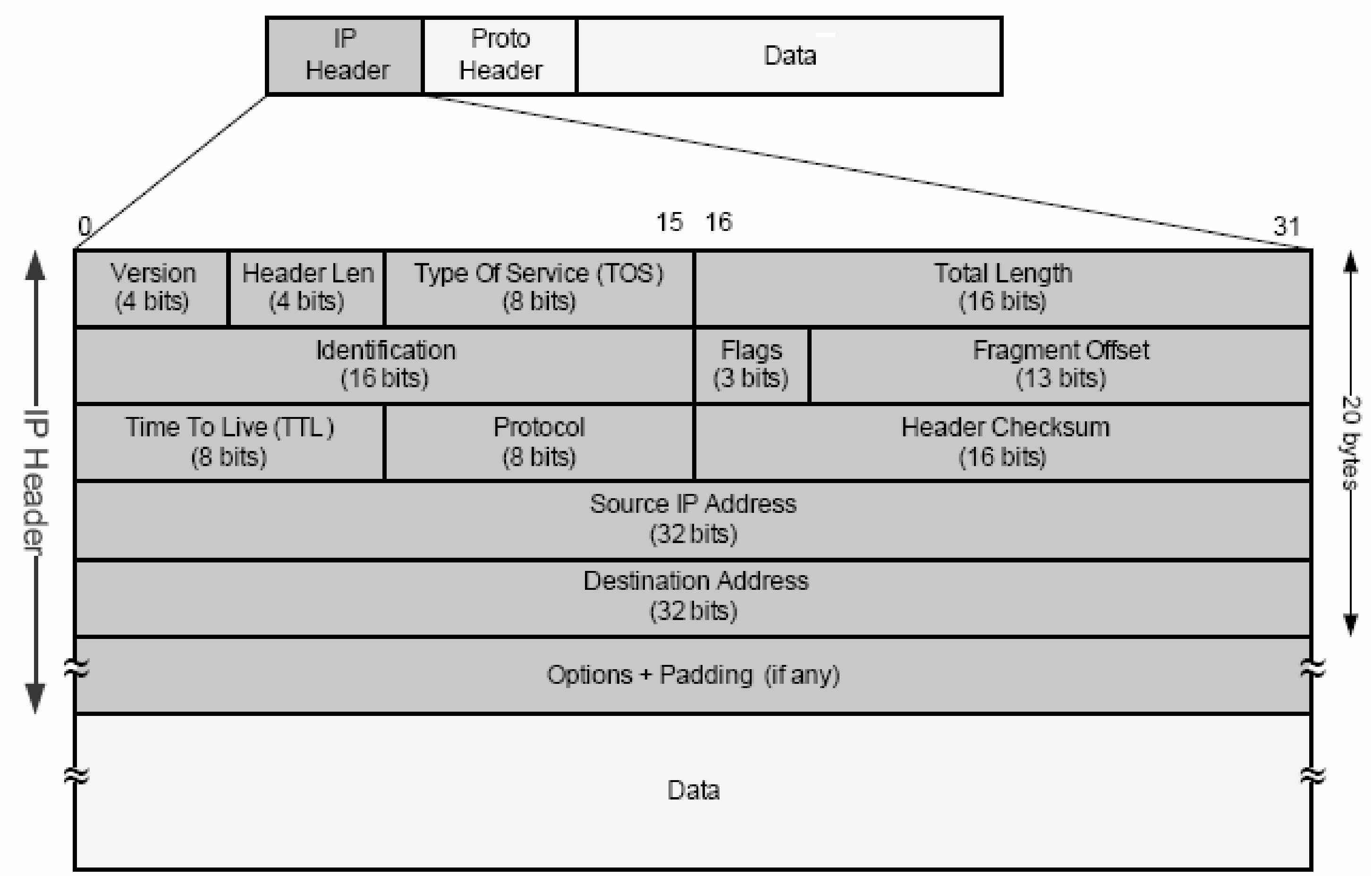
- Allow arbitrary complexity of internetworked LANs within organization
  - By not having one network class for each LAN within the organization
  - Each such LAN is called a subnet
- Such a network with several subnets looks like a single network from the point of view of the rest of internet
- Each subnet is assigned a subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- Subnet mask indicates which bits are network/subnet number and which are host number

פורמט מיוחד של כתובות IP

Prefix (network)	Suffix (host)	Type & Meaning
all zeros	all zeros	this computer (used during bootstrap)
network address	all zeros	identifies network
network address	all ones	broadcast on the specified network
all ones	all ones	broadcast on local network
127	any	loop back (for testing purposes)

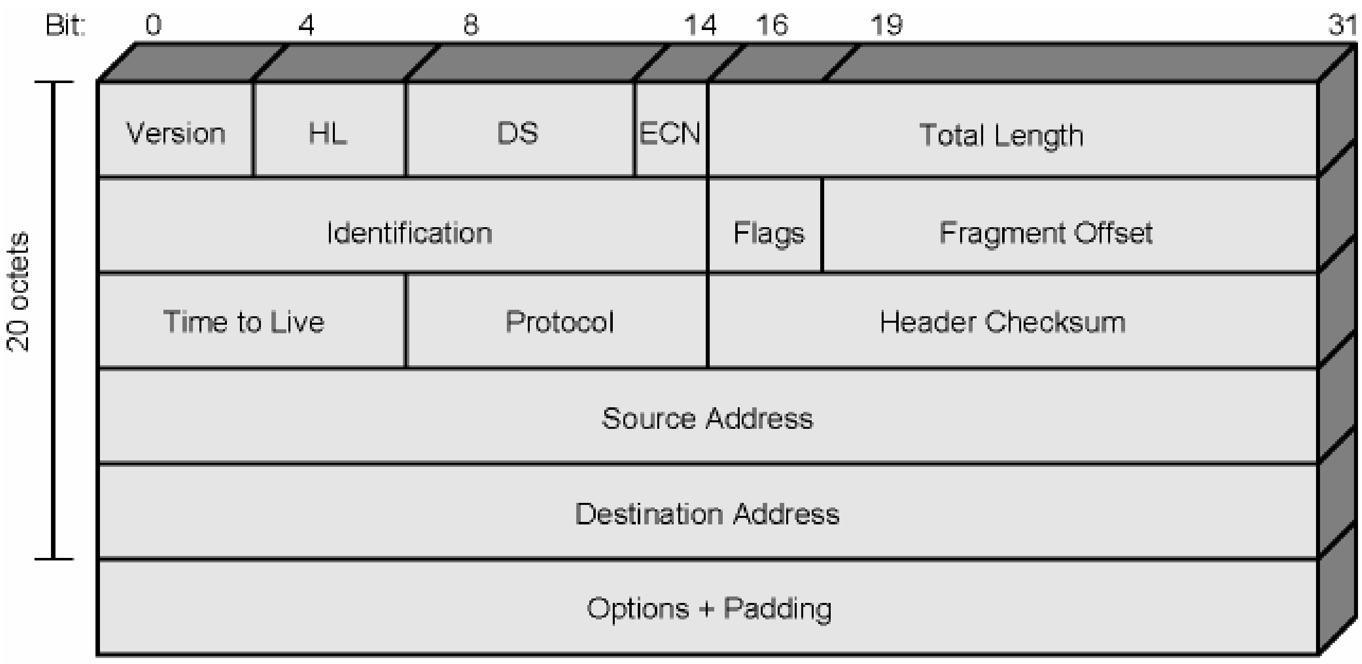
מיבנה ה- IP Header לפי תקן 791

RFC 791 : https://www.ietf.org/rfc/rfc791.txt



מיבנה ה- IP Header לפי תקן 2474

RFC 2474: https://tools.ietf.org/html/rfc2474

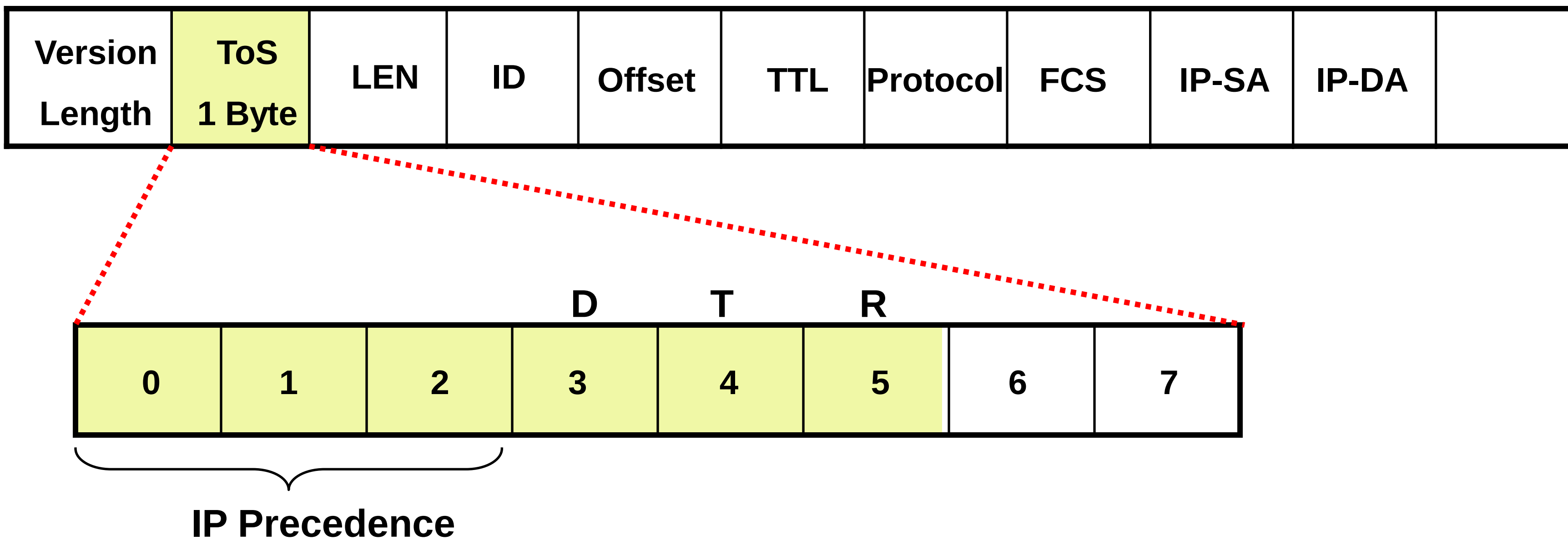


** DS (Differentiated Services) and ECN (Explicit Congestion Notification)

IP Header Fields (1)

- Version
  - IP version 4
- Header length
  - Including options
- Type of Service (RFC 791)
  - Specify treatment of data unit during transmission through networks
- DS (Differentiated Services) and ECN (Explicit Congestion Notification) - RFC 2474
  - previously used for “Type of Service”
  - now used by (interpreted as) DS and ECN
  - DS is for QoS support

Type of Service Indicators



- R - Reliability
  - Normal or high
- D- Delay
  - Normal or low
- T- Throughput
  - Normal or high

IP Header Fields (2)

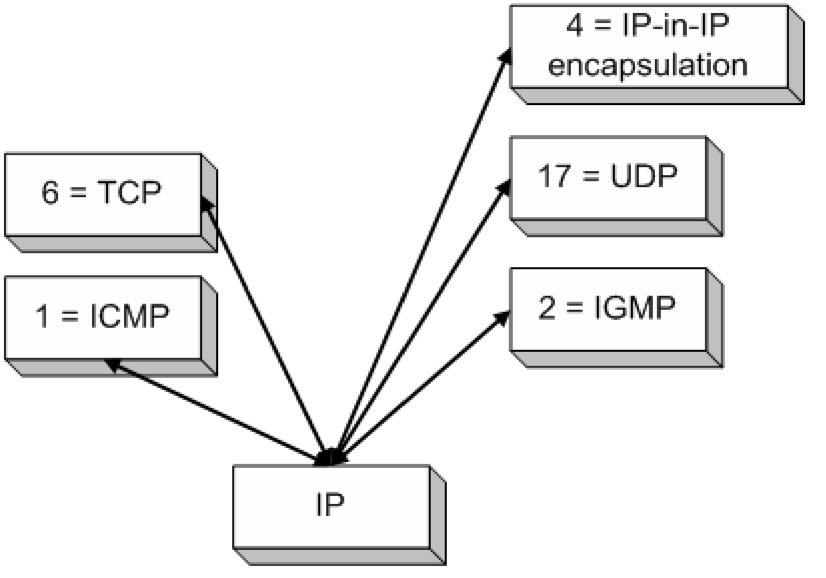
- Total length
  - of datagram (header + data), in octets
- Identification
  - Sequence number
  - Used with addresses and user protocol to identify datagram uniquely
  - Used for Fragmentation and Re-assembly
- Flags (3 bits)
  - First bit always set to 0
  - DF bit (Do not fragment)
  - MF bit (More fragments)

IP Header Fields (3)

- Fragmentation offset

- Time To Live (TTL) (1 byte)
  - Ensure that packet is eventually dropped when a routing loop occurs
  - Used as follows
    - Sender sets the value (e.g., 64)
    - Each router decrements the value by 1
    - When the value reaches 0, the datagram is dropped

- Protocol (1 byte)
    - Specifies the higher-layer protocol



Datagram Lifetime

- Datagrams could loop indefinitely
  - Unnecessary resource consumption
  - Transport protocol needs upper bound on datagram life
- Datagram marked with lifetime
  - Time To Live (TTL) field in IP
  - Once lifetime expires, datagram discarded
  - Hop count
    - Decrement time to live on passing through each router

IP Header Fields (4)

- Header checksum (2 bytes)
  - 16-bit long checksum which is computed for the header of the datagram
  - Verified and recomputed at each router
- Source address
- Destination address
- Options
  - Security restrictions
  - Record Route: each router that processes the packet adds its IP address to the header
  - Timestamp: each router that processes the packet adds its IP address and time to the header

IP Header Fields (5)

- Options (cont.)
    - (loose) Source Routing: specifies a list of routers that must be traversed
    - (strict) Source Routing: specifies a list of the only routers that can be traversed
- Padding
    - Padding bytes are added to ensure that header ends on a 4-byte boundary (32 bits long)
- Data
    - User (upper layer) data
    - any octet length is OK
        - But max length of IP datagram (header plus data) is 65,535 octets

Maximum Transmission Unit

- Maximum size of IP datagram is 65535, but the data link layer protocol generally imposes a limit that is much smaller
  - Ethernet frames have a maximum payload of 1500 bytes → IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes

- The limit on the maximum IP datagram size, imposed by the data link protocol is called **maximum transmission unit (MTU)**

- MTU for various data link protocols:

Ethernet:	1500	FDDI:	4352
802.3:	1492	ATM AAL5:	9180
802.5:	4464	PPP:	negotiated

FDDI - Fiber Distributed Data Interface

Fragmentation and Re-assembly

- Different maximum packet sizes for different networks
  - routers may need to split the datagrams into smaller fragments

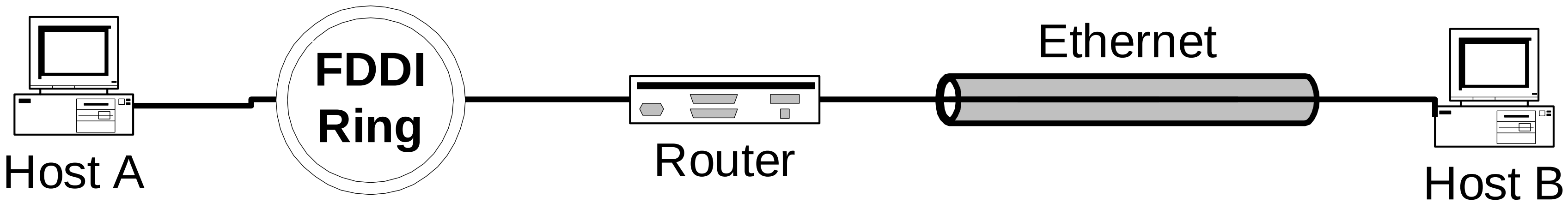
- When to re-assemble
  - At destination
    - Packets get smaller as data travel
      - inefficiency due to headers

  - Intermediate reassembly
    - Need large buffers at routers
    - All fragments must go through same router
      - Inhibits dynamic routing

IP Fragmentation

- What if the size of an IP datagram exceeds the MTU?
- IP datagram is fragmented into smaller units
- What if the route contains networks with different MTUs?

FDDI - Fiber Distributed Data Interface

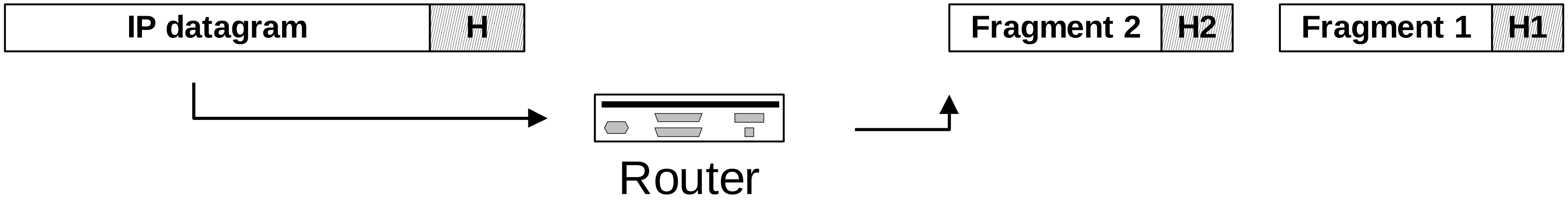


MTUs: FDDI: 4352 Ethernet: 1500

- **Fragmentation**:
  - IP router splits the datagram into several datagram
  - Fragments are reassembled at receiver

Where is Fragmentation done?

- Fragmentation can be done at the sender or at intermediate routers
- The same datagram can be fragmented several times
- Reassembly of original datagram is only done at destination hosts



What's involved in Fragmentation?

version	header length	DS	ECN	total length (in bytes)			
Identification				0	DF	MF	Fragment offset
time-to-live (TTL)		protocol		header checksum			

- Total length: Length of user data in octets (if fragment, length of fragment data) including the header

- Identification: uniquely identify datagram. all fragments that belong to a datagram share the same identifier

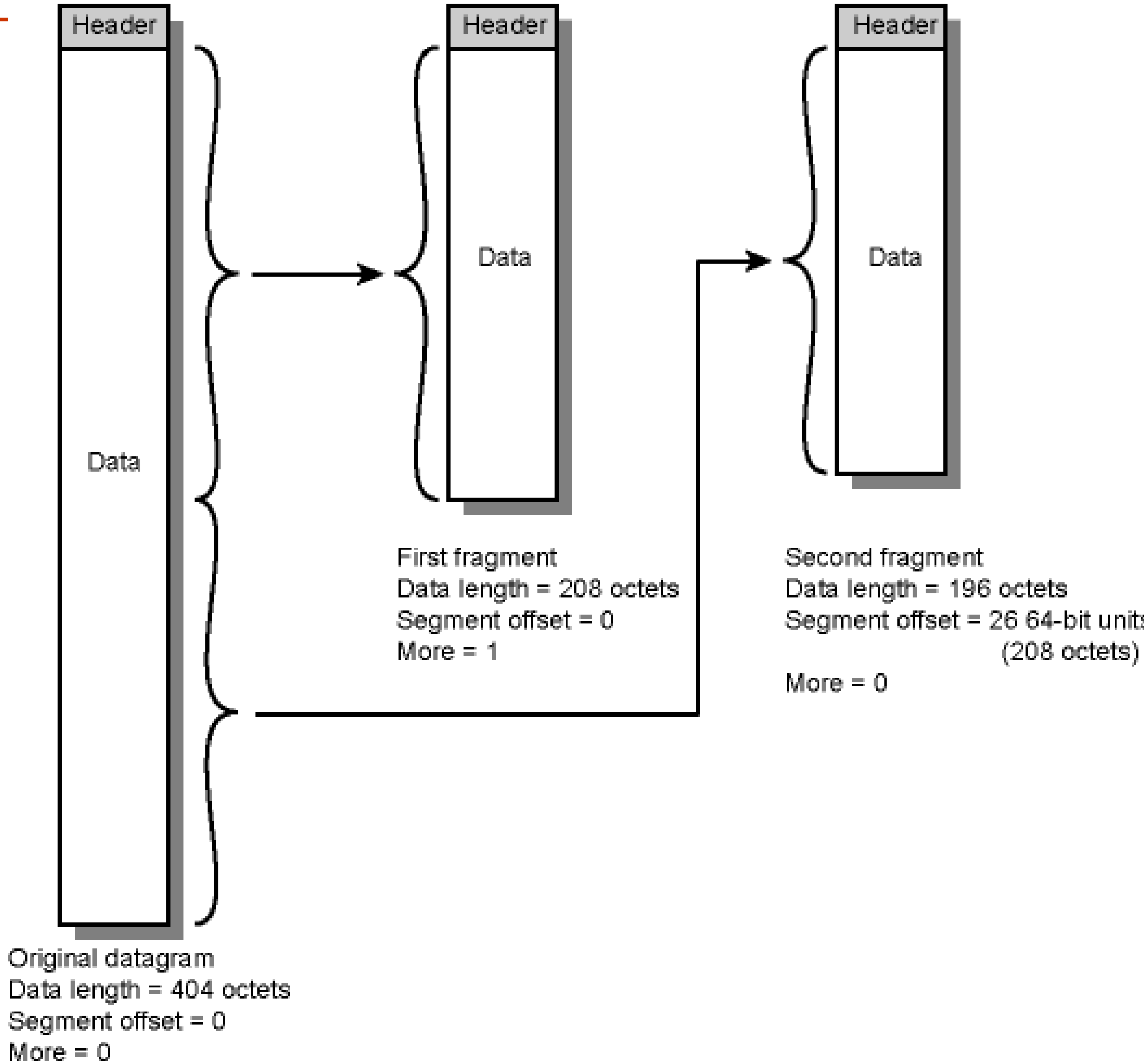
What's involved in Fragmentation?

version	header length	DS	ECN	total length (in bytes)			
Identification				0	DF	MF	Fragment offset
time-to-live (TTL)		protocol		header checksum			

- Flags
  - DF (Do not fragment) bit is set: Datagram cannot be fragmented and must be discarded if MTU is too small
  - MF (More fragments) bit set: This datagram is part of a fragment and an additional fragment follows this one (Indicates that this is not the last fragment)

- Fragment offset
  - Offset of the payload of the current fragment in the original datagram
  - Position of fragment of user data in original datagram In multiples of 64 bits (8 octets)

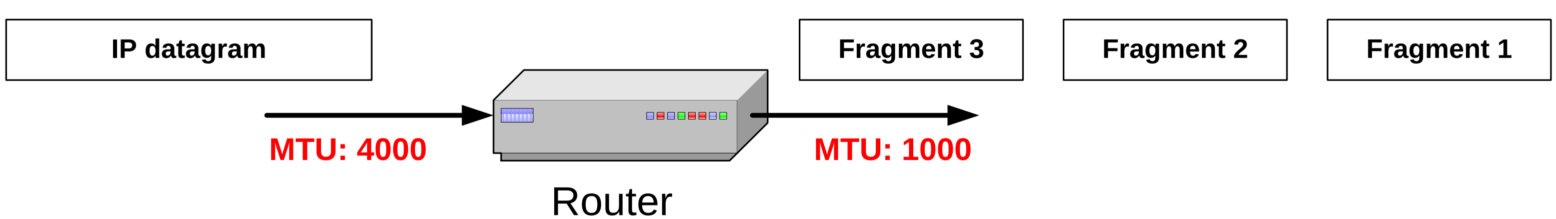
Fragmentation Example (1)



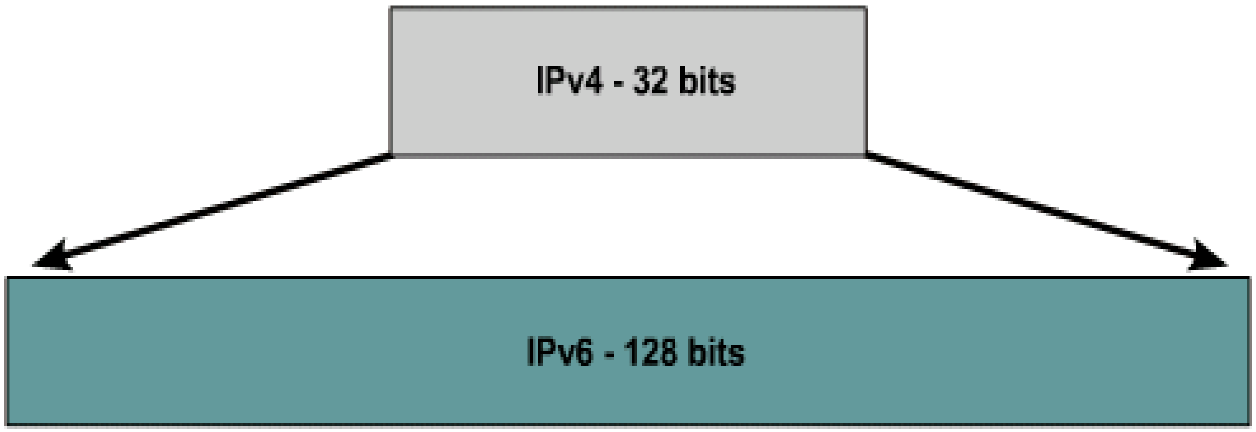
Fragmentation Example (2)

- A datagram with size 2400 bytes must be fragmented according to an MTU limit of 1000 bytes

Header length: 20	Header length: 20	Header length: 20	Header length: 20
Total length: 2400	Total length: 448	Total length: 996	Total length: 996
Identification: 0xa428	Identification: 0xa428	Identification: 0xa428	Identification: 0xa428
DF flag: 0	DF flag: 0	DF flag: 0	DF flag: 0
MF flag: 0	MF flag: 0	MF flag: 1	MF flag: 1
Fragment offset: 0	Fragment offset: 244	Fragment offset: 122	fragment offset: 0



IPv4 to IPv6



IPv4

- 32 bits or 4 bytes long
  - ≅4,200,000,000 possible addressable nodes

IPv6

- 128 bits or 16 bytes: four times the bits of IPv4
  - ≅$3.4 * 10^{38}$ possible addressable nodes
  - ≅340,282,366,920,938,463,374,607,432,768,211,456
  - ≅$5 * 10^{28}$ addresses per person

Major Improvements of IPv6 Header

- **Larger address space**
- **No option field**: Replaced by extension header. Result in a fixed length, 40-byte IP header
- **No header checksum**: Result in fast processing
  - Reduce end-to-end delay
- **No fragmentation at intermediate nodes**: Result in fast IP forwarding
- **Higher level of security**

סיכום

- IP structure
- Routing
- Datagram lifetime
- Fragmentation and re-assembly
- Error control
- Flow control
- Addressing
- IP Fragmentation
- IPV4 versus IPV6