COMPUTER NETWORKS

AY2022-2023 Spring Semester

COMP1047 Systems & Architecture

Ying Weng

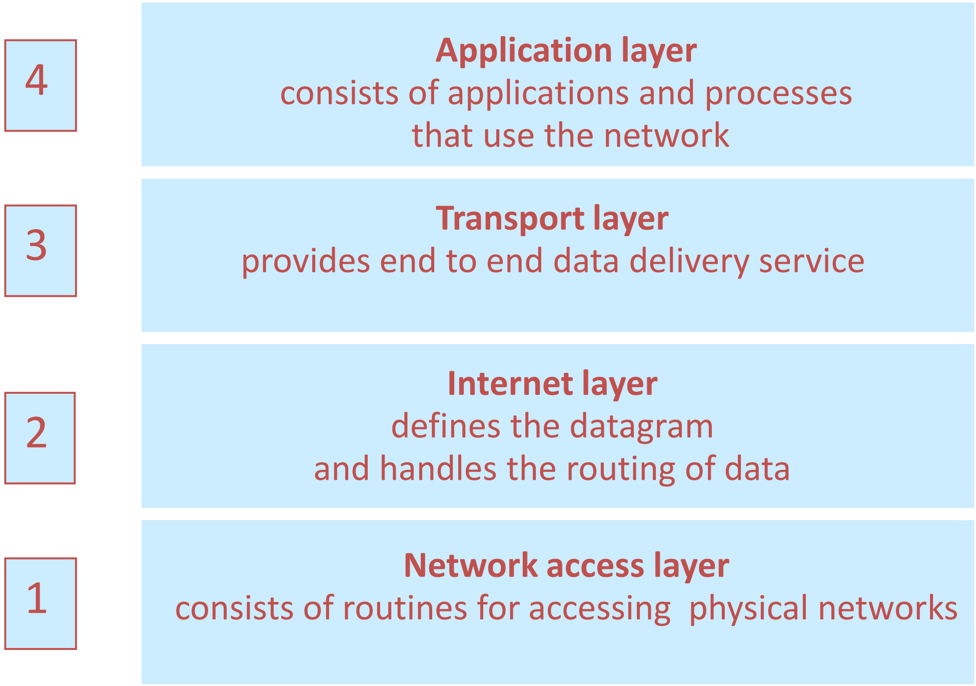
Computer Networks Part-2. TCP/IP Protocols

TCP/IP Protocols

- The best known protocols are the *Transmission Control Protocol (TCP)* and the *Internet Protocol (IP)*
- Not one protocol but a suite of protocols that provide networking capabilities
- Layered type of protocols divide the tasks into modules that may communicate with peer entities in another system
- The operation of the internet is based on a four layer architectural model whose origins go back to research supported by the USA Department of Defence in the late 1960s
- The model is sometimes referred to as the *Department of Defence (DoD) reference model* and now also referred to as the *Internet Reference Model*
- The name is misleading because TCP and IP are *only two* of dozens of protocols that compose the suite. Its name comes from two of the *more important protocols in the suite*, that is, TCP and IP

TCP/IP Reference Model

- The TCP/IP reference model based on four layers and the functionality of each layer is shown below

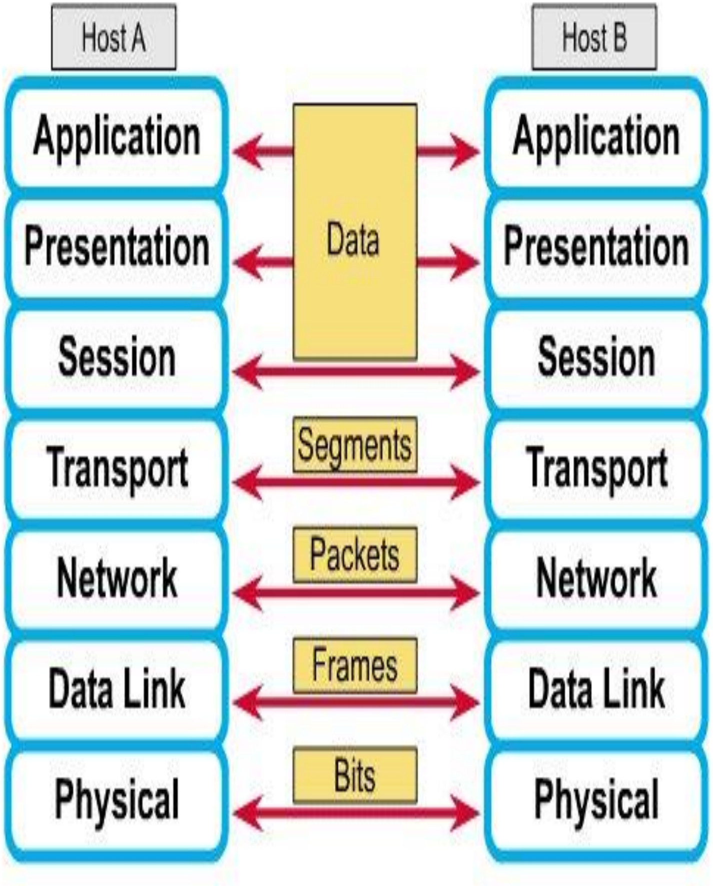


4	**Application layer** consists of applications and processes that use the network
3	**Transport layer** provides end to end data delivery service
2	**Internet layer** defines the datagram and handles the routing of data
1	**Network access layer** consists of routines for accessing physical networks

- In contrast, the OSI model has seven layers
- The IP structure makes possible the optimisation of the operation because there are only four layers to be considered

OSI 7 Layer Model

OSI 7 Layer Model



Each layer has a specific Protocol Data Unit (PDU).

- PDU's are used for peer-to-peer contact between corresponding layers.
- Data are handled by the top three layers,
- Segments by the Transport layer.
- Packets by the Network layer
- Frames by the Data Link layer
- Bits or Symbols by the Physical layer.

The receiving computer reverses the process using the information contained in the PDU.

Functionality of the 7 layers of the OSI Model

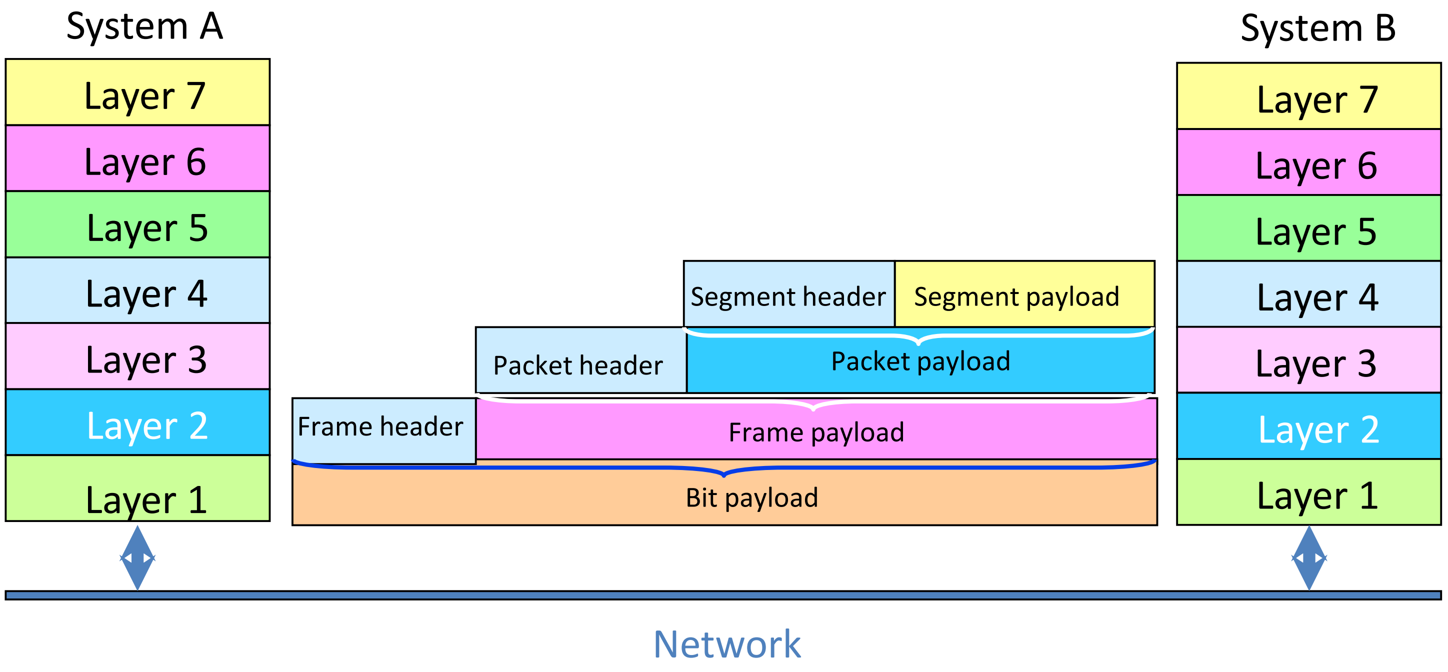
- **The protocols associated with each layer encapsulate**
- **The header**
- **The data of the preceding layer** as if they were data and they append their own header

This Illustrated in the next slide.

- **It should be clear**
  - The independence of the layers
  - The need to communicate between layers through protocols
  - Makes the OSI very robust but also slow and expensive

Functionality of the 7 layers of the OSI Model

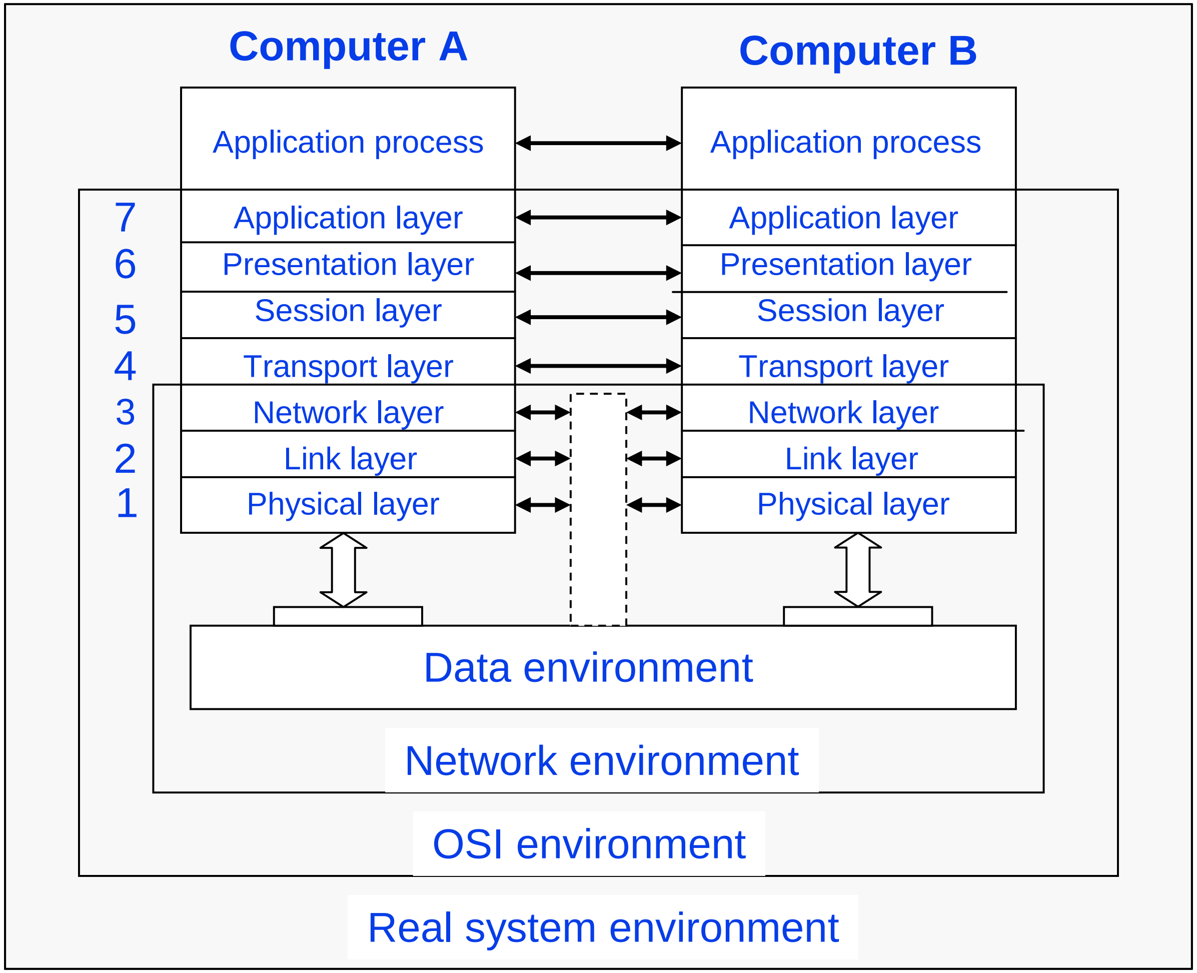
- ❑ **The protocols associated with each layer encapsulate**
  - ➢ **The header**
  - ➢ **The data of the preceding layer** as if they were data and they append their own header



The encapsulation of headers and data during information exchange.

OSI 7 Layer Model

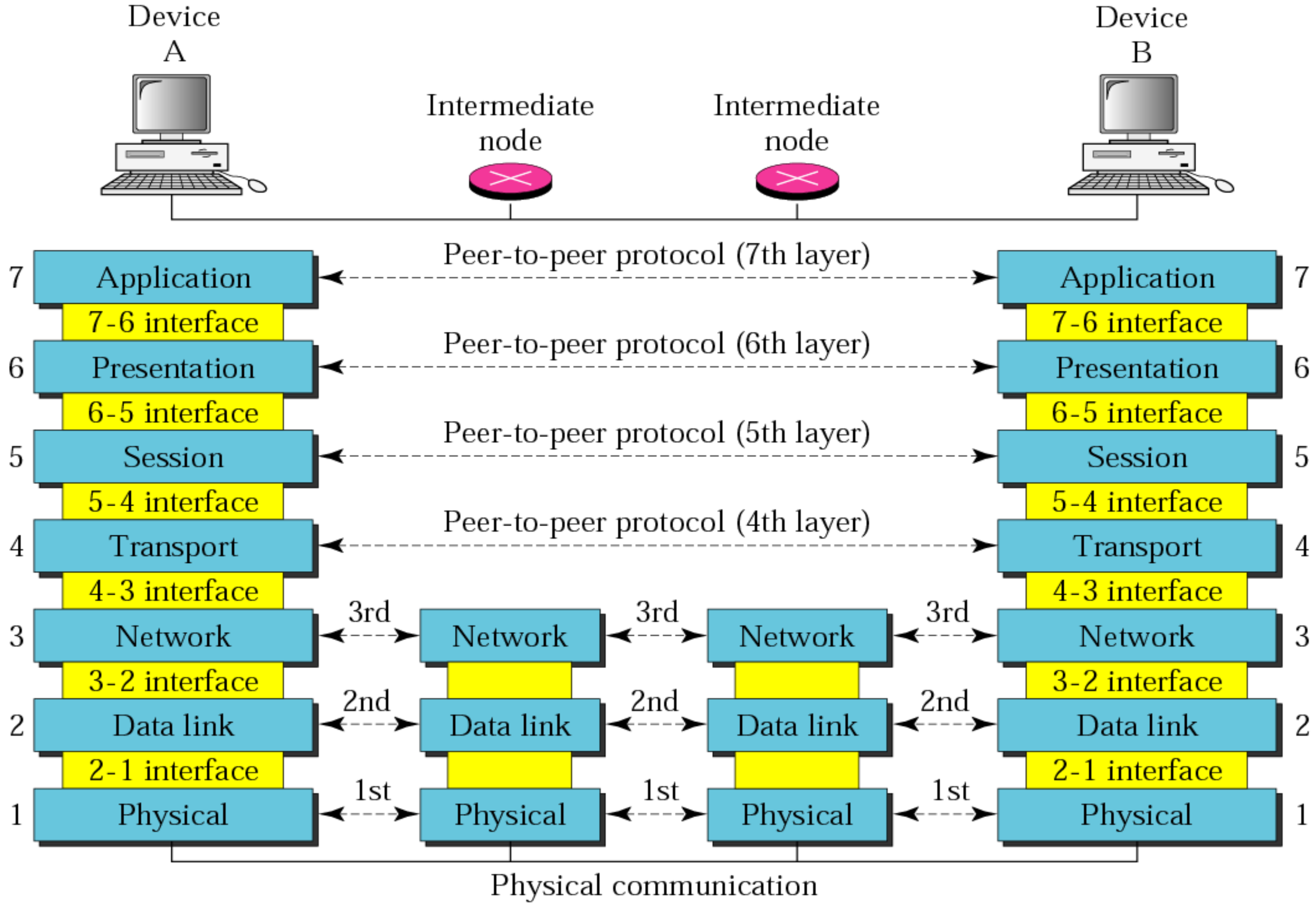
Operational Environments



The logical structure of the OSI reference model showing the Operational Environments.

OSI 7 Layer Model

Intermediate nodes only perform Network environment functions



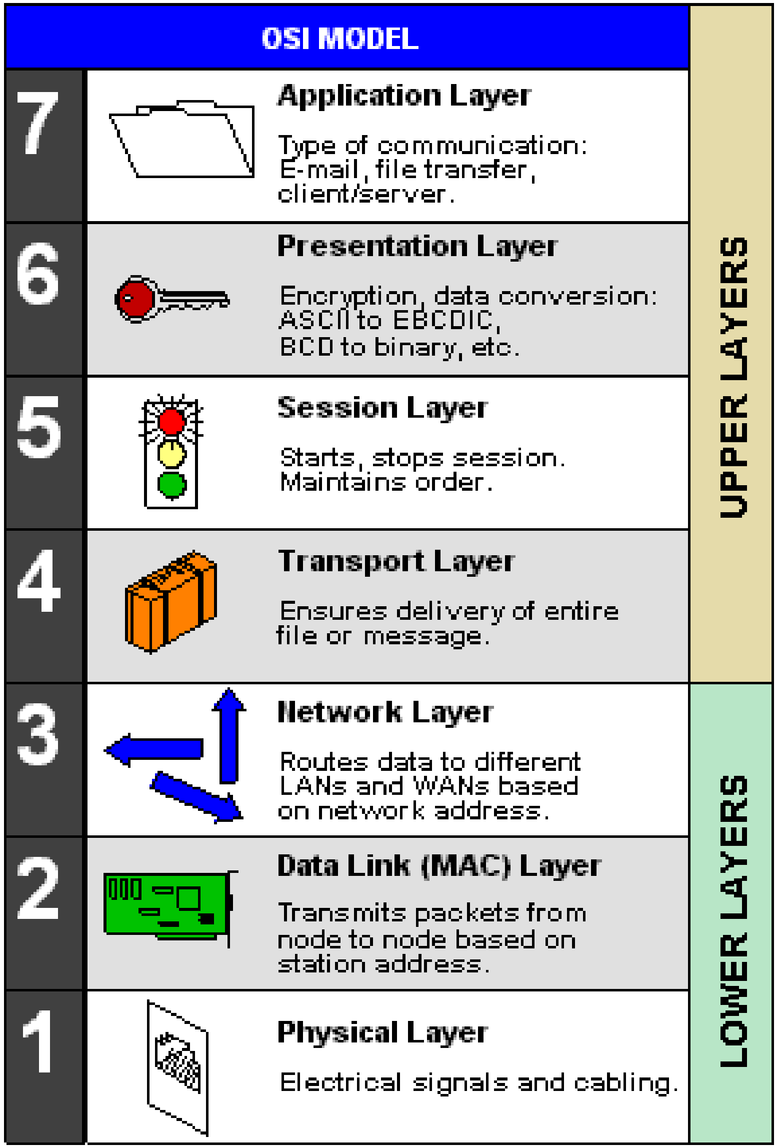
OSI 7 Layer Model

7 - Application	All
6 - Presentation	People
5 - Session	Seem
4 - Transport	To
3 - Network	Need
2 - Data Link	Data
1 - Physical	Processing

1 - Physical	Please
2 - Data Link	Do
3 - Network	Not
4 - Transport	Throw
5 - Session	Sausage
6 - Presentation	Pizza
7 - Application	Away

- Two acronyms on how to remember the seven layers of the OSI reference mode but there others as well !

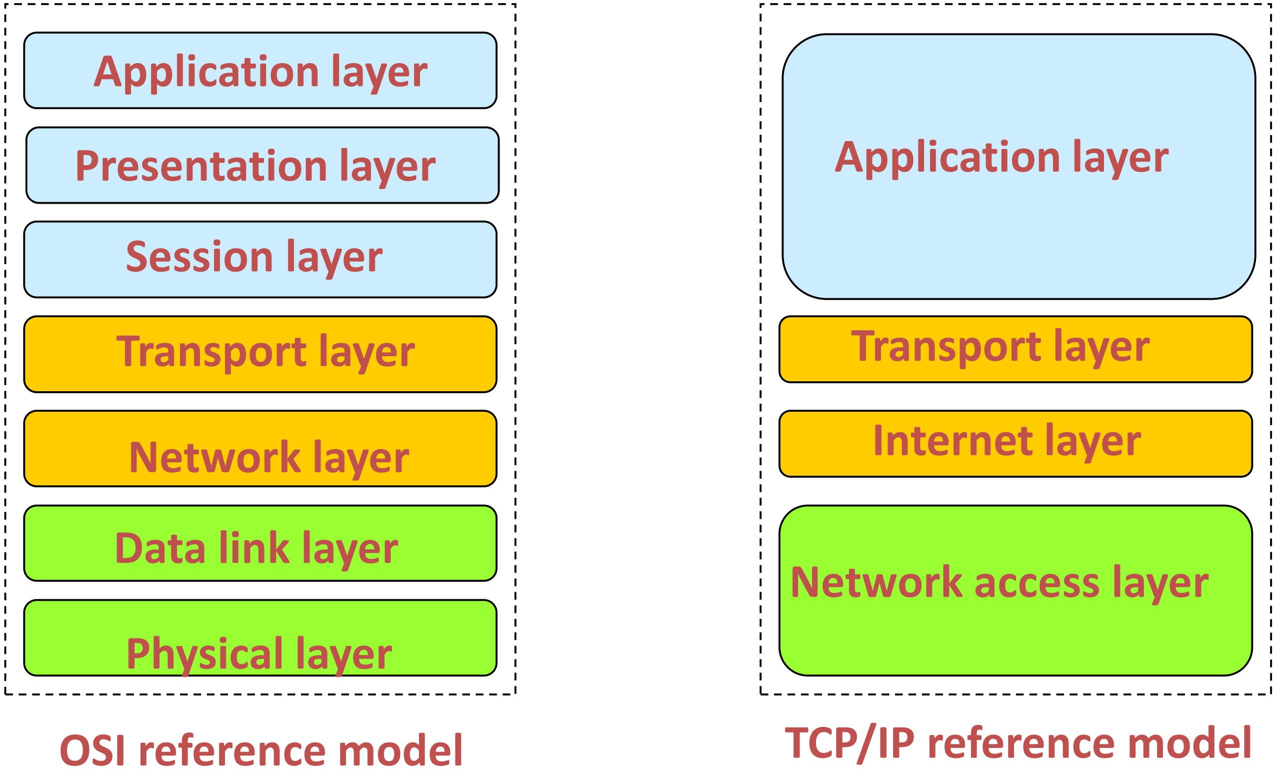
OSI 7 Layer Model



	OSI MODEL	
7	**Application Layer** Type of communication: E-mail, file transfer, client/server.	UPPER LAYERS
6	**Presentation Layer** Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5	**Session Layer** Starts, stops session. Maintains order.	
4	**Transport Layer** Ensures delivery of entire file or message.	
3	**Network Layer** Routes data to different LANs and WANs based on network address.	LOWER LAYERS
2	**Data Link (MAC) Layer** Transmits packets from node to node based on station address.	
1	**Physical Layer** Electrical signals and cabling.	

The OSI reference model in colour!

TCP/IP Reference Model



- The seven-layer OSI reference model vs. the four-layer TCP/IP reference model
- The presentation and session layers of the OSI are not present in the TCP/IP model

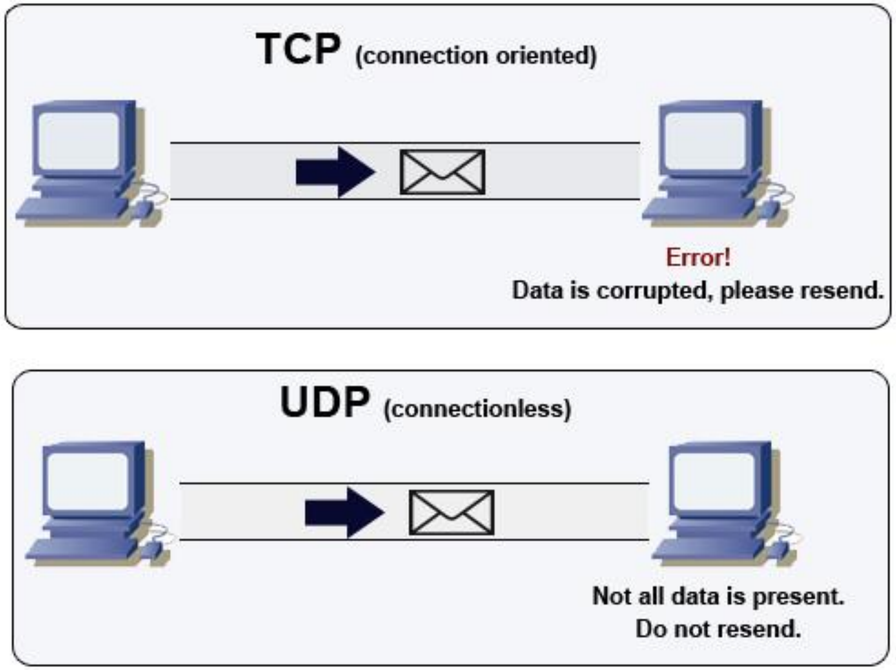
TCP and UDP Protocols

- There are two protocols that are primarily used to transport data: TCP and UDP
- ➢ The TCP/IP provides a user application process with a reliable service known as *Transmission Control Protocol (TCP/IP)*
- ➢ In order to exploit the simplicity, the TCP/IP also provides a connectionless transport protocol known as *User Datagram Protocol (UDP)*

- ❖ TCP is the more common of the two, since it allows for much more error checking functionality and stability
- ❖ UDP lacks extensive error checking but is considered to be much faster than TCP as a result

TCP and UDP Protocols

- Since *TCP guarantees the delivery of data over a network* we call it a *connection – oriented protocol*. If in the event that data isn't sent correctly, the sending computer will be notified and will resend the information
- This is compared to *UDP, which doesn't require that data has been received correctly*. Likewise, we call UDP a *connectionless protocol*



TCP and UDP Protocols

Many common applications use TCP because:

[1] Convenient

[2] TCP handles reliable delivery

[3] Retransmissions of lost packets, re-ordering, flow control etc.

Overall – Reliable service

❖ Examples

➢ Web: HTTP(Hyper Text Transfer Protocol)

➢ e-mail: SMTP (Simple Mail Transfer Protocol), IMAP(Internet Message Access Protocol)

TCP and UDP Protocols

UDP may be used if:

[1] Delays introduced by acknowledgements are unacceptable

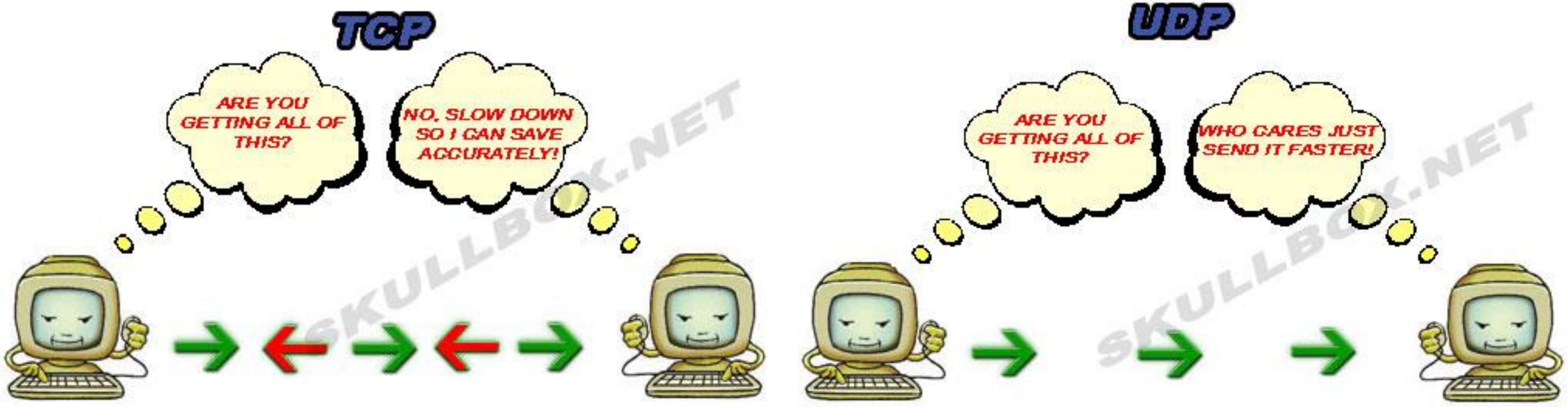
[2] TCP congestion avoidance and flow control measures are unsuitable for your application

[3] Highly delay/jitter sensitive applications

Overall – Best efforts service

- Examples:
- Various types of streaming media: audio-video conference

TCP and UDP Protocols


TCP
ARE YOU GETTING ALL OF THIS?
NO, SLOW DOWN SO I CAN SAVE ACCURATELY!
UDP
ARE YOU GETTING ALL OF THIS?
WHO CARES JUST SEND IT FASTER!
SKULLBOX.NET
SKULLBOX.NET

- TCP vs. UDP: the essence of the two protocols

TCP Protocol – Connection Management

- The objective of connection management is to provide higher layers with the illusion of an end-to-end connection especially in connectionless packet networks
- To achieve this objective two functions are required

  [1] Connection set-up

  [2] Connection tear-down

TCP Protocol – Connection Management

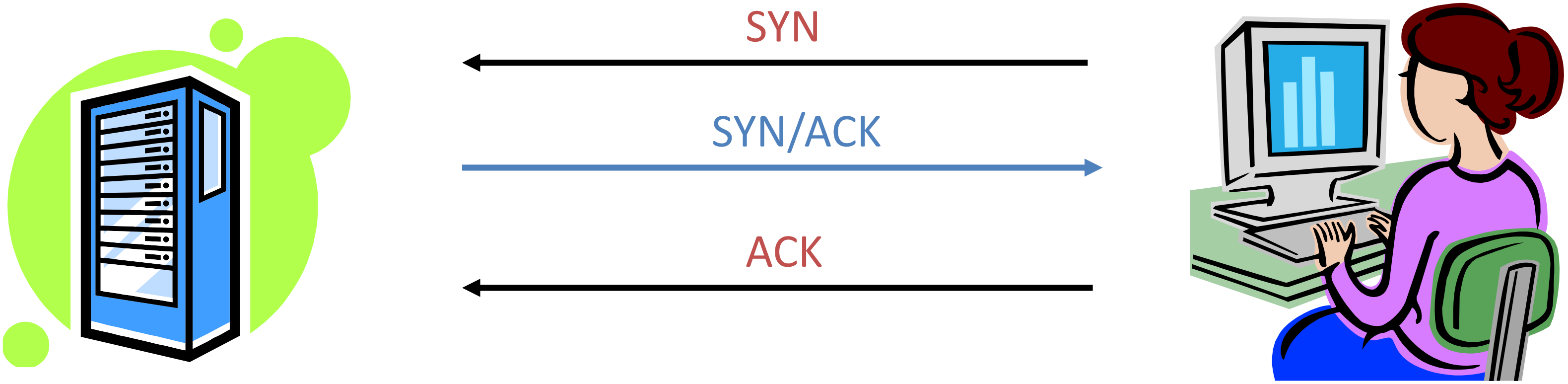
[1] The connection set –up is a three-way handshake

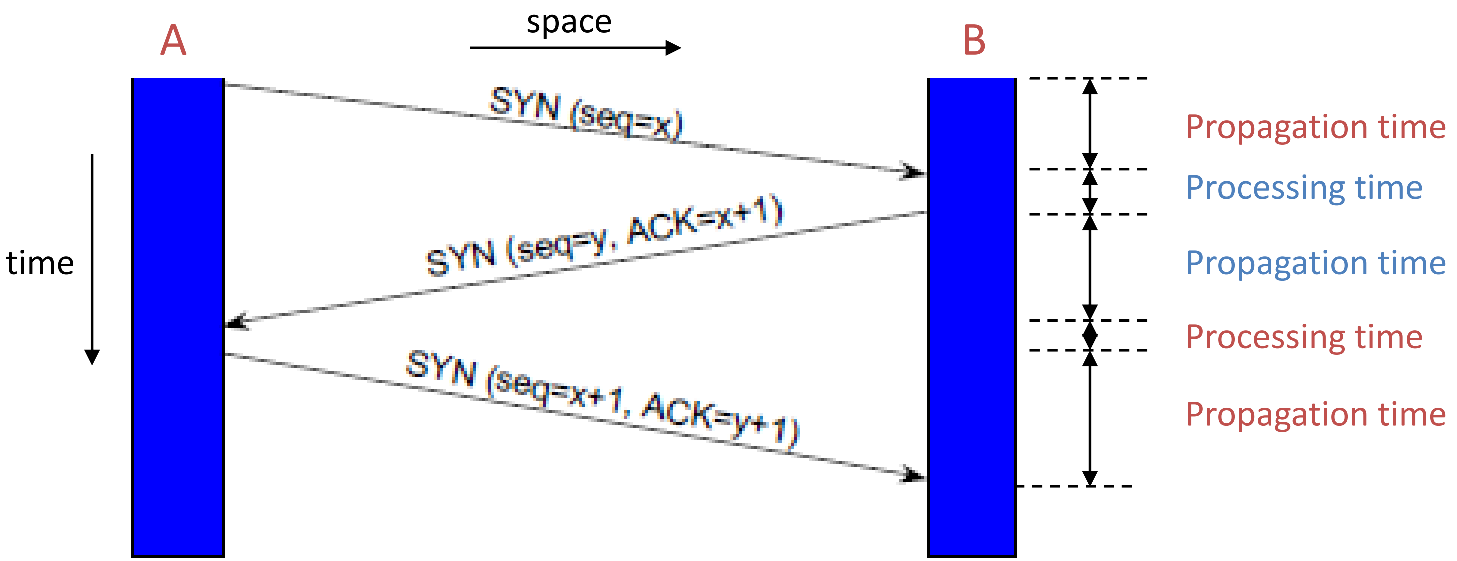
- The sending computer sends a SYN (new connection) packet to the receiving computer; the phone rings!
- The receiving computer responds with a SYN-ACK (acknowledging a connection); hello?
- The sending computer responds with an ACK; Hi!

❖ The connection is now established

- SYN: Synchronize
- ACK: Acknowledge

TCP Protocol – Connection Management





The setting up of a connection in TCP.

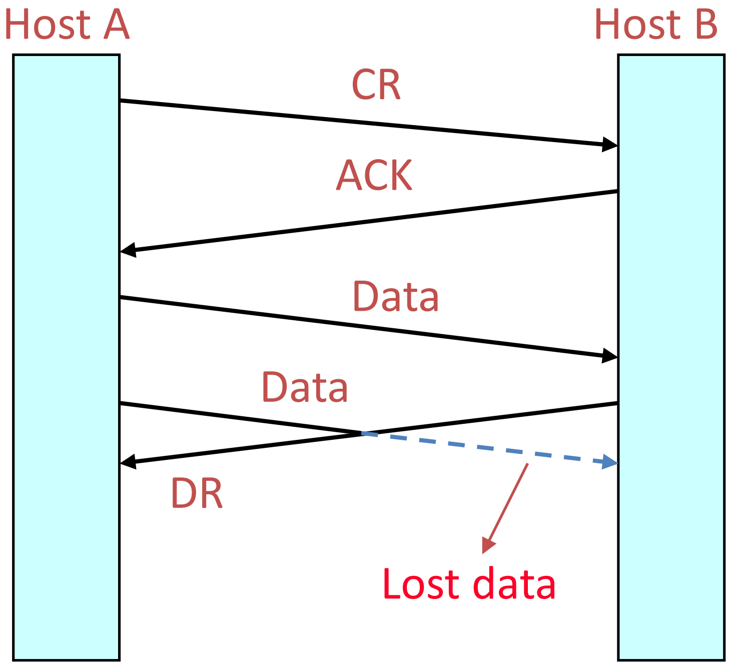
seq: sequence

TCP Protocol – Connection Management

[2] Connection tear-down has two types

(a) Asymmetric release

- Either end may terminate the connection
- Data and requests may be lost and some solutions are available



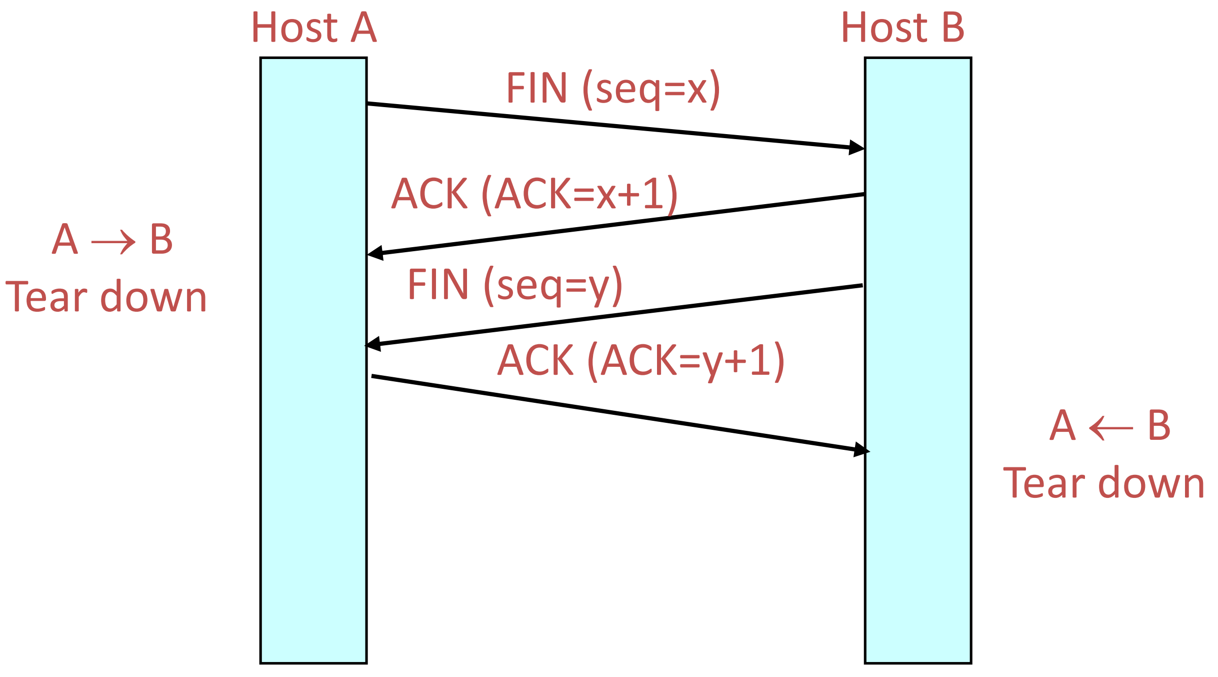
CR: Connection Request

DR: Disconnection Request

TCP Protocol – Connection Management

(b) Symmetric release

- Both ends keep a unidirectional connection to the other
- For each connection the source tears it down when no more data will be sent



FIN: Finish

Two double handshakes.

TCP Protocol – Retransmission

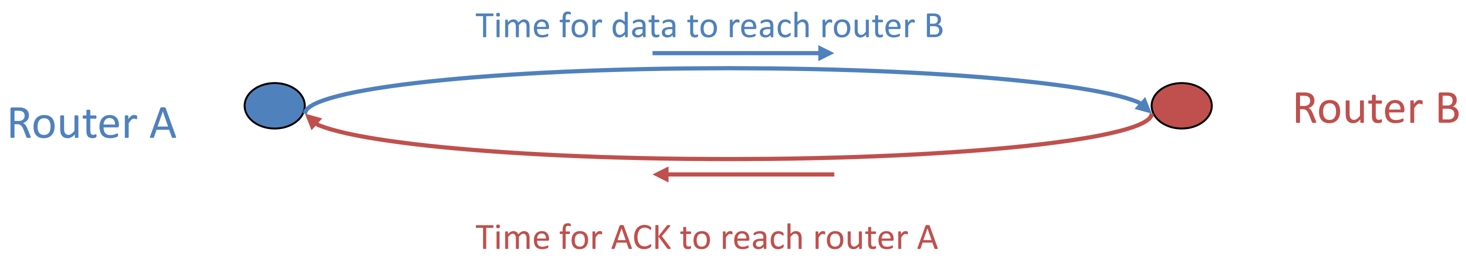
- The objective is good transmission of data
- The basic techniques for reliable transmission in the context of a packet network

[1] Use sequence numbers to identify each data packet and establish the correspondence between the data packet and its reply

[2] Retransmit the same data packet if its reply is not received within a pre-determined time called retransmission time–out (RTO)

TCP Protocol – Retransmission

- When a packet remains unacknowledged for a period of time, TCP assumes it is lost and retransmits it
- In order to minimise the use of the channel for retransmission, TCP must calculate the time of waiting before retransmission
- To achieve this objective, TCP tries to calculate the round trip time (RTT) for a packet and its acknowledgement
- Using the calculated RTT, TCP can estimate the waiting time before timing out the expected acknowledgement, and retransmits the frame
- The geometry of the problem is shown below


Time for data to reach router B
Router A
Router B
Time for ACK to reach router A

RTT $_{\text{minimum}}$ = time for packet to reach B + time for ACK to reach A

TCP Protocol – Performance

- ❑ Network performance depends on the nature of an application
- ❑ A good understanding of the requirements of the application
  - ➢ high throughput
  - ➢ low latency
  - ➢ low jitter

[1] File Transfer

- Needs high throughput
- Intolerant of packet loss
- May be more tolerant of delay

[2] Interactive Video Conferencing application

- Tolerant of some loss
- More intolerant of delay and jitter

TCP Protocol – Performance

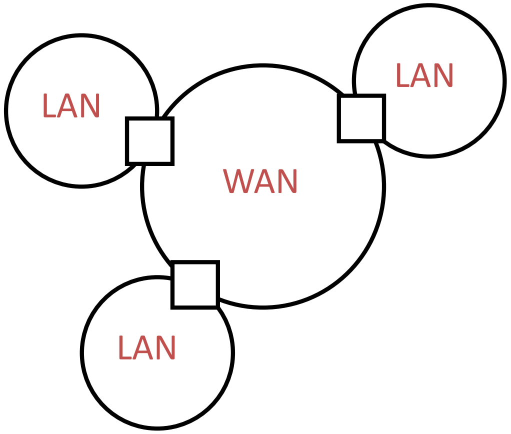
- Quality of Service (QoS) is very important in selecting the channel characteristics of the link
- A method of allocating network resources so that

[a] A mechanism exists to offer varying degrees of service to varying classes of traffic

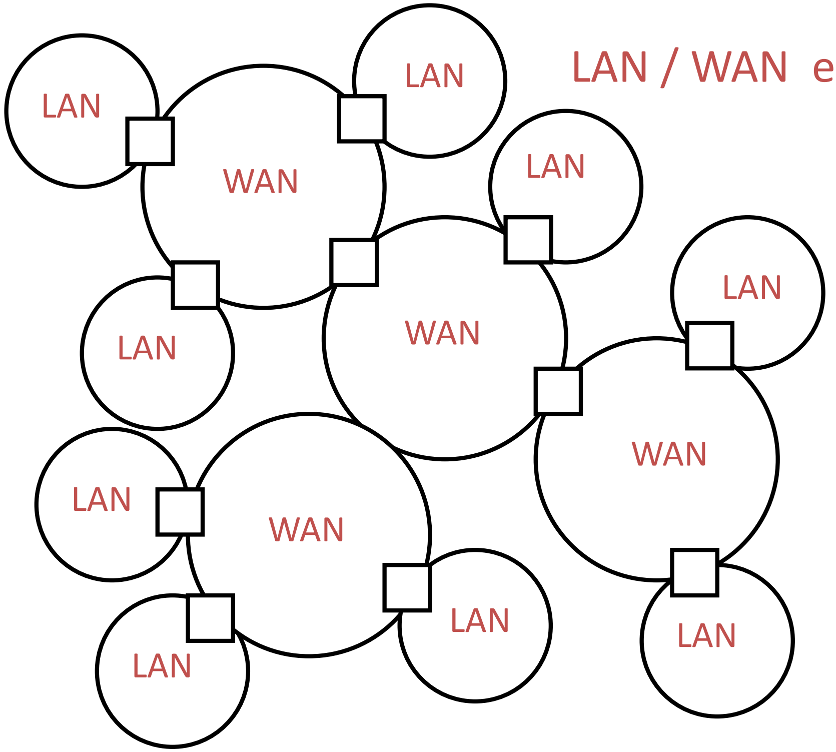
[b] The features of the service are used: delay, jitter, proportion of link bandwidth etc.

Internet Protocol (IP)

- For an internet user the system can provide a defined network service that enables it to communicate with similar users in other systems
- This implies ability to communicate through a number of networks range from LANs to WANs



Single WAN with LANs



LAN / WAN example

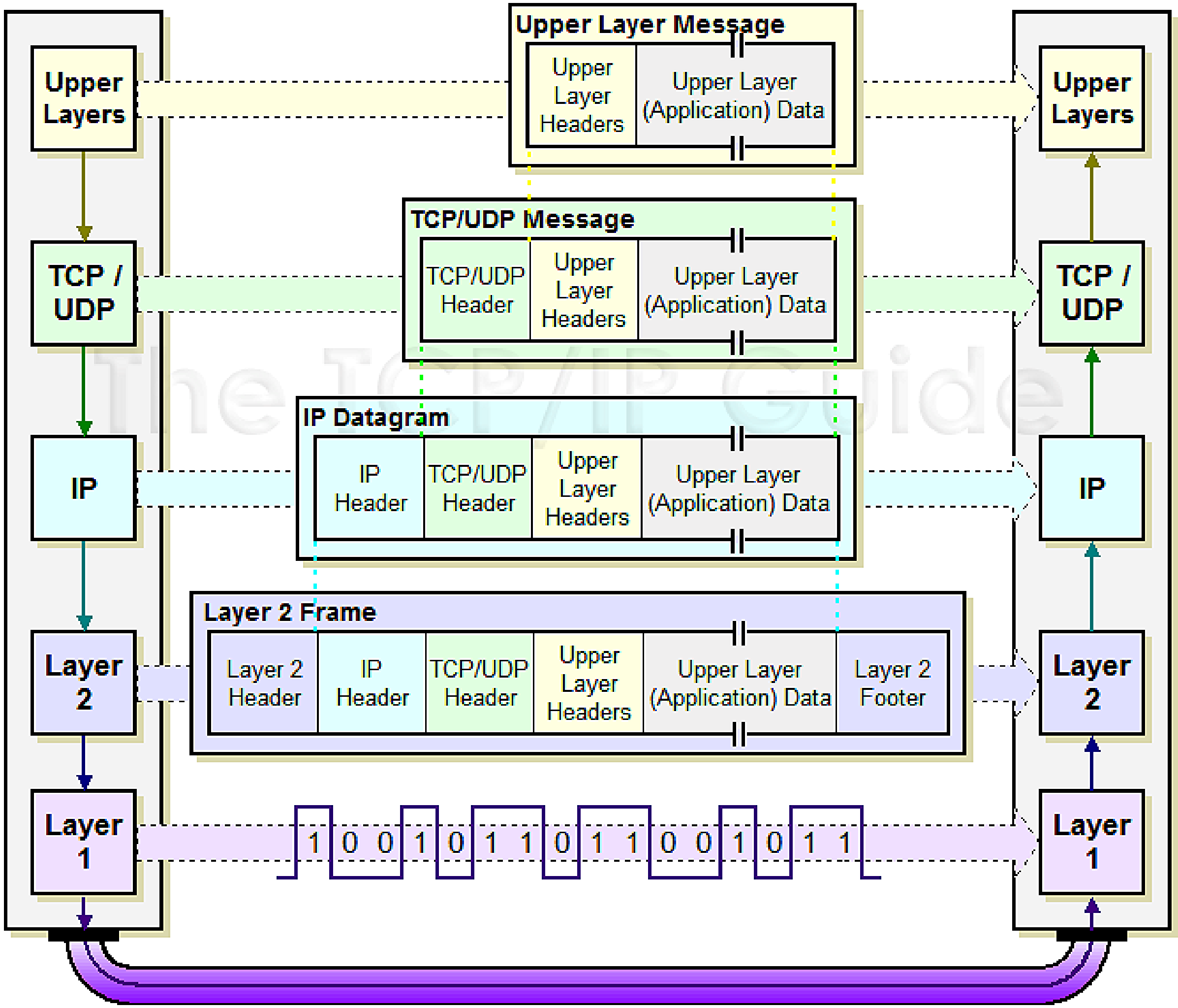
□ Intermediate system / gateway

Encapsulation

- One of the most important concepts in the interaction between protocols is that of encapsulation.
- *Protocol data unit* (PDU) is used for peer-to-peer contact between corresponding layers.
- In order for a protocol to communicate, it must pass down its PDU to the next lower layer for transmission.
- At any particular layer N, a PDU is a complete message that implements the protocol at that layer.
- However, when this “layer N PDU” is passed down to layer N -1, it becomes the ***data*** that the layer N -1 protocol is supposed to ***service***.
- Thus, the layer N PDU is called the layer N -1 *service data unit (SDU)*.
- The job of layer N -1 is to transport this SDU, which it does in turn by placing the layer N SDU into its own PDU format, preceding the SDU with its own headers and appending footers as necessary.
- This process is called *encapsulation*, because the entire content of the higher-layer message is encapsulated as the data payload of the message at the lower layer.

Encapsulation

Encapsulation operation as applied to IP.



Internet Protocol (IP)

❑ In order to achieve this objective, the protocols should provide:

[1] Network services

[2] Addressing

[3] Routing

[4] Quality of service

[5] Maximum packet size

[6] Flow and congestion control

[7] Error reporting

❖ Information on these aspects of the protocols ensures

- There is control over the transmission and reception of data
- The position of the IP layer in relation to the higher and lower layers

IP Address

- An **IP address** is a unique identifier for a node or host connection on a network
- If you wish to talk to another computer on the Internet, you must both have an IP address

IPv4 Address

- **32 bit binary number** is usually represented as 4 decimal values, **each representing 8 bits**, in the range 0 to 255 (known as octets) separated by decimal points
- known as "dotted decimal" notation

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Structure of an IP Address

- Addresses are either statically assigned, or dynamically via a DHCP (Dynamic Host Configuration Protocol) server

- Every IP address consists of two parts
  - One identifying the **network: N** = **Network**
  - One identifying the **node: n** = **node**

IPv4 Network Classes

- **Subnet mask**
- Is used to divide the IP address into the network address and the node address

Example

- Change the following IP address from dotted decimal notation to binary notation

114.34.2.8

01110010 00100010 00000010 00001000

IPv4 Network Classes

- The **class** of the address and the **subnet mask** determines which part belongs to the **network address** or the **node address**
- There are 5 different address classes A – E
- Class A

  NNNNNNNN.nnnnnnnn.nnnnnnnn.nnnnnnnn
- Class B

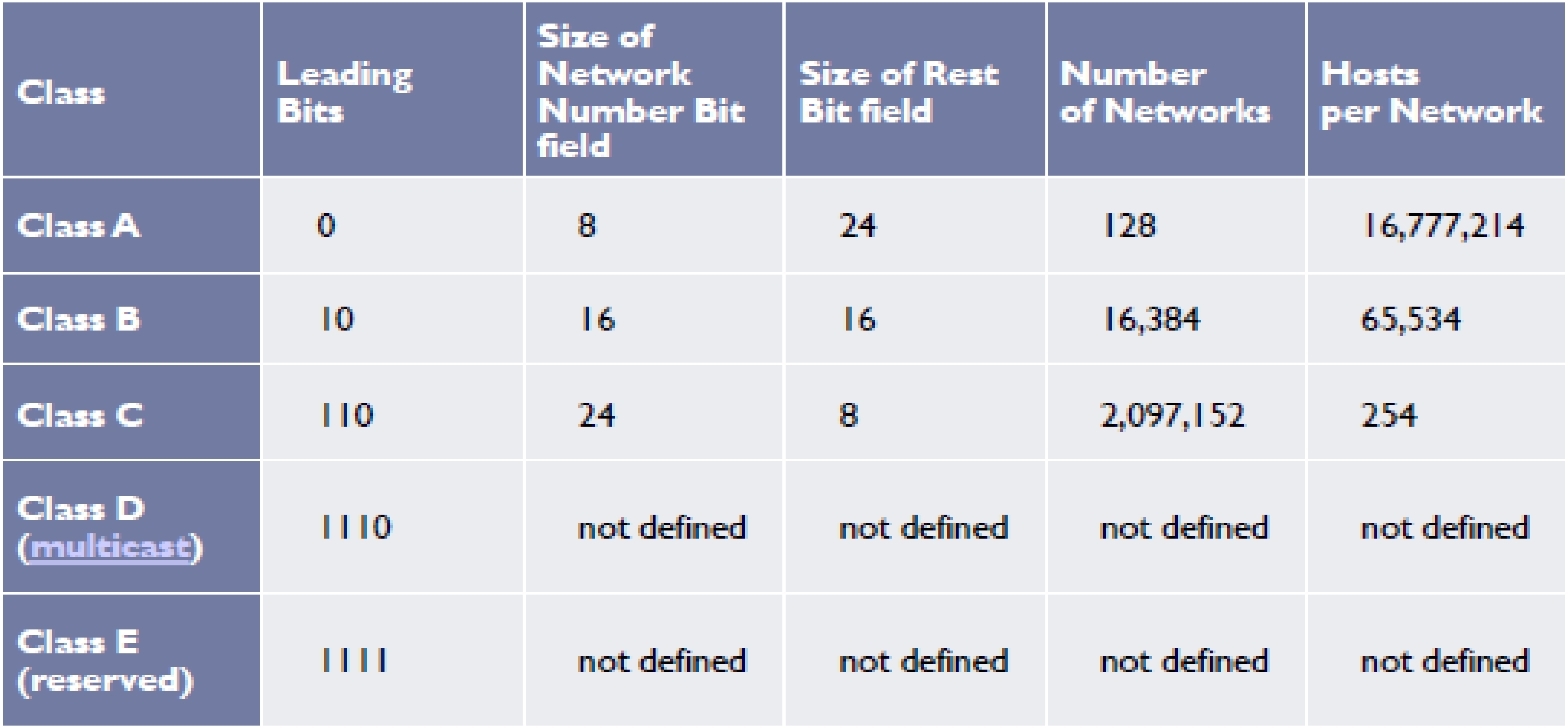
  NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnnn
- Class C

  NNNNNNNN.NNNNNNNN.NNNNNNNN.nnnnnnnn
- Class D – multicast

  1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Class E – reserved for alternative projects and testing

  1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

IPv4 Network Classes



Class	Leading Bits	Size of Network Number Bit field	Size of Rest Bit field	Number of Networks	Hosts per Network
Class A	0	8	24	128	16,777,214
Class B	10	16	16	16,384	65,534
Class C	110	24	8	2,097,152	254
Class D (multicast)	1110	not defined	not defined	not defined	not defined
Class E (reserved)	1111	not defined	not defined	not defined	not defined

IPv4 Network Classes

- You can determine which class any IP address belongs to by examining the ***first 4 bits*** of the binary IP address
- Class A addresses begin with **0xxxxxxx.** (**1 to 126** decimal)
- Class B addresses begin with **10xxxxxx.** (**128 to 191**decimal
- Class C addresses begin with **110xxxxx.** (**192 to 223** decimal)
- Class D addresses begin with **1110xxxx**. (**224 to 239** decimal)
- Class E addresses begin with **1111xxxx**. (**240 to 254** decimal)

Reserved IPv4 Ranges

- IP addresses reserved for private use
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
  - 169.254.0.0 to 169.254.255.255
- **127.0.0.1** is reserved for **localhost (loopback adapter)**
- Any IPs in this range will be dropped by any internet routers

Question

- Can you Find the class of the following binary IP address and convert to dotted decimal format?

11110111 11110011 10000111 11011101

Packets

- The message is divided into a number of packets of reduced length
- Each packet has a header (control information) and the payload that now carries only a fragment of the message

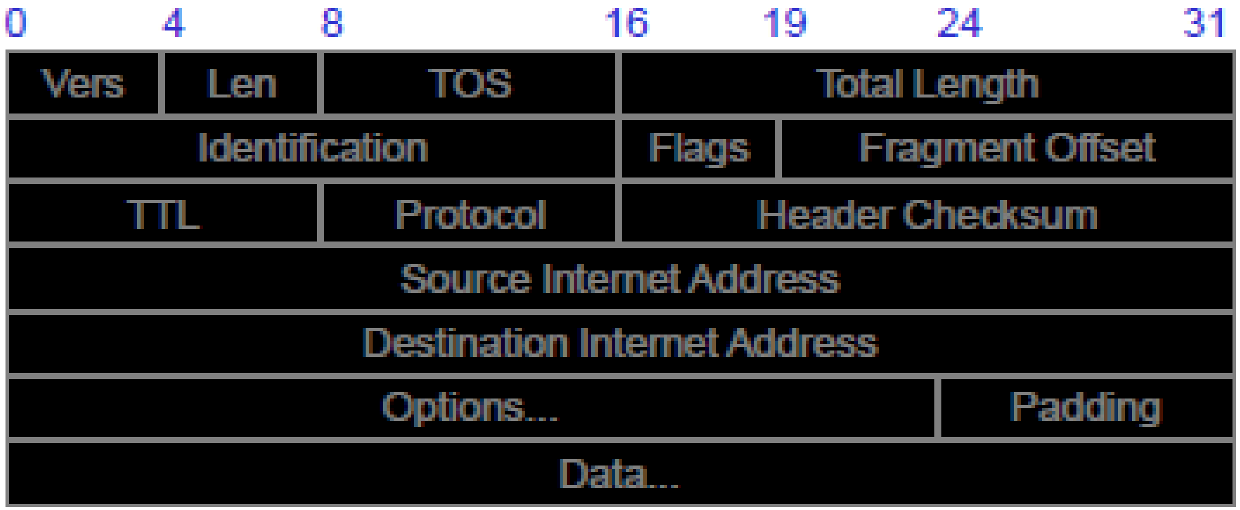
IP Packets

- Source and destination addresses
- Protocol number
  - 1 = ICMP (Internet Control Message Protocol)
  - 6 = TCP (Transmission Control Protocol)
  - 17 = UDP (User Datagram Protocol)
- Various options

  e.g. to control fragmentation
- Time to live (TTL)

  Prevent routing loops

IP Datagram

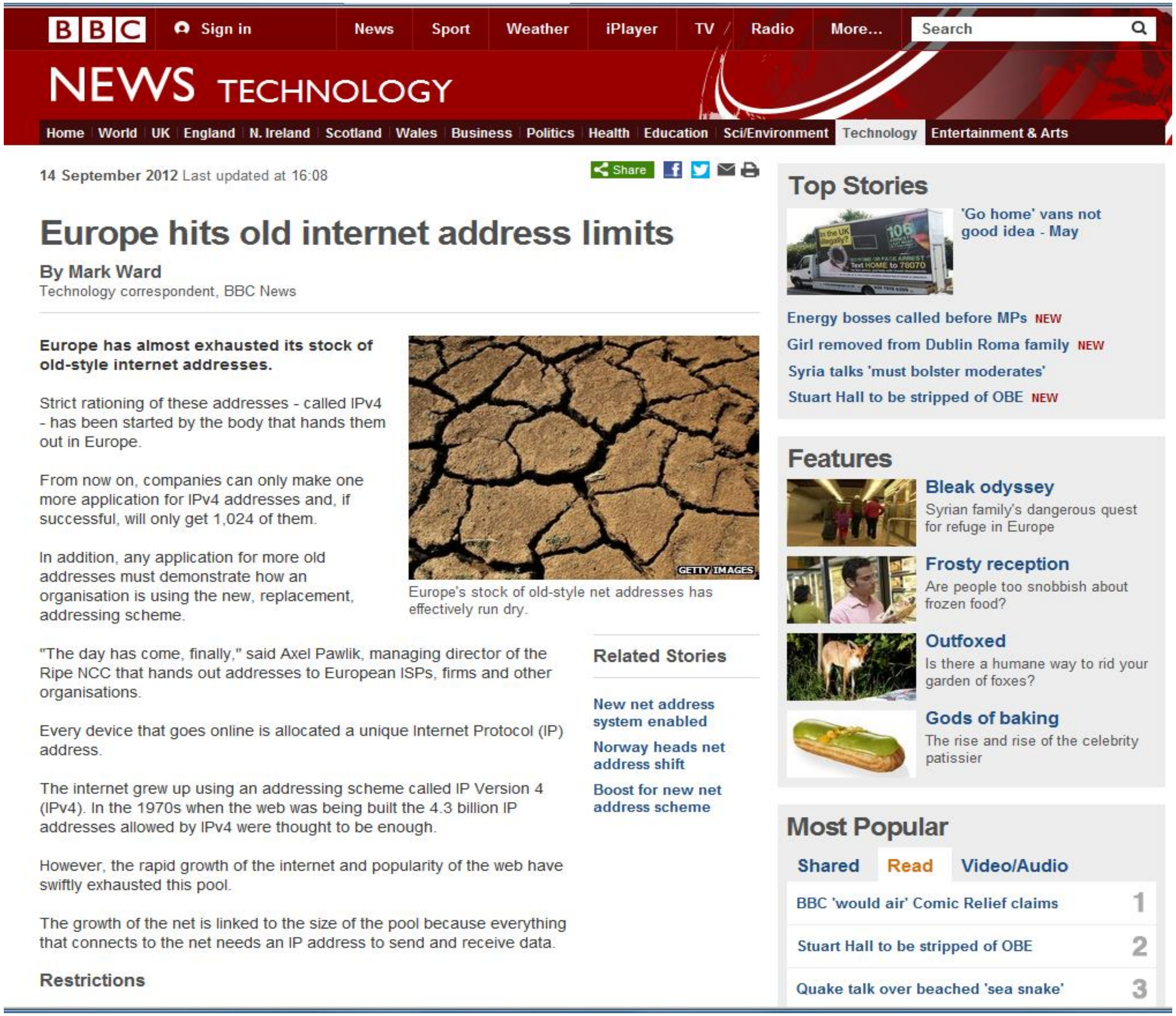


<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>19</td><td>24</td><td>31</td></tr>
<tr><td>Vers</td><td>Len</td><td>TOS</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="3">Fragment Offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="7">Source Internet Address</td></tr>
<tr><td colspan="7">Destination Internet Address</td></tr>
<tr><td colspan="5">Options...</td><td colspan="2">Padding</td></tr>
<tr><td colspan="7">Data...</td></tr>
</table>

Field	Purpose
Vers	IP version number
Len	Length of IP header (4 octet units)
TOS	Type of Service
T. Length	Length of entire datagram (octets)
Ident.	IP datagram ID (for frag/reassembly)
Flags	Don't/More fragments
Frag Off	Fragment Offset

Field	Purpose
TTL	Time To Live - Max # of hops
Protocol	Higher level protocol (1=ICMP, 6=TCP, 17=UDP)
Checksum	Checksum for the IP header
Source IA	Originator's Internet Address
Dest. IA	Final Destination Internet Address
Options	Source route, time stamp, etc.
Data...	Higher level protocol data

Europe hits old internet address limits



14 September 2012 Last updated at 16:08

Europe hits old internet address limits

By Mark Ward
Technology correspondent, BBC News

Europe has almost exhausted its stock of old-style internet addresses.

Strict rationing of these addresses - called IPv4 - has been started by the body that hands them out in Europe.

From now on, companies can only make one more application for IPv4 addresses and, if successful, will only get 1,024 of them.

In addition, any application for more old addresses must demonstrate how an organisation is using the new, replacement, addressing scheme.

Europe's stock of old-style net addresses has effectively run dry.

"The day has come, finally," said Axel Pawlik, managing director of the Ripe NCC that hands out addresses to European ISPs, firms and other organisations.

Every device that goes online is allocated a unique Internet Protocol (IP) address.

The internet grew up using an addressing scheme called IP Version 4 (IPv4). In the 1970s when the web was being built the 4.3 billion IP addresses allowed by IPv4 were thought to be enough.

However, the rapid growth of the internet and popularity of the web have swiftly exhausted this pool.

The growth of the net is linked to the size of the pool because everything that connects to the net needs an IP address to send and receive data.

Restrictions

Related Stories

- New net address system enabled
- Norway heads net address shift
- Boost for new net address scheme

Top Stories

- 'Go home' vans not good idea - May
- Energy bosses called before MPs NEW
- Girl removed from Dublin Roma family NEW
- Syria talks 'must bolster moderates'
- Stuart Hall to be stripped of OBE NEW

Features

- **Bleak odyssey** Syrian family's dangerous quest for refuge in Europe
- **Frosty reception** Are people too snobbish about frozen food?
- **Outfoxed** Is there a humane way to rid your garden of foxes?
- **Gods of baking** The rise and rise of the celebrity patissier

Most Popular

Shared Read Video/Audio

1. BBC 'would air' Comic Relief claims
2. Stuart Hall to be stripped of OBE
3. Quake talk over beached 'sea snake'

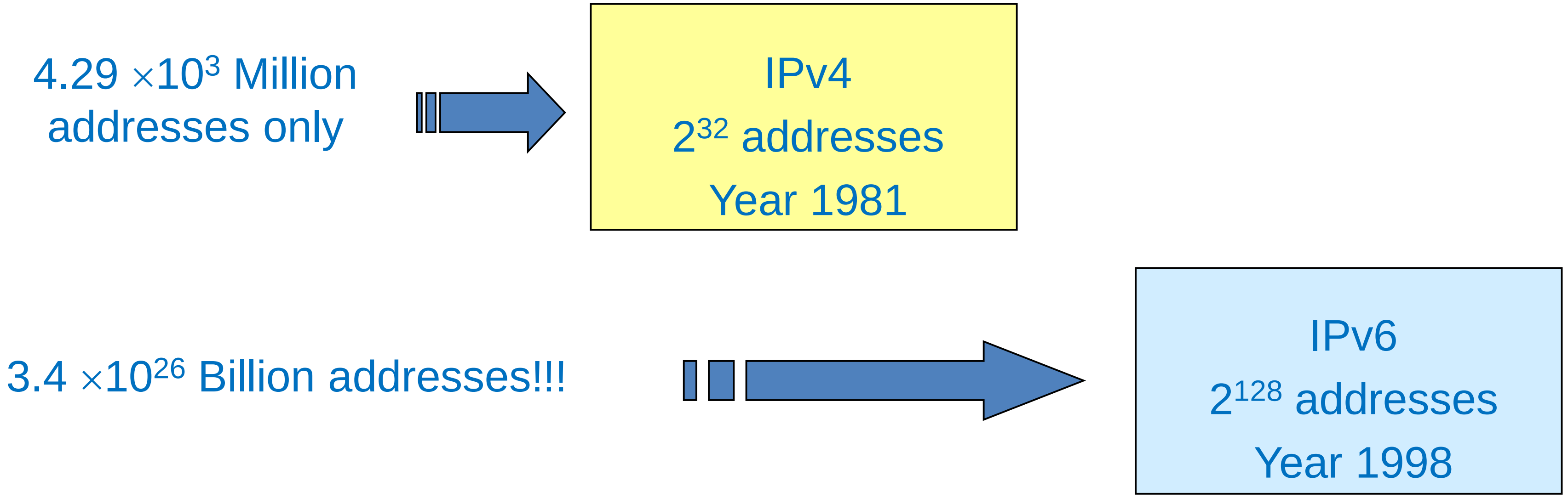
- The internet is running out of IP addresses
- The Class System makes it very wasteful with address allocations

Question:

How to solve this problem?

IPv6

- IPv4 with 2^{32} addresses
- IPv6 with 2^{128} addresses



4.29×10^3 Million addresses only

IPv4
2^{32} addresses
Year 1981

3.4×10^{26} Billion addresses!!!

IPv6
2^{128} addresses
Year 1998

1 Million = 1×10^6
1 Billion = 1×10^{12}

The growth of the address space in the Internet

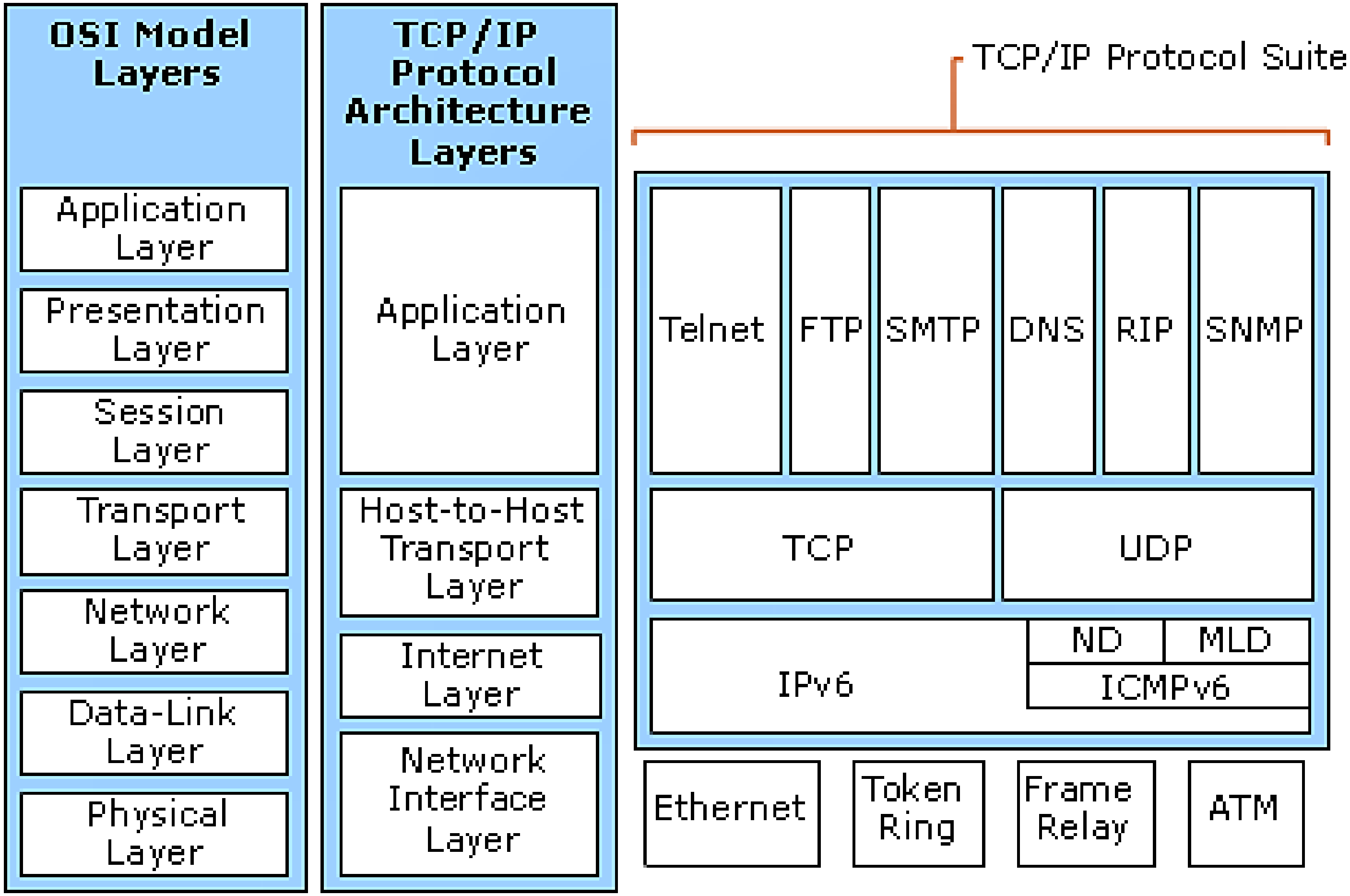
IPv6

- *IPv6 includes the following features*

[1] Better and more compact header format
[2] Larger address space
[3] Support for resource allocation (flow labelling and control options)
[4] Built-in security
[5] Better support for quality of service (QoS)
[6] New protocol for neighbouring node interaction
[7] Extensibility

- The architecture of the IPv6 is shown in the next slide

The Architecture of IPv6



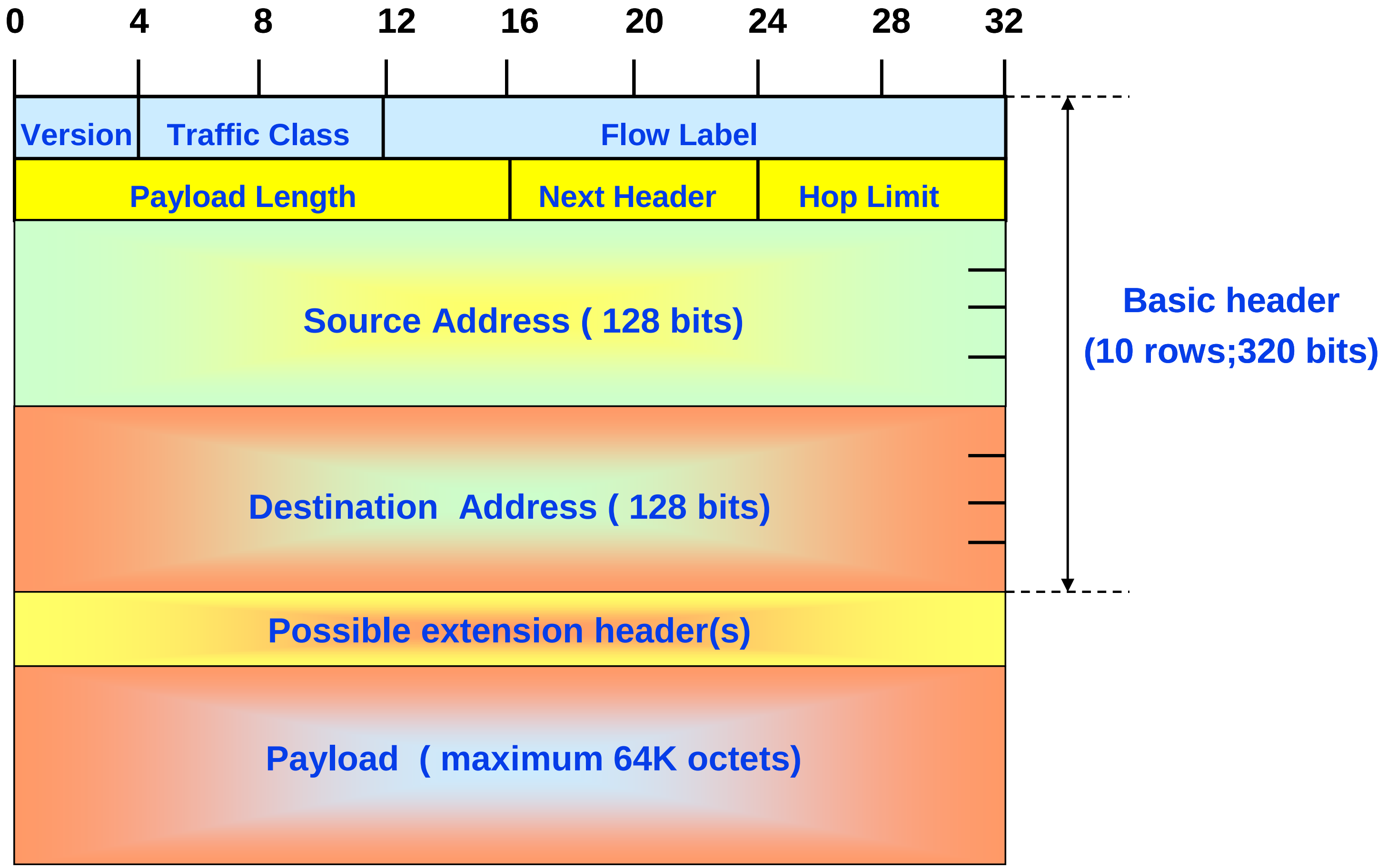
- The architecture of IPv6.

The Core Protocols of IPv6

Protocol	Functions
IPv6	*IPv6 is a routable protocol* that is responsible for the addressing, routing, and fragmenting of packets by the sending host. IPv6 replaces Internet Protocol version 4 (IPv4).
ICMPv6 **(Internet Control Message Protocol)**	*ICMPv6 is responsible for* providing diagnostic functions and reporting errors due to the unsuccessful delivery of IPv6 packets. ICMPv6 replaces ICMPv4.
Neighbour Discovery	*Neighbour Discovery* is responsible for the interaction of neighbouring nodes and includes message exchanges for address resolution, duplicate address detection, router discovery, and router redirects. Neighbour Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message.
Multicast Listener Discovery	*Multicast Listener Discovery* is a series of three ICMPv6 messages that replace version 2 of the Internet Group Management Protocol (IGMP) for IPv4 to manage subnet multicast membership.

- The core protocols of IPv6

IPv6 Datagram


0
4
8
12
16
20
24
28
32
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address (128 bits)
Destination Address (128 bits)
Possible extension header(s)
Payload (maximum 64K octets)
Basic header
(10 rows;320 bits)

- The IPv6 datagram

TCP/IP Protocol Suite

[1] *HTTP* (Hypertext Transfer Protocol): The foundation of the World Wide Web and is used to load web pages using hypertext links.

[2] *Telnet*: A protocol that enables a user on one machine to communicate interactively with an application such as text editor running on a remote machine. It creates the impression that the user terminal were directly connected to it.

[3] *FTP* (File Transfer Protocol): Enables a user at a terminal to access and interact with a remote file system.

[4] *SMTP* (Simple Mail Transfer Protocol): Provides a network wide mail transfer service between the mail systems associated with different machines.

[5] *DNS* (Domain Name Server): An application protocol (process) associated with each institution network. Attached to it there is a data base known as directory information base (DIB) that contains all the directory related information of the institution.

[6] *RIP* (Routing Information Protocol) : A distance-vector routing protocol, which employs the hop count as a routing metric. The maximum number of hops in a path from the source to a destination allowed for RIP is 15.

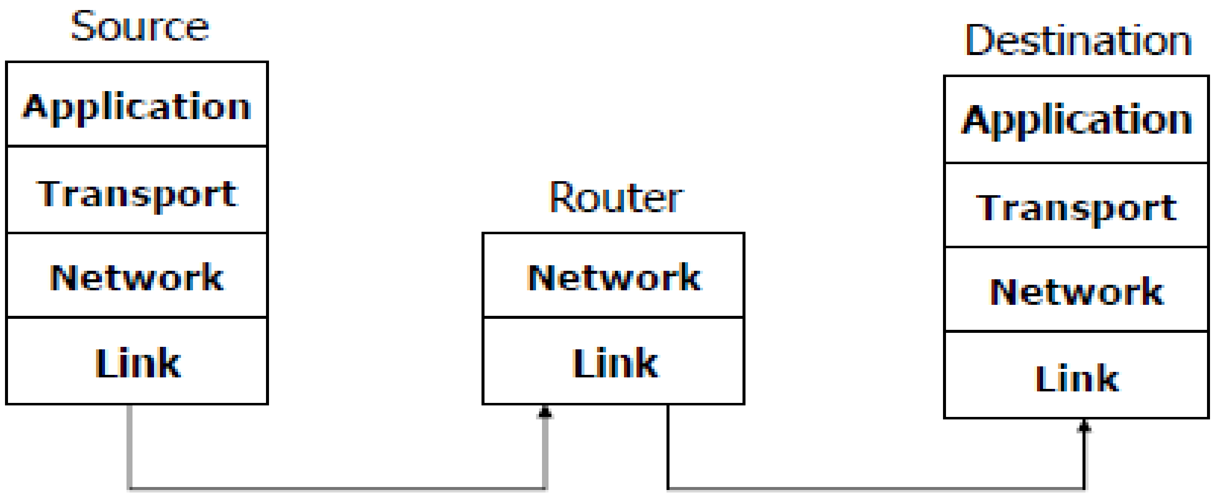
[7] *SNMP* (Simple Network Management Protocol): An "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modems, and more.

Routing

- All devices need to know what IP addresses are on directly attached networks
  - If the destination is on a local network, send it directly there
  - If the destination address isn’t local
    - Most non-router devices just send everything to a single local router
    - Routers need to know which network corresponds to each possible IP address

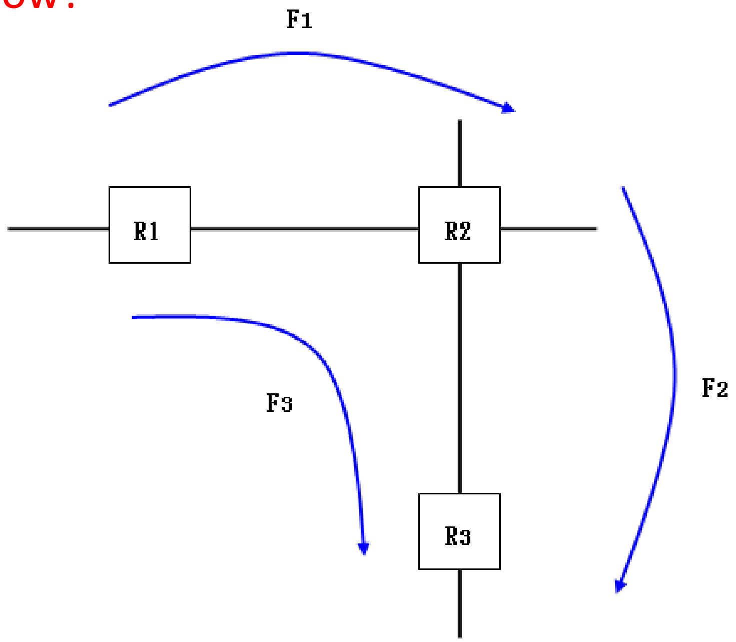
IP Routing

- Routing Table
  - Destination IP address
  - IP address of a next-hop router
  - Flags
  - Network interface specification



Question

- ❑ Consider the network of three routers below. Each link has capacity of 1Mbps. You can assume there is no contention on the access links or for three backplane resources, i.e., the only constraints are the link capacities between routers. There are three flows in the network, labelled *F1*, *F2* and *F3*, which traverse the routers indicated. *F1* travers *R1* → *R2*, *F2* travers *R2* → *R3*, and *F3* shares links with every other flow and traverse *R1* → *R2* → *R3*. Assume that each router implements First In First Out (FIFO) queuing and FIFO drops packets with uniform probability.
- ❑ If each flow consists of an identical, 1Mbps constant bit rate UDP flow with equal packet sizes, what is the resulting rate for each flow?

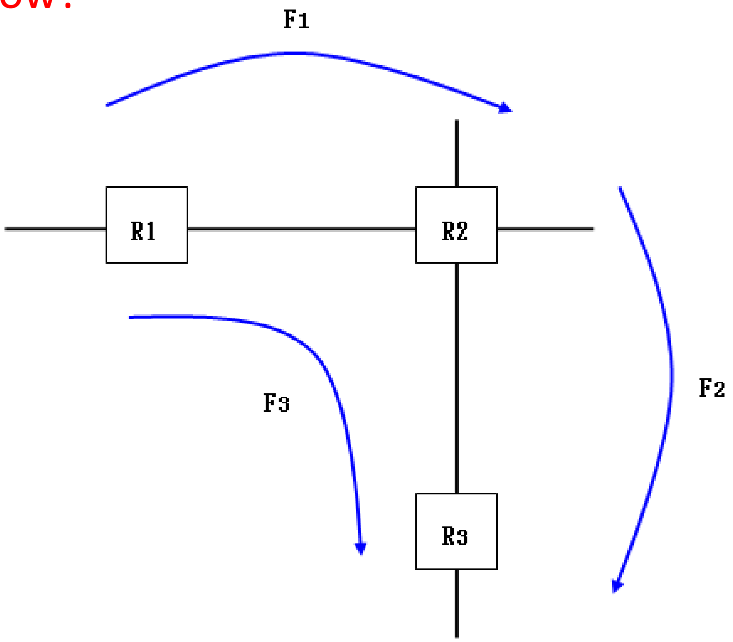


Solution

- ❑ Consider the network of three routers below. Each link has capacity of 1Mbps. You can assume there is no contention on the access links or for three backplane resources, i.e., the only constraints are the link capacities between routers. There are three flows in the network, labelled *F1*, *F2* and *F3*, which traverse the routers indicated. *F1* travers *R1* → *R2*, *F2* travers *R2* → *R3*, and *F3* shares links with every other flow and traverse *R1* → *R2* → *R3*. Assume that each router implements First In First Out (FIFO) queuing and FIFO drops packets with uniform probability.
- ❑ If each flow consists of an identical, 1Mbps constant bit rate UDP flow with equal packet sizes, what is the resulting rate for each flow?

❖The resulting rate for each flow is:

- F3 compete at R1 with F1 at 1:1, giving
  F1: (1/2) x 1Mbps = 0.5Mbps
  F3: (1/2) x 1Mbps = 0.5Mbps
- F3 then compete at R2 with F2 at (1/2):1, giving
  F2: (2/3) x 1Mbps = 0.67Mbps
  F3: (1/3) x 1Mbps = 0.33Mbps



Network structures

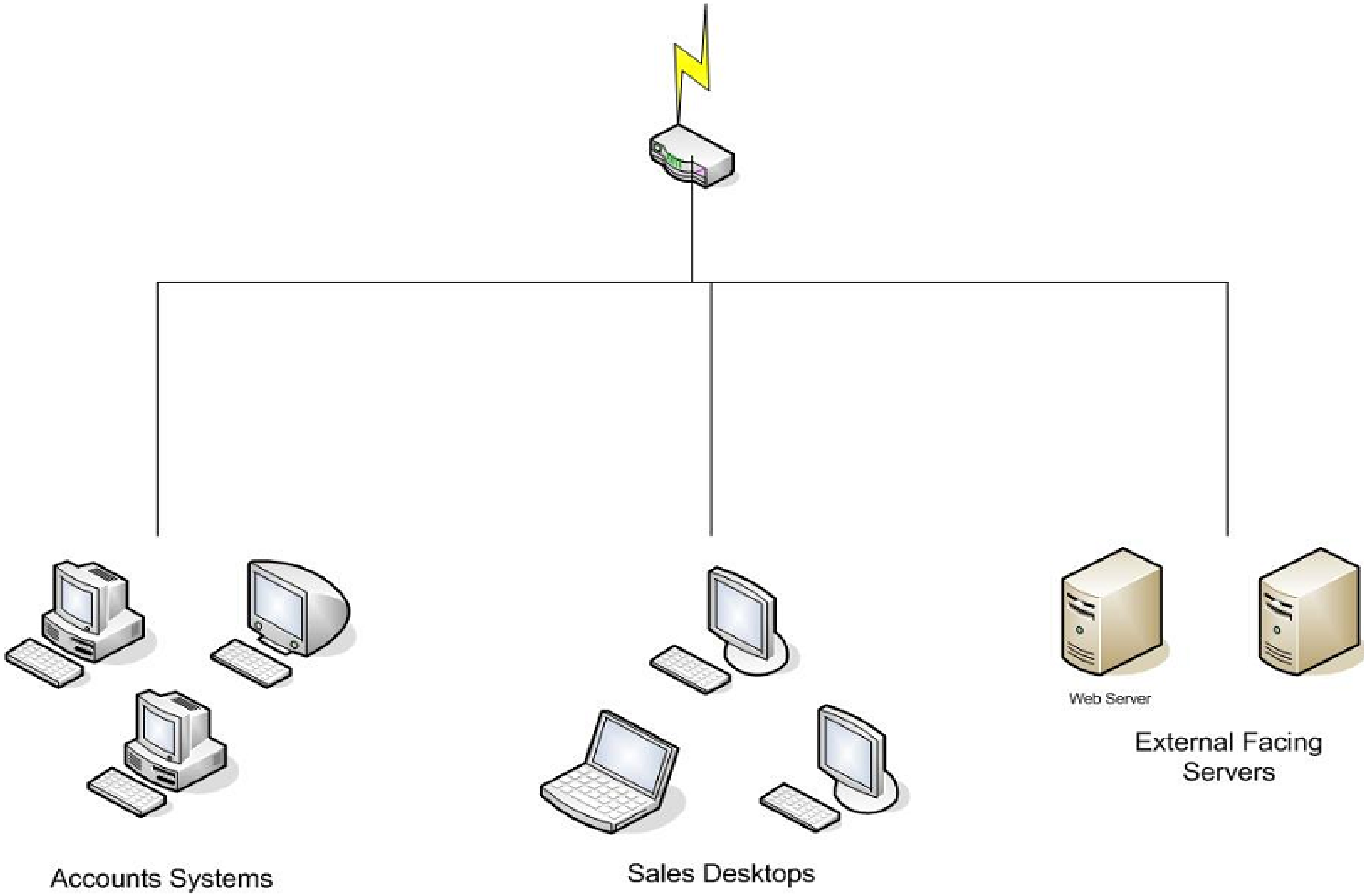
- The days of simply connecting all computers together with cable are over!
- A well-designed network should be segregated depending on what hosts provide and require
- The key is separating our hosts
- Dividing networks into subnets is a logical step

Subnet

- Used to divide an organisation
  - By media
  - By organisation
- TCP/IP's natural way of dividing groups of hosts
- Helps to control network traffic
- A host in a subnet (A) cannot directly talk to a host in another subnet (B)
- Hosts in subnet A must always communicate via a router (normally at least 2) to contact subnet B's hosts
- By using subnets to divide groups of hosts, you can reduce the risk of damage and spreading of malware (malicious software)

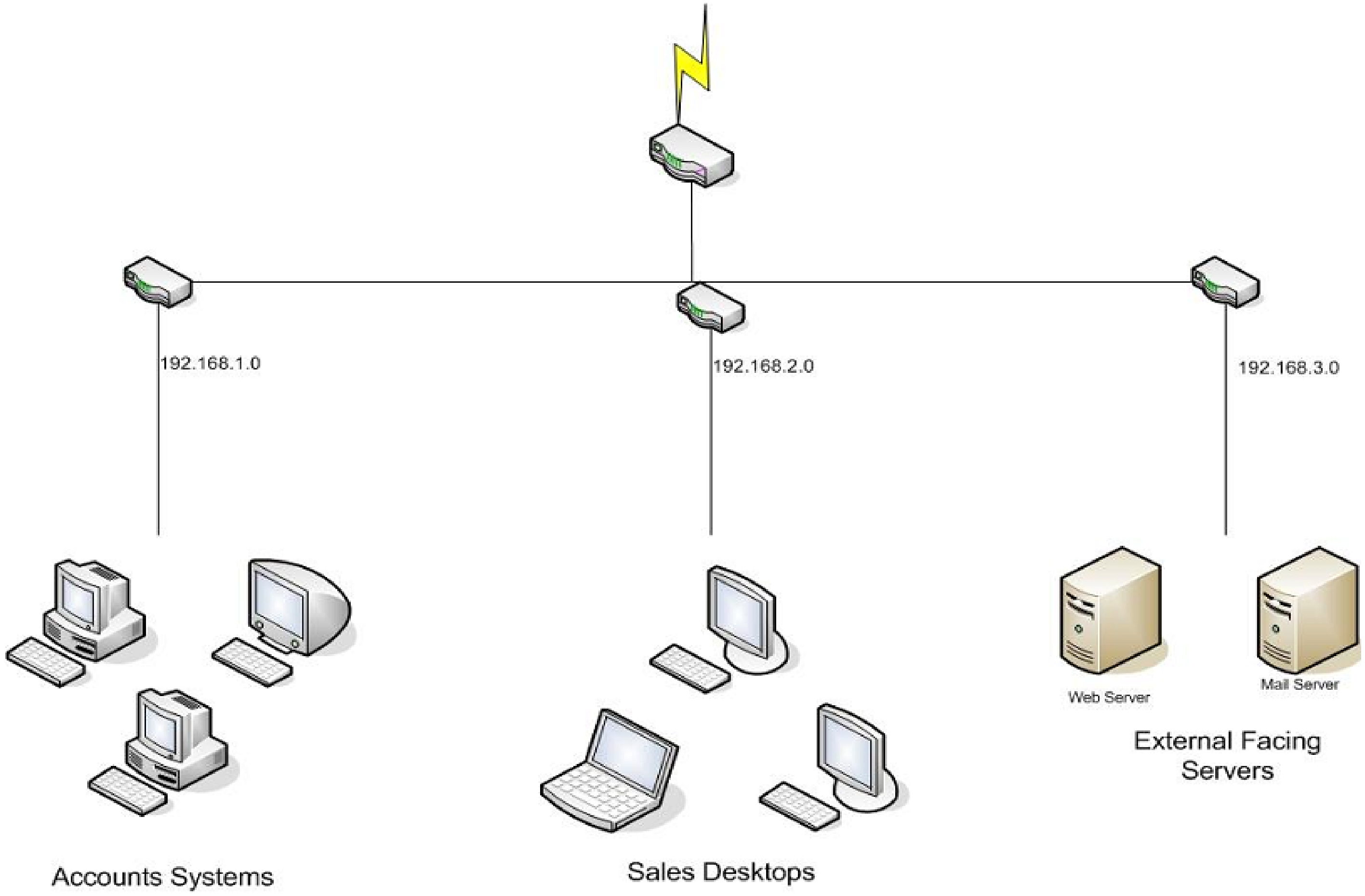
Subnet Examples

- An example of a company network



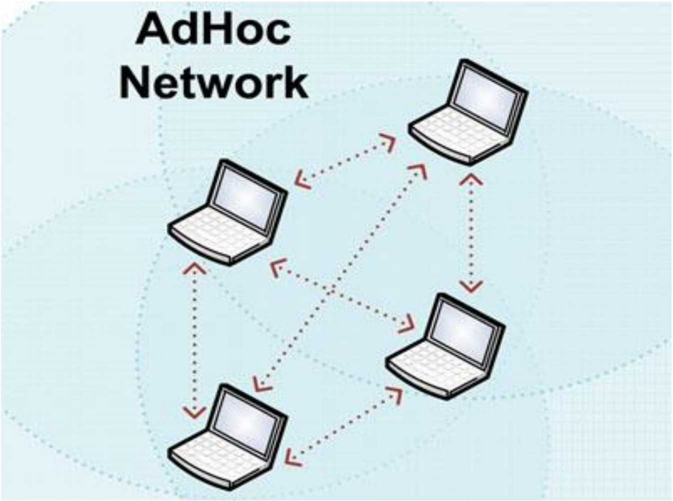
Subnet Examples

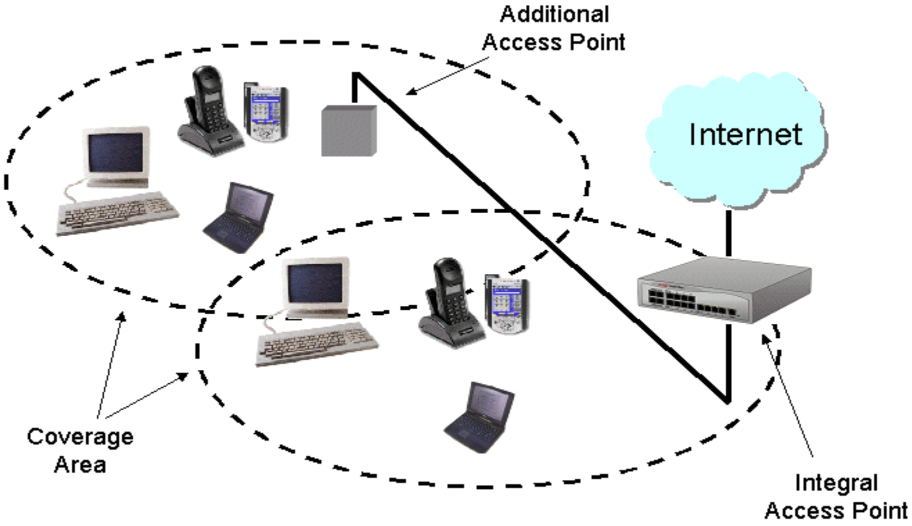
- IPs



Wireless Network Structures

- **Peer to Peer (Ad-hoc)**
  - Clients – all participate in a workgroup
  - No structure to the network – every node has equal status
- **Access Point (Structured)**
  - Clients must connect to an access point
  - Structure is imposed normally along with security





Thank you