



Data Communications and Networking

Lecturer: Toby Daniel

Data Communication Protocols

- Network Protocols
- General format and error handling
- Ethernet
- Data collisions
- OSI model
- Internet protocol suite

Network Protocols

- A set of rules for the exchange of information, such as those used for successful data transmission.
- These rules are implemented in hardware or software to facilitate communications and provide a well defined interface between different hardware and software systems.

Network Protocols

Protocol rules cover:

- format of data (size, order, etc.)
- timing and sequencing of data
- error handling
- message acknowledgment
- data compression
- access methods
- permitted topologies
- types of cabling

Network Protocols - Format

Formatting rules specify how data is packaged into messages.

- The basic unit of a physical network is a frame.
 - General form of a network frame:



Network frame formats

Ethernet frames

- Version 2 format

PREAMBLE (Bytes 1-4)	
PREAMBLE (Bytes 5-8)	
DEST MAC ADDRESS (Bytes 1-4)	
DEST MAC ADDRESS (Bytes 5-6)	SRC MAC ADDRESS (Bytes 1-2)
SRC MAC ADDRESS (Bytes 3-6)	
TYPE*	DATA (Bytes 1-2)
DATA (Bytes 3-1500)	
FRAME CHECK SEQUENCE	

Network frame formats

- IEEE 802 format

PREAMBLE (Bytes 1-4)		
PREAMBLE (Bytes 5-8)		
DEST MAC ADDRESS (Bytes 1-4)		
DEST MAC ADDRESS (Bytes 5-6)	SRC MAC ADDRESS (Bytes 1-2)	
SRC MAC ADDRESS (Bytes 3-6)		
LENGTH	DSAP (AA)	SSAP (AA)
CONTROL (03)	ORGANIZATION CODE (000000)	
TYPE	DATA (Bytes 1-2)	
DATA (Bytes 3-1492)		
FRAME CHECK SEQUENCE		

Byte Order

- Big-endian and little-endian are terms that describe the order in which a sequence of bytes are stored and transmitted.
- **Big-endian** is an order in which the "big end" (most significant value) is sent first.
 - TCP/IP uses the big-endian approach (and is sometimes called *network order*).
- **Little-endian** is an order in which the "little end" (least significant value) is sent first.
 - URLs and e-mail addresses are little-endian.

Error Handling

- Errors occur in the transfer of information across a network.
- Network protocols need to implement error handling.
- Error handling requires that the system can identify if the data is missing and if the data has changed.
 - Parity bits
 - Checksum
 - CRC checks

Error Handling – Parity Bits

- Parity bits are one of the simplest ways of detecting errors in transmitted data.
- A parity bit is a single binary digit that is added to ensure that the number of 1 bits is always even. Example:

11010011 = 5 x 1 (odd)

11010011**1** = even (blue = parity bit)

11000011 = 4 x 1 (even)

11000011**0** = even (blue = parity bit)

11011011**1** = odd - therefore an error has occurred!

Error Handling – Checksum

- This works by adding up the individual bits in the message and storing the resulting value as the Checksum.
- Anyone can later perform the same operation on the data and compare the result to the checksum value.
- If the result and the checksum are different, then an error has occurred in the data.

Error Handling - Problems

- Both Parity bits and simple Checksum cannot detect the following errors in a message:
 - Reordering of the bytes in the message.
 - Inserting or deleting zero-valued bytes.
 - Multiple errors which sum to zero.
- A more sophisticated error handling is needed to check not only the value of each byte but also its position.

Error Handling – CRC

- Cyclic Redundancy Check (CRC) is a more sophisticated error-detecting code.
- It is a long division computation in which the quotient is discarded and the remainder becomes the resulting checking code.
- The transmitter adds an extra sequence to every frame called the Frame Check Sequence (FCS)
- A calculation is then performed at the other end on the whole frame. The result of the calculations indicates if an error has occurred during transmission.

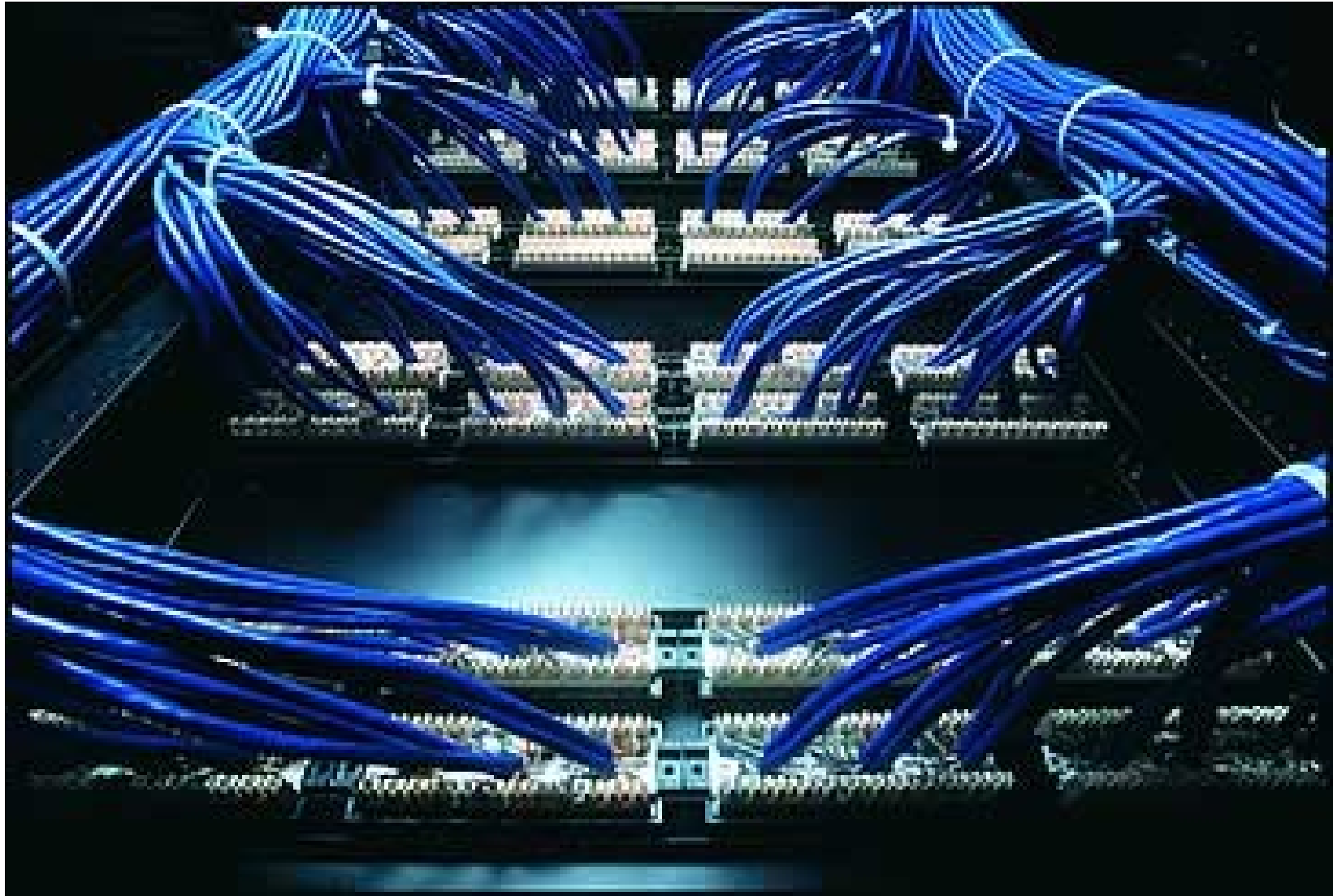
The CRC creation process:

1. Get the raw frame
2. Left shift the raw frame by n bits and then divide it by P (P = predefined CRC number)
3. The remainder of step 2 is the FCS.
4. Append the FCS to the raw frame. The result is the frame to transmit

The CRC check process:

1. Receive the frame.
2. Divide it by P .
3. Check the remainder. If not zero then there is an error in the frame.

Ethernet

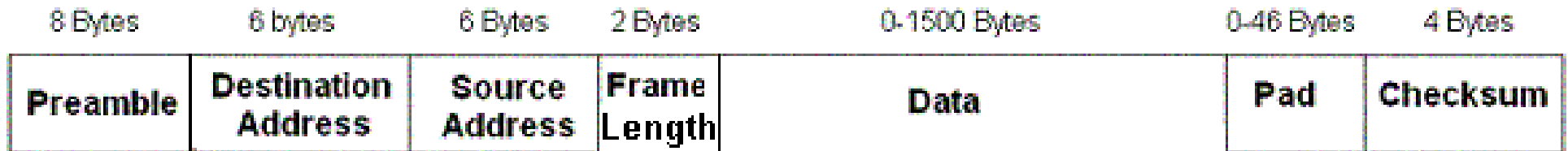


Ethernet

- Ethernet is a group of frame-based computer networking protocols for LANs.
- Within these specifications Ethernet protocol allows for different topologies:
 - bus
 - star
 - tree
- Data can be transmitted over:
 - wireless
 - twisted pair cable
 - coaxial cable
 - fiber optic cable
- at speeds of 10 Mbps to 10 Gbps.

Ethernet Frames

- Data is transmitted across an Ethernet network in discreet messages known as frames.
- The format of the frames is shown here with the number of bytes for each part.



Ethernet at 10 Mbps

- 10Base5 and 10Base2
 - Ethernet on coaxial cable using Bus topology.
 - Bus topology broadcasts messages to all nodes.
 - Ethernet has to be able to detect data collisions.
- 10BaseT with hubs
 - Ethernet on UTP cable using a Star topology.
 - Hubs broadcast messages to all nodes.
 - Ethernet has to be able to detect data collisions.
- 10BaseT with switches
 - Ethernet on UTP cable using a Star topology.
 - Switched networks allows for more than one connection at a time.
 - Significantly less collisions occur.

Ethernet Collision Detection

- CSMA/CD is the collision detection system used by the Ethernet protocol.
- CSMA/CD is the *Access Method* for standard Ethernet.

CSMA/CD

Carrier Sense Multiple Access
with Collision Detection

CSMA/CD

Carrier Sense Multiple Access

- This gives the nodes on a network the ability to monitor the network cable.
- They can detect if it is being used or if it is idle.
- If the cable is clear then data can send.

- Problems occur when two computers transmit at the same time.
- This leads to a data collision *\$}bang!@*&

CSMA/CD

Collision Detection

- CSMA behaves inefficiently when a collision occurs because both stations continue to transmit.
- Collision detection is used to check that the message on the network is the same as the one that was sent.
- If it is not the same then the message is aborted.
- Both sending nodes then wait a random amount of time before sending again – to avoid another collision.

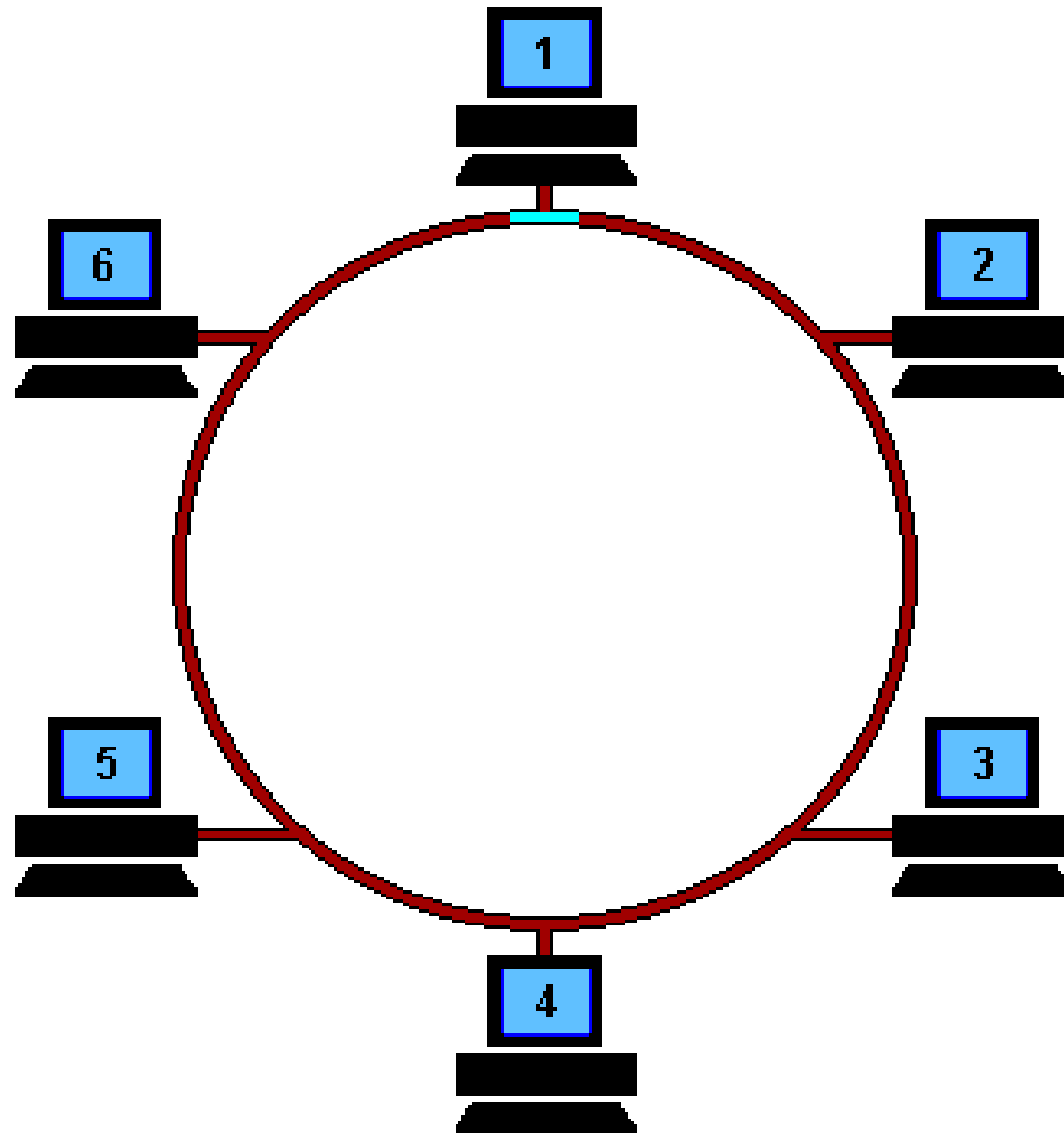
Other Access Methods

- CSMA/CD is used by Ethernet, but it is not the only Access Method.
- **Token-passing** – is an Access Method that is used on Ring Topology networks.
- ARCNET, token bus and FDDI use the Token-passing access method.

Token-passing

- Token-passing means that a machine can only use the network when it has control of a **Token**.
- The token is passed from one machine to another in a ring.
- This ensures that there are no collisions because only one machine can use the network at any given time (when they have access to the token).

Token-passing



Token-passing

- After a machine uses the token to transmit to another machine it waits for an acknowledgment that the message was received.
- After the machine receives the acknowledgment it releases the token so that the next machine can have a chance to use it.
- Token-passing is more “fair” than CSMA/CD as every machine has the same chance of using the token.

Ethernet at 100 Mbps

- IEEE802.3u defines a standard for faster LANs
 - sometimes called Fast Ethernet
- Fast Ethernet keeps the same frame format, interfaces and procedural rules as Ethernet.
- Backwards compatible with standard Ethernet.
- Fast Ethernet increases the number of bits a node sends within a set time.
 - The bit time has changed to 10nsec rather than the previous 100nsec.

Ethernet at 100 Mbps

- 100Base-TX - cat. 5 twisted pair cables.
 - Two twisted pairs per node are used, one pair for each direction.
 - Full duplex communication.
 - Maximum cable lengths of 100m.
- 100Base-FX - multimode optical fibre
 - A cable for each direction.
 - Full duplex with 100 Mbps in each direction.
 - The maximum cable lengths can be up to 2 km.

Ethernet at 1000 Mbps

- Gigabit Ethernet – 1000Mbps, backwards compatible with standard Ethernet and Fast Ethernet Nodes.
- A decrease in bit time allows us to reach this speed, **but** it would limit the cable length to 10m!
- So other ways are used to reach transmission rates of 1000Mbps.

Gigabit Ethernet

- 1000BASE-T – cat. 5 or 6 UTP cable.
 - uses all four cable pairs for simultaneous transmission in both directions
 - uses echo cancellation and pulse amplitude modulation
 - maximum cable length 100m
- 1000BASE-SX - multi-mode optical fiber
 - maximum cable length 500m
- 1000BASE-LX - single-mode optical fiber
 - maximum cable length 2 km
- 1000BASE-ZX - single-mode fiber
 - requires 1550 nm wavelength
 - maximum cable length 70 km

Faster ... Faster



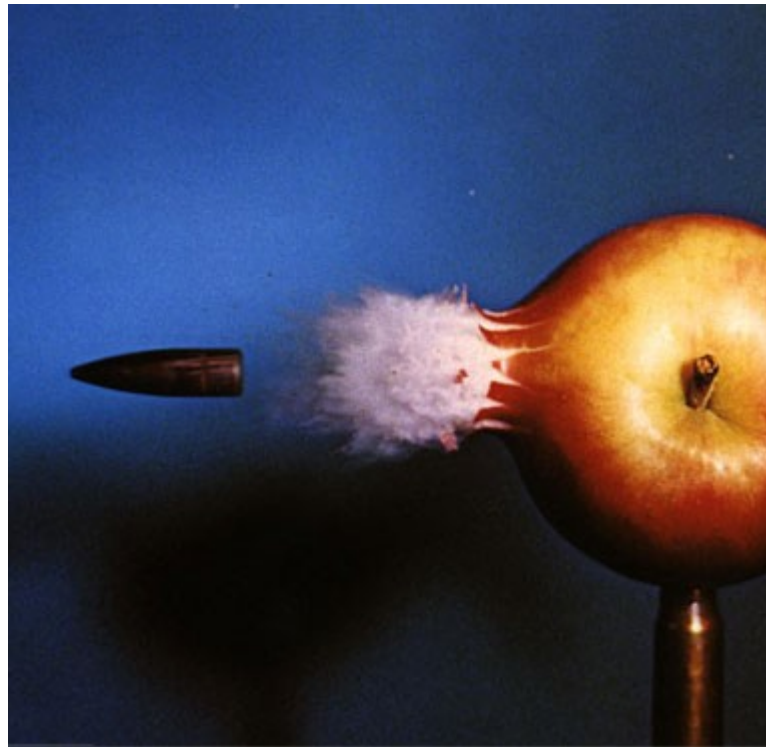
- **10 Gigabit Ethernet** is the most recent and fastest of the Ethernet standards.
- 10 Gigabit Ethernet no longer uses:
 - half duplex links
 - hubs and repeaters
 - CSMA/CD
- 10 Gigabit Ethernet uses full duplex links connected by switches.

10 Gigabit Ethernet

- 10GBASE-T requires cat 6a UTP
 - special NICs and switches (expensive and rare)
 - maximum cables lengths 55m-100m
 - 10GBASE-LR single-mode fiber
 - requires 1310 nm wavelength
 - maximum cable length of 25km
- * There are other 10 Gigabit Ethernet standards for other optical fibre types.

100 Gigabit Ethernet

... not a standard yet – but just wait!



OSI

Open Systems Interconnection

- A model to standardise networking
- Started in 1982 by the International Organization for Standardisation.



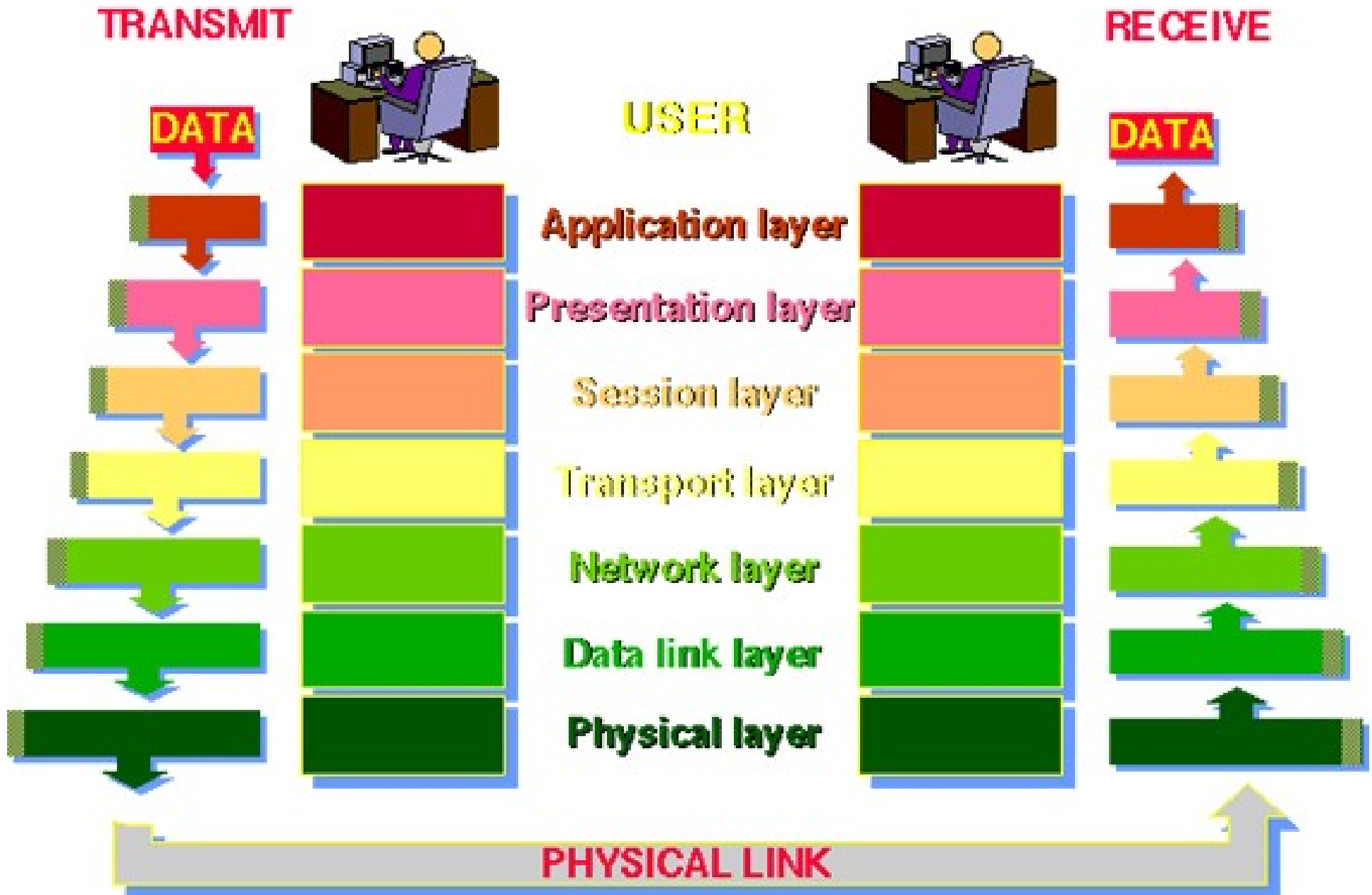
The OSI Reference Model

- The OSI reference model teaches network concepts using a layer approach.
- A layered model allows communication between computers from different vendors using different network architectures.
- Communications are divided into seven layers. Each layer performs a specific task and builds upon the preceding layer until the communication is complete.

Benefits of using OSI

- The benefits of using an accepted layered reference model are:
- the complete process of network communication is divided into more easily understood layers.
- one part (or layer) of the model can be changed without changing all the other parts of the model.
- it is a universally accepted standard interface that allows cable makers, network hardware manufacturers and software designers to integrate their products.

The OSI Reference Model



“Please Do Not Throw Sausage Pizza Away”



Application (Layer 7)

- This layer allows network functions to user applications.
- Application services for file transfers, web browsing (http), e-mail, Telnet and FTP.
- The application layer organises input into a **block** or block(s) of data.
- The OSI model does not include human interfaces.

7
6
5
4
3
2
1

Presentation (Layer 6)

- Data representation and encryption.
- The presentation layer converts the data block into a common code/format.
- If data needs to be **compressed** it happens at this layer.
- **Encryption** can also happen at this layer to encode data for security purposes

7
6
5
4
3
2
1

Session (Layer 5)

- The sending computer opens a **Session** with the receiving computer to agree on communications such as:
 - Full-duplex or
 - Half-duplex
- **Error checking** (checksums) are added to the data.
- **Start and stop markers** are added to the block of data.

7
6
5
4
3
2
1

Transport (Layer 4)

- The data is usually subdivided into **Segments**.
- These segments are marked with their sequence order in the message.
- A copy of all segments is kept in case of the need to re-transmit lost pieces.
- The **header** for each segment contains the sequence number and error checking information.

7
6
5
4
3
2
1

Network (Layer 3)

- The segments are broken up into **Packets** ready for delivery across a network.
- The packet size will depend on the type of network architecture.
- A network header is added to each packet with the **destination address** and the sequence number of the packet within the segment.

7
6
5
4
3
2
1

Data Link (Layer 2)

- Network **Frames** are created from the packets with a header, trailer and error detection information added.
- Frames are copied and stored in case of the need to re-transmit.

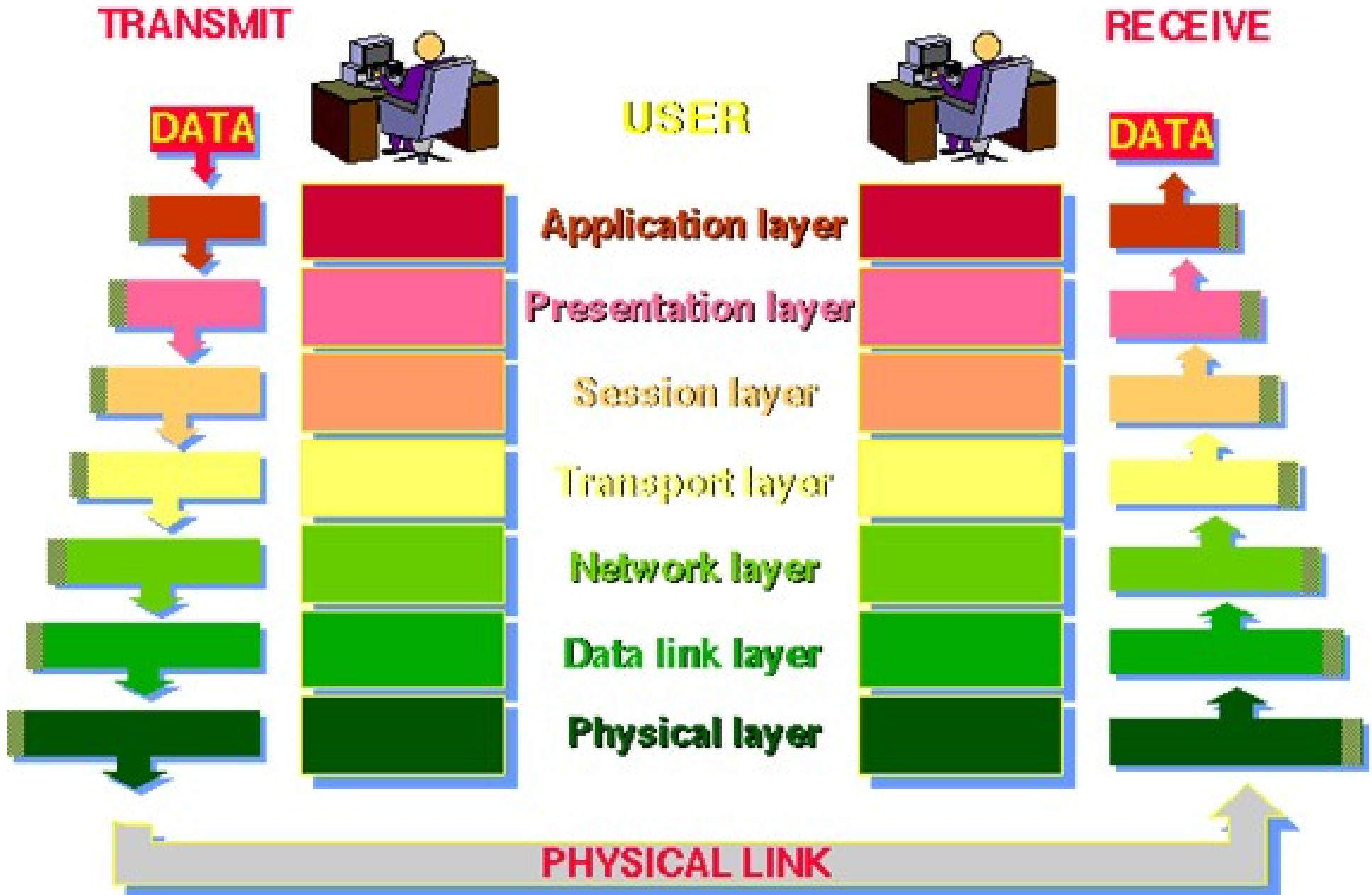
7
6
5
4
3
2
1

Physical (Layer 1)

- This is where the frames are sent across the network.
- The physical layer defines a number of network functions, including:
 - Hardware, cables and cards.
 - Encoding and signalling (UART).
 - Transmitting and receiving data.
 - Topology and Physical Network Design.

7
6
5
4
3
2
1

The OSI Reference Model



Networking Hardware and OSI

- Layer 1:
 - Cables
 - Network cards
 - Hubs
- Layer 2:
 - MAC addresses
 - Switches
 - Bridges
- Layer 3:
 - IP addresses
 - Routers



TCP/IP

Transmission Control Protocol / Internet Protocol

- A suite of protocols that is the standard communication protocol for using Internet based networks.
- TCP/IP includes:
 - IP addressing
 - HTTP
 - SMTP
 - FTP
 - DNS

TCP/IP and the OSI model

