Contents

[1. OSI and TCP Layer 2](#_Toc127039050)

[2. Ethernet Frame: - 4](#_Toc127039051)

[2.1. Ethernet frame structure: - 4](#_Toc127039052)

[3. Hub and Switch 6](#_Toc127039053)

[3.1. Hub: - 6](#_Toc127039054)

[3.2. Switch: - 6](#_Toc127039055)

# OSI and TCP Layer

Diagram

Description automatically generated

Figure - 1

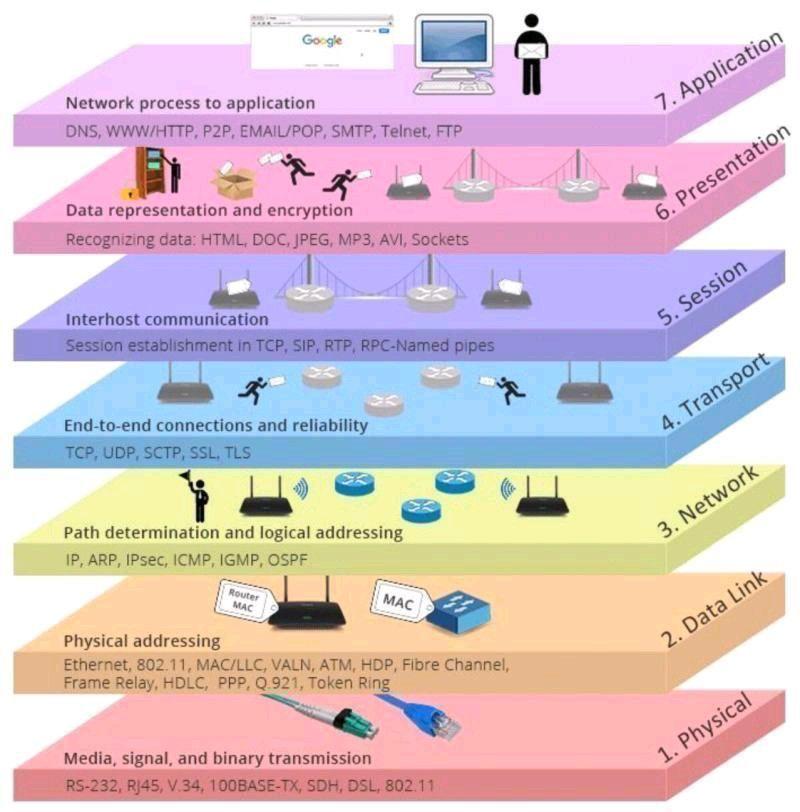


Figure – 2

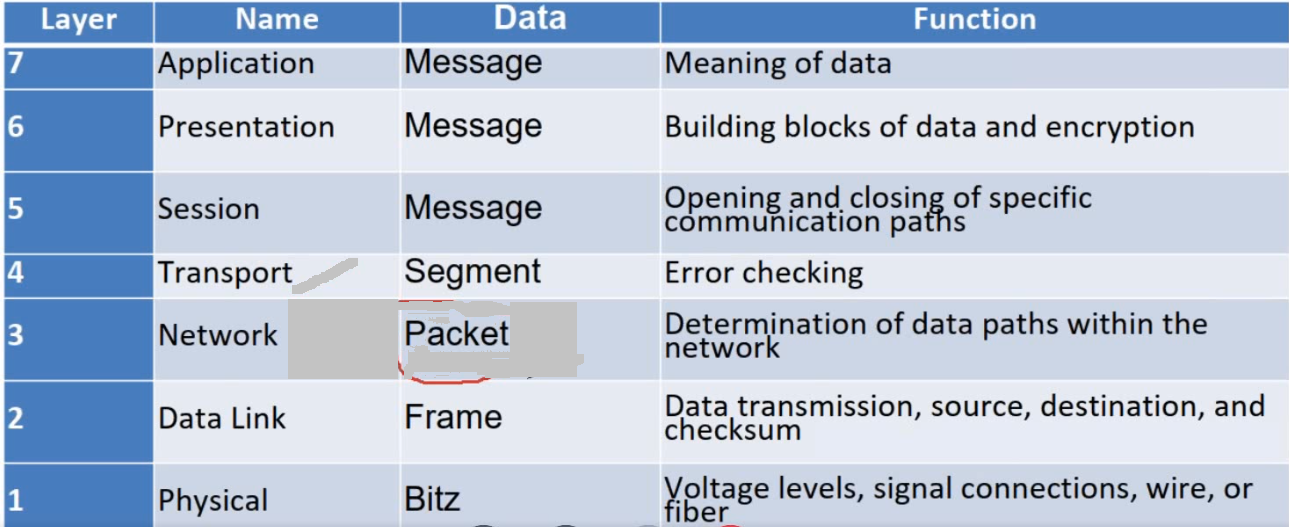


Figure – 3

# Ethernet Frame: -

Standard: -

IEEE 802.3 - Ethernet

IEEE 802.11 – Wi-Fi

## Ethernet frame structure: -

Ethernet frame Normal IEEE 802.3 compliant Ethernet frames are between 64 and 1518 bytes long. They are made up of five or six different fields:

* destination MAC address
* source MAC address
* Type/length field
* Data payload
* Optional Padding field
* CRC
* Additionally, when transmitted on the Ethernet medium, a 7-byte preamble field and Start-Of-Frame (SOF) delimiter bytes are appended.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Preamble | SOF Delimiter | Destination address  (such as Multicast, Broadcast and Unicast) | Source address | Type/Length | DATA/ Payload  (with optional padding) | CRC |

**Preamble: -**

Preamble is a series of 56 bits alternating with 1 and 0. These bits are used for synchronization

and give each participant the time to observe the activity on the bus before the actual data arrives.

**SFD: -**

The start of frame delimiter (10101011), the last byte of the preamble, indicates to the receiver that the actual data is on its way.

**MAC address: -**

Size of MAC address: 6 bytes (48 bits). The MAC broadcast address is FF FF FF FF FF FF.

**TYPE: -**

The TYPE field is different for IEEE802.3 and Ethernet II (DIX standard).

For Ethernet II, the field type refers to the higher-level protocol that uses an Ethernet frame to send data. Xerox assigns a code of 2 bytes to every protocol that is developed for Ethernet. Some examples:

0600h XNS

0800h IP (Internet Protocol)

0806h ARP protocol

0835h Reverse ARP protocol

8100h IEEE802 1.q tag frame (VLAN)

The IEEE802.3 defines the field TYPE as LENGTH field in order to be able to send the number of actual data bytes.

**DATA: -**

The data field contains the data to be sent. This data field is transparent- this means that the content of this field is completely free for Ethernet. Only the length has to be a minimum of 46 bytes and not more than 1500 bytes.

**PAD: -**

The padding bits are random data bits that, if necessary, can be added to the data in order to reach the minimum required 46 bytes.

**FCS: -**

The check sum is a 4-byte CRC value that the sender creates and sends. The receiver can check the integrity of the data with this code.

Note: -

Ping: - ICMP is used for testing network connections using ping program.

# Hub and Switch

## Hub: -

A hub is actually a multiport repeater: it regenerates incoming signals to all other ports as can be seen from figure below.

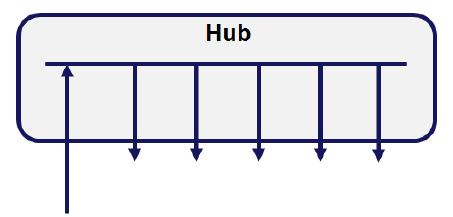


Figure – 4

## Switch: -

Switch is used to interlink LAN segments with more intelligence. Before a packet is transmitted from one segment to the other segment via a switch, it checks the MAC address and on this basis it decides whether to transport to the other segment or not. Switch in accordance with OSI model is shown below.

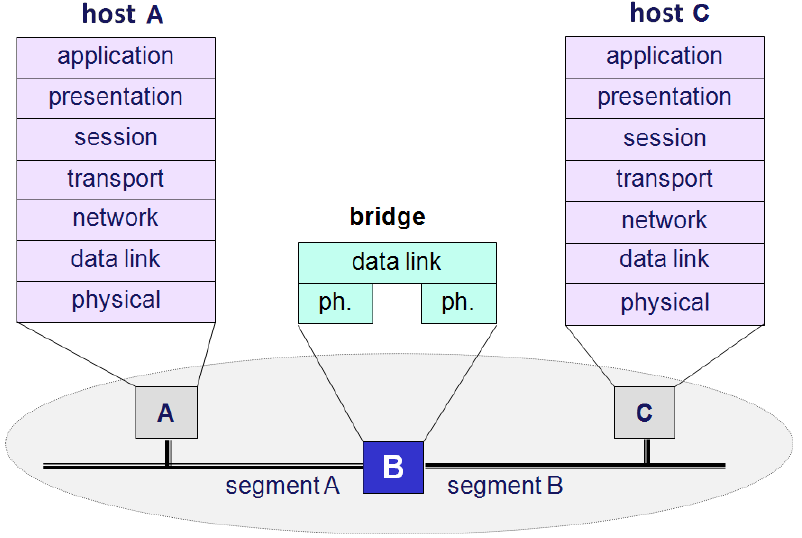


Figure – 5

A MAC address table is updated from a software point of view for every port. This table is filled by listening on the relevant segment of the network and by copying all MAC addresses that occur on that segment to the table. Every address is retained for a limited time and is deleted again as soon as a certain time (the hold time) has lapsed. This technique avoids that inactive stations are addressed or that stations are not recognized anymore.

Linking the segments of a local network via a switch has a number of advantages over the link with a repeater or a hub. When using a switch, a segment is not loaded with the frames of the other segment that do not belong there from an addressing point of view. The load per segment is reduced by this bridge function. At the same time, fault situations are not transmitted as the switch also checks the correct building of the frame.

# IEEE802.1Q tagged frame and VLAN Tag

The IEEE802.1Q describes 4 extra bytes, divided into two extra fields in the Ethernet frame in

order to use for new applications. One of these applications is VLAN.

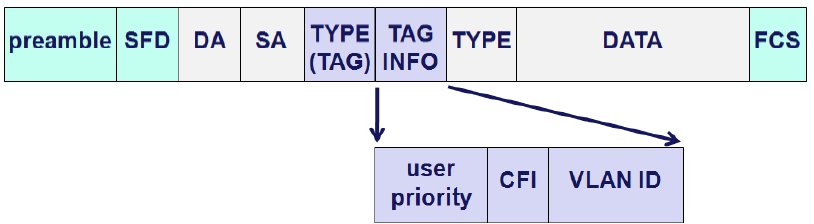


Figure – 6

Description of the extra fields:

* TYPE(TAG), 2 bytes: has the value 8100h to specify that this frame is a tagged frame

and therefore contains an extra information field

* VLAN TPID, 2 bytes: VLAN Tag Protocol Identifier

**–** User priority, 3 bits:

The priority of the frame is included; the priority code (a number between 0 and 7) is described in IEEE802.1p.

**–** CFI: Canonical Format Indicator.

The IEEE802.1Q is only developed for Ethernet or Token Ring. This bit is 0 for Ethernet and 1 for Token Ring.

**–** VLAN ID: Identification of the VLAN, 4094 possibilities.

FFFFh reserved

0000h no VLAN, frames with priority (Profinet IO)

# Virtual LAN (VLAN)

A VLAN or Virtual Local Area Network is a group of participants in a large network that form

a separate network in a logic manner. This means that several logic groups can be created

on a large physical network. A VLAN has an own broadcast domain. Data packets are only

transmitted within a VLAN. The participants may physically be far away from each other but

have to be on one and the same physical network. Some examples of the organization of a

network:

* By department: one VLAN for Sales, another VLAN for Engineering and another VLAN

for Automation.

* By hierarchy: one VLAN for management, another VLAN for managers and another

VLAN for employees.

* By use: one VLAN for users that require e-mail and another for multimedia users.

## Advantages of VLANs

The greatest advantage of VLANs is the segmentation of the network. Other examples are

additional security and restriction on network load.

* **Moving devices around**: it is easier to move devices around in the network in a traditional network, cabling has to be changed when a user moves from one subnet to another. The relocation from one VLAN to another does not require change in cabling. It only requires a setting on the switch. A station from Sales can, for example, be moved to a network connection that belongs to Engineering. The port has to be set up as a member of the VLAN Engineering but does not require new cabling.
* **Additional security**: devices of a VLAN can only communicate with devices in the same VLAN. If a device of VLAN Sales wants to communicate with the VLAN Automation, then this connection has to be set up in a router.
* **Restriction on network traffic**: for a traditional network, broadcasts can cause an overloaded network. Broadcast messages are often sent to devices that do not need these messages. VLANs limit this problem as a broadcast message from one VLAN is not sent to the other VLAN.

## Trunking

Trunking is a method to send data from different VLANs between two switches. Only one port

per device is required for this. There are different ways of trunking.

* ISL: InterSwitch Link, this is a widely used proprietary protocol of Cisco
* IEEE802.1Q: this is a standard that is supported by several switch manufacturers.

For trunking, a piece of code (tag) is added that states which VLAN the sent package comes

from. Thanks to this system, the benefits of VLAN are retained. A router is needed to route data traffic between the different VLANs.

## VLAN types

The different types of VLANs can be divided into two types: static and dynamic VLANs.

* **Static VLANs :**

Static VLANs are port-based. Depending on the port of a switch to which a user connects, this belongs to one or the other VLAN.

Advantages:

**–** Easy to configure

**–** Everything is done using the switch. The user hardly notices anything

Disadvantages:

**–** If a user connects his PC to the wrong port, then the administrator has to do a

reconfiguration.

**–** If a second switch is connected to a port that belongs to a certain VLAN, then   
 all computers that one connects to this switch will automatically belong to this   
 VLAN.

* **Dynamic VLANs :**

Dynamic VLANs are not based on ports of a switch but on the address of the user or the used protocol.

Advantage:

Everyone can connect his computer to any port and still be part of the correct VLAN.

Disadvantage:

The cost of this VLAN type is higher as it requires special hardware.

# TCP/IP: -

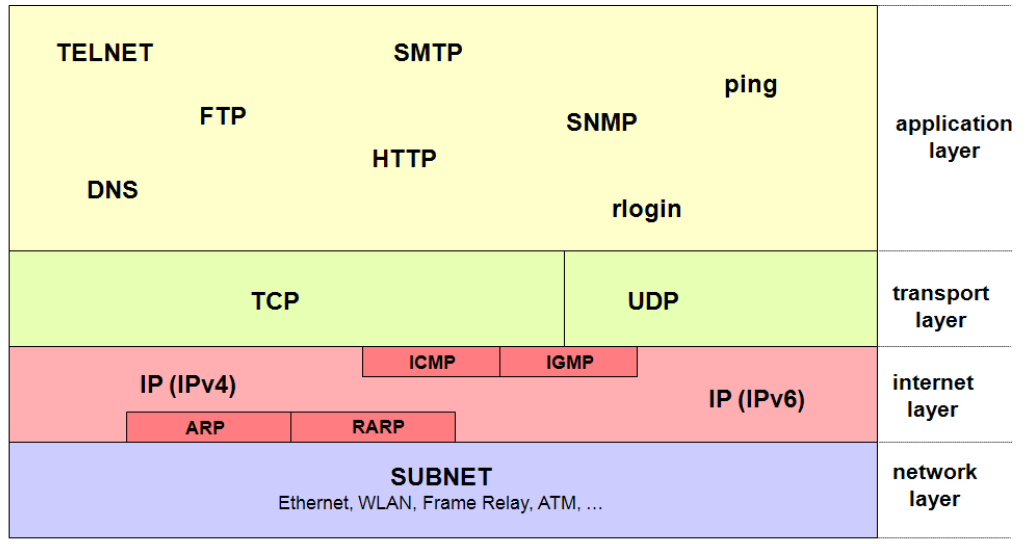


Figure – 7

[Done till page – 43 of Ethernet\_Basic pdf and 30:00 of KM-44 level-2 video]