An ethernet payload has:

An ethernet header. Within that there is an IP payload, within that is a TCP (or UDP) payload and within that there is HTTP data, and an ethernet trailer

When someone says OSI layer 4 they are referring to TCP/UDP data

Multiplexing: use many different applications at the same time (TCP and UDP)

TCP is connection oriented, a formal open or close to the connection. "Reliable" delivery, there is a return receipt for each packet. There is recovery from errors and can manage out of order transmissions. Flow control: the receiver can manage how much data is sent

UDP is connectionless, no formal open or close to the connection. "Unreliable" delivery, no error recovery, no reordering of data or retransmissions, no flow control (sender determines the amount of data transmitted).

Different port number are associated with different applications

IPv4 sockets:

Server ip address, protocol, server application port number

Client ip address, protocol, client port number

Non-ephemeral ports: permanent port numbers. Ports 0-1023 (usually on a server or service)

Ephemeral ports: temporary port numbers. Ports 1024-65535

Determined in real-time by client

TCP and UDP ports can be between 0 and 65535. Most services use non ephemeral ports but this is not always the case. Port numbers are for communication, not security. Service port numbers need to be "well known"

Tcp port numbers aren't the same as udp port numbers

Layering:

different protocols at different levels

cooperating protocols make up a family or suite eg. IPX/SPX, AppleTalk, TCP/IP

TCP is connection oriented (three way handshake) (reliability)

UDP is connectionless (speed)

**Ports:**

OSI layer 4 (transport)

16 bit number

used by TCP and UDP

major application use standard, well known ports

well known ports are > 1024, ephemeral ports are < 1024

Port Binding:

grouping transport protocol, port and IP

single binding

source conflicts or “port already in use” messages

port examination: firewalls, routers and switches use ports

**Layer 2:**

common switched infrastructure (switches and switching) & MAC addressing

PDUs are frames

**Layer 3:**

Sending information via IP addressing (routers and routing), encapsulated

Device1 => L3 => L2 => L1 => L2 => L3 => L3 => Device2

the PDUs at this layer are packets

**Layer 4:**

TCP – segment

UDP – segment

segment is made up of header and data

**Layers 5-7**

PDUs are data: compressed, encrypted and clear text

**Frames**

L2 PDU

framing bits, packet payload and FCS

FCS for error detection

**Address resolution protocol (ARP)**

L3 to L2 IP address mapping

Request and response system

Can be used for duplicate IP detection

**Internet Control Messaging Protocol (**ICMPv6 replaces ARP for IPv6 L2 resolution)

Redirects: notification of alternate gateways (disabled for security by routers)

TTL expires; sends back ICMP to host, used to troubleshoot with traceroute

**Internet Group Management Protocol:**

allows hosts and routers to join multicast groups

used on IPv4 networks only

a host solicits router to join multicast grouping

IGMP with switches: don’t source traffic from multicast hosts

IGMP snooping

You must know the name of each layer (eg OSI level 4) and their functions

OSI 7 layer model:

Physical: cables and hardware

data link: network cards and switches

network: logical addressing

transport: of ip packets

session:

presentation: is the data you received in a form that your computer or app can read?

application: API are the smarts that are built into an app to make it network-aware

tcp/ip model:

network interface / link layer

interface

transport

application

data packets are held within frames. Frames are 1500 bytes and contain:

frame check

port number

mac address

ip address

The repeater sends the frame to all other connected devices

topologies

Full mesh :

all devices connected to all other devices. Provides full redundancy and is the most expensive type of topologies because every node must be directly connected to every other node. Will we used in WAN environments typically

partial mesh topology: each node is connected to 2 or 3 other nodes. Some redundancy and reduced cost. The internet is based on partial mesh

bus topology: not part of the current TIA/EIA 568-C standard

one main line and all the computers are connected to this main cable

one of the oldest networking topologies

all nodes connect directly to main cable called the bus

it is simple to put together

only one node can send a signal at a time

contention: used to determine which node sends the signal

the more nodes active, the more collisions on the network (cancelled out)

too many collisions overload and bring down the network. Less than 30 nodes is safest.

DdoS attacks run on this principle

ring topology: not part of the current TIA/EIA 568-C standard

an older network tech

similar to bus but connected in a circle

packets move around in a ring network: each node given an opportunity to send a signal

no contention between nodes

heavy traffic will not bring down the net work but may slow it down

a single damaged node or cable can bring down the network

hierarchical star topology:

most common topology used in LANs

more expensive than bus because it needs more cables

don’t bring down network with one damaged node

all nodes connected to central hub or switch easy to troubleshoot

has single point of failure

if the whole network goes down, central device is the problem

if a single node goes down the problem will be that node

it is the only topology recognized on the standard for LAN networks

hybrid star topology:

combines one topology with another

physical hybrid topology

physical / logical topology

SNMP v3 has authentication and encryption

Open Systems Interconnection Reference Model (OSI Model)

Mnemonic: All People Seem To Need Data Processing

Layer 1: Physical

Signaling, cabling, connectors. This layer is not about protocols. Fix cabling, punch downs, run loopback tests, replace cables, check connection, swap NIC cards. The signal itself.

Electrical signals

Layer 2: Data Link

The basic network “language”

The foundation of communication at the data link layer

Data Link Control (DLC) protocols

NIC cards connect via MAC addresses on the ethernet

Frames

Switching / Bridging

ethernet

Layer 3: Network

“Routing” layer. Internet protocol layer. IP addresses.

Fragments frames to traverse different networks.

IP encapsulation

**IP fragmentation:** always in multiples of 8 because of the number of fragmentation offset bits in the Ip header

Layer 4: Transport

The “post office” layer. Think of packets as parcels and letters. To load a page, you need a lot of data packets. TCP segment and UDP datagram

TCP encapsulation

Layer 5: Session

Communication management between devices. Start, stop, restart. Control and tunneling protocols

Link the presentation to the transport

Layer 6: Presentation

Character encoding / application encryption

Often combined with the application layer

SSL / TLS encryption

Layer 7: Application

The layer we see. A browser window, file transfer, mail

This is not the same at the OSI protocol suite.

There are unique protocols at every layer.

Wireshark shows you packets.