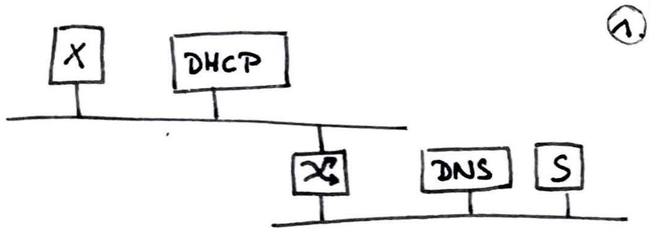
Protocol (1)

ARP between layer 2 and 3.
Layer 2 is done by IEEE and layer 3 is done by IETF who uses RFC to get feedbacks (ex: 1918, 2626, 7230)
Everything beginning by 10/8, 192.168/16, 172.16/12 is for private networks. Those IP don't go on the internet.
So ARP is the way we translate any protocol of layer 2 so that IP can run on it. The iP is a universal adress that network use to speak to each other.
iP adress → $\underset{ARP}{\square}$ → mac adress.
ARP is used to talk locally on a network.

DHCP Gives you the IP+ subnet mask.
Only inside a local network.



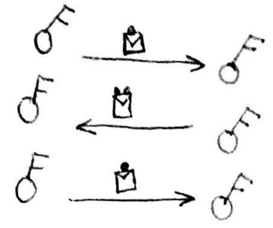
1. Discover phase :
DHCP just received the mac address of the X machine.
2. Offer
3. Request
4. Acknoladge.

= DORA protocol.

CRYPTOGRAPHY | theart of encrypting a communicat°.
Confidentiality : No one can understand
Integrity : No one can be placed between the 2 persons / modify.
Autentication : Verify that the other is the right one.

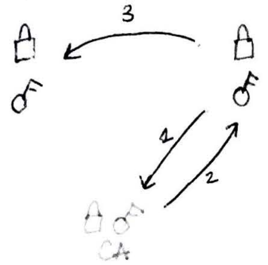
TLS : successor of SSL.

ES (Advanced Encrypton Skim) : A way of encoding with a bag of keys.
More advanced Ceasar encriyption) The most used way is AES - GCM.
t is symmetrical because both speaker use the same keys.
ok at RSA.
DH algorithm.
e pb to solve is that you have to agree on a key but you cannot
t send it to the other but if you want to encrypt it you will need
use a key which itseff has to be encrypted, ...
algorithm uses prime numbers to create the keys.



Red and Blue want to ~~give~~ exchange the key they will use to communicate. o are locks which only can be opened by the key of the same color (Asymetric) Once the key is agreed you start symetric crypto.

Autentication: For this state we need a trusted 3rd partie. That's why we have public keys that prove that we are the owner of the lock. It can be found in a certificate (CSR) delivered by CA.



1 Asked for a CSR

2. CA insped you and your keys. It gives you back a certificate for which the last part is encrypted w/ a private key. Anyone can check that the certificate is right by decrypting w/ CA public key but noone can encrypte and do a false certificate.

3 Starts DH algorithm where Red can check the identity of Blue.

Trust chain: A chain of CA that trust each other up to a root which is very protected and self-signed.

All of this is called $\boxed{\text{PKI}}$.

The list of the roots we can trust is given in the files of our computer.

Recap: Symetric → both have the same key

Asymetrical → Pair of key: 1 public, 1 private. If you encrypt w/ 1 only the other one can decrypt

DISTRIBUTED SYSTEMS.

Several machines that looks like one.

Why? more storage, IO perf, backup (HA = High Availability), geographical optimisat°.

Commodity hardware = standard machine.

2 ways: - Partitioning (having a database you seperate it between the ≠ machine = sharding): good for more storage and IO perf but not for HA.

- Replication (machines are replicated): good for everything but more storage and IO.

Most of the time we use both.

The difficult part is synchronision the machines that has been replicated.

Failure model:

- Crash stop: worst thing is a machine crashing
- crash recovery: same but the machine connects back.
- byzantine. (ex: bitcoin).

ynchronicity model

Protoc

- synchronous model : sending a message I fix a upper bound on(2)
- asynchronous model : a message can be lost, delayed, disordered, repeated.

*the time the other received it.

Time model

Consensus problem

Need to be solved for replication.

"Given a set of machine and some models we need to agree on a value which has been proposed. If no consenesus was found the algorithm might pick one and no machine can leave before all of them agrees".

FLP impossibility theorem state that consensus algo don't exist.

In asynchronous model if 1 machine crashes then FLP.

To "solve" that we add a partially synchronous models which states that most of the time we use synchronous model but sometimes it punctually fails (= asynchronous model). Pb: when is it asynchronous?

CAP theorem : Consistency.
↳ when strong it waits to synchronise before telling to user that it's OK.

Availability.
↳ System tells you if it's available

Partition tolerance
↳ System that assumes that when it cannot reach an other it's network partition.

Network partition : when the connect° between two computers disapears creating subgroups in the network.

o CAP stated that you can only have two of the three true. Now we consider that 3 can be possible but if 1 is really needed (ex: twork partit°) you have to sacrify one of the two others. So we n differenciate CP, AP or CA systems.

 systems : When a network partition happends there is only group that keeps run and the others wait. The one running the majority so the part having $\lfloor n/2 \rfloor$ machine out of n. If no jority is reached every partit° waits. = quorum.

: algorithm based on leaders election.

S : super hard algorithm.

PV6

urrently we have to use tricks like NAT to be able to attribute everyone an IP adress. = ugly. = IPV6 better.

IPV4 → 32 bits → 2^{32} possibitíes

IPV6 → 128 bits → 2^{128} possibilities. → written in hexa in blocks of 16 bits = 4 digits. ⊛

IPV6 have fixed header so it's quicker

IPV4 header contains a checksum + TTL, the checksum is computed taking account of TTL which is itself decremented by one at each router. So you have to recompute the checksum which takes time.

In IPV6 there is no more broadcast, it's replaced by multicast that was barely used by IPV4.
↳ NO MORE ARP.
↳ @ start w/ FF_S with S being the scope

IPV6 : introduce SCOPES : - Node local S=1
- Link local : valid on a lan S=2
- Global @ : go on the Internet S=9

IPV6 have TTL = better for privacy.

NDP (Neighboor Discovery Protocol) :

Mailing lists : FF0S :: 1 → all devices of the scope
FF0S :: 2 → all ~~devi~~ routers of the scope.

To contact someone you put its id on the last 24 bits(?).

Leading 0 can be ignored :
01.0888.0000.0000.0000.0000.0001 can be 2001.888.0.0.0.0.1 or even
01.888 :: 1