

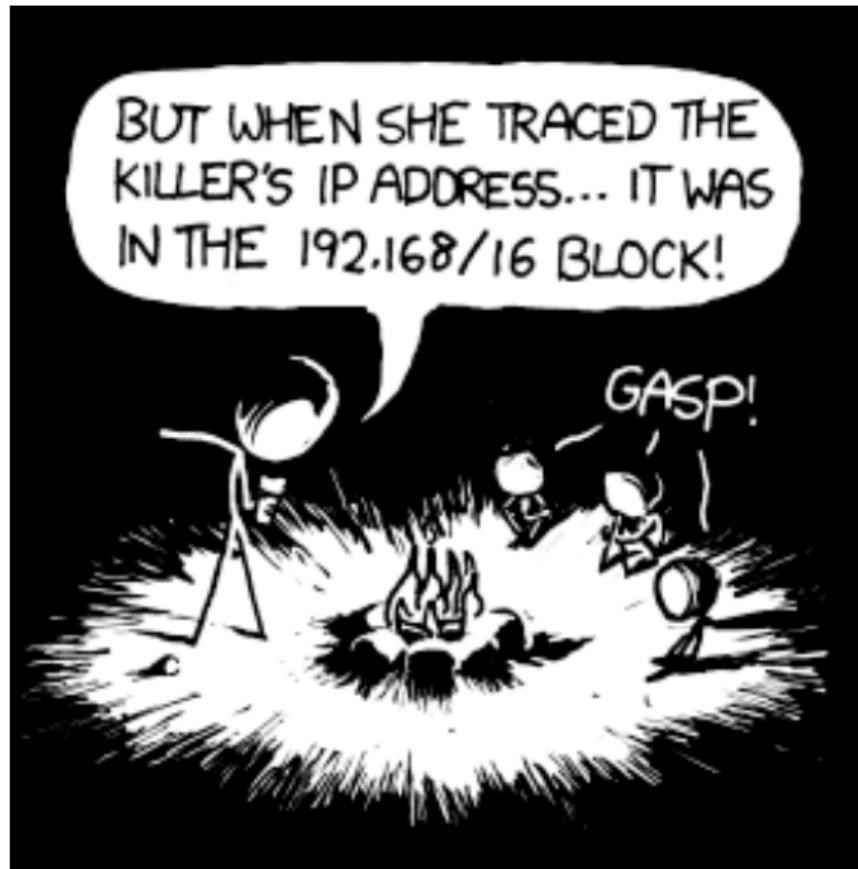
Base de réseaux

2^e année – Majeure Informatique

Christophe Barès



2022-2023



100 years later, this story remains terrifying – not because it's the local network block, but because the killer is still on IPv4.

<https://www.xkcd.com/742/>

Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

Accès au réseau et routage

Section 4

TCP/IP stack

Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

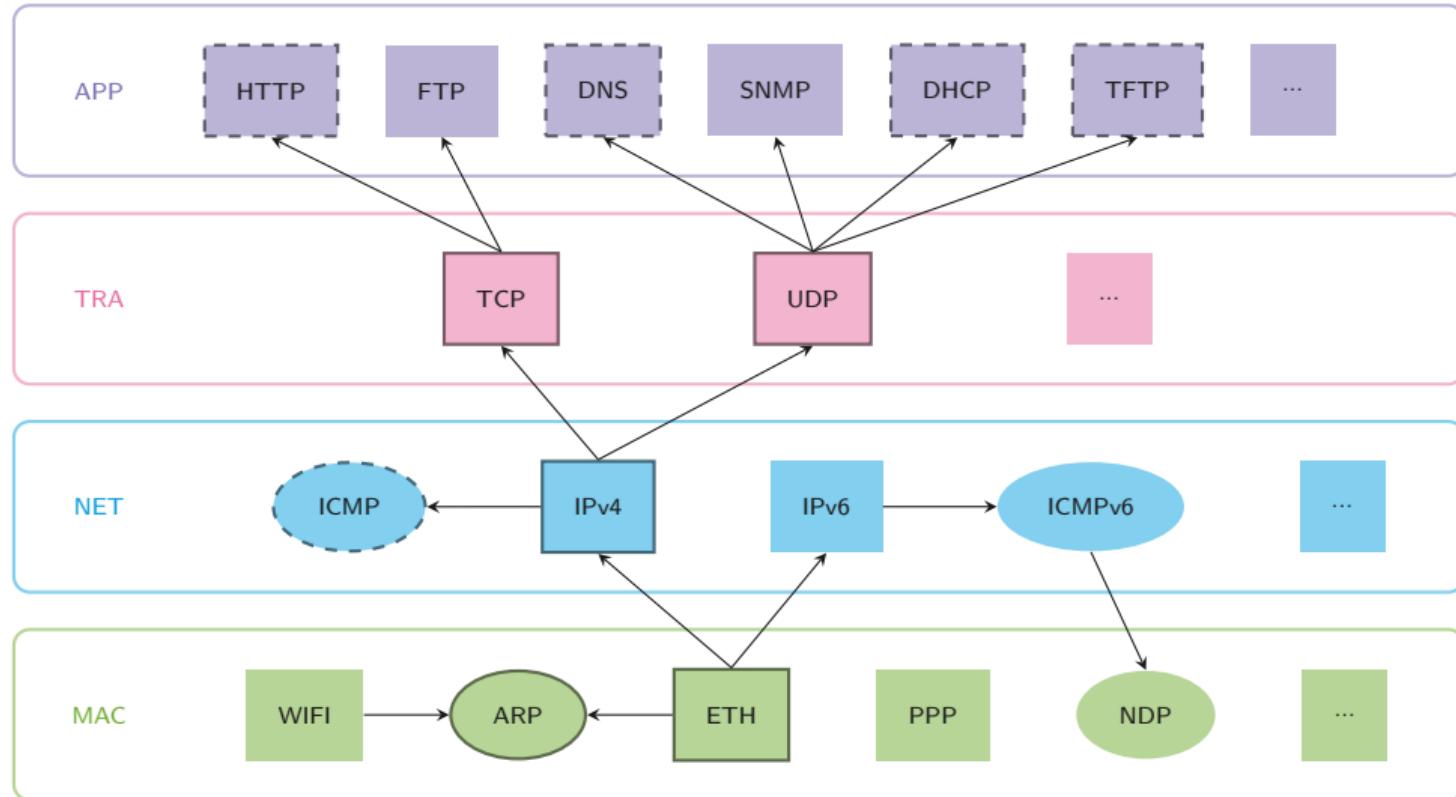
Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

TCP/IP Stack



Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

La couche physique

Couche la plus basse -> Circulation des bits (0, 1) ou groupes de bits (00, 01...)

Support physique de la transmission :

- ▶ Optique : IR, Fibre, Laser, Li-Fi
- ▶ Cuivre : paire torsadée, câble coaxial
- ▶ Ondes radio : Wi-Fi, WiMax, satellite

Matériels :

- ▶ Carte réseau : interface NIC (Network Interface Card) ;
- ▶ Matériels passifs (niveau L1) : concentrateur, répéteurs, ponts ;
- ▶ Matériels actifs (niveaux L2 et +) : commutateurs, routeurs, pare-feux...
=> reposent sur des normes, principalement IEEE

La couche physique

Optiques

Optic Fiber:



Laser FSO (Free Space Optic):



LiFi:



La couche physique

Ondes EM

WiFi (802.11)



WiMax (802.16)



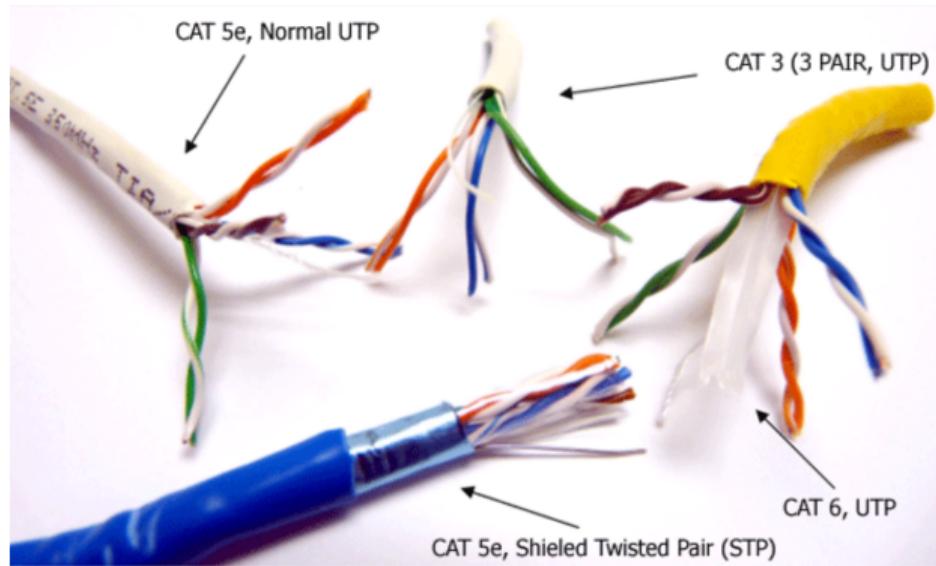
Satellite (Starlink)



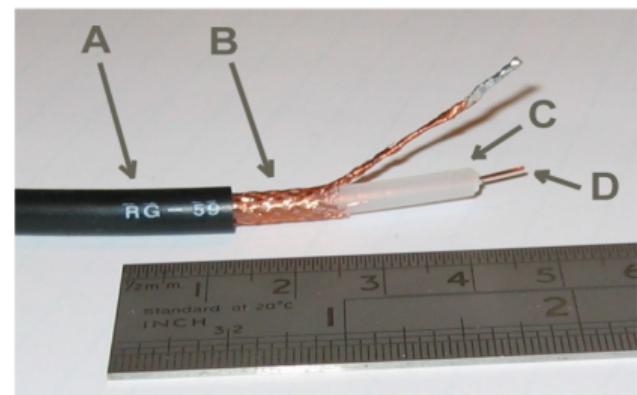
La couche physique

Cuivre

Twisted pair:



Coaxial:



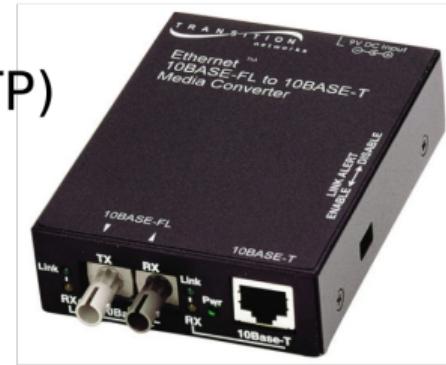
La couche physique

Équipements passifs

Hub:



Bridge:
(fiber - TP)



Repeater:
(submarine optic fiber)



La couche physique

Équipements actifs

Switch (DELL 48 ports + 4 SPF):



Firewall (E-Wall 3 ports):

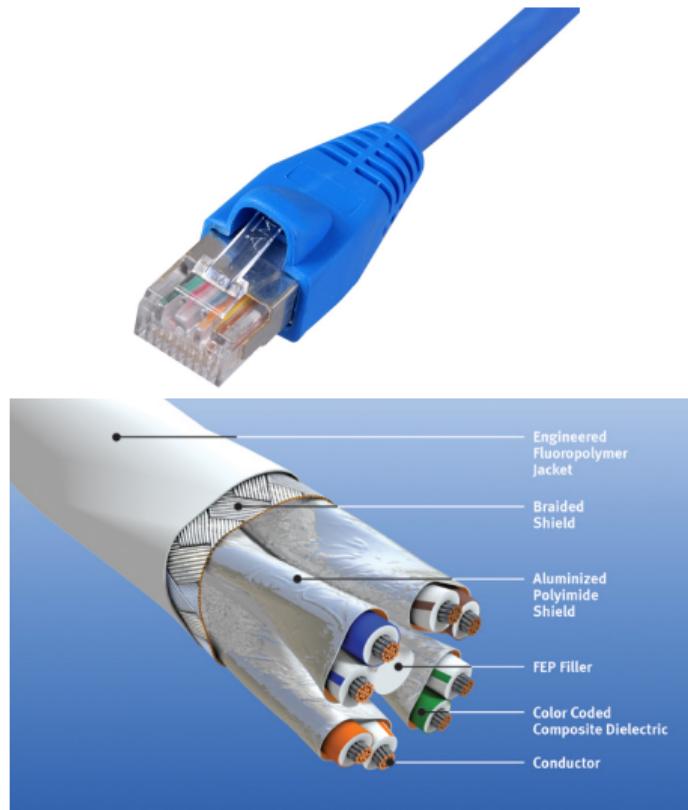


Router (Cisco 2 ports + 2 extension slots):

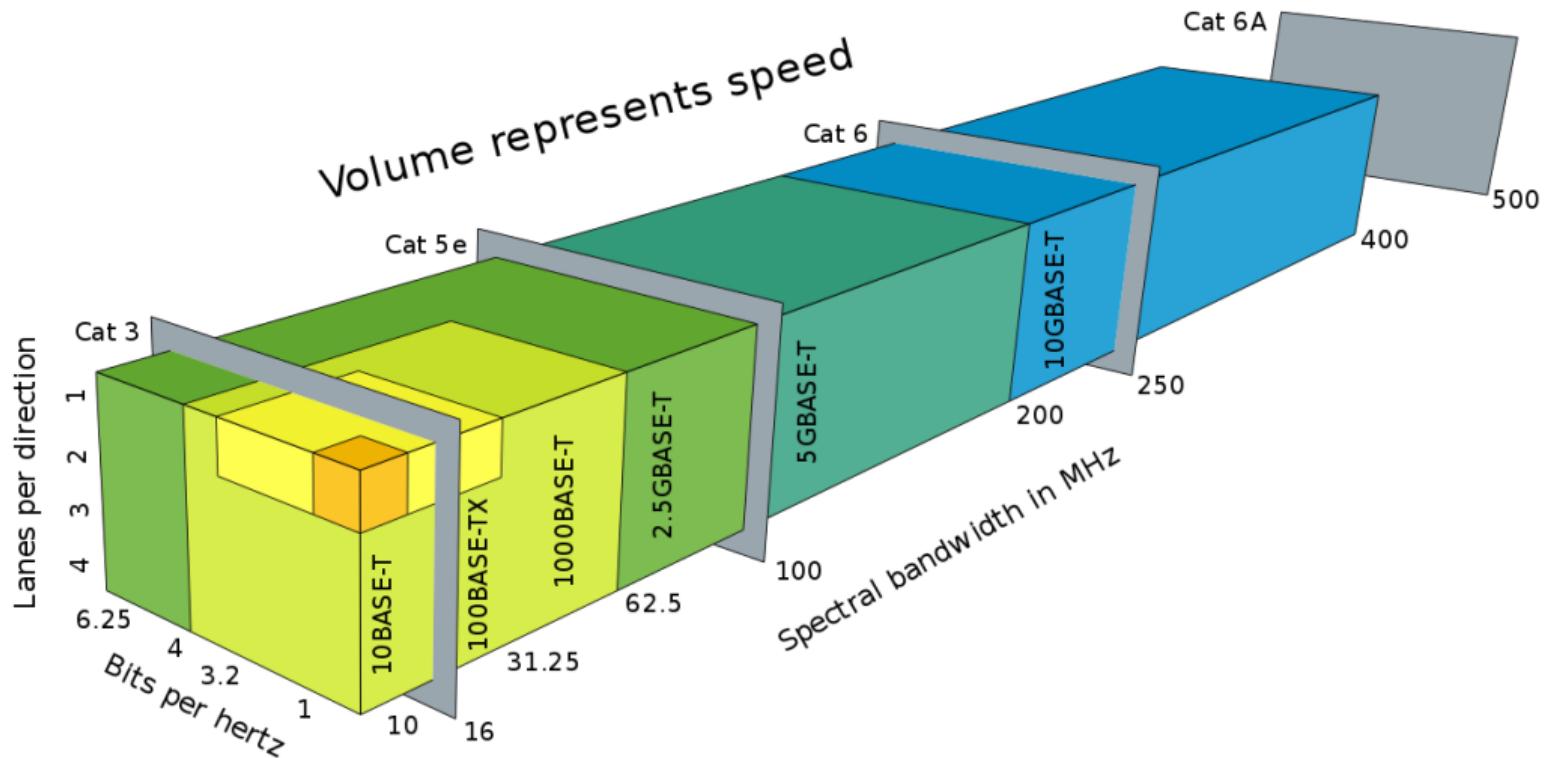


IEEE Std 802.3 : Câbles ou Fibres Ethernet

PHY Type	Data rate	Distance	Media
IEEE Std 802.3-1985 Ethernet MAC, 10BASE5			
10BASE5	10Mb/s	500m	Coaxial
IEEE Std 802.3c-1985 Repeater, FOIRL			
FOIRL	10Mb/s	1km	Two multimode
IEEE Std 802.3a-1988 10BASE2			
10BASE2	10Mb/s	185m	Coaxial
IEEE Std 802.i-1990 10BASE-T			
10BASE-T	10Mb/s	100m	Twisted-pair
IEEE Std 802.3j-1993 10BASE-F			
10BASE-FP	10Mb/s	1km	Two multimode
10BASE-FL	10Mb/s	2km	Two multimode
10BASE-FB	10Mb/s	2km	Two multimode
IEEE Std 802.3u-1995 100BASE-T			
100BASE-TX	100Mb/s	100m	2 pair Cat 5
100BASE-T4	100Mb/s	100m	4 pair Cat 3
100BASE-FX	100Mb/s	2Km	Two multimode
IEEE Std 802.3ab-1999, 1000BASE-T			
1000BASE-T	1Gb/s	100m	Twisted-pair

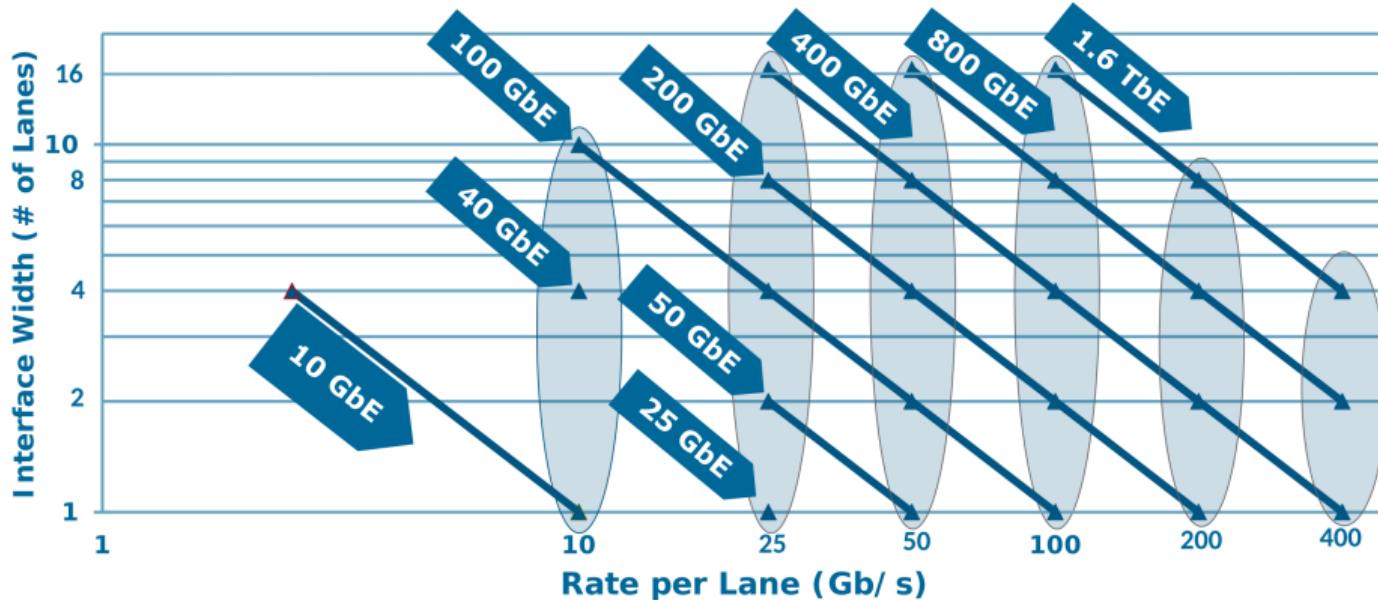


IEEE Std 802.3 : Câbles ou Fibres Ethernet



IEEE Std 802.3 : Câbles ou Fibres Ethernet

Beyond 400 Gb/ s Ethernet - Leveraging 100 Gb/ s Signaling



Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

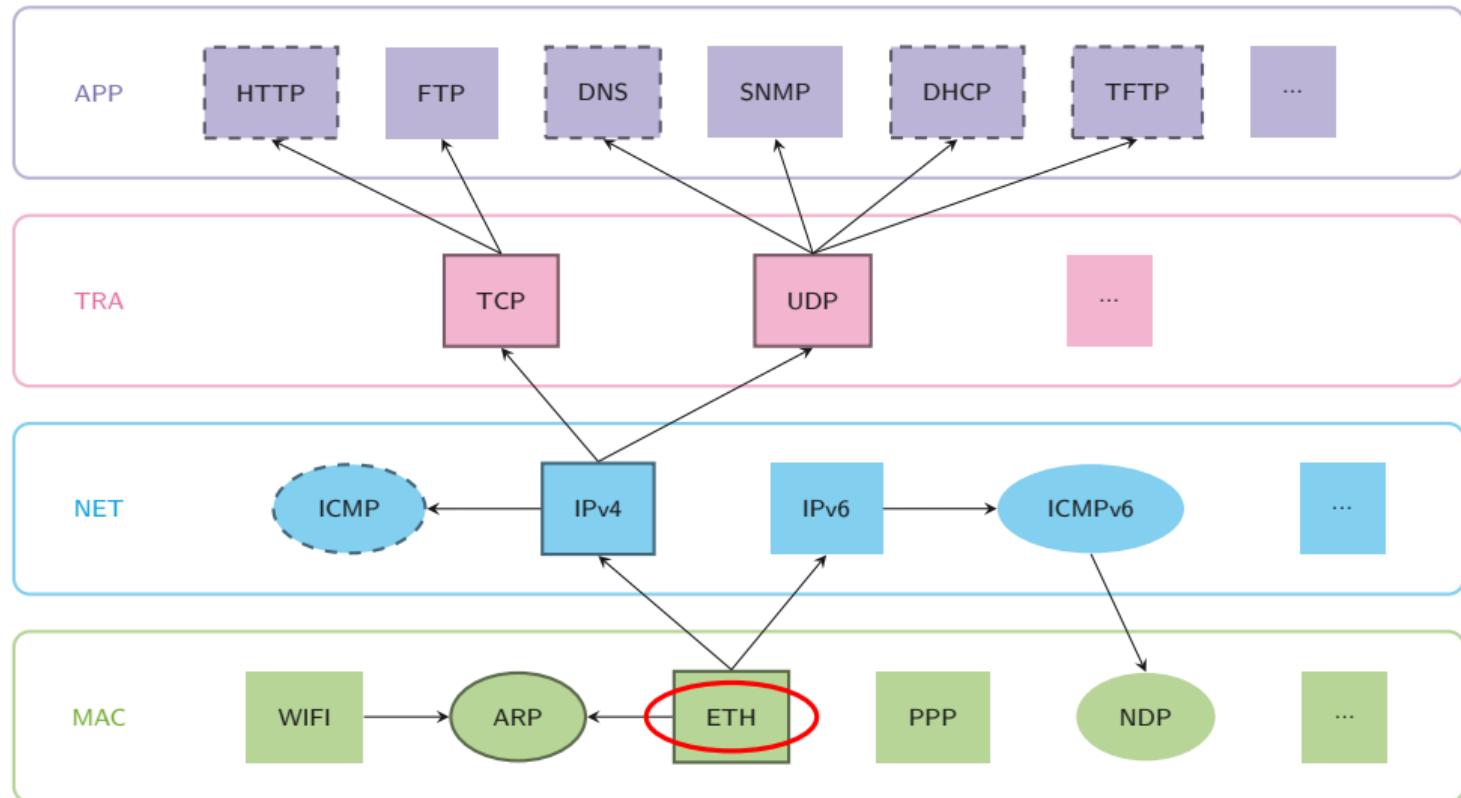
Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

Suite TCP/IP (RFC IETF)



ALOHAⁿet

Ancêtre d'Ethernet : ALOHAⁿet (1971)

Liaison de données radio UHF entre les îles de l'archipel d'Hawaii

Protocole à bas coût utilisant 1 seule fréquence

=> Partage du même media physique

=> Risque de collision des transmissions

Solution : Protocoles CSMA : Carrier Sense Multiple Access

- ▶ CSMA/CD : Collision Detection => Ethernet
- ▶ CSMA/CA : Collision Avoidance => Wifi
- ▶ CSMA/CR : Collision Resolution => CAN, I²C

Principe du CSMA/CD

When a node wants to send a frame :

1. it detects the presence of a carrier on the media ;
2. if no signal is present, it starts to transmit its frame ;
3. it monitors the media to determine if there is a collision ;
4. if so, it waits for a random time before attempting to retransmit.

The node will try again several times, increasing its waiting time.

Existence of a "Collision Domain".

Passive equipments extend this collision domain, active equipments reduce it.

Ethernet is a CSMA/CD protocol

Couche Liaison de données (Data Link Layer)

2 sous-couches :

- ▶ MAC : Medium Access Control (IEEE 802.2 [Ethernet], IEEE 802.11 [Wifi]...)
- ▶ LLC : Logical Link Control (IEEE 802.2)

La couche Data Link définit le LAN (Local Area Network)

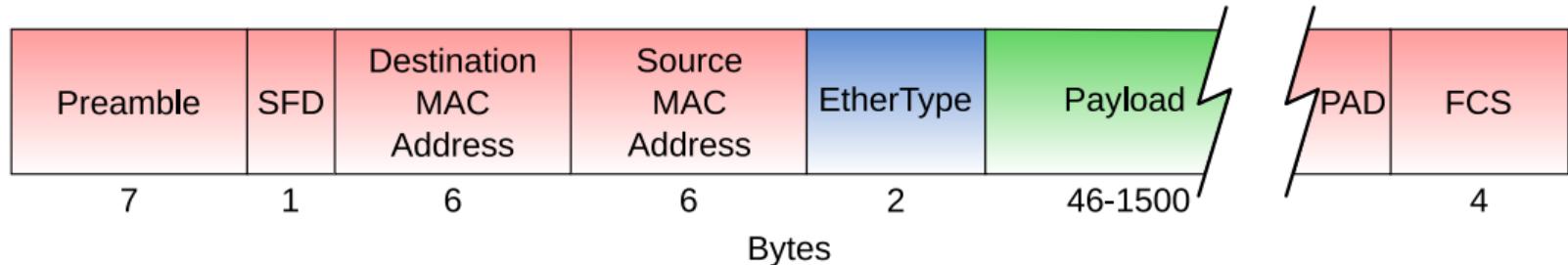
2 nœuds appartiennent au même LAN :

- ▶ s'ils peuvent communiquer directement par des protocoles de niveau 2.
- ▶ on dit qu'ils sont dans le même « domaine de diffusion »

Pour Ethernet : 2 formats co-existent :

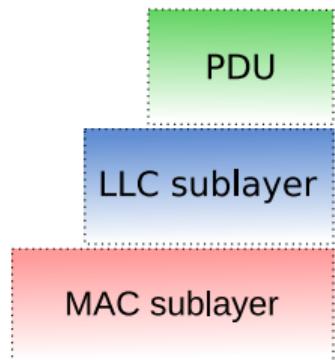
- ▶ IEEE 802.3
- ▶ Ethernet DIX = Ethernet II <- standard de fait

Trame Ethernet (Frame)



- ▶ Preamble : $7 \times 0xAA = 10101\dots10$ (56 bits)
- ▶ Start Frame Delimiter (SFD) : $0xAB = 10101011$
- ▶ EtherType : code for layer 3 protocol
- ▶ PAD : 0 padding to exceed 46 bytes payload length
- ▶ Frame Check Sequence (FCS) : CRC32 Error detection

Legend:

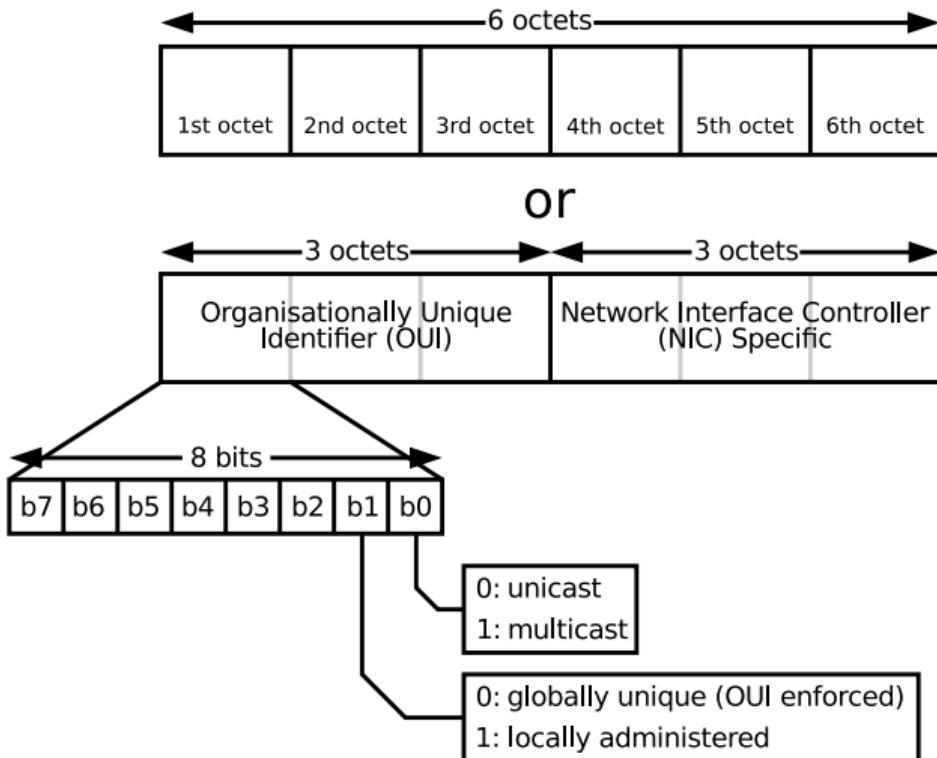


EtherType (Hors standard IEEE 802.3 !)

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN
0x8035	Reverse Address Resolution Protocol (RARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x86DD	Internet Protocol Version 6 (IPv6)
0x8870	Jumbo frames (proposed)
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet

Valeurs assignées par Internet Assigned Numbers Authority (IANA)

MAC Address



Exemple :

48:51:b7:aa:05:1e

OUI : 48:51:b7

Base de donnée sur internet :

<http://standards-oui.ieee.org/oui/oui.txt>

<https://www.wireshark.org/tools/oui-lookup.html>

48-51-B7 (hex)	Intel Corporate
4851B7 (base 16)	Intel Corporate
	Lot 8, Jalan Hi-Tech 2/3
	Kulim Kedah 09000
	MY

Broadcast address (*adresse de diffusion*) :
ff:ff:ff:ff:ff:ff

Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

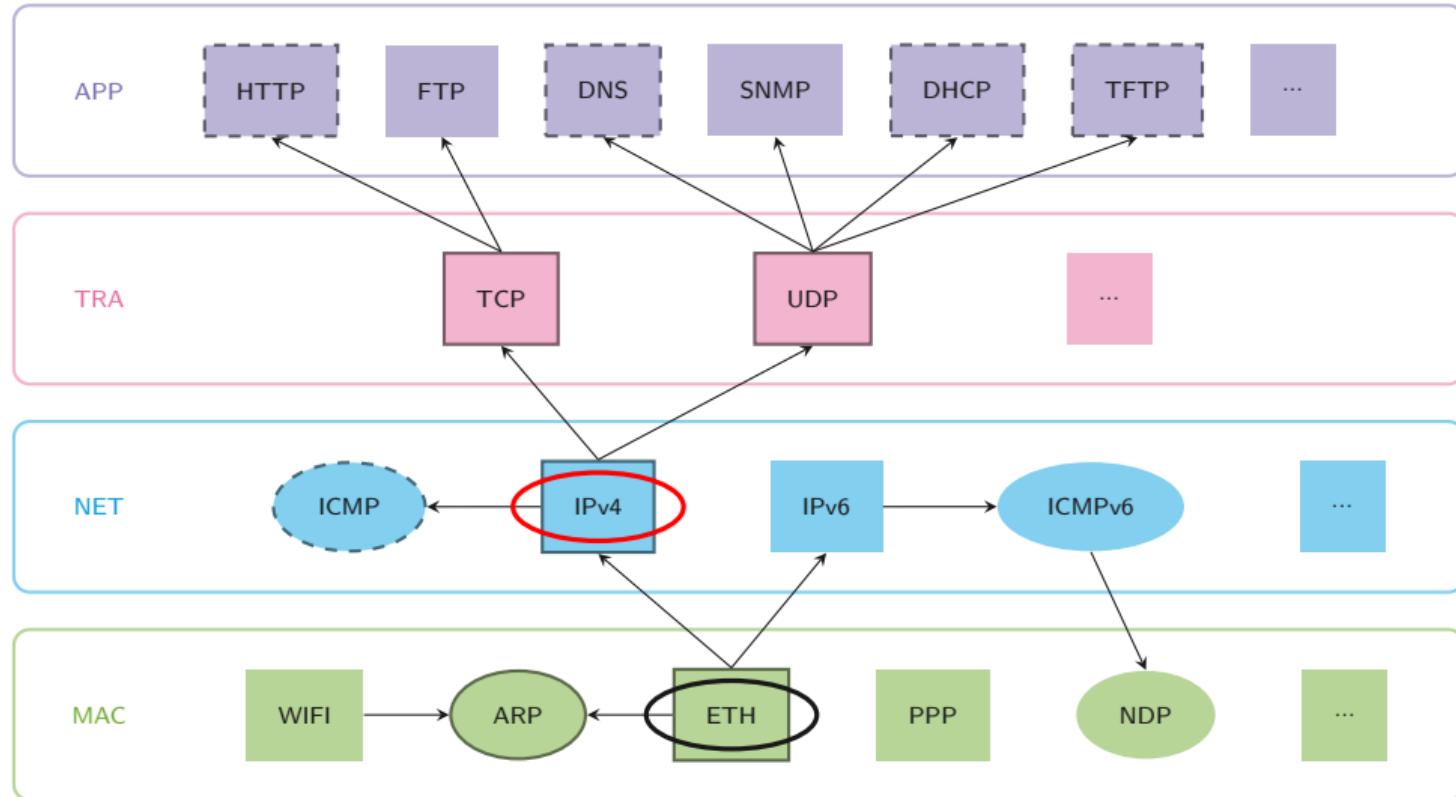
Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

TCP/IP Stack



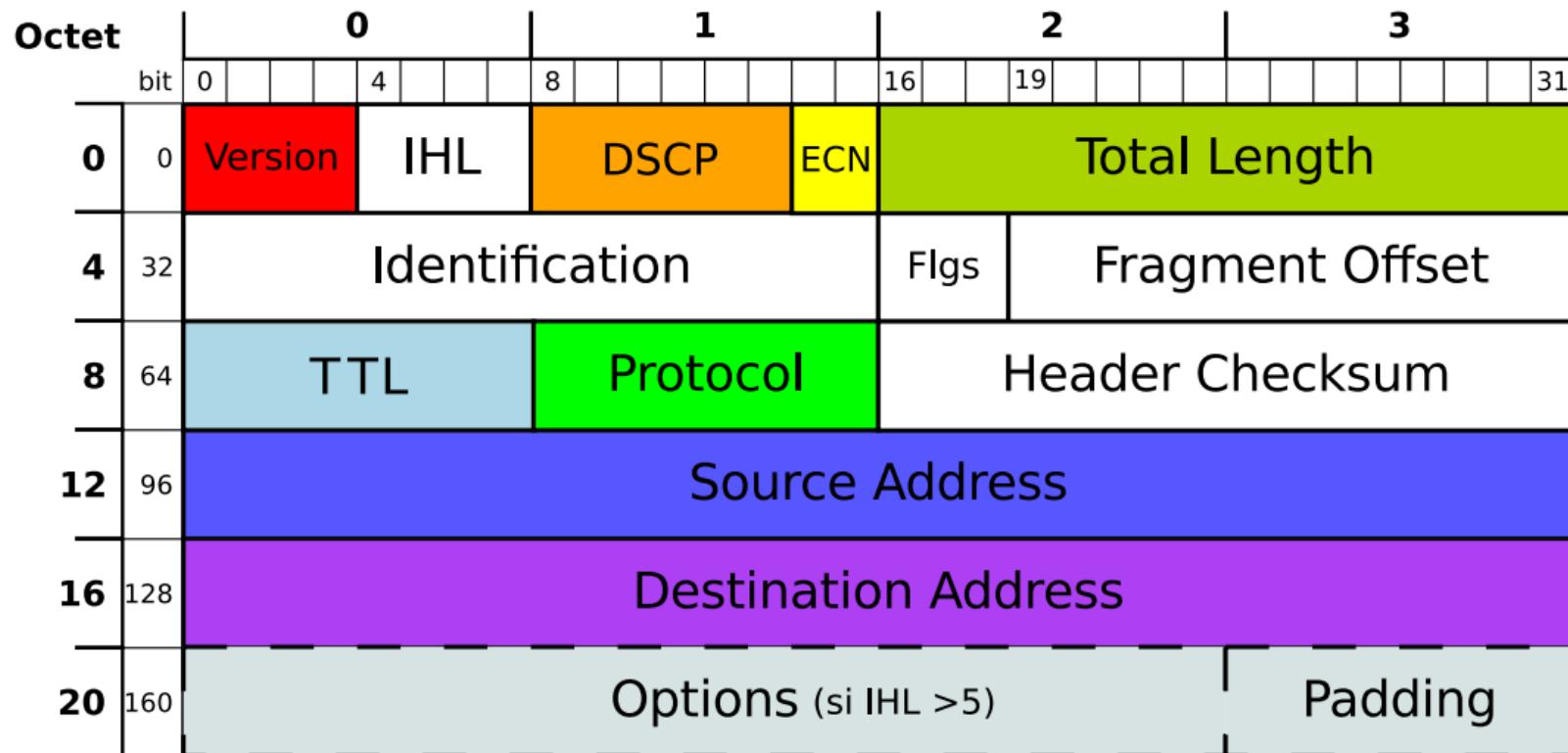
Internet Protocol version 4 (IPv4)

- ▶ RFC 791 (Septembre 1981)
- ▶ Apporte une abstraction de la couche MAC.
- ▶ Permet de sortir du LAN -> Routage Inter-net
- ▶ C'est le protocole le plus utilisés au niveau 3
- ▶ Mais c'est un protocole en bout de course (-> IPv6).

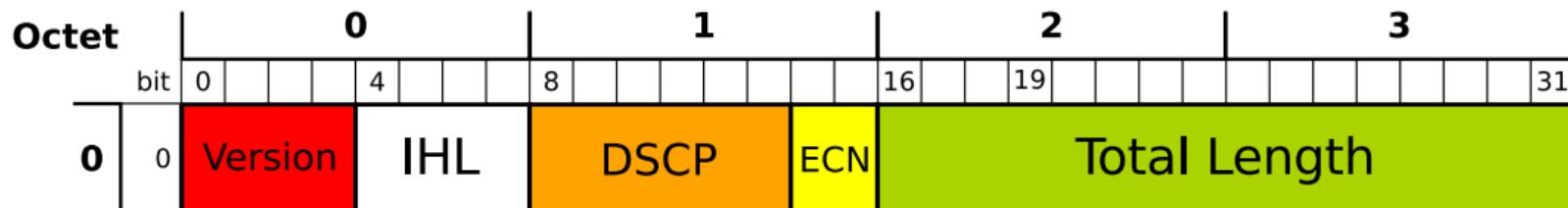
Entête :

- ▶ de 20 à 60 octets = 160 à 480 bits
- ▶ 14 champs dont 13 obligatoires

IPv4 Header



IPv4 Header - 1st Word



Version (4 bits) toujours fixé à 0100 (4)

IHL (4 bits) Internet Header Length

Nombre de mot de 32 bits dans l'entête :

vaut en général 5 sauf si Options (max 15, donc 60 octets)

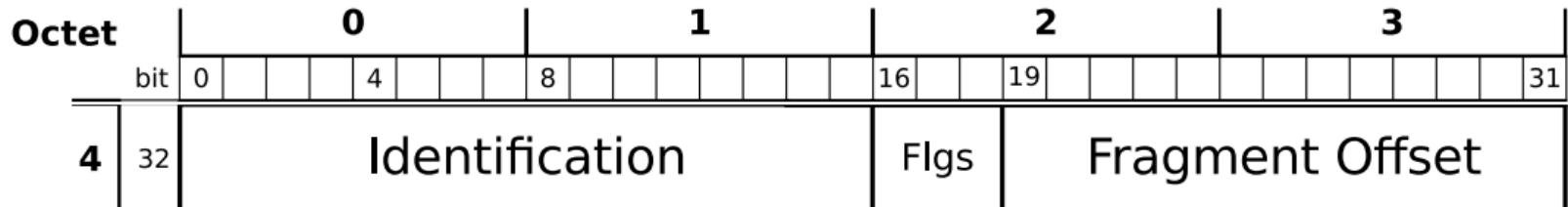
DSCP (6 bits) Differentiated Services Code Point (QoS)

ECN (2 bits) Explicit Congestion Notification (QoS)

Total Length (16 bits) Taille total du paquet en octets, Header+Data

Min : 20B (no Data) Max : 65535B

IPv4 Header - 2nd Word - Fragmentation system



Identification (16 bits) identifiant du paquet d'origine

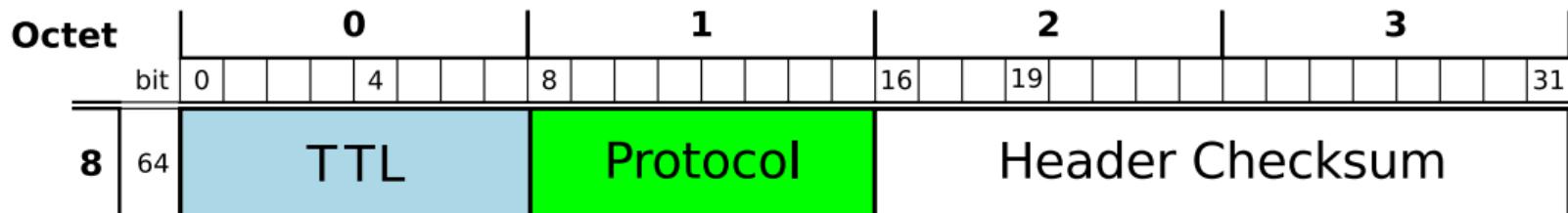
Flags (3 bits) bit 0 : réservé, fixé à 0

bit 1 : Don't Fragment (DF)

bit 2 : More Fragments (MF)

Fragments Offset (13 bits) décalage du fragment en unité de 8 octets

IPv4 Header - 3rd Word



TTL (8 bits) Time To Live

Champs réduit de 1 à chaque routeur traversé (hop count)

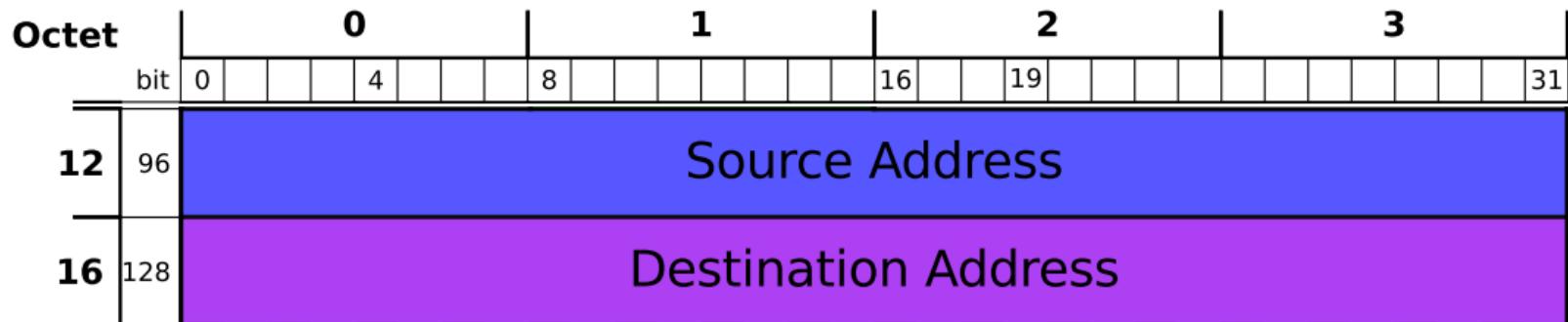
Le paquet est détruit si TTL=0 (+ ICMP)

Protocol (8 bits) Code du protocole de niveau 3 encapsulé (IANA)

Header Checksum (16 bits) Somme de contrôle calculée sur tout le header

Doit être recalculer à chaque changement ! (TTL)

IPv4 Header - Words 4 & 5



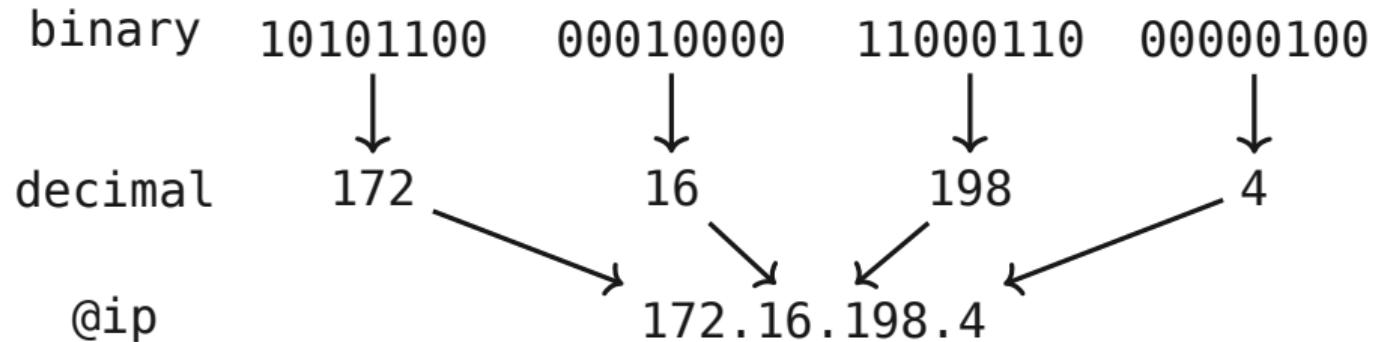
Adresses logiques de l'expéditeur et du destinataire.

Champs fondamentaux pour le routage inter réseau.

Elles doivent être uniques sur le réseau public (ou local).

Adresses IPv4

Codées sur 32 bits, mais écrite en notation décimale pointée, par groupe de 8 bits



Cette représentation permet d'avoir 4 294 967 296 (2^{32}) adresses différentes.

Masque de sous-réseau

Le masque permet de retrouver le NET_ID à partir d'une IP.

Il est donné sous en notation décimale pointé : par exemple 255.255.224.0

The mask allows to retrieve the NET_ID from an IP.

It is given in dotted decimal notation : for example 255.255.224.0

IP address : 172.16.198.4 → 10101100 00010000 11000110 00000100

L'adresse IP 172.16.198.4, associée au masque de sous-réseau 255.255.224.0, appartient au réseau 172.16.192.0.

Masque de sous-réseau

Le masque permet de retrouver le NET_ID à partir d'une IP.

Il est donné sous en notation décimale pointé : par exemple 255.255.224.0

The mask allows to retrieve the NET_ID from an IP.

It is given in dotted decimal notation : for example 255.255.224.0

IP address : 172.16.198.4	→	10101100	00010000	11000110	00000100
& netmask : 255.255.224.0	→	11111111	11111111	11100000	00000000

L'adresse IP 172.16.198.4, associée au masque de sous-réseau 255.255.224.0, appartient au réseau 172.16.192.0.

Masque de sous-réseau

Le masque permet de retrouver le NET_ID à partir d'une IP.

Il est donné sous en notation décimale pointé : par exemple 255.255.224.0

The mask allows to retrieve the NET_ID from an IP.

It is given in dotted decimal notation : for example 255.255.224.0

IP address : 172.16.198.4	→	10101100	00010000	11000110	00000100
& netmask : 255.255.224.0	→	11111111	11111111	11100000	00000000
=		10101100	00010000	11000000	00000000

L'adresse IP 172.16.198.4, associée au masque de sous-réseau 255.255.224.0, appartient au réseau 172.16.192.0.

Masque de sous-réseau

Le masque permet de retrouver le NET_ID à partir d'une IP.

Il est donné sous en notation décimale pointé : par exemple 255.255.224.0

The mask allows to retrieve the NET_ID from an IP.

It is given in dotted decimal notation : for example 255.255.224.0

IP address : 172.16.198.4 → 10101100 00010000 11000110 00000100

& netmask : 255.255.224.0 → 11111111 11111111 11100000 00000000

= NET address : 172.16.192.0 ← 10101100 00010000 11000000 00000000

Masque de sous-réseau

Le masque permet de retrouver le NET_ID à partir d'une IP.

Il est donné sous en notation décimale pointé : par exemple 255.255.224.0

The mask allows to retrieve the NET_ID from an IP.

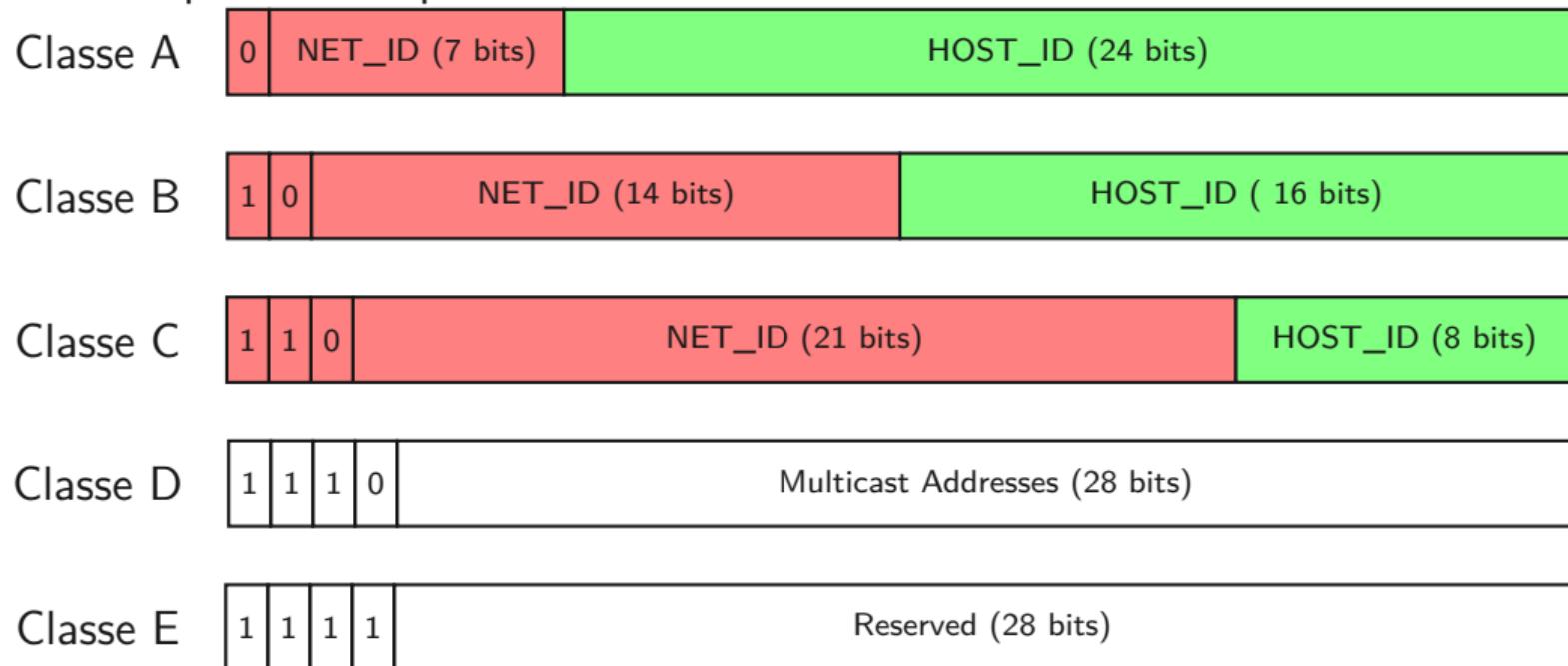
It is given in dotted decimal notation : for example 255.255.224.0

IP address : 172.16.198.4	→	10101100	00010000	11000110	00000100
& netmask : 255.255.224.0	→	11111111	11111111	11100000	00000000
<hr/>					
= NET address : 172.16.192.0	←	10101100	00010000	11000000	00000000

L'adresse IP 172.16.198.4, associée au masque de sous-réseau 255.255.224.0, appartient au réseau 172.16.192.0.

Classes d'adresse IP (obsolète : 1981–1993)

Les masques sont implicitement déduits des adresses IP :



Classes d'adresse IP (obsolète : 1981-1993)

Class	IP Range	Netmask	Mask 1's count	max nodes count
A	0. – 127.	255.0.0.0	8	$2^{24} - 2$
B	128. – 191.	255.255.0.0	16	$2^{16} - 2$
C	192. – 223.	255.255.255.0	24	$2^8 - 2$

-2 ?

Classes d'adresse IP (obsolète : 1981-1993)

Class	IP Range	Netmask	Mask 1's count	max nodes count
A	0. – 127.	255.0.0.0	8	$2^{24} - 2$
B	128. – 191.	255.255.0.0	16	$2^{16} - 2$
C	192. – 223.	255.255.255.0	24	$2^8 - 2$

-2 ?

- ▶ HOST_ID = 0 ("All-Zeros" address) reserved as network address
- ▶ HOST_ID = 1...1₂ ("All-Ones" address) reserved for broadcast

Classless Inter-Domain Routing (CIDR)

De nos jours, tous les masques de réseau sont de la forme : 1...10...0
Il est donc plus simple de donner le nombre de 1 dans le masque :

172.16.198.4 avec le masque 255.255.224.0

devient en notation CIDR :

172.16.198.4/19

Le nombre de 1 dans le masque de réseau est appelé : « préfixe »

Classless Inter-Domain Routing (CIDR)

De nos jours, tous les masques de réseau sont de la forme : 1...10...0
Il est donc plus simple de donner le nombre de 1 dans le masque :

172.16.198.4 avec le masque 255.255.224.0

devient en notation CIDR :

172.16.198.4/19

Le nombre de 1 dans le masque de réseau est appelé : « préfixe »

Avantages :

La taille du masque est facilement variable :

Un réseau peut avoir n'importe quelle taille entre /8 et le /30

En pratique : Un établissement se voit affecter une taille de réseau,
l'administrateur peut créer autant de sous-réseau qu'il le souhaite.

Blocs d'adresses IP Réservées

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 6890
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 6890
169.254.0.0/16	link-local address Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 6890
192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5737
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255/32	Broadcast	RFC 919

Fragmentation et MTU (Maximum Transmission Unit)

Ethernet : MTU = 1500 (due to an old trade-off)

Avantages d'un grand MTU :

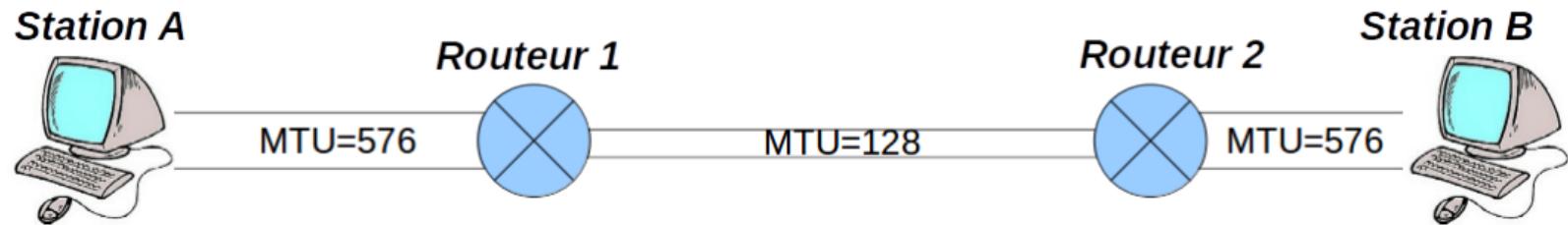
- ▶ Meilleur taux d'utilisation de la Liaison (PDU length/ Total Length)
- ▶ Moins de paquets à traiter (routage, filtrage)

Inconvénients :

- ▶ Partage de Bande Passante => lag
- ▶ En cas d'erreur => plus de données à réémettre

protocol	MTU	
Ethernet II	1500	
Ethernet Jumbo Frames	1501 - 9198	Utilitaire : tracepath - (tracecert on Windows)
ADSL ou ATM25	1468	
PPPoE	1492 (1500-8)	
WLAN (802.11)	7981	
FDDI	4352	

Fragmentation : exemple sur un réseau de MTU = 128

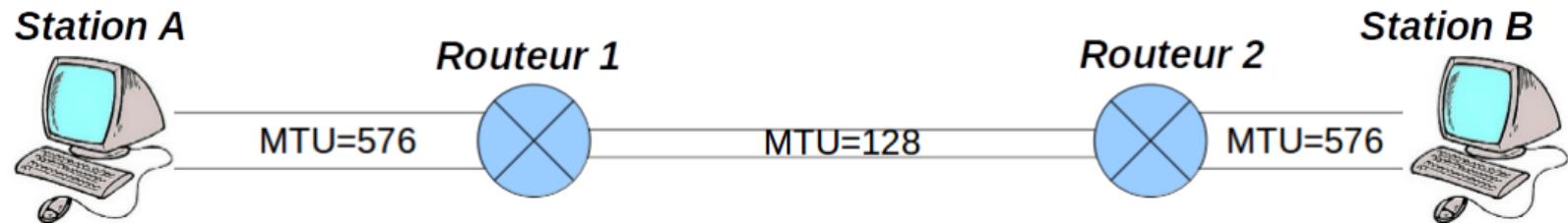


Que se passe-t-il quand la Station A envoie un paquet à la station B ?

Le paquet arrive au routeur 1, alors :

- ▶ Si $TL \leq 128 \Rightarrow$ le paquet est transmis au routeur 2 puis à B

Fragmentation : exemple sur un réseau de MTU = 128

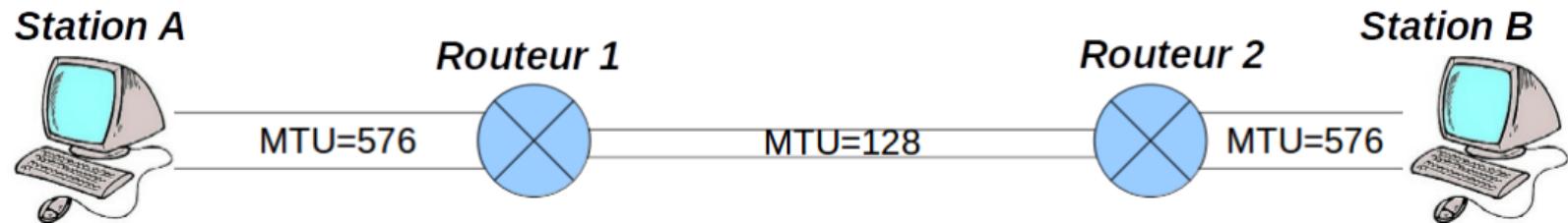


Que se passe-t-il quand la Station A envoie un paquet à la station B ?

Le paquet arrive au routeur 1, alors :

- ▶ Si $TL \leq 128 \Rightarrow$ le paquet est transmis au routeur 2 puis à B
- ▶ Si $TL > 128$ et $DF=1 \Rightarrow$ le routeur 1 détruit le paquet

Fragmentation : exemple sur un réseau de MTU = 128

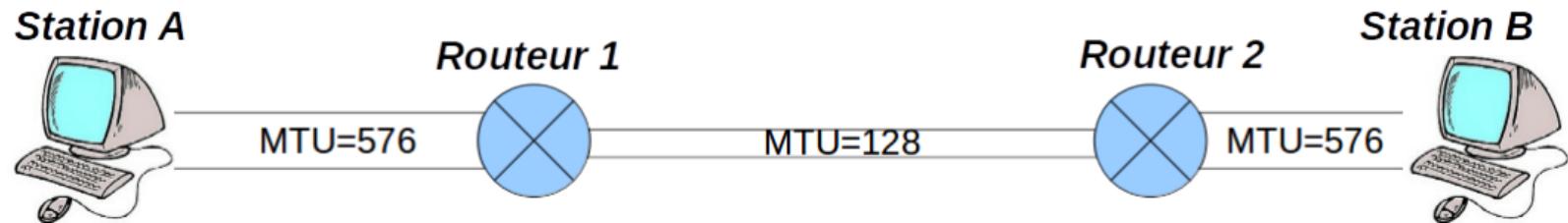


Que se passe-t-il quand la Station A envoie un paquet à la station B ?

Le paquet arrive au routeur 1, alors :

- ▶ Si $TL \leq 128 \Rightarrow$ le paquet est transmis au routeur 2 puis à B
- ▶ Si $TL > 128$ et $DF=1 \Rightarrow$ le routeur 1 détruit le paquet
- ▶ Si $TL > 128$ et $DF=0 \Rightarrow$ le routeur 1 fragmente le paquet

Fragmentation : exemple sur un réseau de MTU = 128



Que se passe-t-il quand la Station A envoie un paquet à la station B ?

Le paquet arrive au routeur 1, alors :

- ▶ Si $TL \leq 128 \Rightarrow$ le paquet est transmis au routeur 2 puis à B
- ▶ Si $TL > 128$ et $DF=1 \Rightarrow$ le routeur 1 détruit le paquet
- ▶ Si $TL > 128$ et $DF=0 \Rightarrow$ le routeur 1 fragmente le paquet

$MTU = 576 \Rightarrow data = 556B \text{ max}$ $MTU = 128 \Rightarrow data = 108B \text{ max}$

Routeur 1 va donc découper ces 556B en 5 fragments de 104B et un de 36B.

Taille maximum fragmentable ? MTU minimal pour utiliser le protocole IP ?

Protocoles défini par l'IANA

Protocol Number	Protocol Name	Abbreviation
0x01	Internet Control Message Protocol	ICMP
0x02	Internet Group Management Protocol	IGMP
0x04	IP in IP (encapsulation)	IP-in-IP
0x06	Transmission Control Protocol	TCP
0x11	User Datagram Protocol	UDP
0x29	IPv6 encapsulation	IPv6
0X59	Open Shortest Path First	OSPF

Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

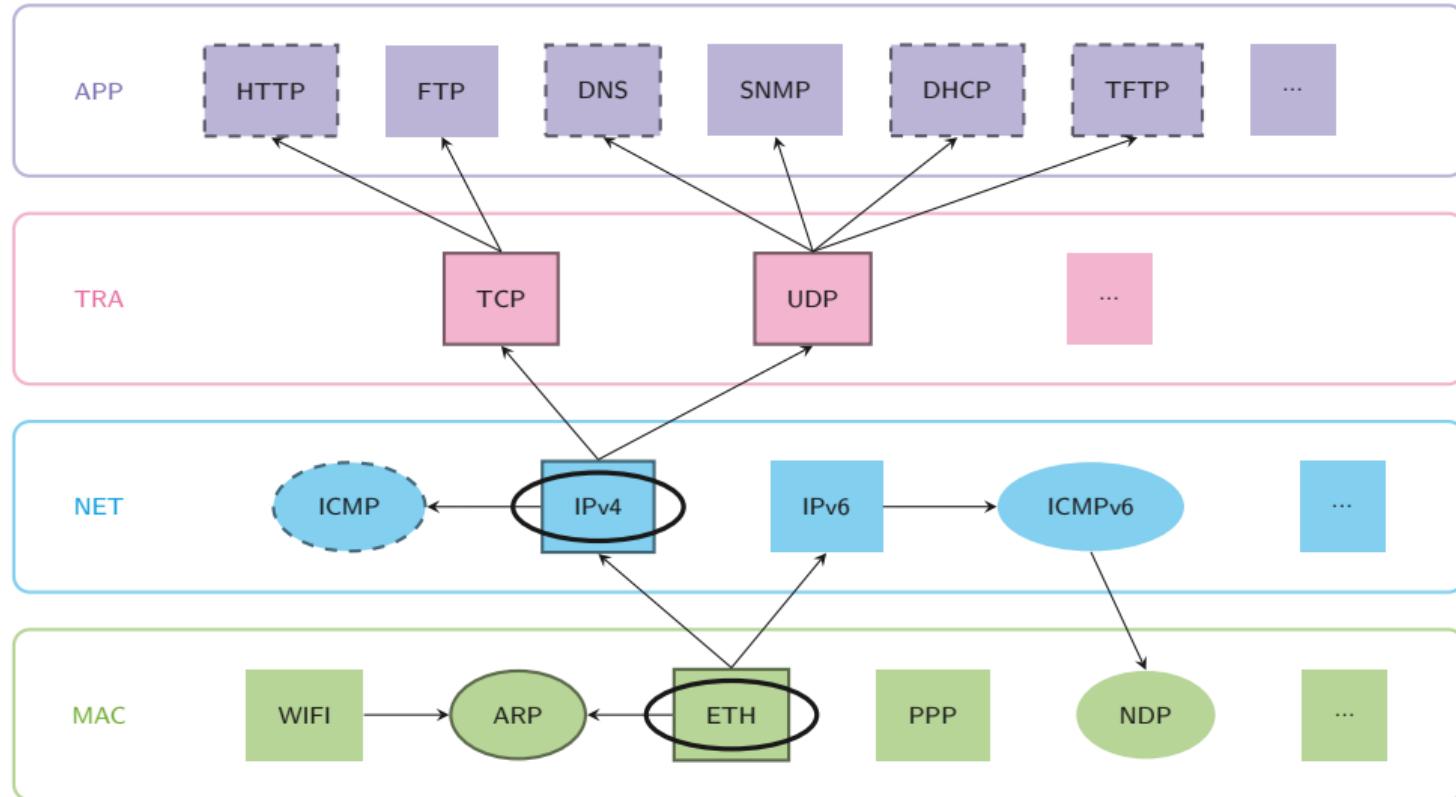
Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

TCP/IP Stack



Transport Layer

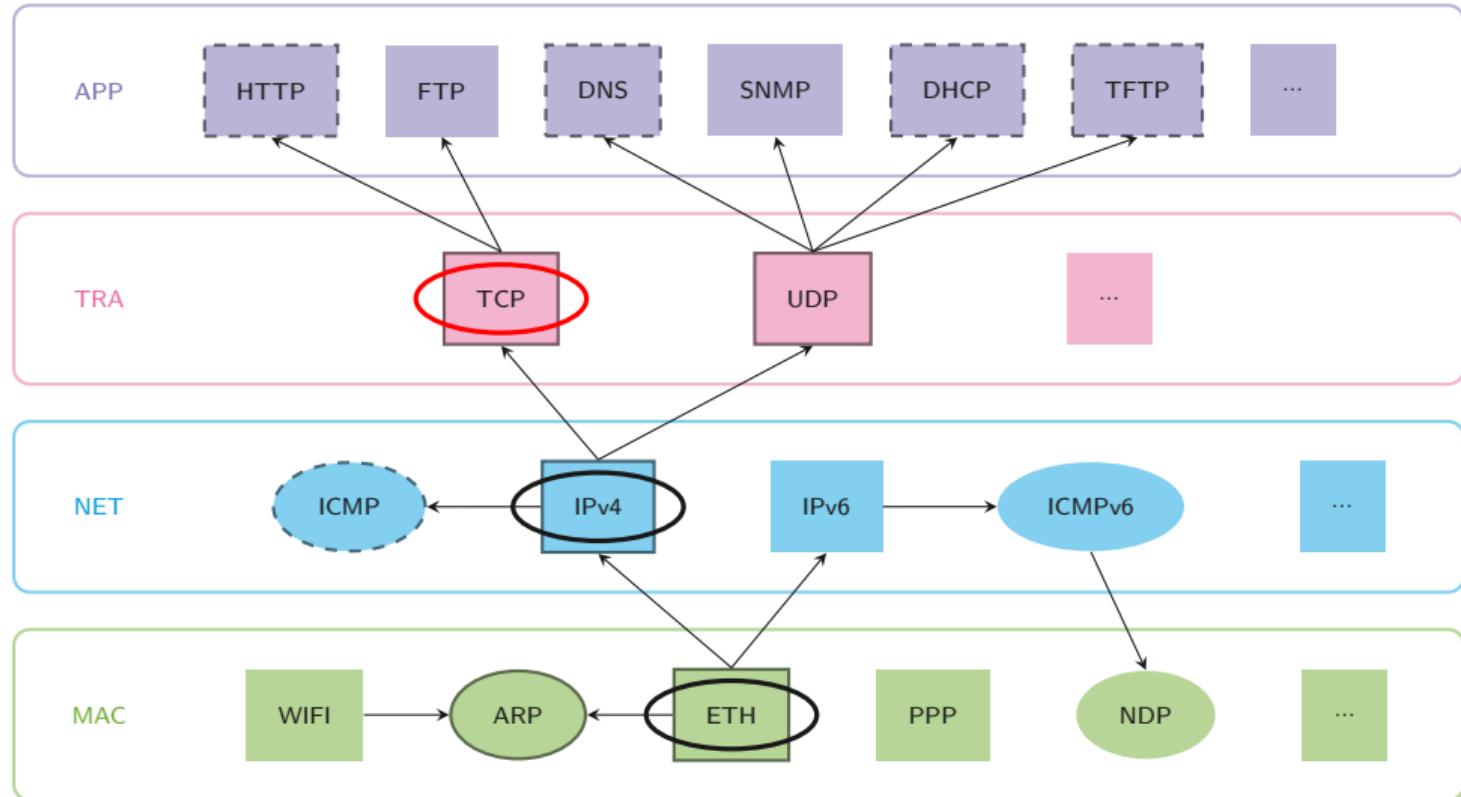
Gestion de la communication d'un hôte à l'autre :

- ▶ pertes de paquets,
- ▶ ordre d'arrivée,
- ▶ détection de doublon,
- ▶ détection d'erreurs,
- ▶ multiplexage,
- ▶ surcharge (congestion).

2 types :

- ▶ mode connecté (stream) : TCP, SCTP, QUIC...
- ▶ mode datagramme : UDP, RTP, DCCP...

TCP



TCP : Transmission Controlled Protocol

Défini en Septembre 1981 par le RFC 793

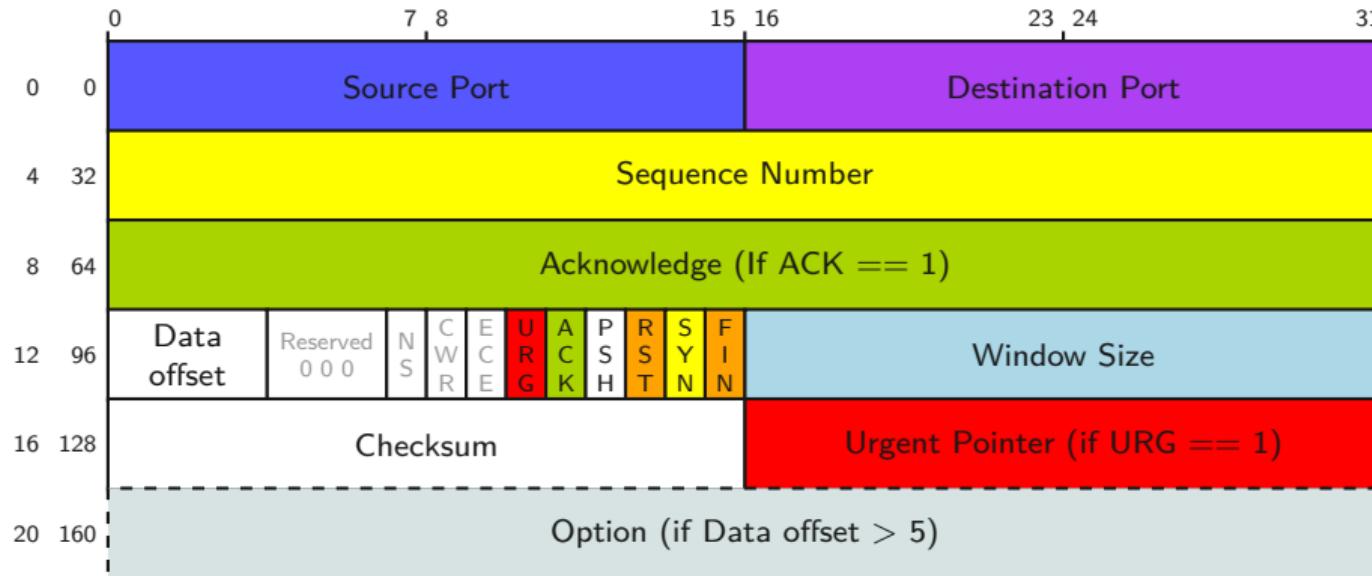
TCP garantit un flux d'octet (stream) :

- ▶ sans corruption,
- ▶ sans pertes,
- ▶ sans réordonnancement,
- ▶ sans duplication,
- ▶ sans engorgement.

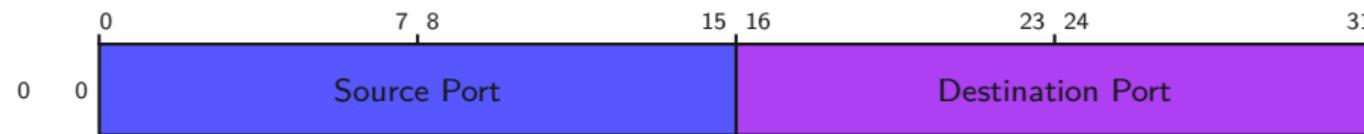
TCP est un protocole fiable mais lourd, pratiquement incontesté sur Internet.

Le principe de base est la numérotation des segments et l'acquittement.

TCP Header



TCP Header



Entiers 16 bits => [0, 65535]

Le port est comme un numéro de porte (de bureau).

« port » en anglais signifie « sabord »

Derrière chaque port(e) se trouve un service (un logiciel). Différentes catégories :

0 – 1023 Well-known ports : réservés au système (root)

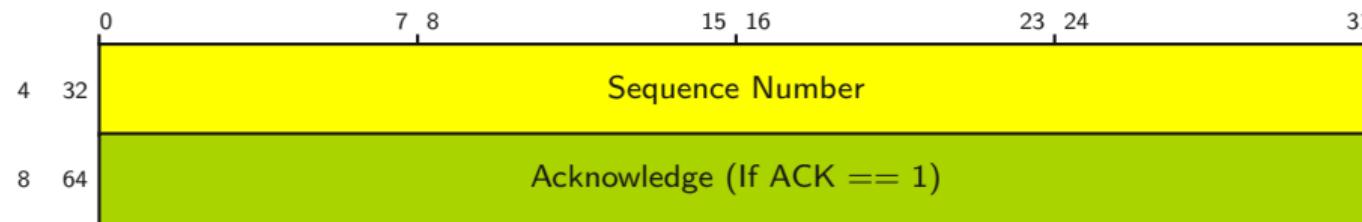
1024 – 32767 Registered ports : pour les applications utilisateurs

32768 – 65535 Dynamic or Private Ports : ports éphémères

TCP port name (IANA)

Port	Service
20/21	file exchange FTP
22	Secure SHell (SSH) and SFTP : secured distant login
23	Telnet : distant login
25	Simple Mail Transfer Protocol (SMTP) : sending mail
53	Domain name resolution (DNS)
67/68	ip address attribution(DHCP and bootpc)
80	web server HTTP
110	Post Office Protocol (POP) : receiving mail
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) : receiving mail
389	name directory (annuaire) (LDAP)
443	HTTP over TLS (HTTPS) : secured web server
465	SMTPTS : secured SMTP
636	LDAPS : secured LDAP
1723	Virtual private Network (VPN) PPTP
3306	database server MySQL
3389	remote control RDP
5432	database PostgreSQL
6667	messaging server Internet Relay Chat (IRC)

TCP Header



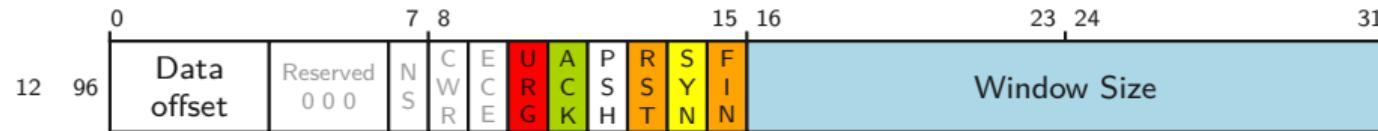
Entiers 32 bit => $[0, 2^{32} - 1]$

Numéro de séquence (seq) et d'acquittement (ack)

=> établissement et suivi de la connexion

Garantissent l'absence de pertes et de réordonnancement.

TCP Header



Data offset <=> IHL pour IP (nombre de mots de 32 bits dans l'entête)

URG Données urgentes (URGent) (obsolète)

ACK Le paquet transporte un accusé de réception (ACKnowledge)

PSH Données à transférer immédiatement aux couches supérieures (PuSH)

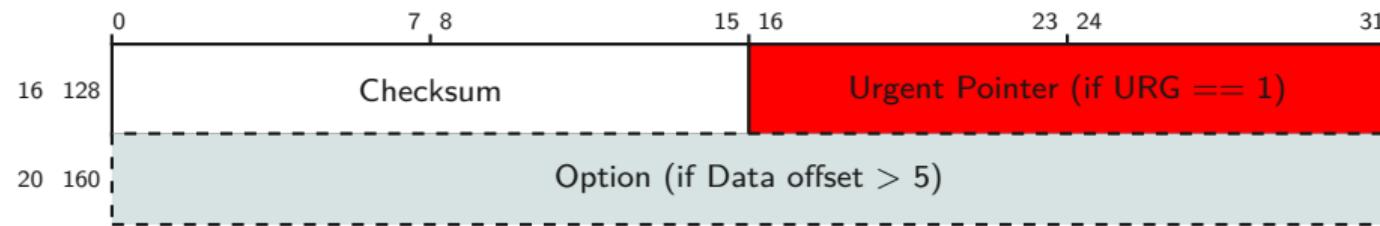
RST Réinitialiser la connexion (ReSeT)

SYN Établir une connexion (SYNchronize)

FIN Terminer la connexion, plus aucune donnée à envoyer (FINish)

Window size : Contrôle du flux (taille du buffer de reception)

TCP Header

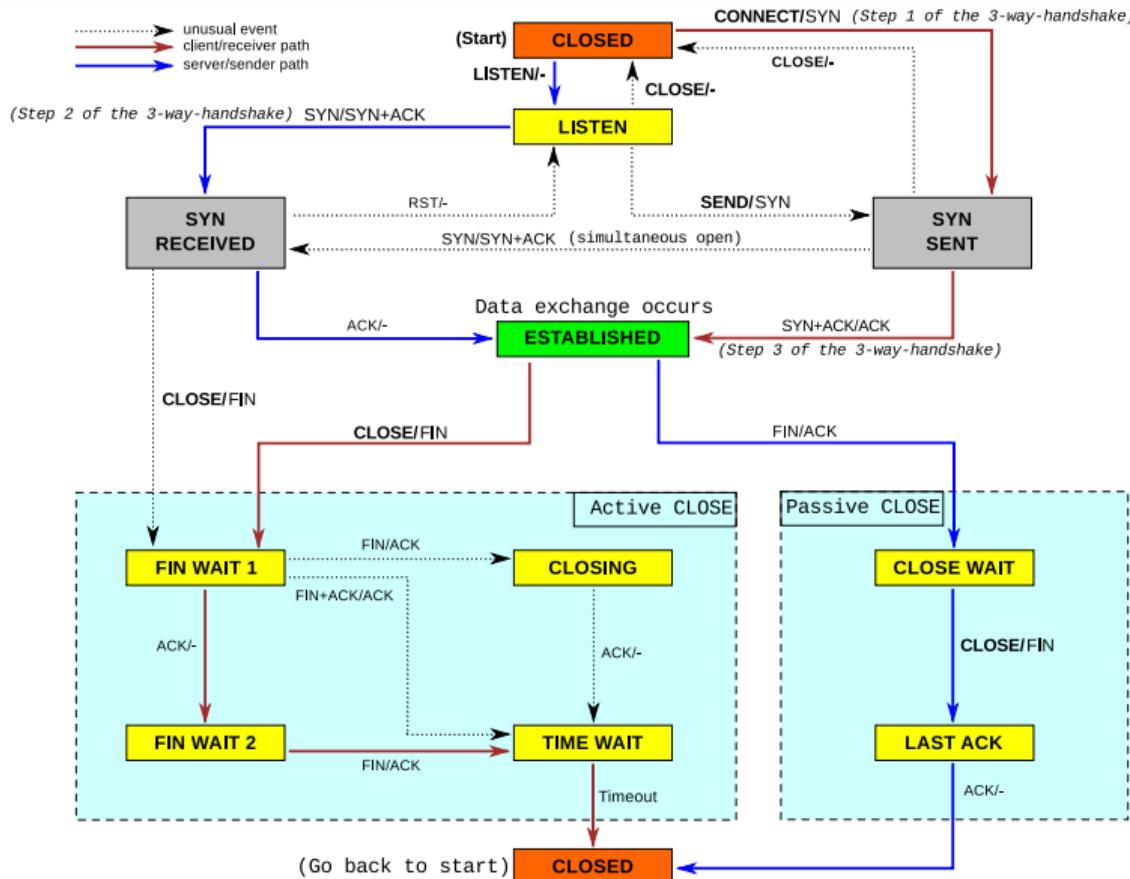


Checksum (16 bits) : Calculé sur TCP Header + PDU + éléments IP

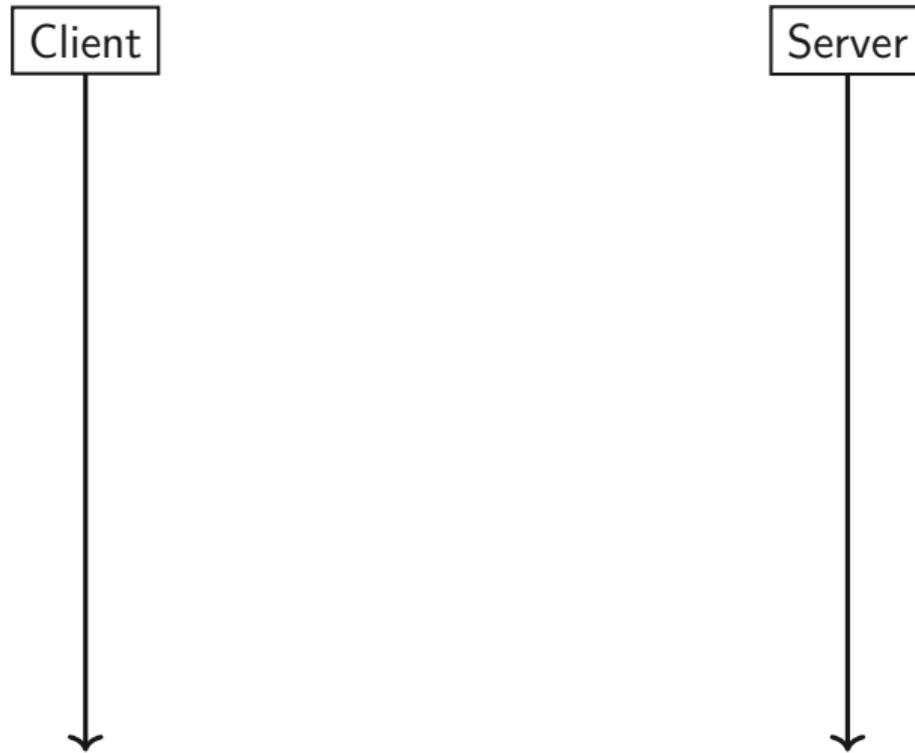
Urgent : obsolète

Options : MSS (Maximum Segment Size), TCP timestamp, Selective ACK...

TCP State Diagram



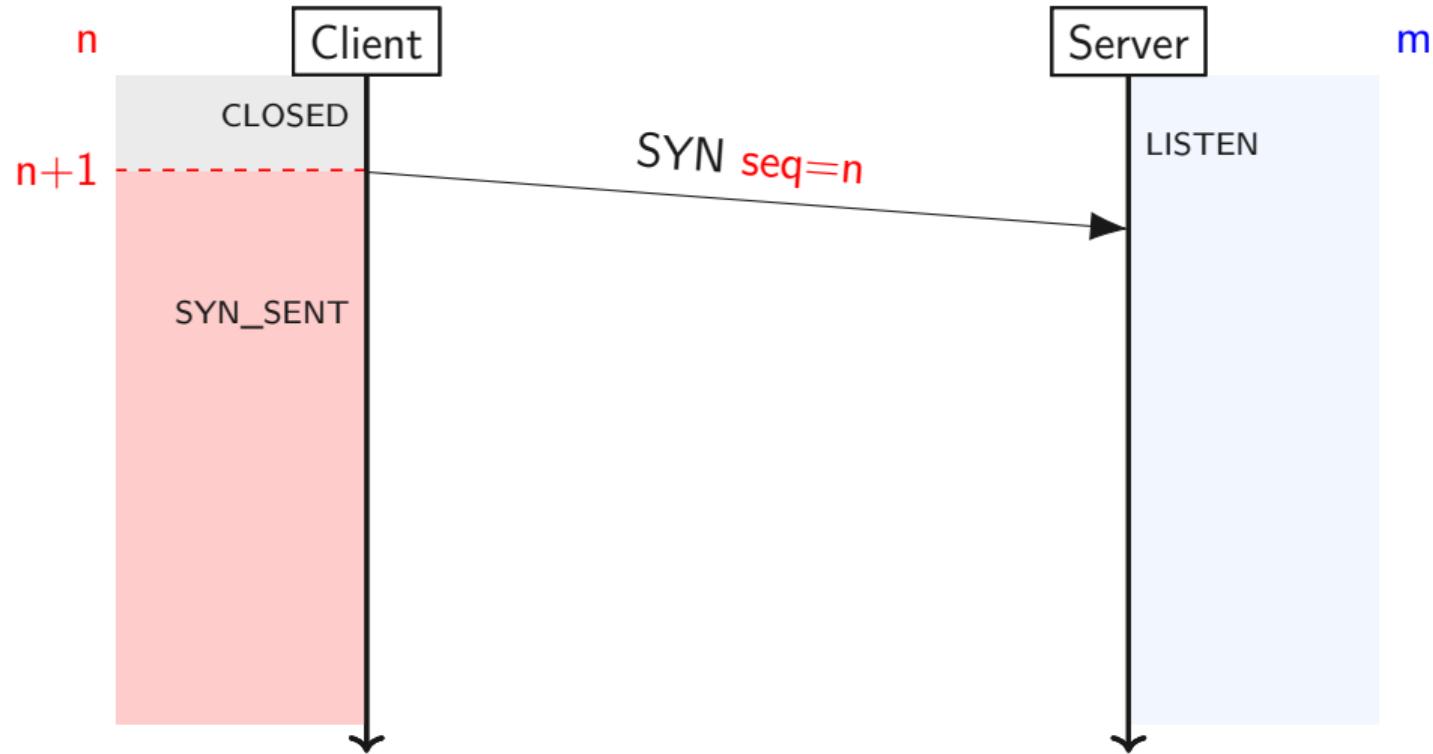
TCP Ouverture de session



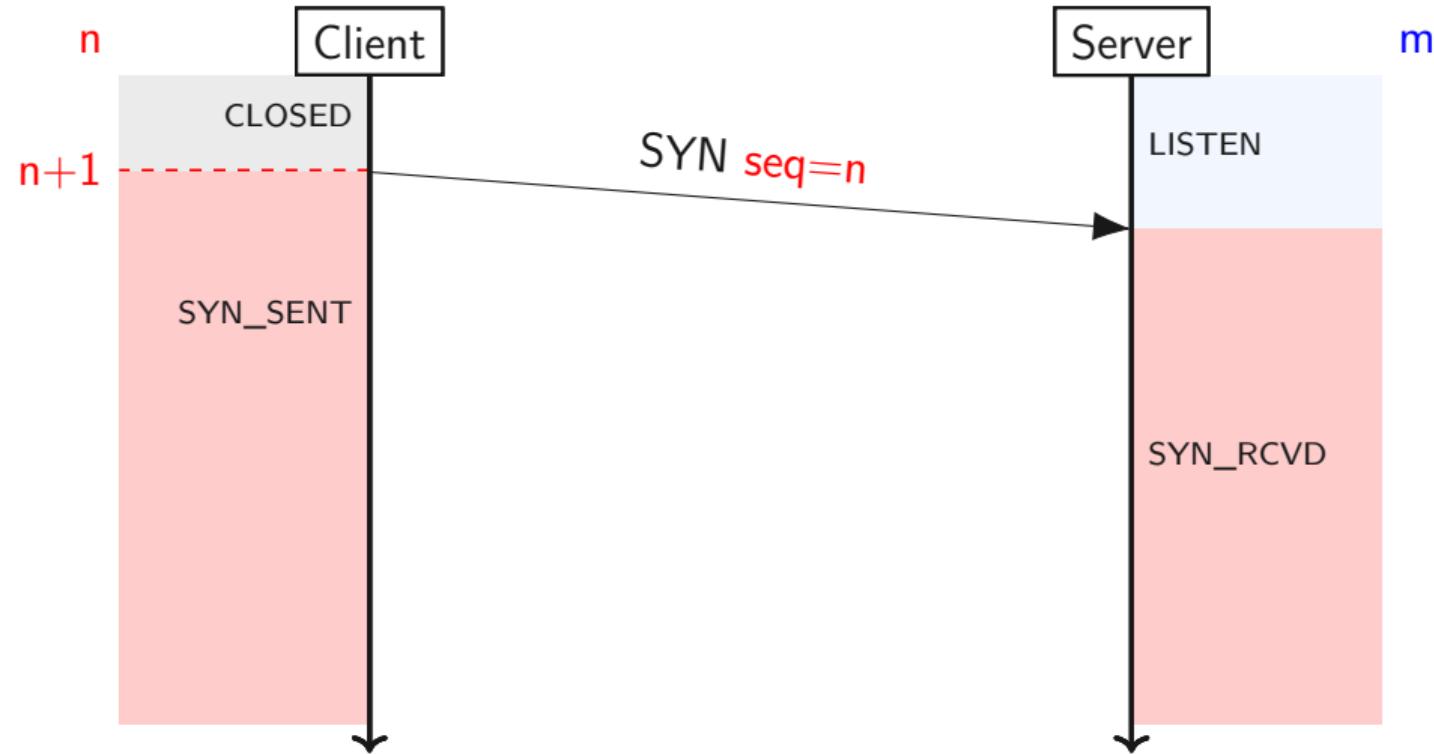
TCP Ouverture de session



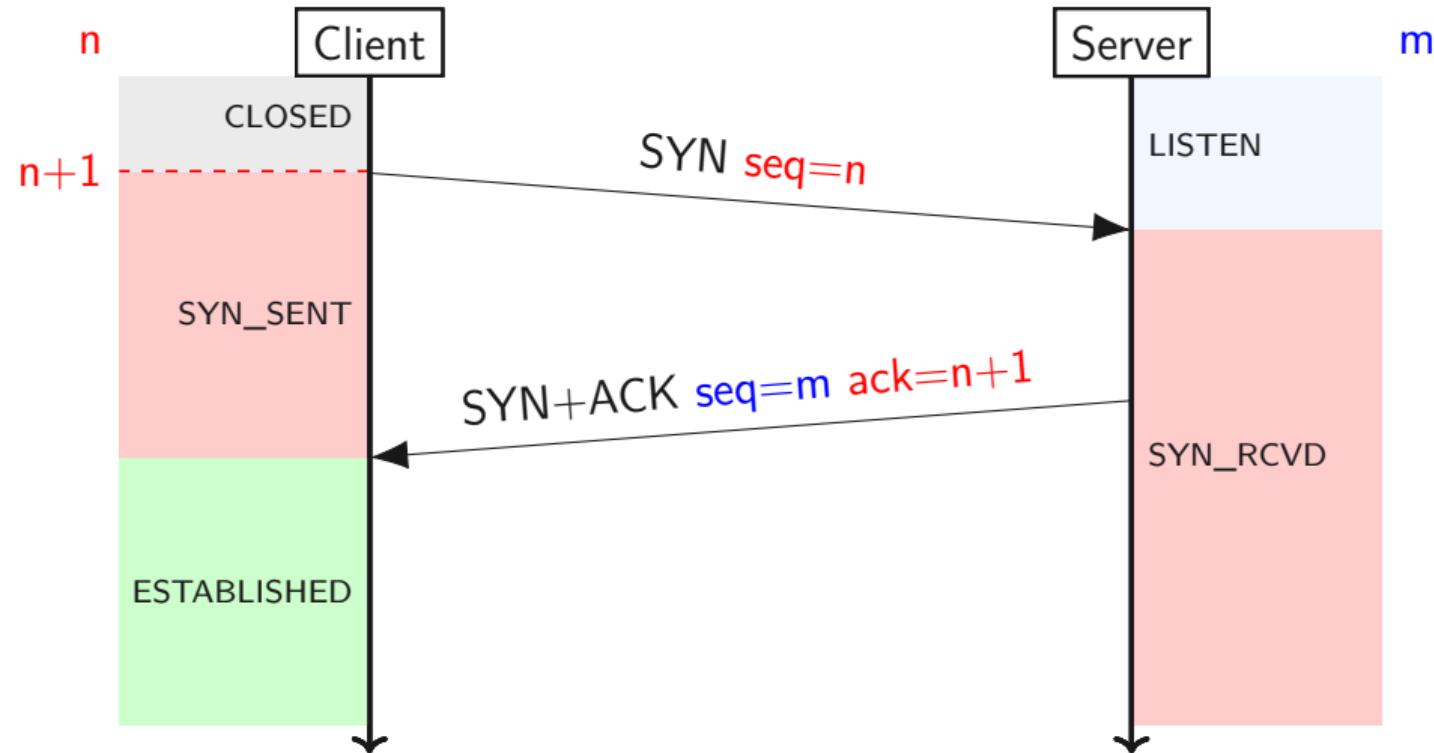
TCP Ouverture de session



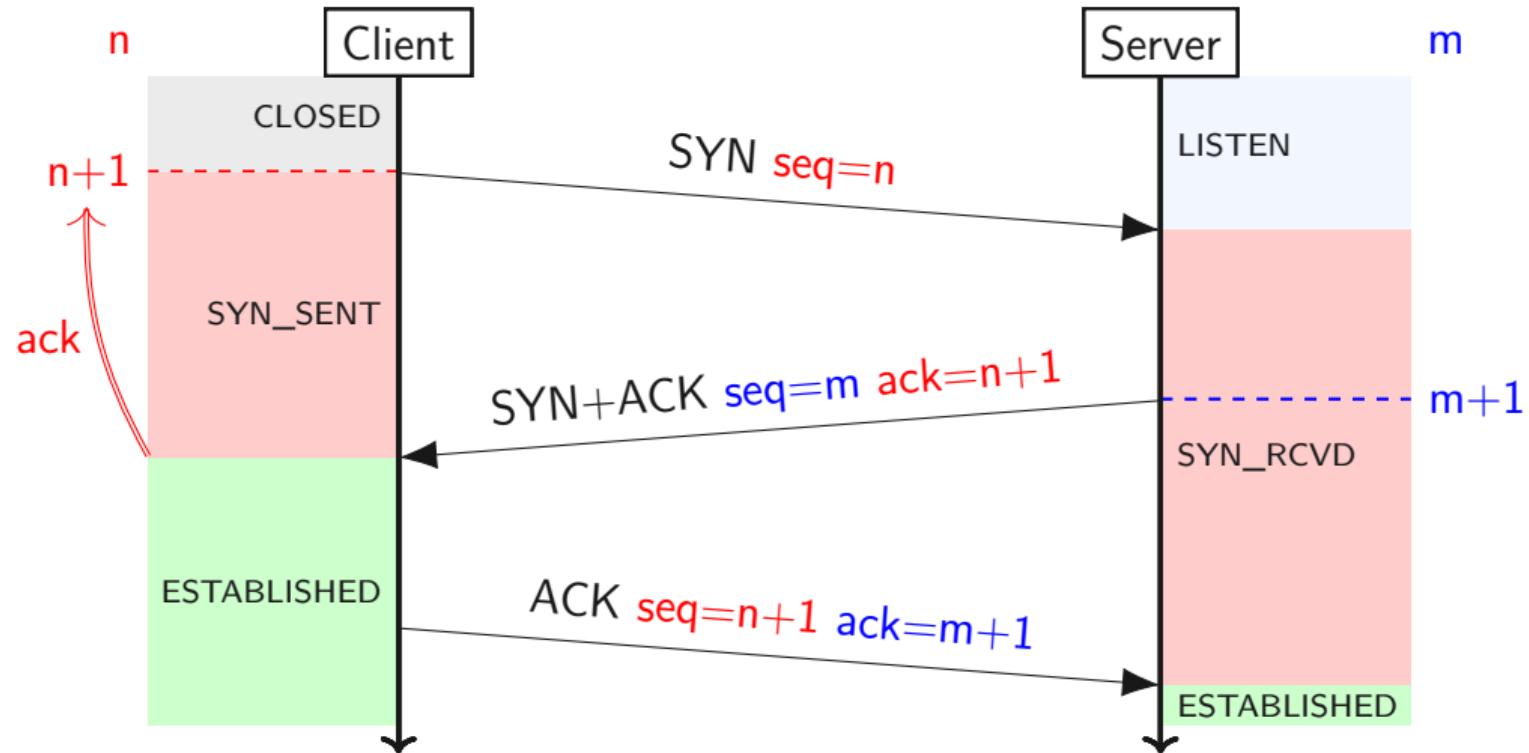
TCP Ouverture de session



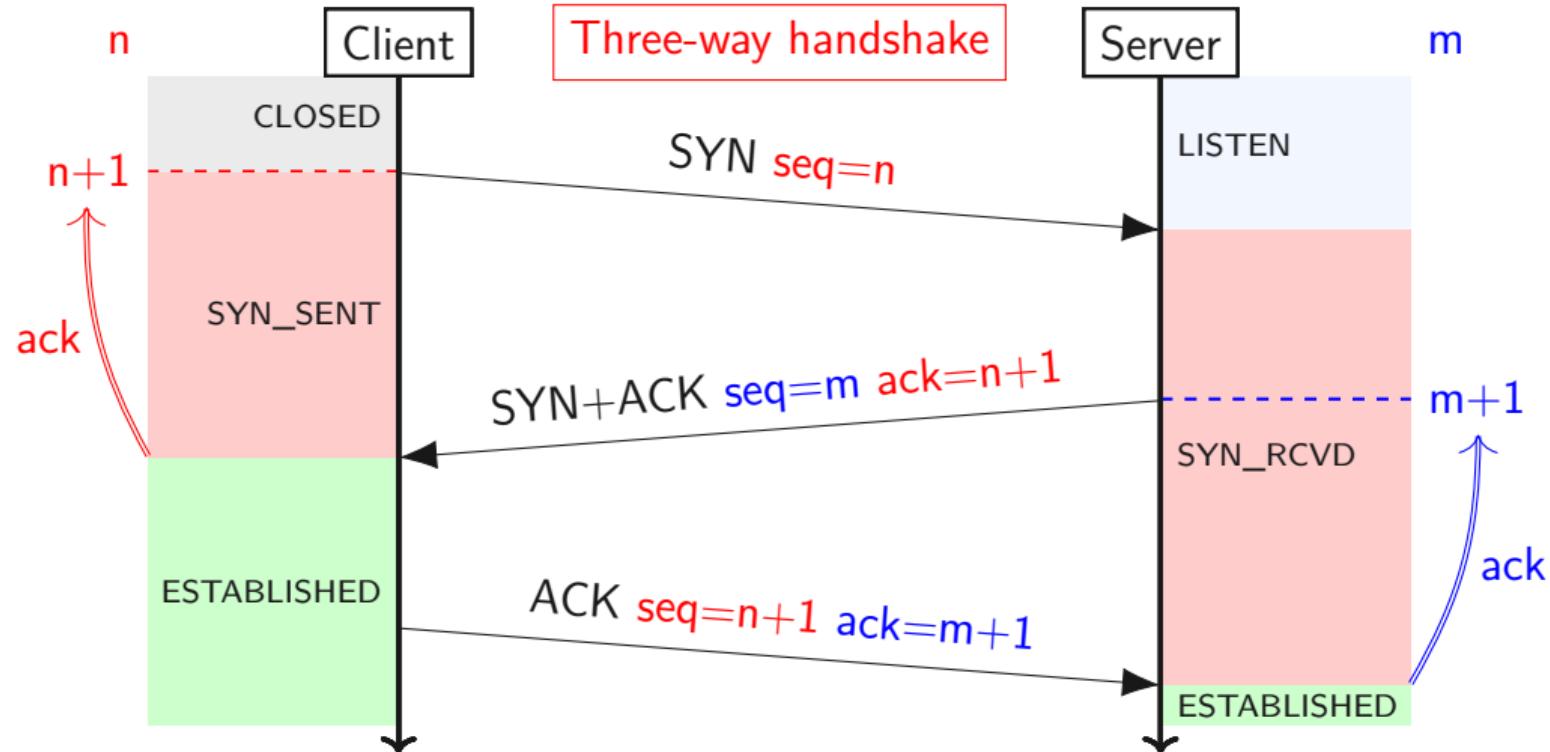
TCP Ouverture de session



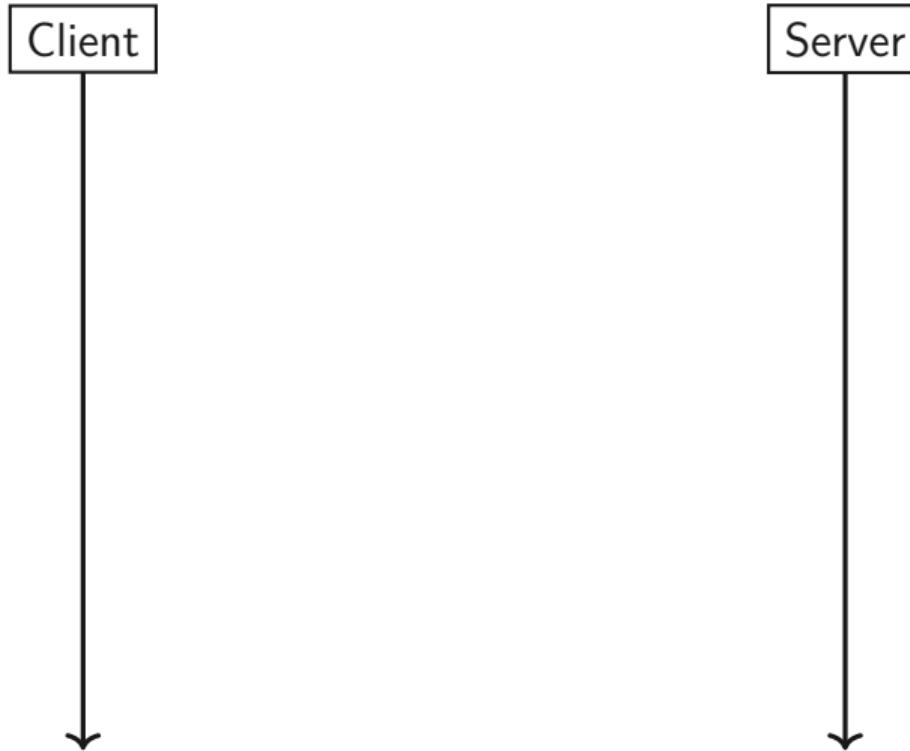
TCP Ouverture de session



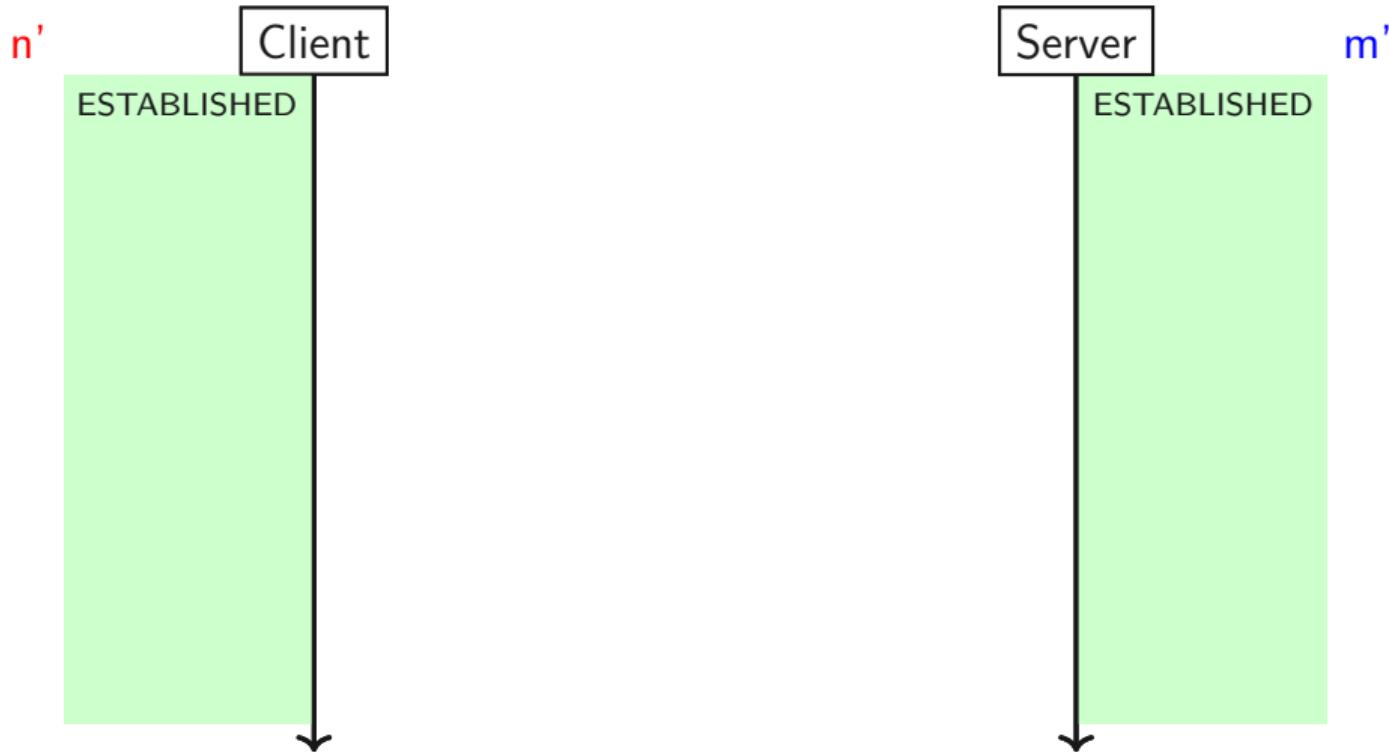
TCP Ouverture de session



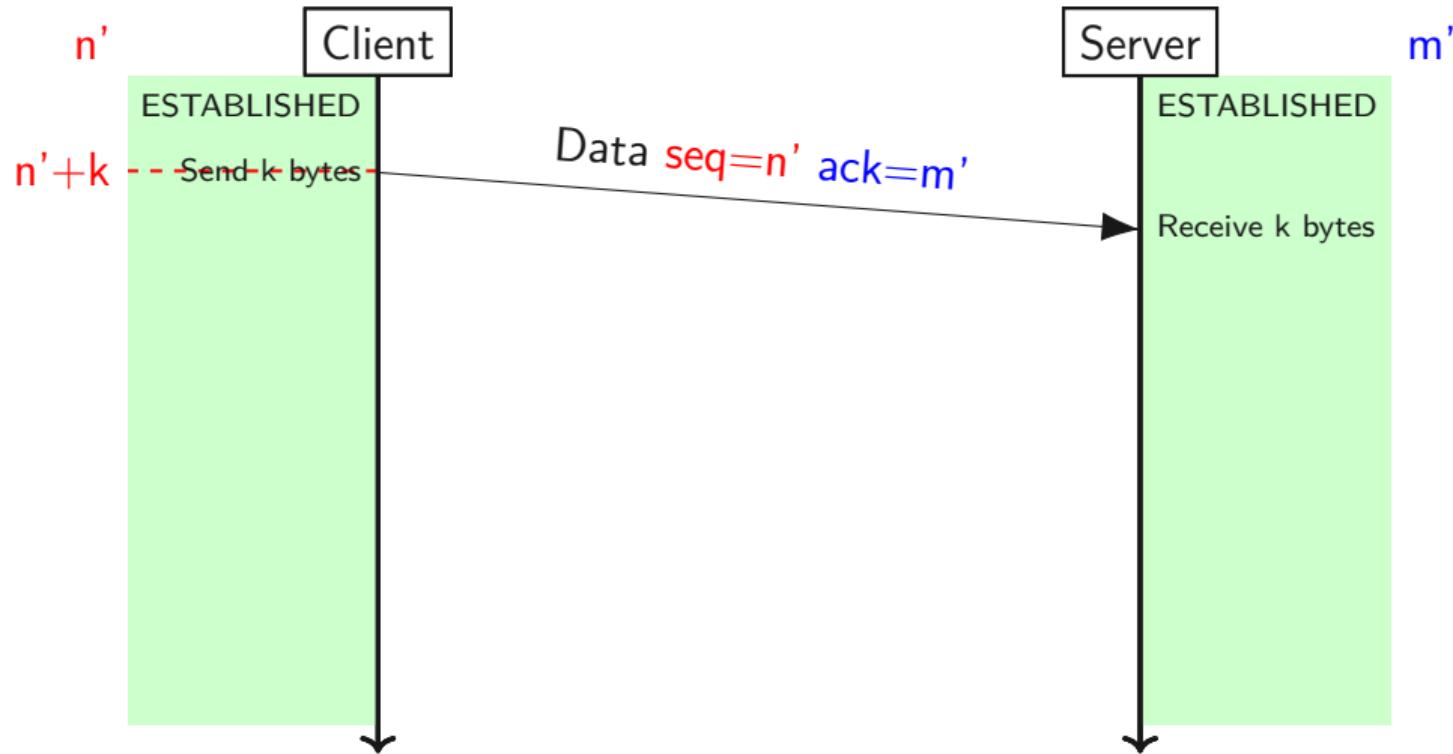
TCP Envoi de données – ACK simple



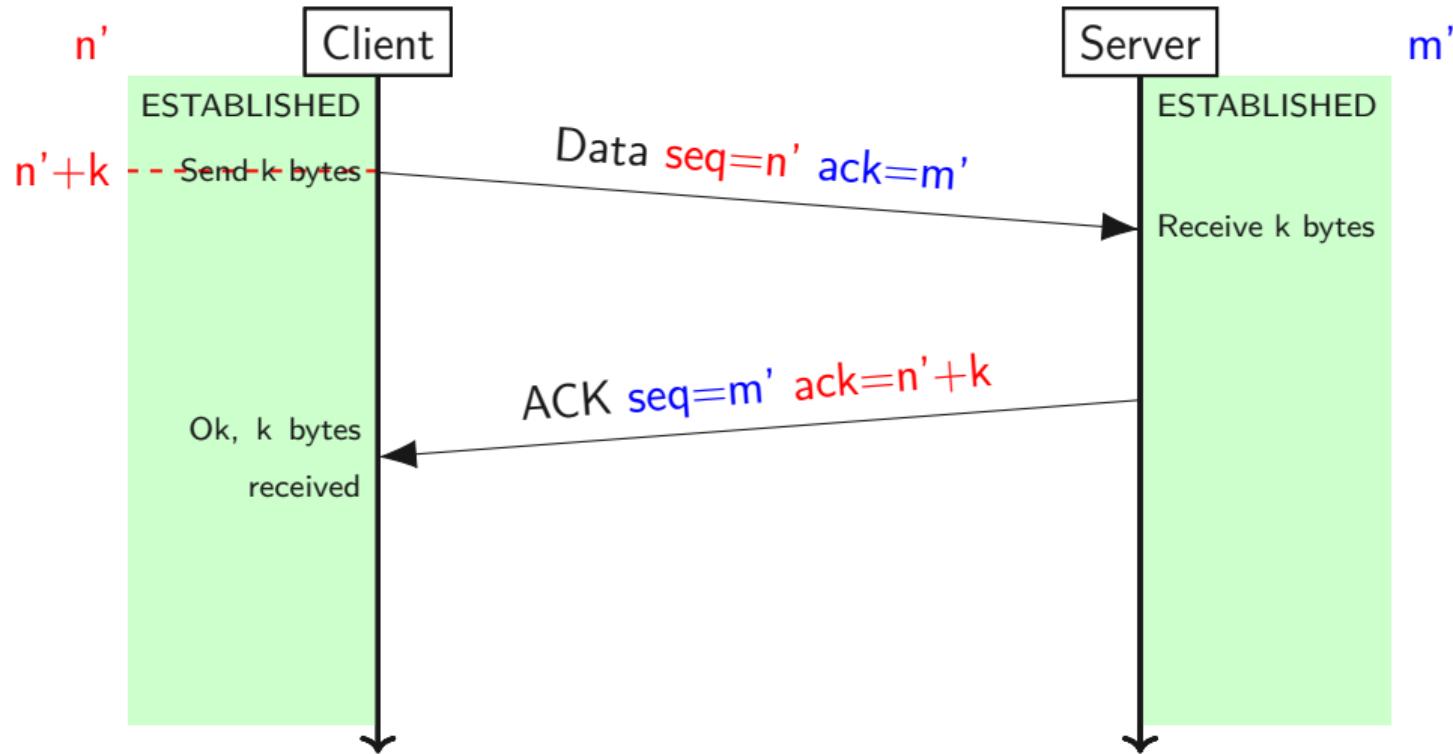
TCP Envoi de données – ACK simple



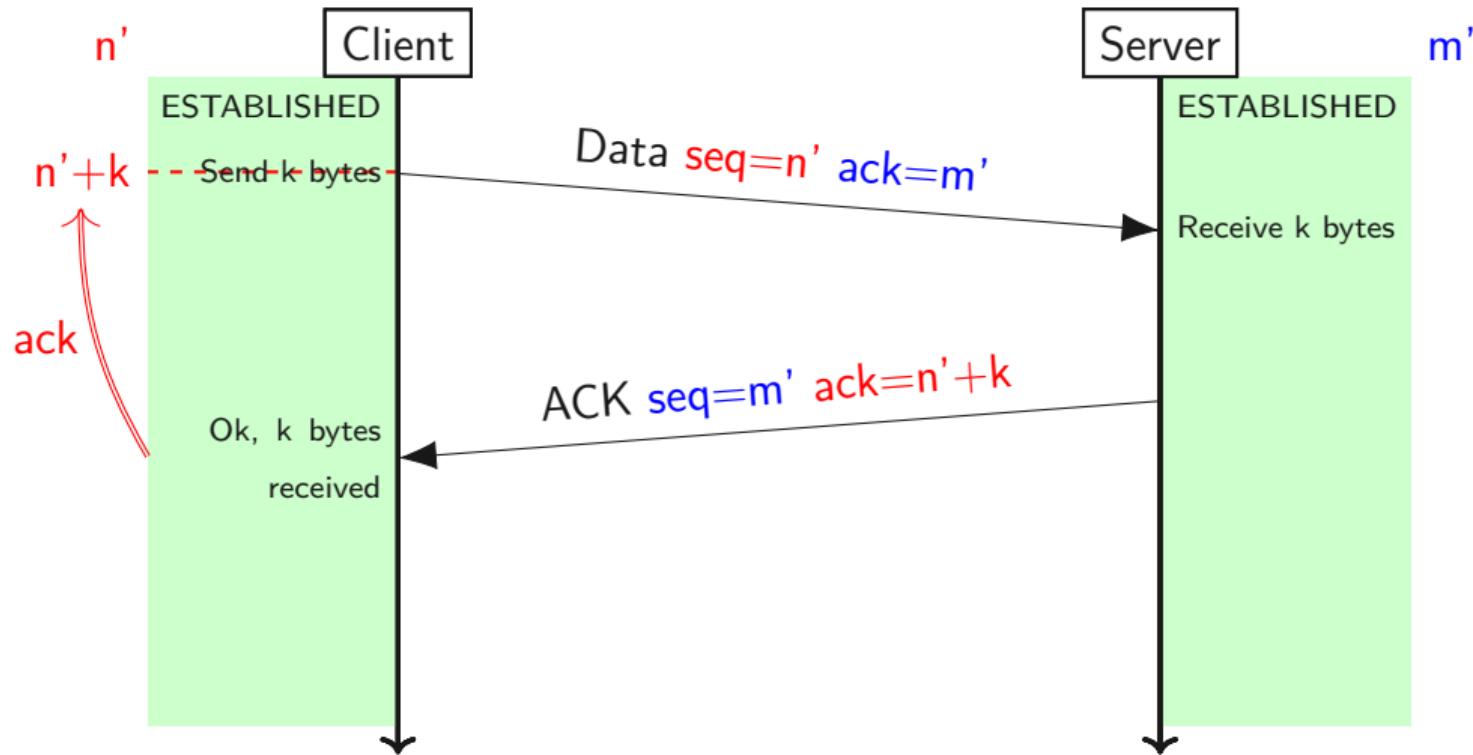
TCP Envoi de données – ACK simple



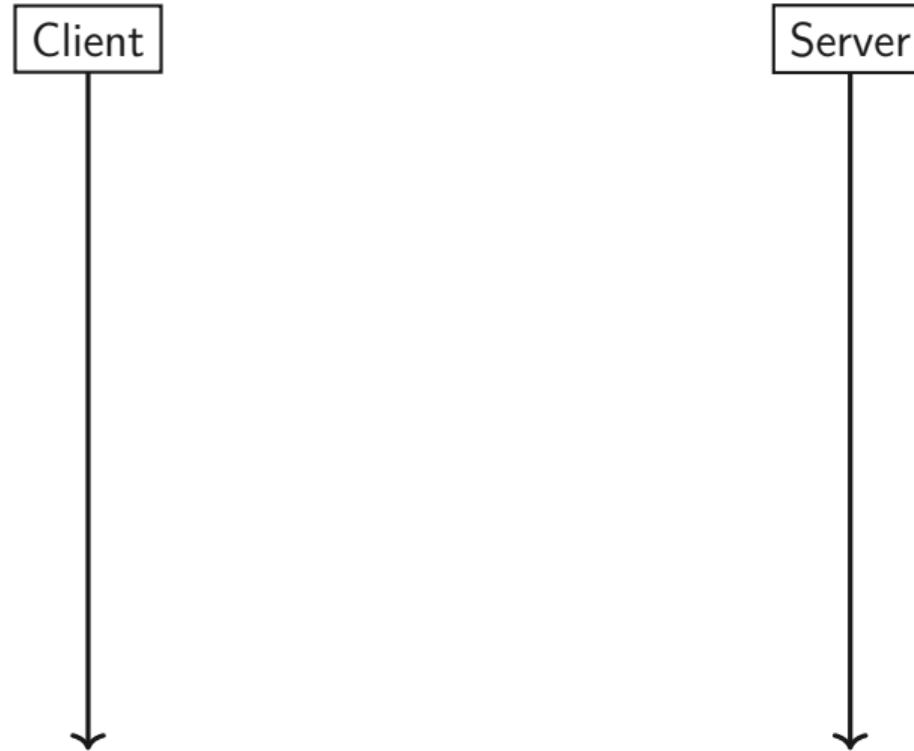
TCP Envoi de données – ACK simple



TCP Envoi de données – ACK simple



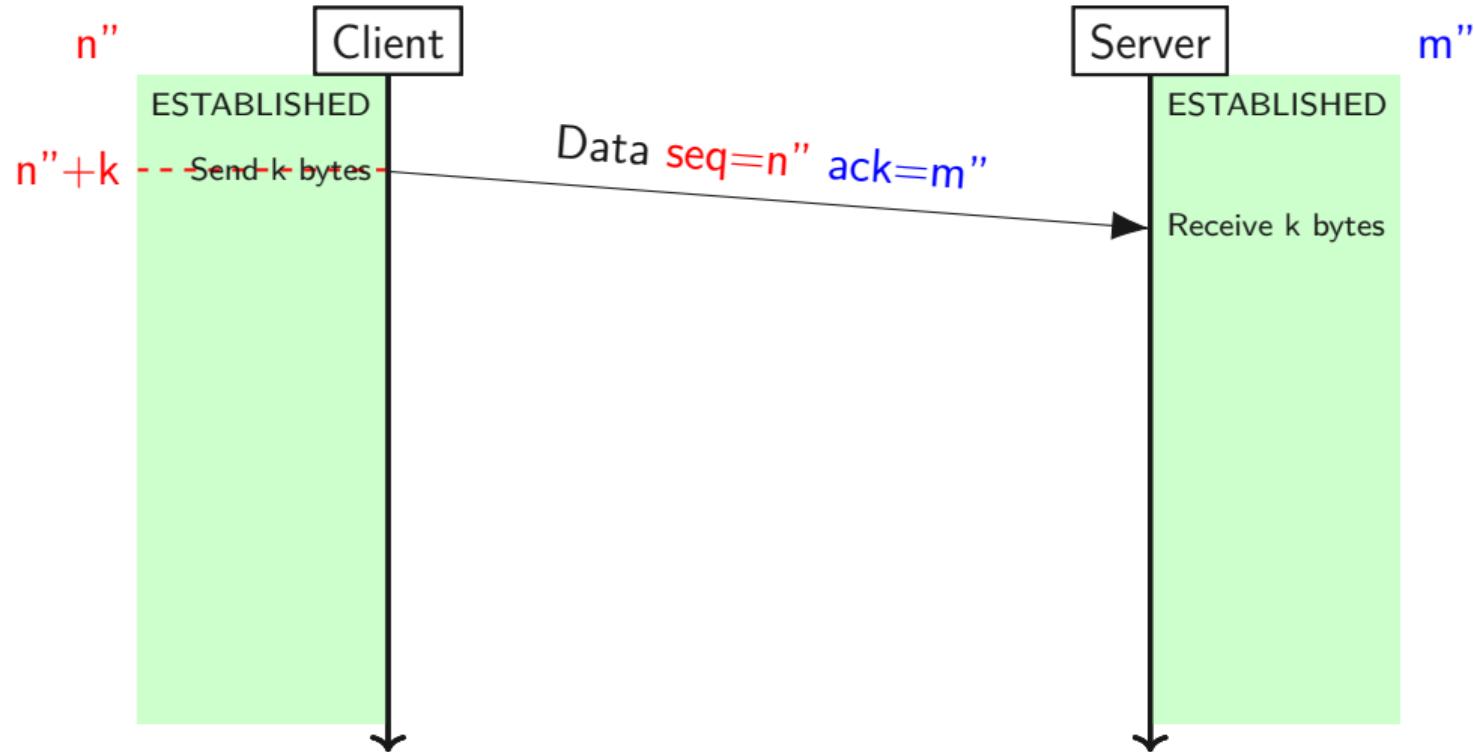
TCP Envoi de données – ACK cumulatif



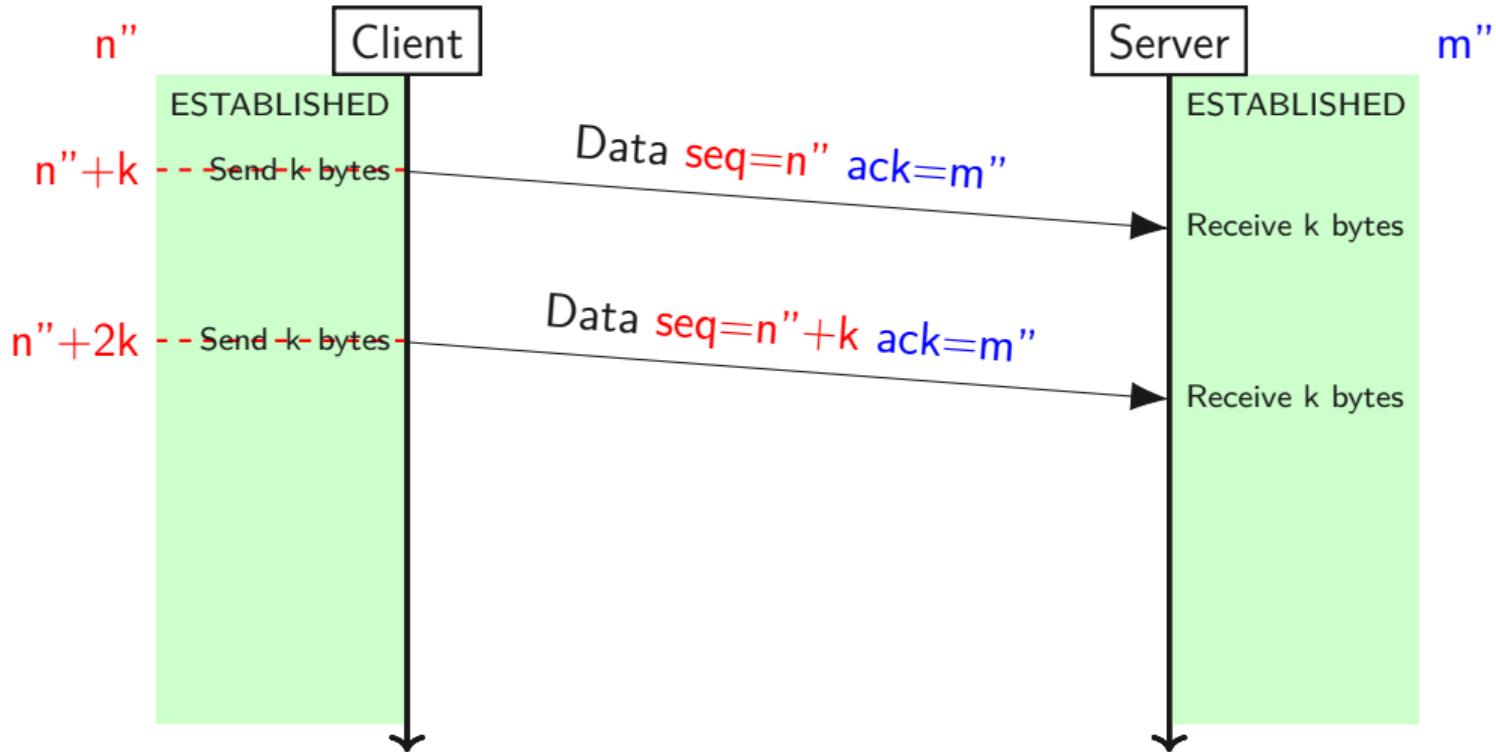
TCP Envoi de données – ACK cumulatif



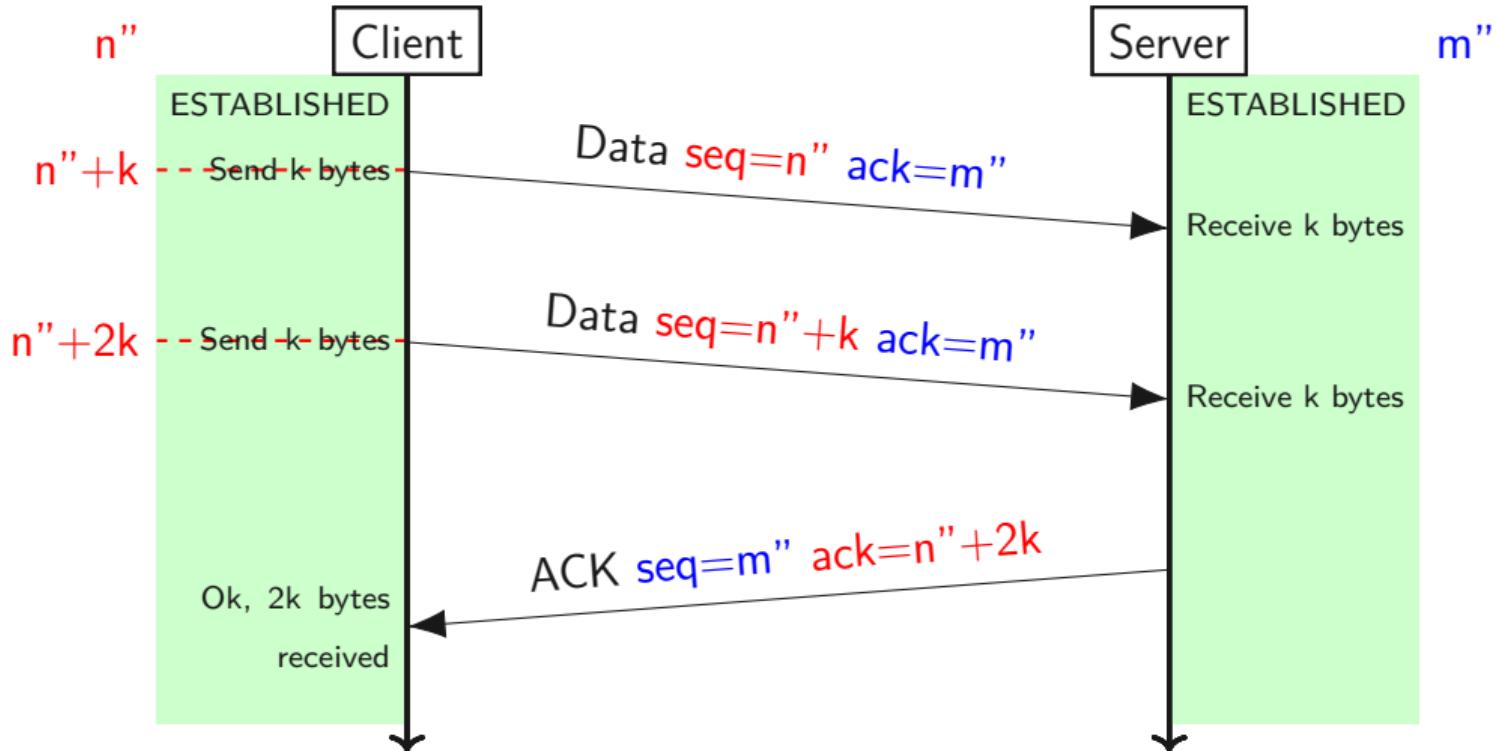
TCP Envoi de données – ACK cumulatif



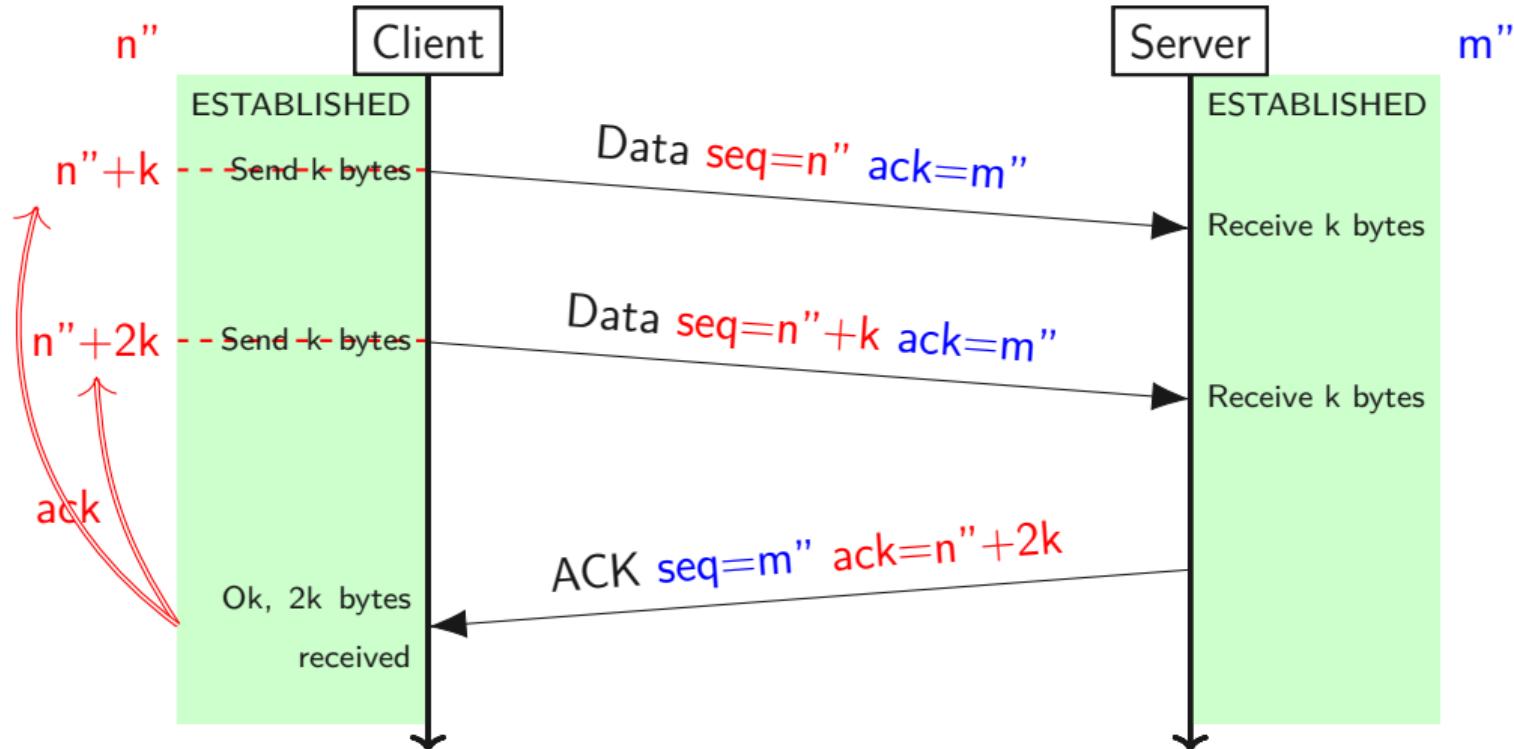
TCP Envoi de données – ACK cumulatif



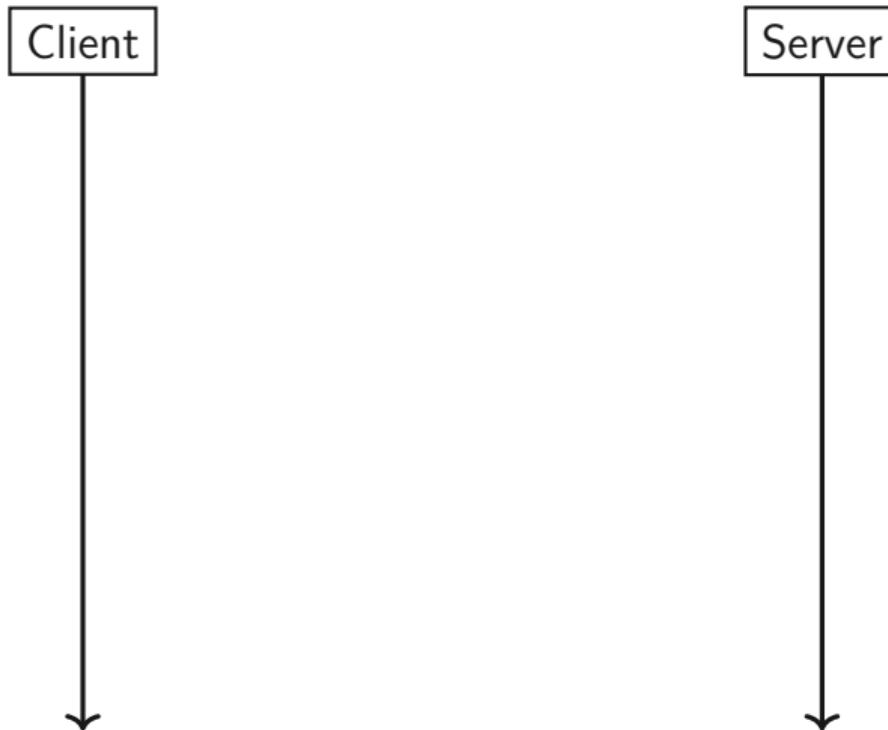
TCP Envoi de données – ACK cumulatif



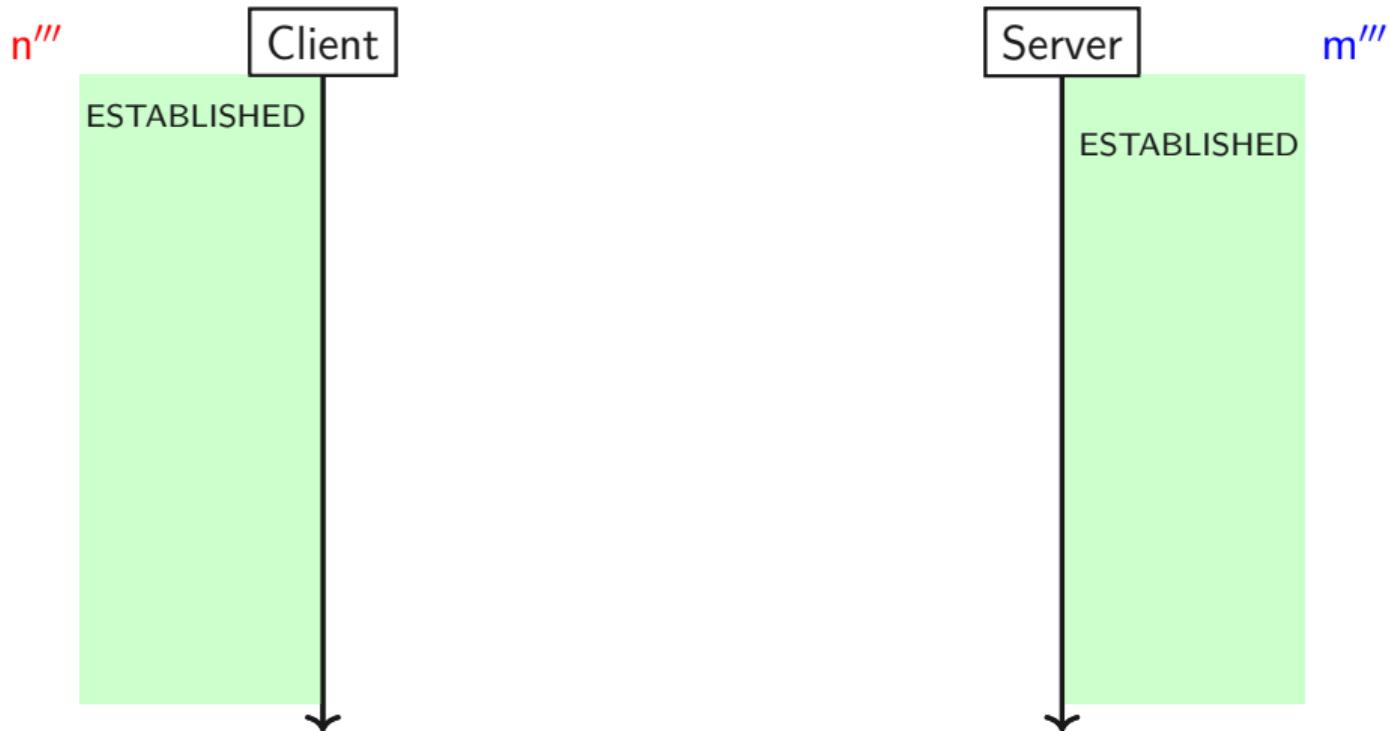
TCP Envoi de données – ACK cumulatif



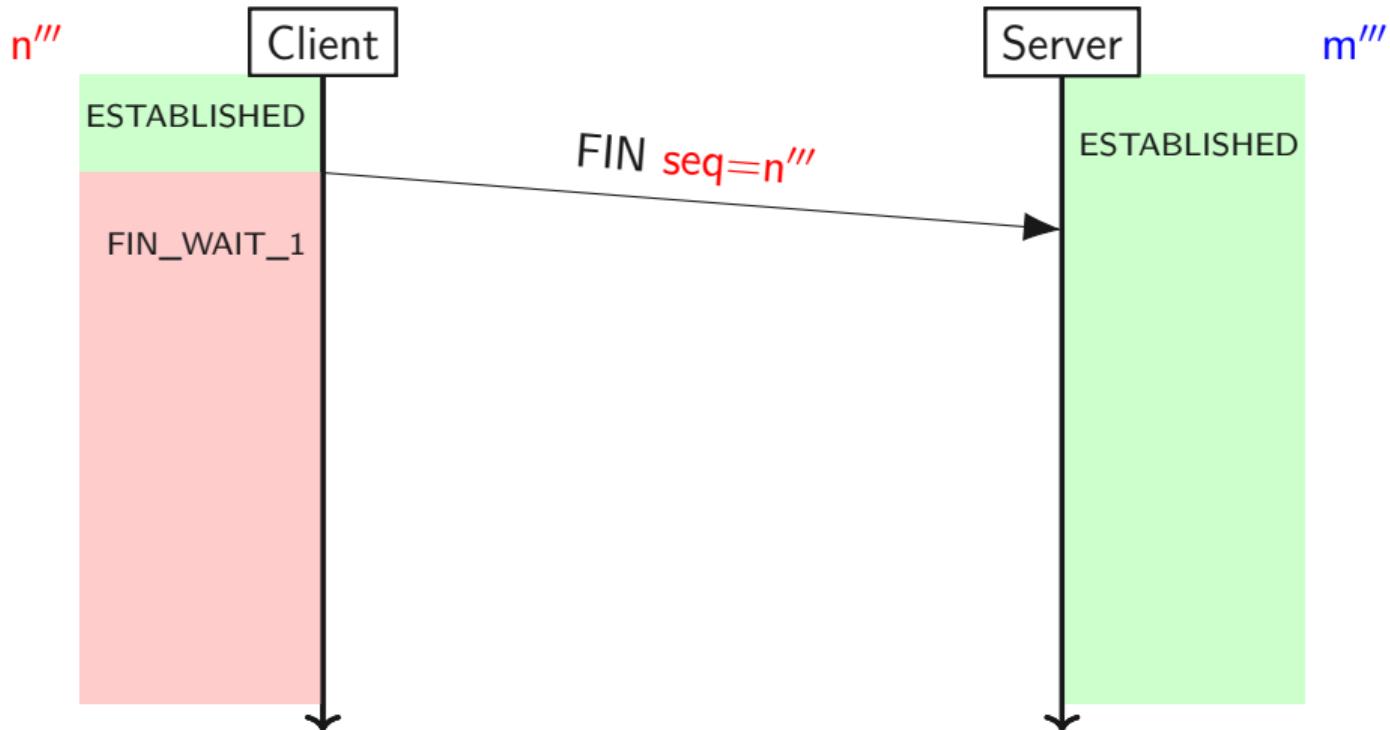
TCP Fermeture de session



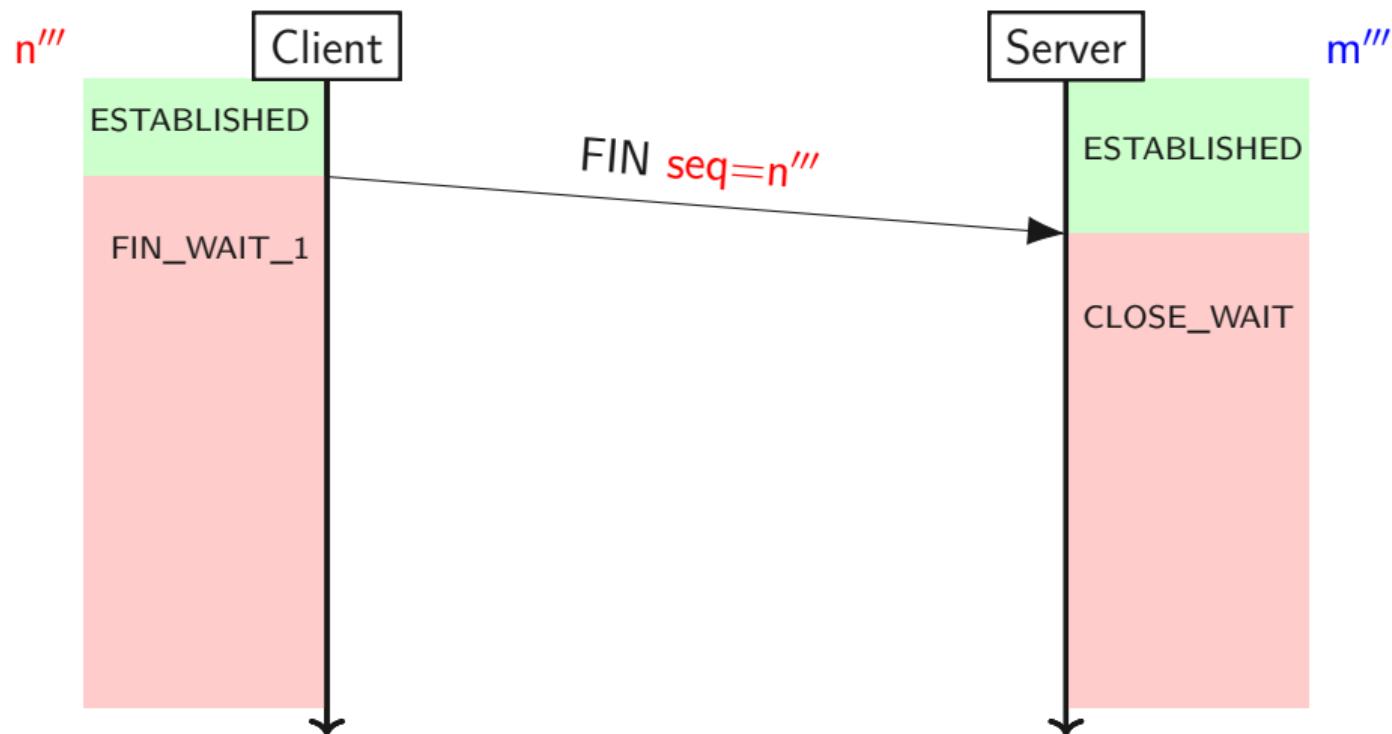
TCP Fermeture de session



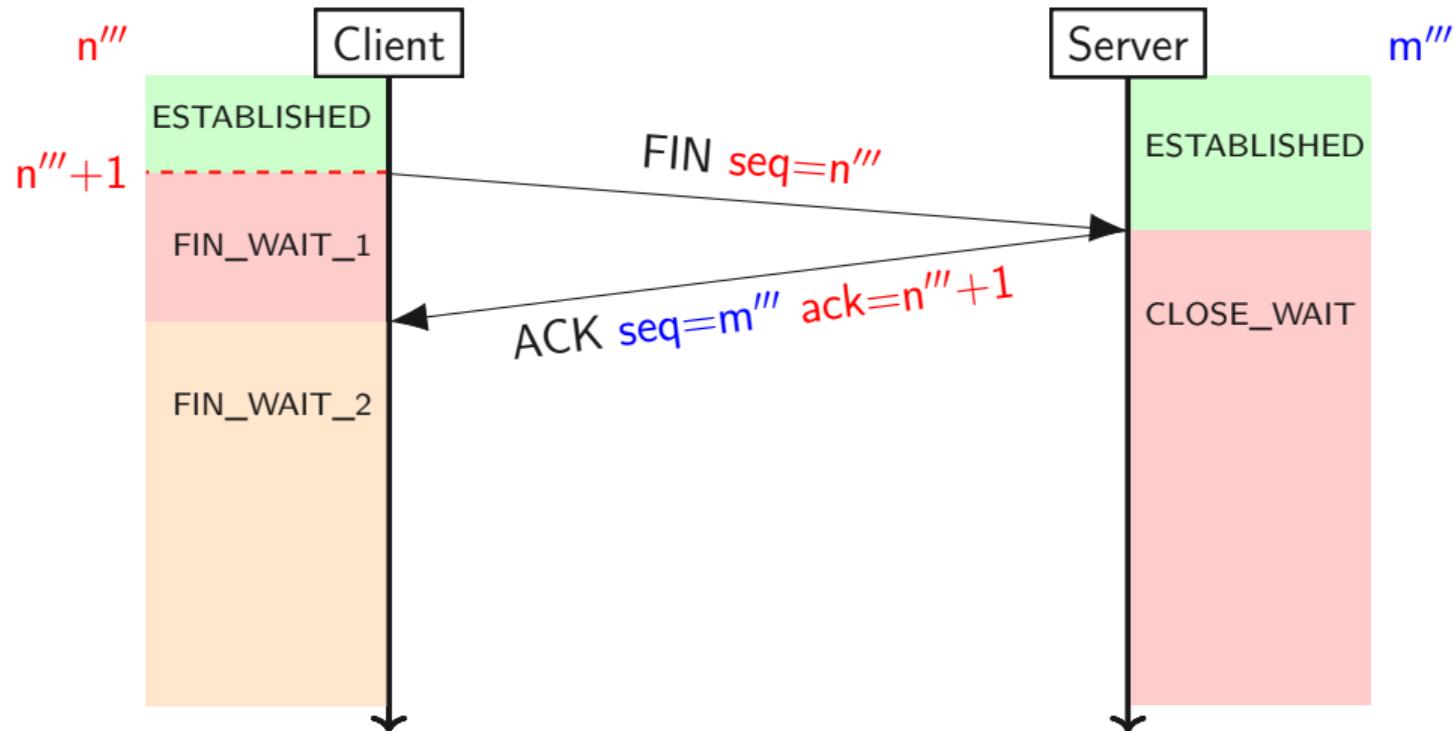
TCP Fermeture de session



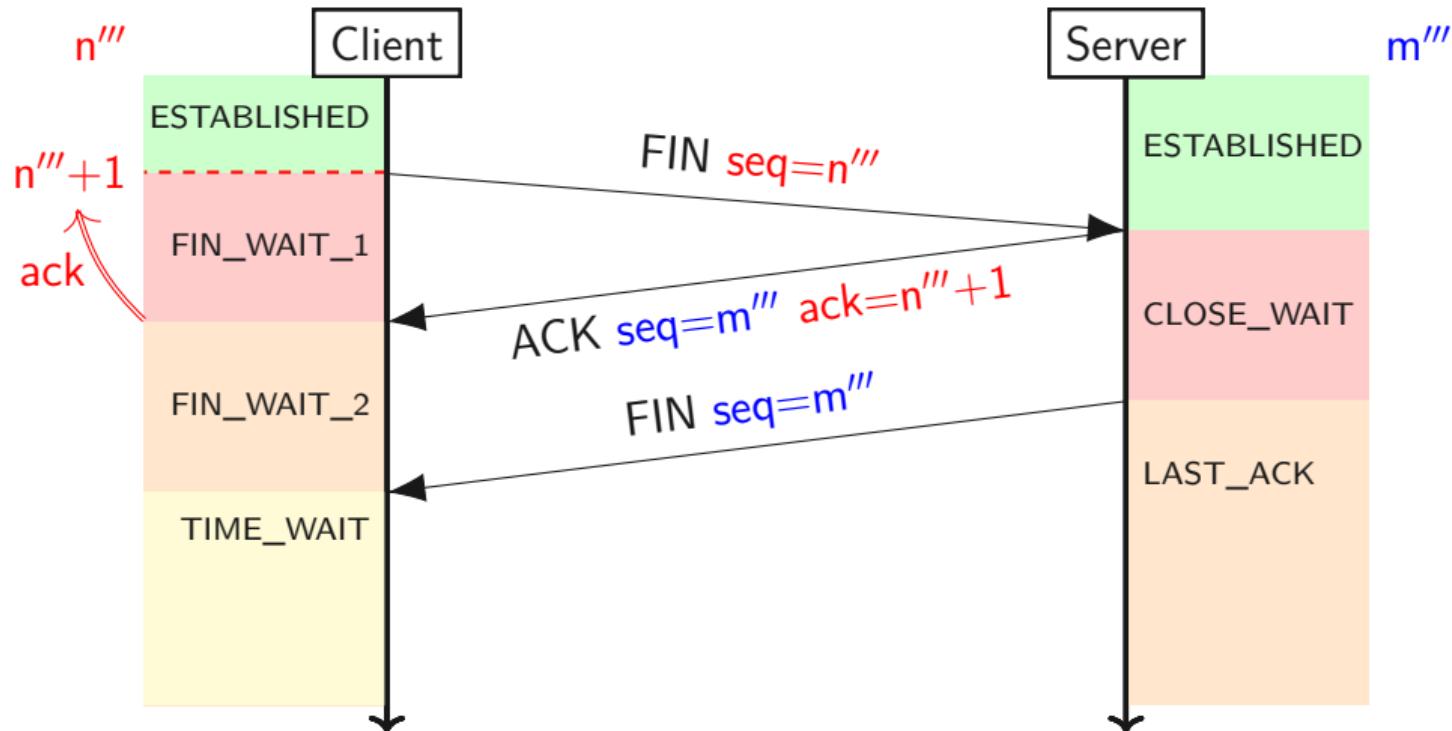
TCP Fermeture de session



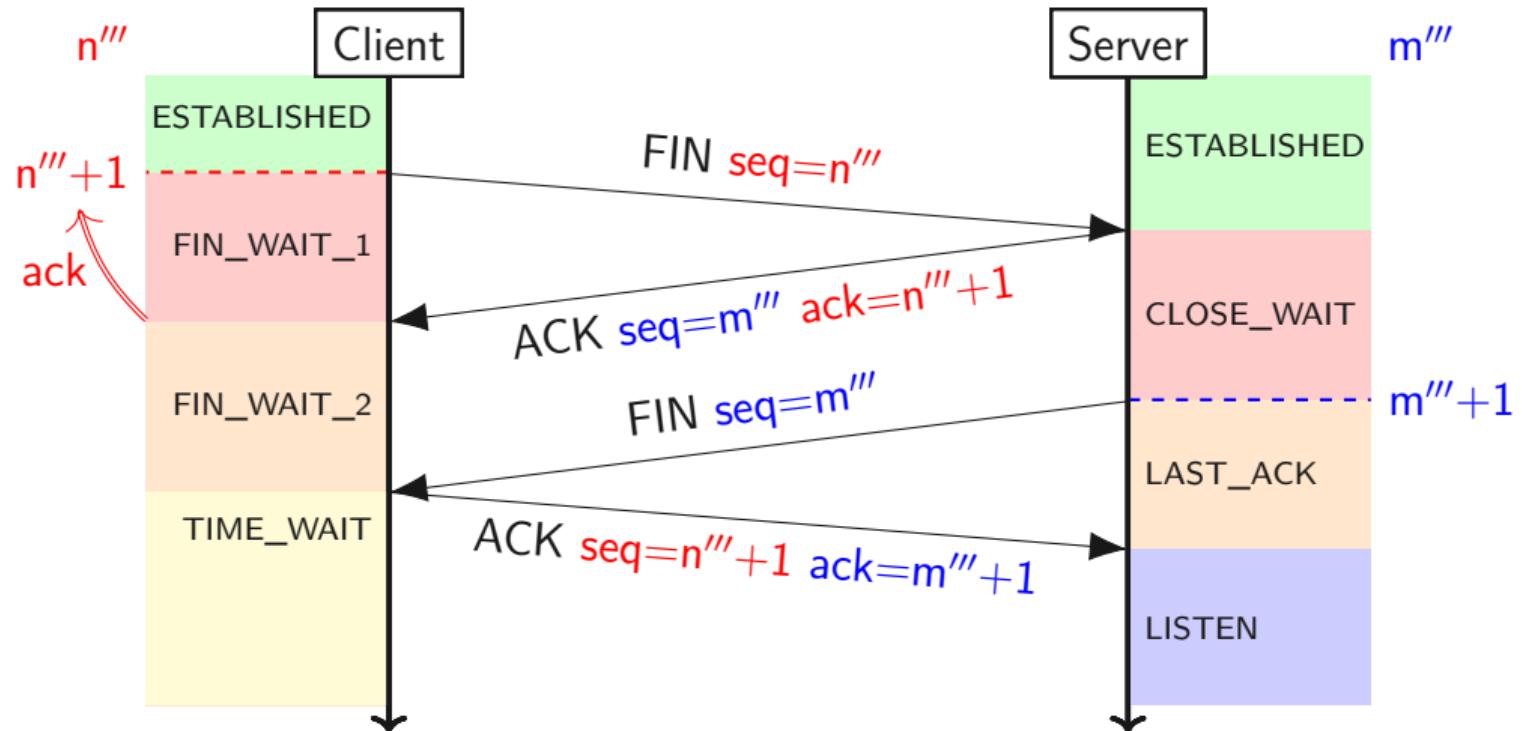
TCP Fermeture de session



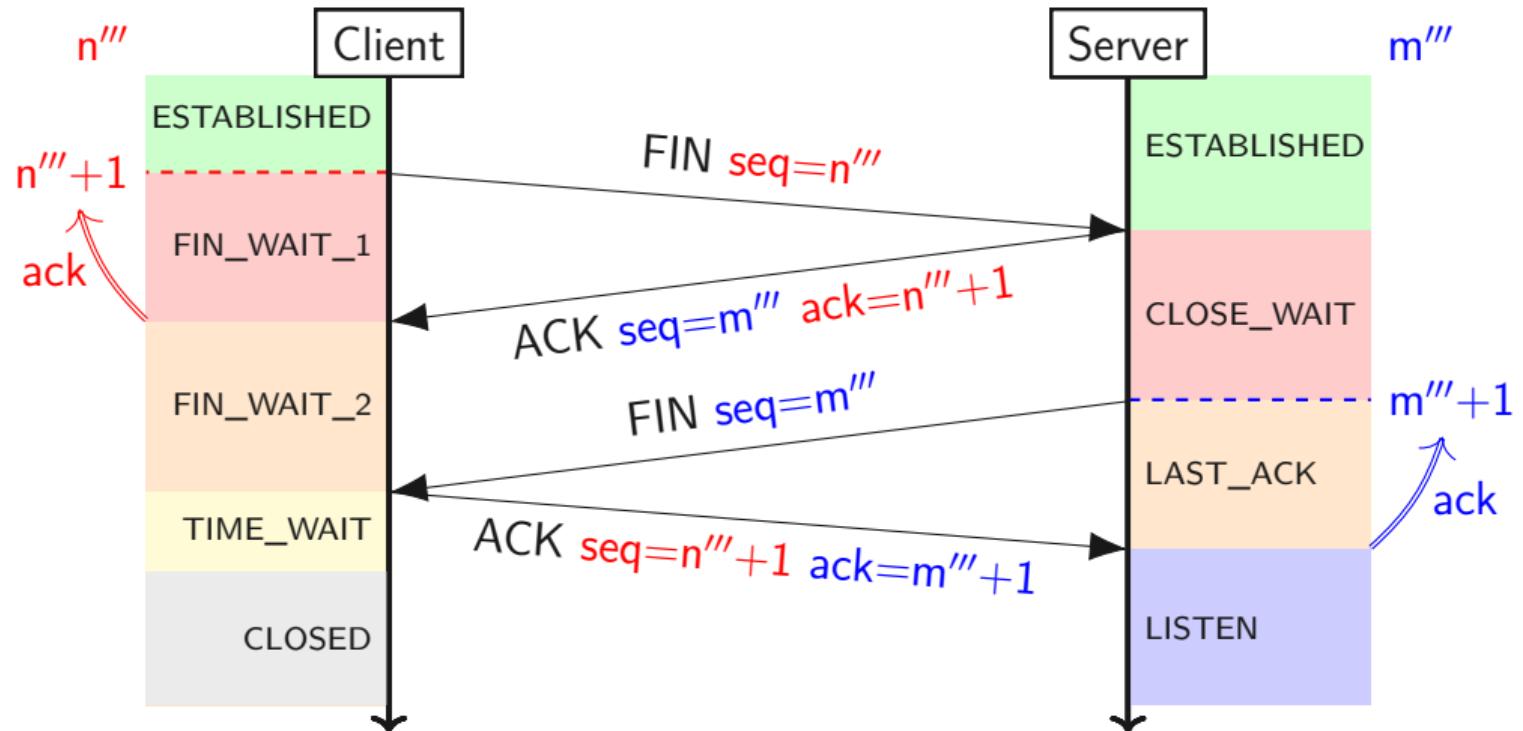
TCP Fermeture de session



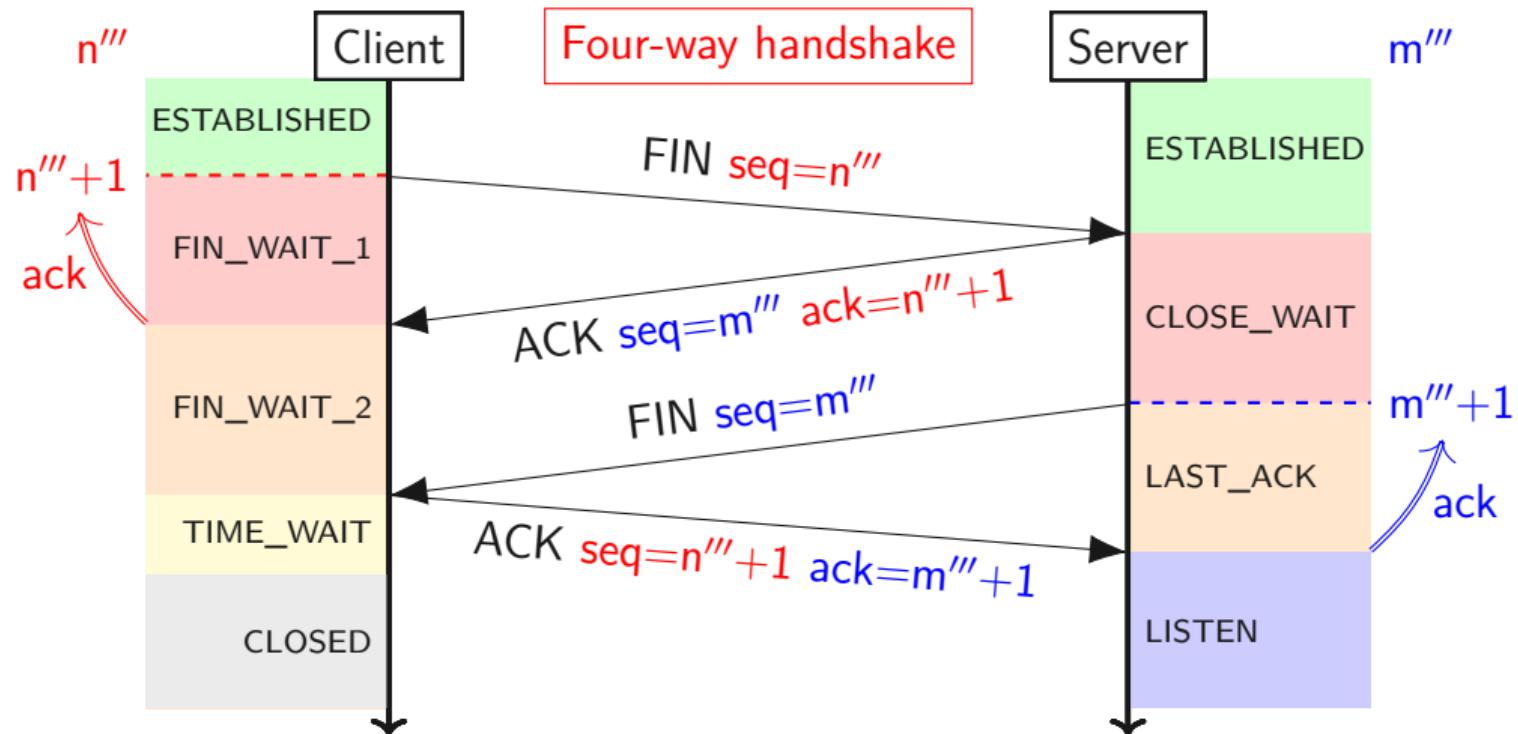
TCP Fermeture de session



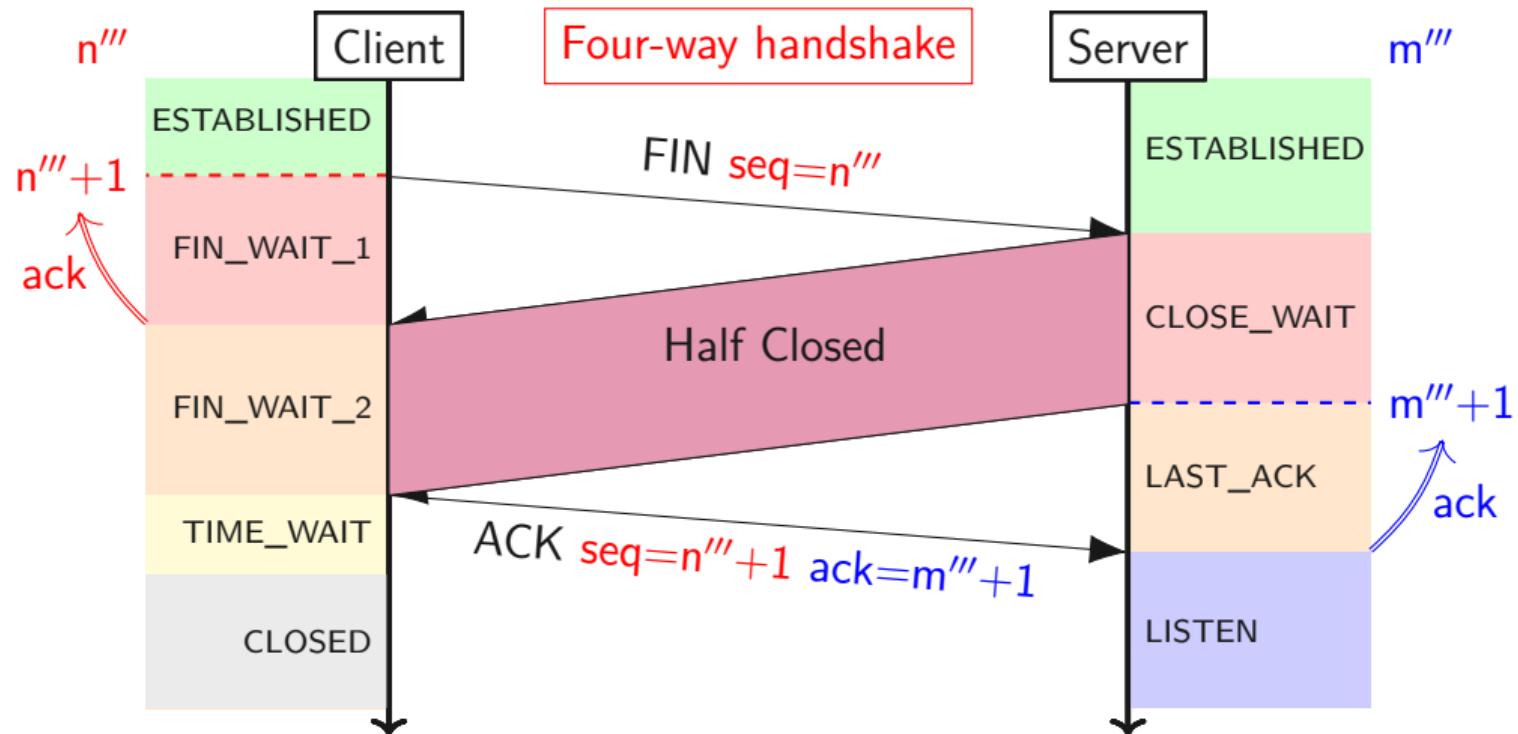
TCP Fermeture de session



TCP Fermeture de session



TCP Fermeture de session



Lignes directrices

Introduction

Modélisations en couches

TCP/IP stack

TCP/IP stack

Couche physique

Network Access Layer

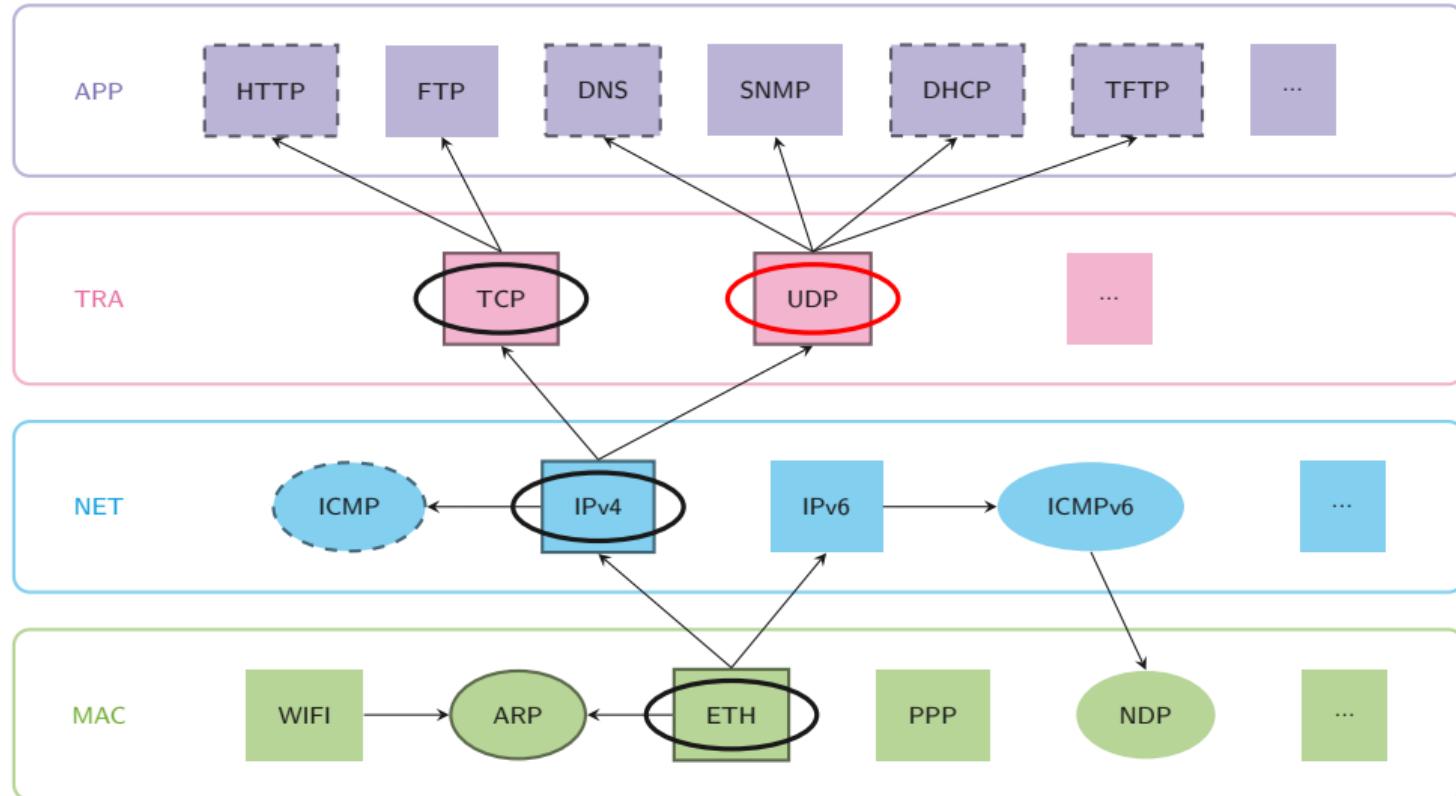
Internet Layer

Transport Layer

Application Layer

Accès au réseau et routage

TCP/IP Stack



User Datagram Protocol (UDP)

Défini en Août 1980 par le RFC 768 (3 pages !)

UDP **ne garantit pas** un flux d'octet :

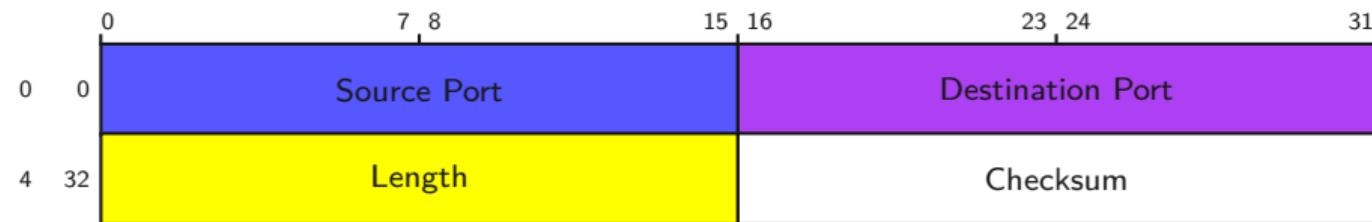
- ▶ sans pertes,
- ▶ sans doublon,
- ▶ sans réordonnancement,
- ▶ sans congestion,

juste sans erreur et avec multipexage.

UDP est un protocole simple et léger, donc rapide, et sans état.

UDP est utilisable en multicast. Principe de base : Envoi rapide de petits paquets (datagrammes).

UDP Header



Seulement 4 entiers 16 bits => 8 octets en tout !

Ports : Les mêmes que pour TCP (IANA)

Length : Longueur du Datagramme

Checksum : (16 bits) : Calculé sur : UDP Header + PDU + éléments IP

Il n'y a pas de Handshake en UDP => latence faible

Utilisation : flux multimedia, temps-réel (VoIP, jeux),

Question/réponse (DNS, SNMP)