

Module M2102

Architecture des réseaux

Chapitre 1

Introduction & Réseaux Ethernet et Wi-Fi

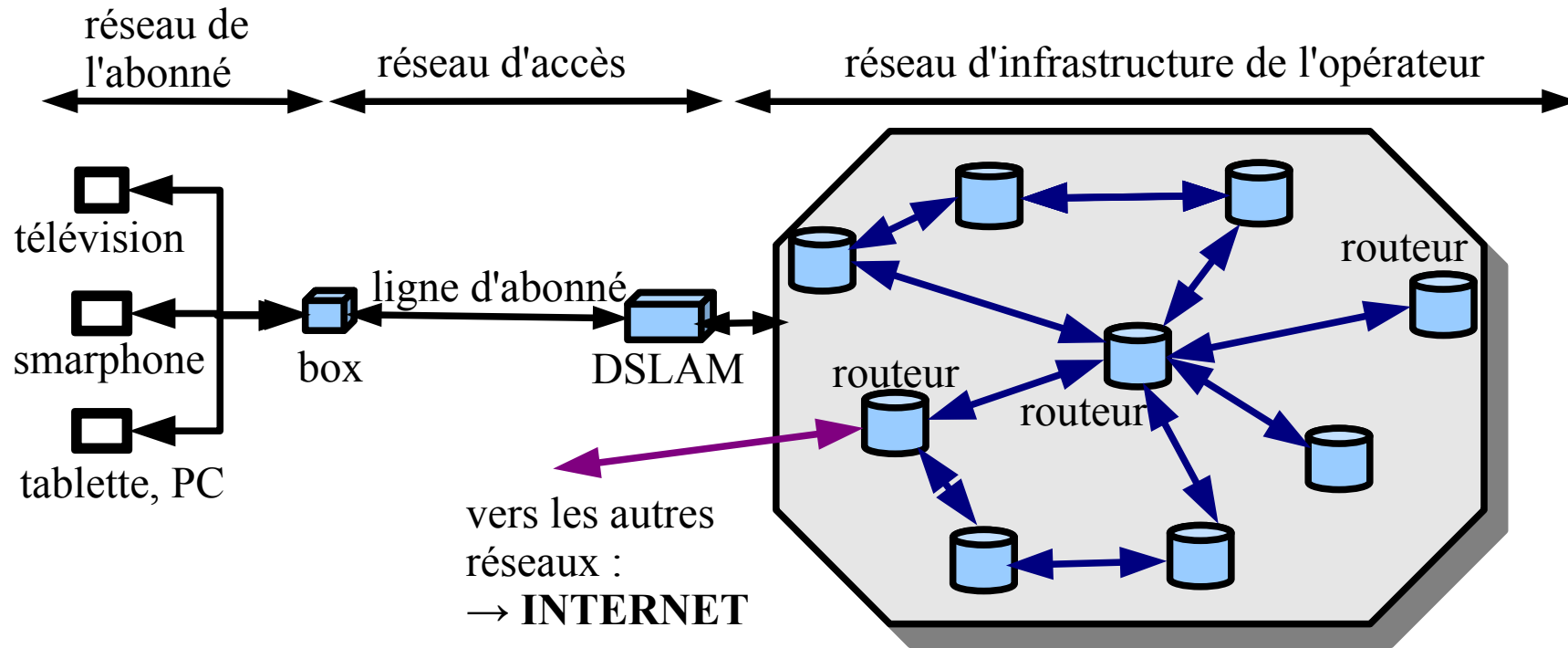
Lectures préalables :

- Notions de « réseau informatique » sur [Wikipédia](#), sur "[Openclassrooms](#)", sur "[Comment Ça Marche](#)"
- Ethernet sur [Wikipédia](#), Ethernet sur "[Comment Ça Marche](#)"
- Wi-Fi sur "[Comment Ça Marche](#)", Wi-Fi sur [Wikipédia](#)

Sommaire du chapitre 1

1. Qu'est-ce qu'un réseau ?
2. Réseaux Ethernet
 - 1.Principales normes Ethernet
 - 2.Niveau physique : câblage, signaux, topologie
 - 3.Format des trames Ethernet
 - 4.Réseaux Ethernet 100baseT sur commutateurs
3. Réseaux Wi-Fi
 - 1.Introduction à la transmission sans fil
 - 2.Les normes Wi-Fi
 - 3.Protocoles Wi-Fi de la couche MAC
4. Compléments sur Ethernet (en ligne uniquement)
5. Compléments sur Wi-Fi (en ligne uniquement)

1. Qu'est-ce qu'un réseau ?



Un réseau informatique est :

- un ensemble **d'équipements**
- reliés entre eux pour échanger
- des **informations**

(source Wikipédia)

Quels équipements et quels supports ?

- Équipements « nœud » d'interconnexion : commutateur (ou switch), routeur, firewall, « box », DSLAM (Digital Subscriber Line Access Multiplexer), etc.
- Supports de transmission :
 - **Paire torsadée** de fils de cuivre, dans un câble => signal électrique.
 - **Fibre optique**, dans un câble optique => signal = **onde lumineuse**, de **longueur d'onde** entre 700 à 400 nm (et la fréquence 430 à 750 THz)
 - **(Micro)-onde** => signal = **onde électromagnétique** supérieure à 2 Ghz.
 - Autres : câble coaxial, **CPL** (Courant Porteur en Ligne).
- Propriétés des supports :
 - Débit d'émission **De = Volume de données / temps, en b/s**
 - Temps de propagation **Tp = distance / Vitesse de propagation**
 - Qualité de service (taux d'erreur, synchronisation dans les échanges...)
 - Facilité d'utilisation : connectivité, mobilité.

« Échanger des informations » ?

- Identifier l'émetteur et le/les récepteurs :
 - notion d'adresse des personnes, des applications, des machines, ...
- Réaliser des échanges de « bonne qualité » :
 - Fiabilité : gestion des erreurs de transmission et des équipements pour que les applications fonctionnent quels que soient les aléas du réseau.
 - Adaptabilité : gestion des différents flux (texte, audio, vidéo).
 - Équité d'accès aux ressources (**MAC** : Medium Access Control).
 - « parler » le même langage : standardisation du format des données échangées.
 - respecter les mêmes règles : « protocole ».
- Gérer les ressources « réseau » : liens, routeurs ; techniques de partage (multiplexage, commutation), contrôle de congestion.

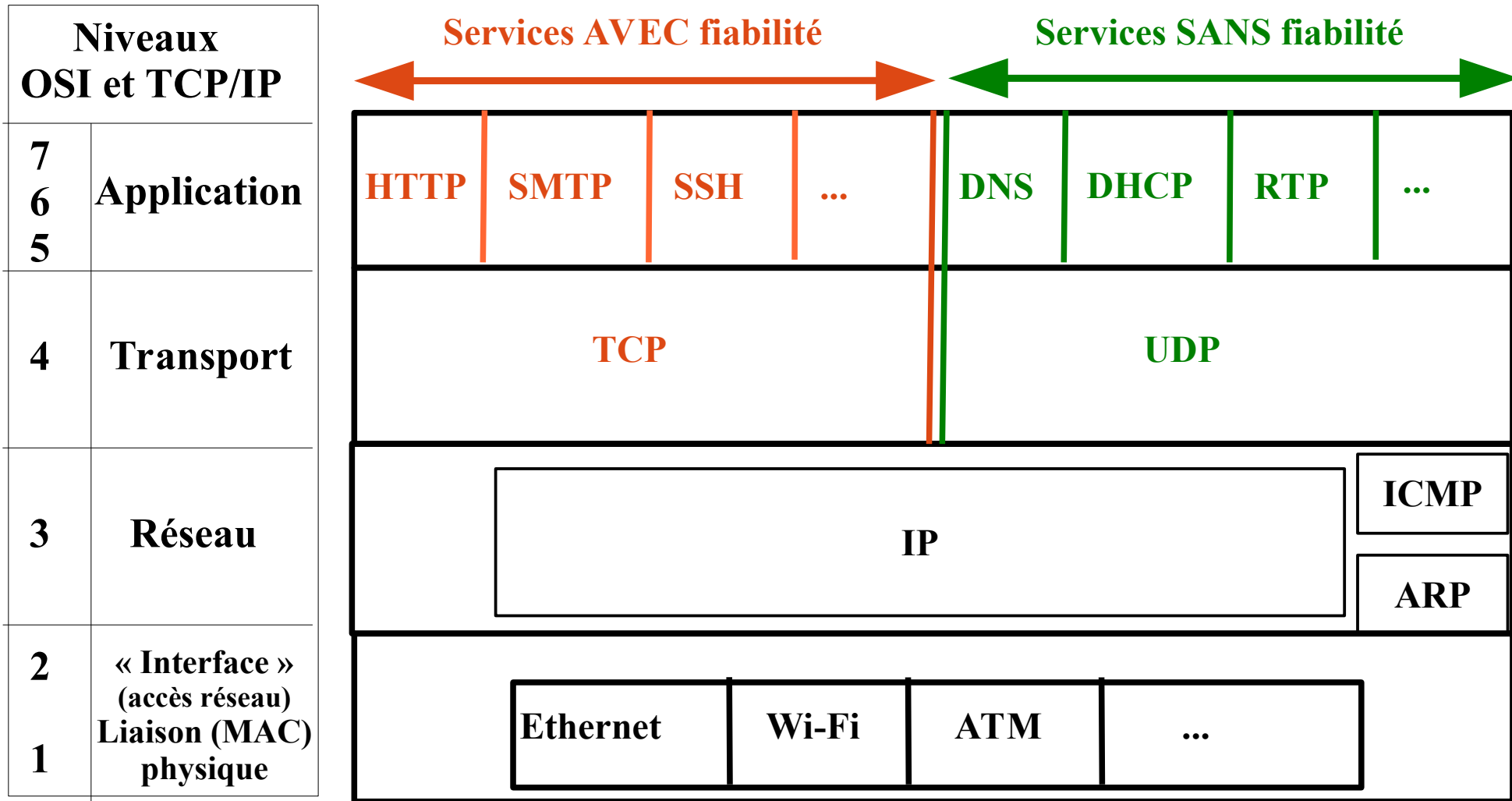
Architecture réseau et protocoles

- Organisation des fonctions réalisées dans un réseau sous forme d'une **architecture en niveaux**, chaque niveau est défini par :
 - Des **entités** logicielles ou matérielles qui implantent les fonctions : circuits ou (micro-)programmes.
 - Des **protocoles** qui fixent la structure des données et les règles d'échange entre les entités.
- Architecture en niveaux de protocoles :
 - Niveau application, échange de **messages** (web, mail...).
 - Niveau transport : échange de datagrammes ou de **segments** (protocole TCP)
 - Niveau réseau : acheminement de **paquets** entre réseaux (protocole IP).
 - Niveaux liaison/physique : échange de **trames** (Ethernet, Wi-Fi, DWDM).
- Principe d'encapsulation :



- Débit utile **Du** : quantité de données « utilisateur » transmise par sec.

Architecture TCP/IP et protocoles



Adressage dans les réseaux

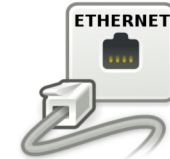
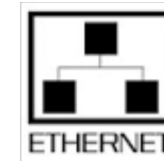
- Adresses de niveau **application** : identifiants utilisés dans les applications : adresse mail, uri, nom dns, etc.
- Adresses du niveau **transport**: Numéros de port TCP ou UDP pour identifier les processus : port 80 (HTTP)
- Adresses du niveau **réseau** : « **adresses IP** » pour identifier les **équipements d'un réseau**, indépendamment de la localisation géographique :
 - IPv4 (sur 32 bits) : 194.62.123.43
 - IPv6 (sur 128 bits) : 1fff:0000:0a88:85a3:0000:0000:ac1f:8001
- Adresses du niveau **liaison/physique** : adresses « **physiques** » (« HWaddr », « MAC ») des cartes réseau des stations, des routeurs.
 - Exemple : adresses Ethernet **MAC** sur 48 bits notés en hexa : 00:C0:4F:26:E1:CF

Réseaux locaux

- Technologies principales :

- **Ethernet :**

transmission par câble, signal électrique,
topologie arborescente, norme IEEE 802.3



- **Wi-Fi :**

transmission par onde électromagnétique,
topologie point à point ou arborescente, norme IEEE 802.11



- **Bluetooth :**

comme Wi-Fi mais sur de plus courtes distances et
avec des débits plus faibles, norme IEEE 802.15



- **CPL : Courant Porteur en Ligne,**

transmission sur câble du réseau électrique,
standardisé par « Homeplug Alliance » et IEEE 1901



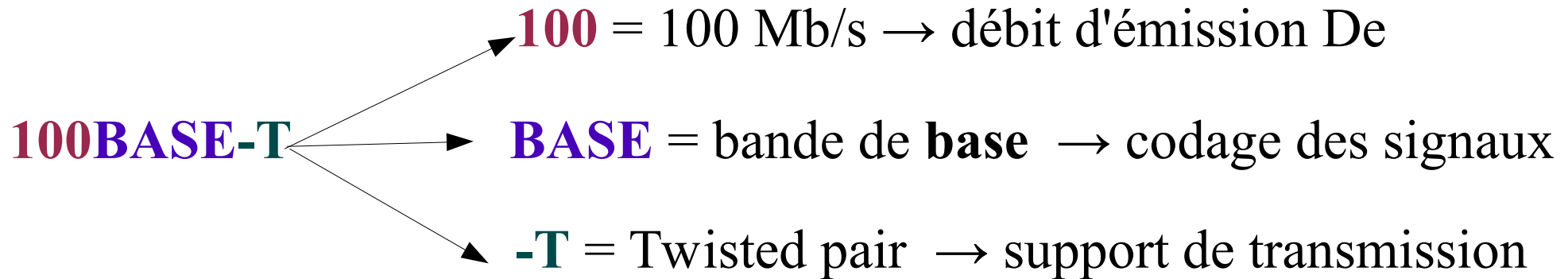
- Standardisation de chaque technologie au niveau **MAC** « Medium Access Control », pour définir le **format des trames** et la méthode d'accès au support pour la transmission de ces trames,

2. Réseaux locaux Ethernet

1. Principales normes Ethernet et IEEE 802.3
2. Niveau physique : câblage, signaux, topologie
3. Niveau liaison : format des trames Ethernet
4. Réseaux Ethernet 100baseT sur commutateurs

2.1. Normes de la famille Ethernet

Invention en 1973/76 par Bob Metcalfe et David Boggs (Xerox)

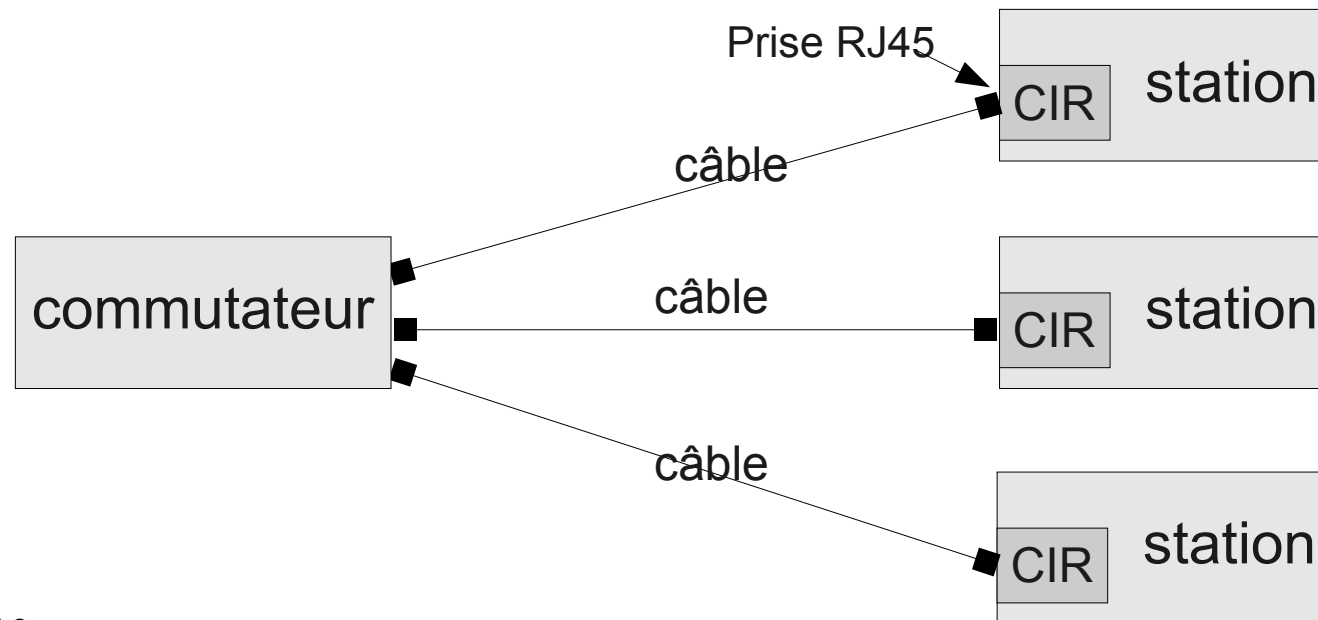


- Débit d'émission **De** : 10 Mb/s, 100 Mb/s, 1 Gb/s (= 1000Mb/s), 2,5 Gb/s, 5 Gb/s ou 10Gb/s
- Support de transmission :
 - paires torsadées : 100BASE-T, 1000BASE-T
 - câble coaxial : 1000BASE-CX
 - fibres optiques : 100BASE-FX, 1000BASE-LX
- Interopérabilité entre les réseaux de cette famille :
 - **format de trame commun**
 - règles de câblage compatibles.

2.2. Réseau Ethernet 1xxxBase-T

Commutateur (ou switch) : nœud d'interconnexion qui redirige les trames en fonction de l'adresse du destinataire. Le **temps de latence** est le délai de transit dans le switch (ex : il est de 7,4 μ s dans les switchs HP2350 de l'IUT).

- **Câble** : 4 paires torsadées de fil de cuivre. Transmission des signaux avec $V_p \sim 200\,000$ Km/s. Longueur max = 100m pour que l'atténuation du signal ne génère pas d'erreur. 100BaseT : 2 paires du câble sont utilisées, une par sens de transmission. 1000BaseT : les 4 paires sont utilisées.
- **Carte CIR** : Carte Interface Réseau (interne ou externe) : code et décode les trames en signaux, détecte les erreurs, assure la synchronisation.



Transmission sur un réseau Ethernet

- La carte CIR d'une station émet et reçoit des **trames** :
 - soit en mode **Unicast** : 1 émetteur vers 1 destinataire.
 - soit en mode **Broadcast** (diffusion) : 1 vers toutes les stations.
- Les trames sont transformées en signaux électriques ou optiques.
- Transmission en **full-duplex** (dans les 2 sens en même temps).
- Les trames sont émises à la demande, avec un délai entre chacune appelé « **silence inter-trames** ».
 - Ce silence est nécessaire pour garantir la dissipation du signal écho produit par tout signal de trame. Sinon, cet écho agirait comme un bruit aléatoire sur le signal de la trame suivante... et générerait des erreurs.
 - La valeur du silence inter-trames est équivalente à la durée d'émission de 96 bits, c'est-à-dire égale à **96 / De**, soit $0,96 \mu\text{s}$ en 100Base-T et $0,096 \mu\text{s}$ en 1000Base-T.

2.3. Format des trames Ethernet

Préambule	Adresse MAC destination	Adresse MAC source	Type trame	Informations	FCS
8 octets	6 octets	6 octets	2 oct.	entre 46 et 1500 octets	4 octets

- **Préambule** : $(AA\ AA\ AA\ AA\ AA\ AA\ AA\ AB)_{16}$ pour permettre au récepteur de se synchroniser. Rappel : $A_{16} = 1010_2$, $B_{16} = 1011_2$
- **Adresses Destination et Source** : adresses MAC ou « HWAddr ».
- **Type trame** : identifiant du protocole du niveau hiérarchique supérieur (**IP**=\$0800, **ARP**=\$0806, ...).
- **Information** : contient les données du niveau supérieur :
 - Taille minimale : 46 octets (compatibilité avec les « hub »).
 - **Taille maximale** : 1500 octets.
(pour assurer un taux d'erreur suffisamment faible).
- **FCS (Frame Check Sequence)** : 32 bits de détection d'erreur.

Adressage Ethernet

- Chaque carte CIR est identifiée par une **adresse MAC unique** (mondialement!) allouée par le fabricant de la carte CIR.
 - Rq: une station a autant d'adresses MAC que de cartes CIR.
 - Chaque carte est identifiée par un nom donné par le système d'exploitation de la machine : ce nom s'appelle « interface », par ex : eth0, enp0s25,... À voir avec la commande **ip addr**.
- **Adressage MAC** « Medium Access Control » :
 - longueur : 6 octets.
 - **notation par groupes de 2 chiffres hexa séparés par « : »**
 - exemple : **00:0B:DB:DF:6F:35**
 - les 3 premiers octets identifient le **fabricant** (ex : Dell_77:58:c2).
- Adresse de **diffusion** pour accéder à **toutes** les machines du réseau :
FF:FF:FF:FF:FF:FF

Exemple de trame

0: **0800 2087 b044 0800 1108 c063 0800** 4500
 16: 0048 49ba 0000 1e06 698d c137 33f6 c137
 32: 3304 1770 96d4 397f 84c2 bf3a 21fd 5018
 48: 111c 99bc 0000 0e00 313f 02c0 0011 0000
 64: 3ec1 0000 0011 0000 0002 2828 a7b0 8029
 80: eafc 8158 9070 +**FCS**

Adresse MAC destination : **0800 2087 b044**

Adresse MAC source : **0800 1108 c063**

Type trame = \$**0800** : la trame contient un paquet IP.

rq : le préambule et le code de détection d'erreur FCS ne sont pas affichés.

2.4. Commutateur Ethernet (switch)

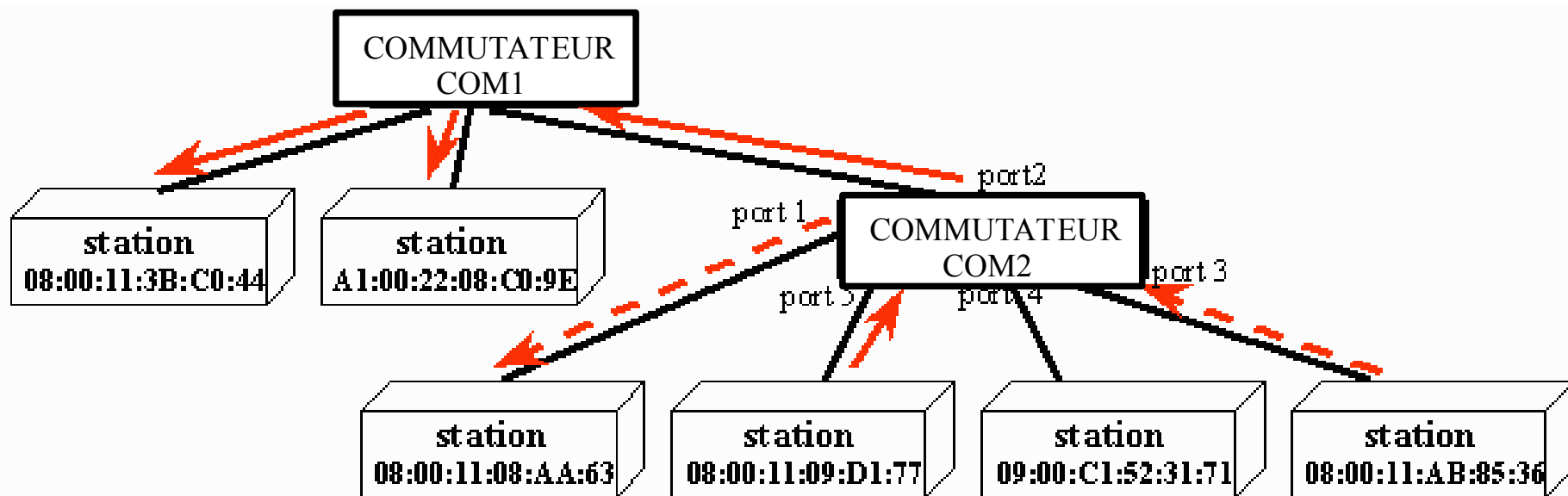


Table de commutation : indique, pour chaque adresse Ethernet, le numéro de port associé.

Algorithme de commutation :

@source -> mise à jour de la table

@dest -> utilise la table pour rediriger la trame vers le bon port.

Si l'@dest n'est pas dans la table (ou si c'est l'@diffusion), la trame est envoyée vers tous les ports, sauf le port d'arrivée de la trame.

Table de COM2

Adresse destination	Port associé
08:00:11:08:AA:63	1
08:00:11:AB:85:36	3
08:00:11:3B:C0:44	2
09:00:C1:52:31:71	4
A1:00:22:08:C0:9E	2
08:00:11:09:D1:77	5

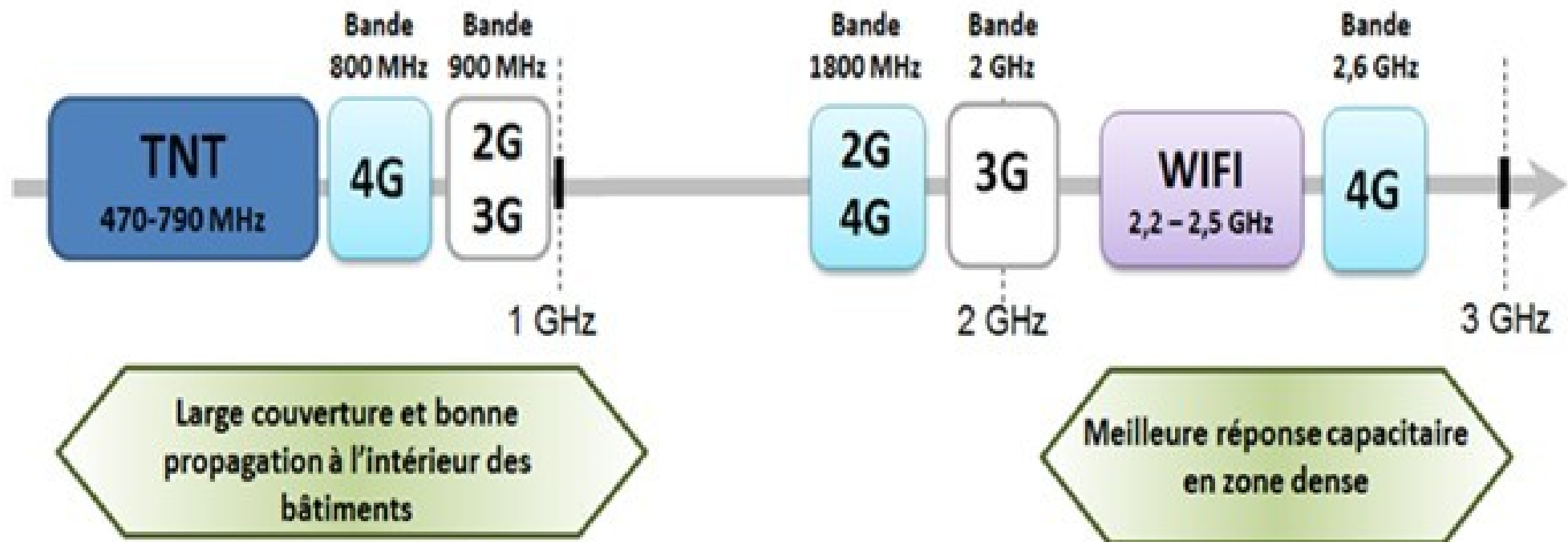
3. Réseaux locaux Wi-Fi

1. Introduction à la transmission sans fil
2. Les normes Wi-Fi
3. Protocoles Wi-Fi de la couche MAC

3.1. Technologies sans fil

La transmission sans fil utilise comme support des ondes électromagnétiques modulées. On différencie les réseaux sans fil par :

- La nature de ce qui est transporté : données et/ou voix.
- La distance : très courte (BlueTooth), local (Wi-Fi), réseau d'accès (WiMax, LTE), téléphonie, lien grande distance (liaisons hertziennes).
- Le type de réseau : réseau Internet, réseau (téléphonique) cellulaire.



Source : Agence Nationale des fréquences (ANFR)

<http://www.recevoirlatnt.fr/4g-lte/quest-ce-que-la-4g/definition-de-la-4g-lte/#.UzAH01bbw88>

3.2. Les normes Wi-Fi

- Wi-Fi (Wireless Fidelity) : label de certification défini sur des tests d'interopérabilité pour les équipements 802.11 (plus de 23000 produits certifiés).



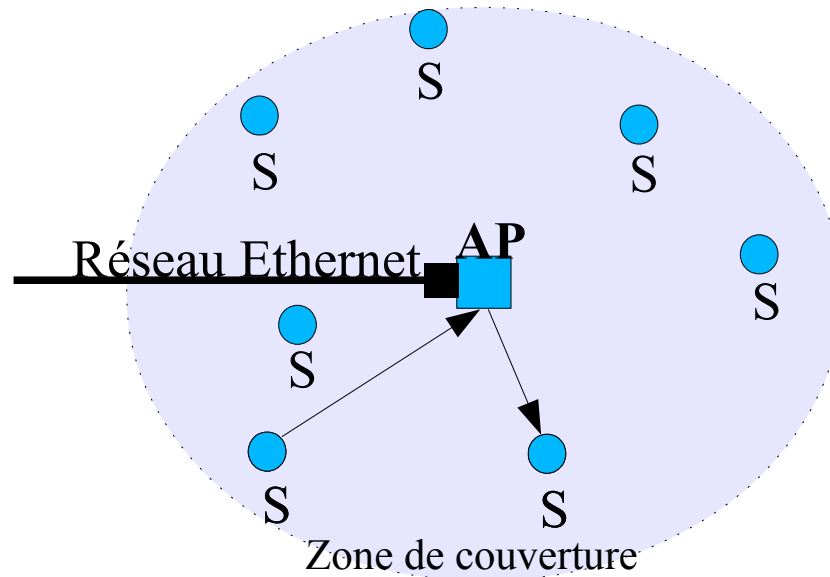
- Organisation : Wi-Fi Alliance (créée par 6 fabricants en 1999 ... + 600 entreprises en sont membres aujourd'hui)
<http://www.wi-fi.org>

Désignation	Débit max	Débit réel moyen	Bande fréquentielle
802.11a	54 Mb/s	30 Mb/s	5 Ghz
802.11b	11 Mb/s	6 Mb/s	2,4 Ghz
802.11g	54 Mb/s	30 Mb/s	2,4 Ghz
802.11n	540 Mb/s	100 Mb/s	2,4 et 5 Ghz

Principes de la transmission Wi-Fi

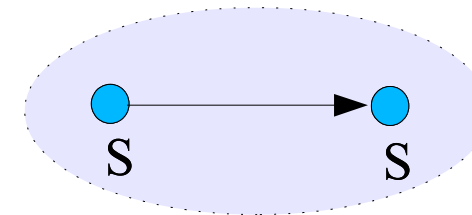
- Méthode :
 - transmission d'une onde radio
 - de haute fréquence (2 à 5 Ghz)
 - à courte/moyenne portée (10 à 100 mètres)
 - à faible puissance (30 mW)
 - avec un taux d'erreur compatible avec les besoins de la transmission de données.
- Propriétés :
 - Affaiblissement du signal très important avec la distance.
 - Taux d'erreur plus important qu'en transmission filaire.
 - Pas de diffusion fiable.

Modes de fonctionnement d'un réseau Wi-Fi



Mode infrastructure :

toute communication entre stations
passe par le point d'accès AP



Modes ad hoc et Wi-Fi Direct :

communication directe
entre stations

- Modes d'utilisation : infrastructure (avec point d'accès AP « Access Point »), ou direct entre stations (ad-hoc, Wi-Fi Direct), mais les échanges se font toujours en mode **point à point par compétition sur le canal**.
- **Zone de couverture** autour d'un point d'accès : espace accessible depuis/vers le point d'accès.

Équipements d'un réseau Wi-Fi

- Pas de système de câblage !
- Cartes réseaux (adaptateurs) et antennes :
 - Émission (modem : modulation).
 - Réception (modem : démodulation).
 - des signaux hertziens (analogiques).
 - Fonctions de la couche MAC : accès au support, gestion des trames, détection des erreurs, sécurité.
- Routeurs / points d'accès :
 - Connexion à un autre réseau (par Ethernet).
 - Routage des flux entre les réseaux.



© 2002 CNET Networks, Inc.

3.3. Protocoles Wi-Fi niveau MAC

<i>2 octets</i>	<i>2 octets</i>	<i>6 octets</i>	<i>6 octets</i>	<i>6 octets</i>	<i>2 octets</i>	<i>6 octets</i>	<i>0 - 2312 octets</i>	<i>4 octets</i>
contrôle	durée	adresse1	adresse2	adresse3	Numéro de séquence	adresse4	données	CRC

- **Format de trames :**

- Format d'adresses : MAC (sur 6 octets), comme celui d'Ethernet.
- Adressage à deux niveaux : adresse de station (MAC) et adresse du réseau Wi-Fi (= adresse MAC du point d'accès AP = BSSID).
- Plusieurs types de trames : trames de gestion, trames de contrôle des échanges et trames d'information.

- **Acheminement des trames :**

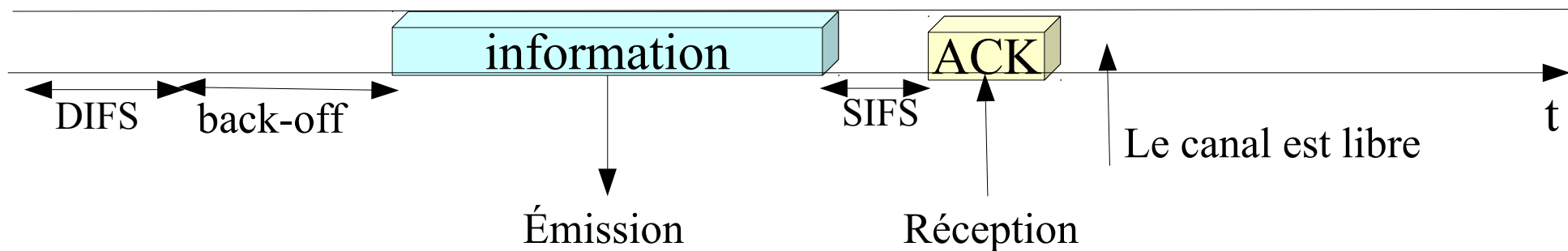
- « **best-effort** » -> fiabilité non garantie
- **Accès** au support (bande fréquentielle de 22 Mhz) par compétition, de façon distribuée et équitable entre les stations -> collisions possibles.

Accès au support

- Principe de partage du support (appelé canal) par **compétition** :
 - Écoute avant d'émettre, émission si le canal est libre.
 - Si deux stations détectent en même temps que le canal est libre, deux trames seront émises et il y aura collision de signal.
- Comme il n'y a pas de détection de collision possible par l'émetteur au niveau physique, le récepteur envoie un **acquiescement** systématiquement.
- Pour limiter les collisions, **un protocole d'évitement** de collision est mis en place : CSMA/CA (Collision Avoidance) :
 - **Pré-réservation** du canal (optionnelle) : trames spécifiques RTS/CTS.
 - **Attente de durée aléatoire** appelée « back-off » avant toute tentative d'émission.
 - **Priorité** de l'envoi des acquiescements.

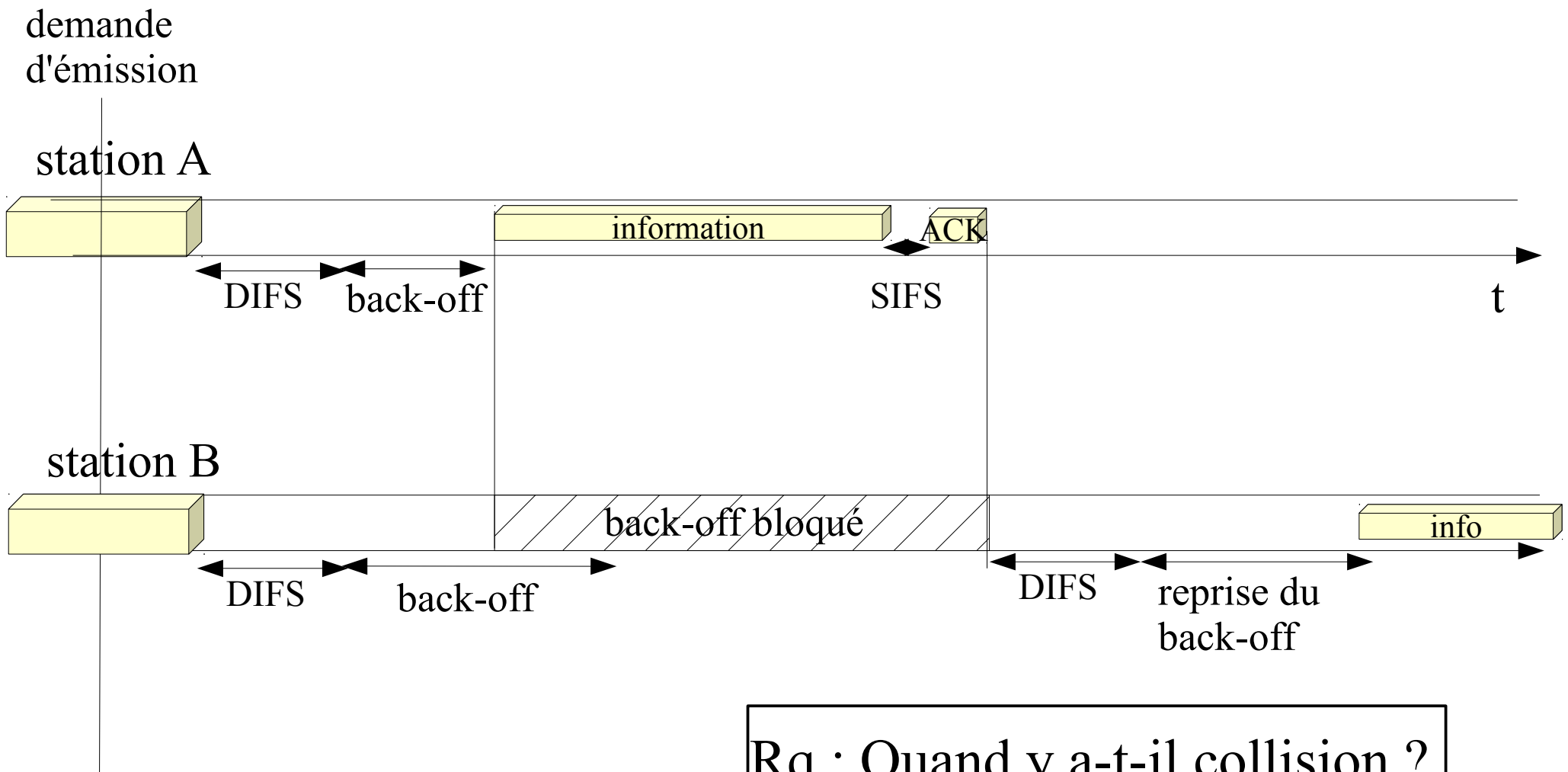
Étapes de l'émission d'une trame

- Écoute jusqu'à ce que le canal soit libre.
- Attente DIFS (délai fixe) et back-off (délai aléatoire).
- Émission de la trame d'information (ou de gestion).
- A la fin du dernier bit émis, attente d'un délai SIFS (plus court que DIFS).
- Réception de l'acquittement au bout du délai SIFS : si l'acquittement n'arrive pas, la station détecte qu'il y a eu collision.



Cas de multiples demandes d'émission

- Hypothèse : A et B veulent émettre en même temps,
le back-off de A est d'une durée plus courte que B



Fonctions de gestion au niveau MAC

- **Association / désassociation** d'une station auprès d'un AP.
Trames de requête (*req ASSOC*) et de réponse (*rép ASSOC*).
- **Chiffrement** par clé symétrique partagée par toutes les stations du réseau : niveau de sécurité WEP (Wired Equivalent Privacy), ou WPA (WiFi Protected Access) et WPA-2 (802.11.i).
- **Synchronisation** avec une trame « *Balise* » ou « *beacon* » émise régulièrement et contenant une estampille temporelle.
- **Économie d'énergie** : l'AP stocke les trames à destination des différentes stations et émet à intervalle régulier des trames « *Balise* » indiquant quelles stations ont des trames en attente. Les stations n'écoutent le réseau que de temps en temps, pour recevoir les trames « *Balise* » ; le reste du temps, elles sont en veille.

Association d'une station à un AP

- Identifiants :
 - BSSID Basic Service Set Identifier : @MAC du point d'accès AP.
 - ESSID (ou SSID), Extended Service Set Identifier : nom du réseau sous la forme d'une chaîne de 32 octets (caractères ASCII).
- Étapes :
 - La station entrant dans le réseau émet une trame **probe request** avec le ESSID avec lequel elle est configurée.
 - Lorsqu'un AP reçoit une telle requête, il compare le ESSID reçu avec le sien. Si OK, il répond avec des infos (charge du AP, débit offert, ...).
 - La station peut alors choisir de s'associer avec l'AP lui offrant le meilleur débit (si plusieurs disponibles).
 - Remarque : chaque AP émet régulièrement ($\sim 0,1$ s) une trame **balise (beacon)** avec son BSSID et son ESSID (+ info de débit).

Glossaire

- 100BaseT
- AP
- BSSID
- CIR
- CPL
- CSMA/CA
- De
- DSLAM
- Du
- FCS
- Full-duplex
- HWaddr
- MAC
- Tp
- WEP
- WPA

Module M2102

Architecture des réseaux

Chapitre 2

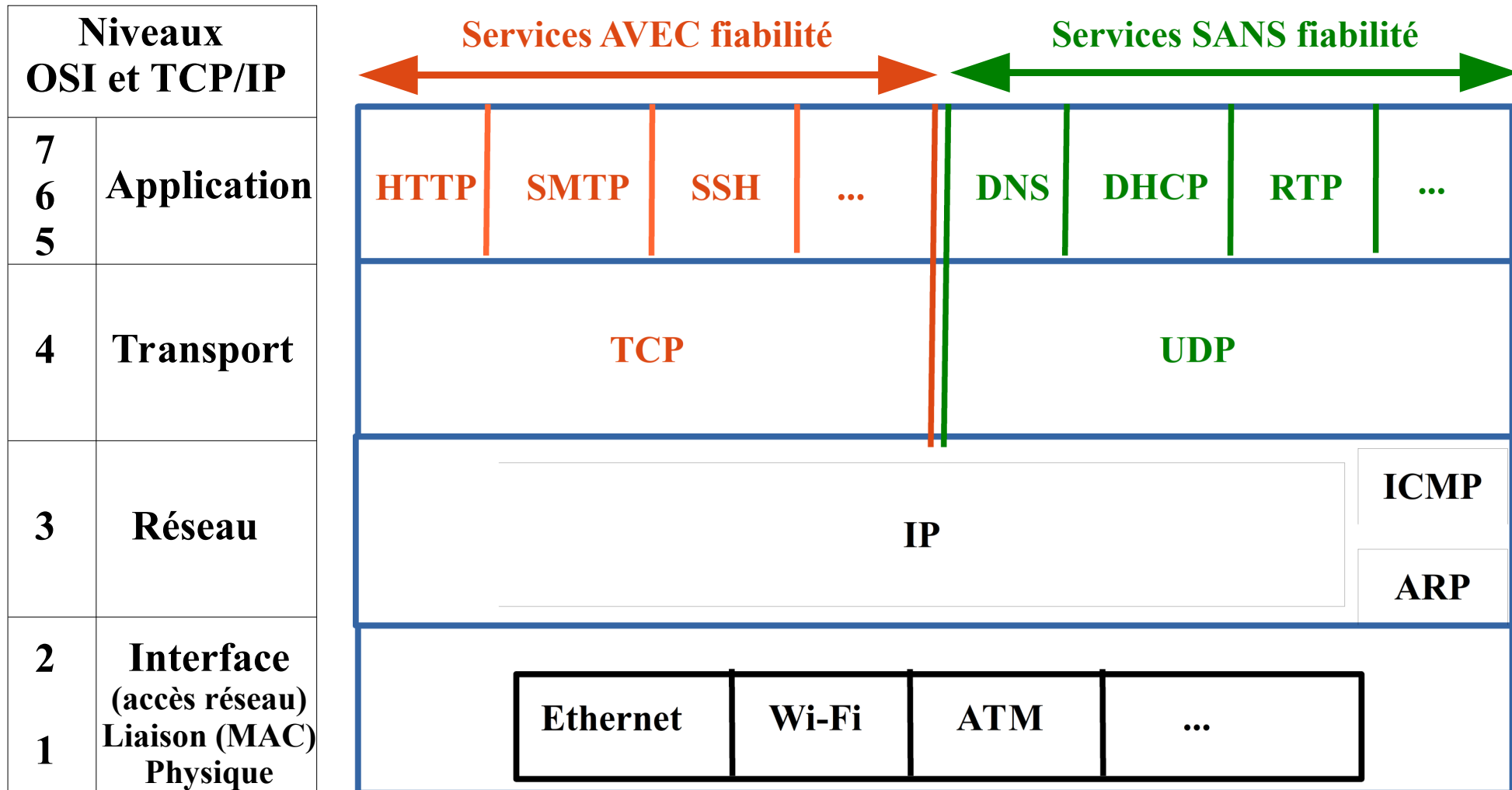
Protocole Internet IP : adressage IP

Lectures préalables :

- [Suite des protocoles Internet sur wikipedia](#)
- [Réseaux TCP/IP sur wikibooks](#)

Internet et son architecture TCP/IP

- Internet : Interconnexion de réseaux « Inter Net » ou inter-réseau
- L'architecture de l'Internet, appelée « Architecture TCP/IP », a pour objectif le déploiement d'applications sur un inter-réseau, indépendamment des technologies physiques de ces réseaux.



Les quatre niveaux de l'architecture TCP/IP

- **Application**

- applications standard : FTP, HTTP, SMTP, POP, IMAP, SSH, ...
- applications de service : DNS, DHCP, NFS, X11, SNMP
- applications spécifiques

- **Transport**

- Protocole UDP (User Datagram Protocol) : service de transport minimal
- Protocole TCP (Transmission Control Protocol) : + fiabilité des connexions

- **Réseau**

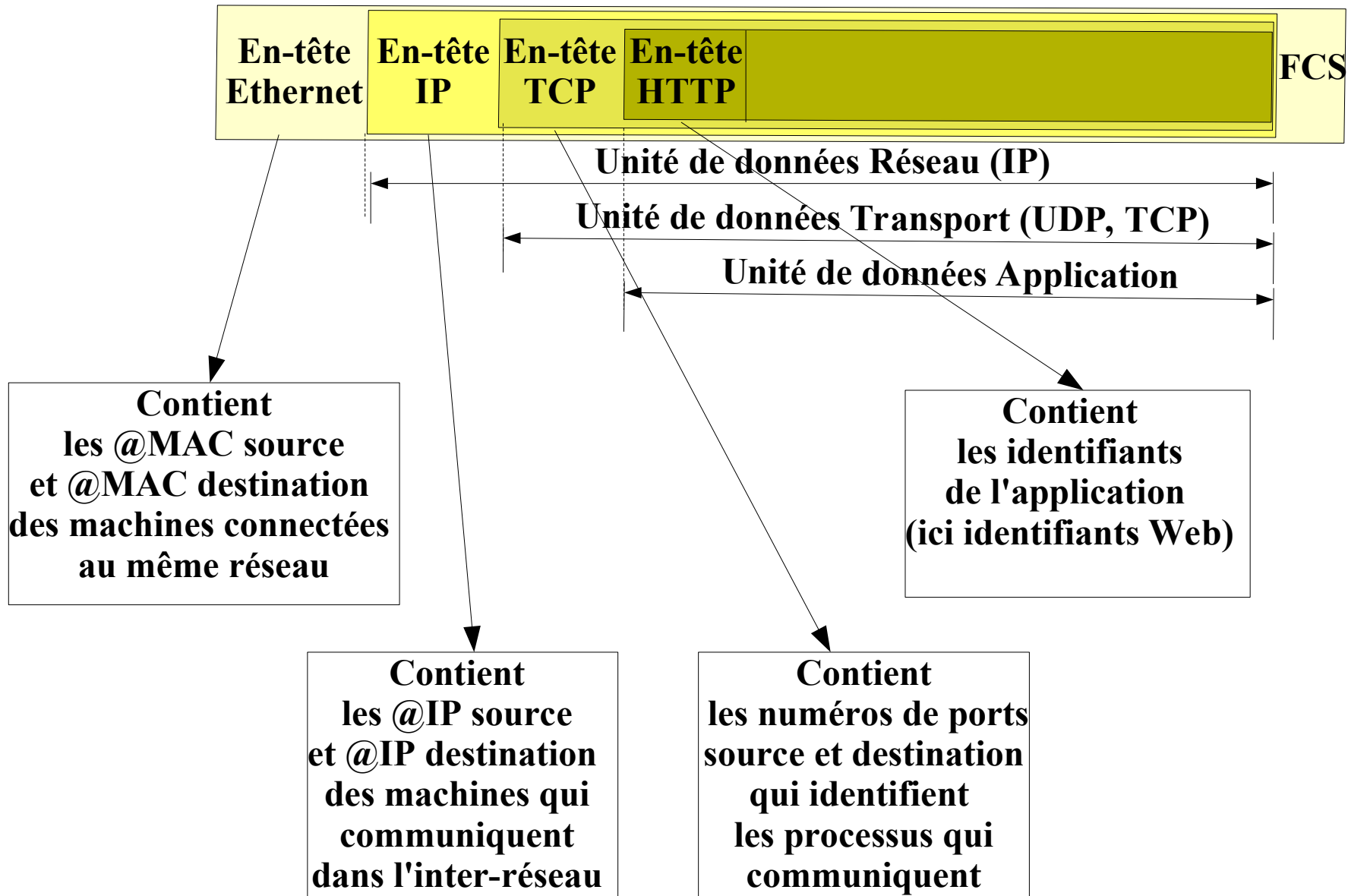
- Protocole IP : bâti sur un adressage logique des stations « l'adresse IP »
- Protocoles de service : ICMP (contrôle), ARP (adressage)

- **Interface (accès réseau) : assure l'accès aux différents réseaux physiques (correspond aux niveaux liaison et physique)**

Identifiants dans l'architecture TCP/IP

- Identification des utilisateurs/ressources dans les **applications** :
[adresse mail](#), [URL](#), etc...
- Identification des processus au niveau **transport** :
 - [numéro de port](#) (+ adresse IP de la station)
- Adresse du niveau **réseau** :
 - [Adresse IP](#) : adresse « logique », comprenant une partie identifiant le réseau et une partie identifiant la machine dans le réseau
 - Remarque : un [Routeur IP](#) est une machine connectée à plusieurs réseaux, donc ayant **plusieurs** adresses IP
- Adresse physique du niveau **interface (accès réseau)** :
 - dépend du réseau physique (ex. [adresses MAC](#) Ethernet ou Wi-Fi)

Adressage et encapsulation



Le protocole IP

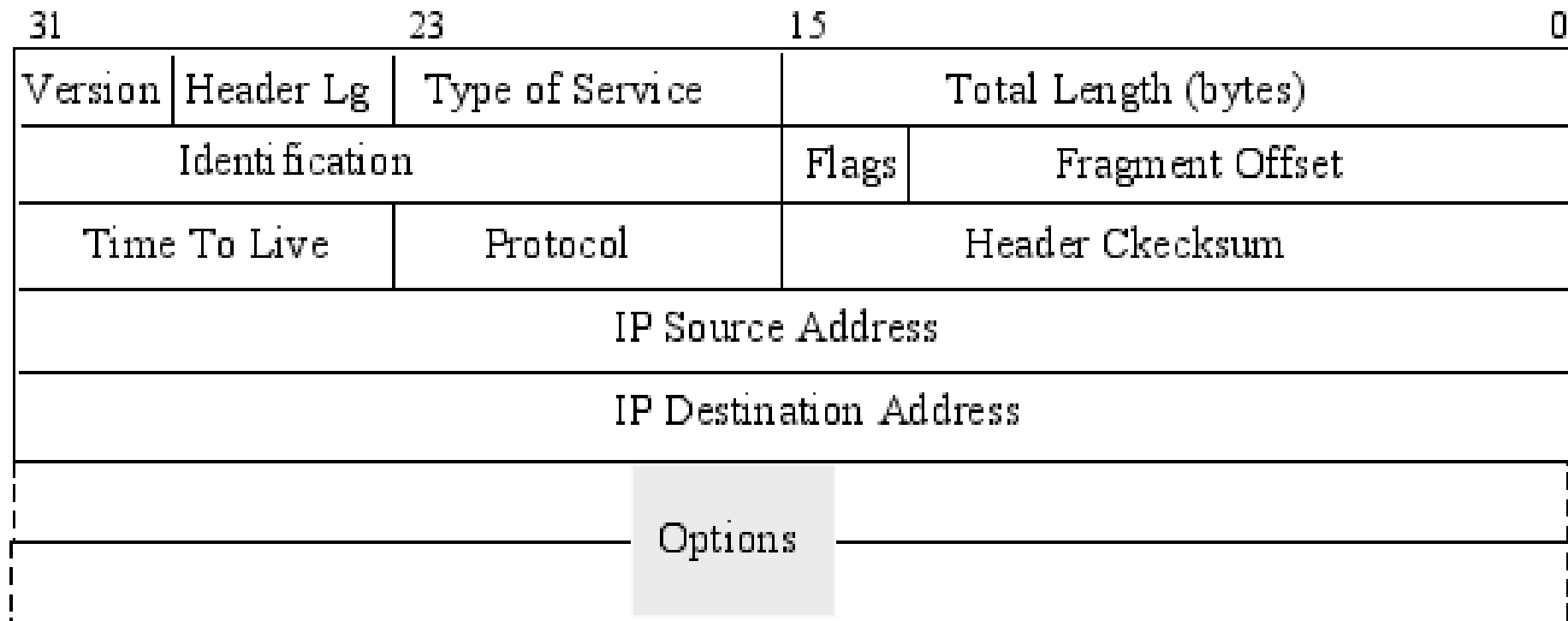
- **Fonction** : assurer l'**acheminement** des unités de données « paquets IP » ou « datagrammes IP » dans l'inter-réseau.
- Service **sans** contrôle d'erreur ni contrôle de flux de bout en bout.
- Service de base de type BE « **Best Effort** », d'autres classes de services sont définies : LBE (Less than Best Effort), BBE (Better than Best Effort), Real-Time, etc.
- Service de **fragmentation** des données si les réseaux traversés ont des **MTU** « **Maximum Transfer Unit** » de valeurs différentes.
- Deux versions du protocole :
 - **IPV4** : adresses sur 32 bits (**IETF RFC 791, 1981**)
 - **IPV6** : adresses de 128 bits (**IETF RFC 2460, 1998**)

Format des paquets IPv4

20 octets (+ options)



Longueur maximale: configurable, inférieure à 64 Koctets



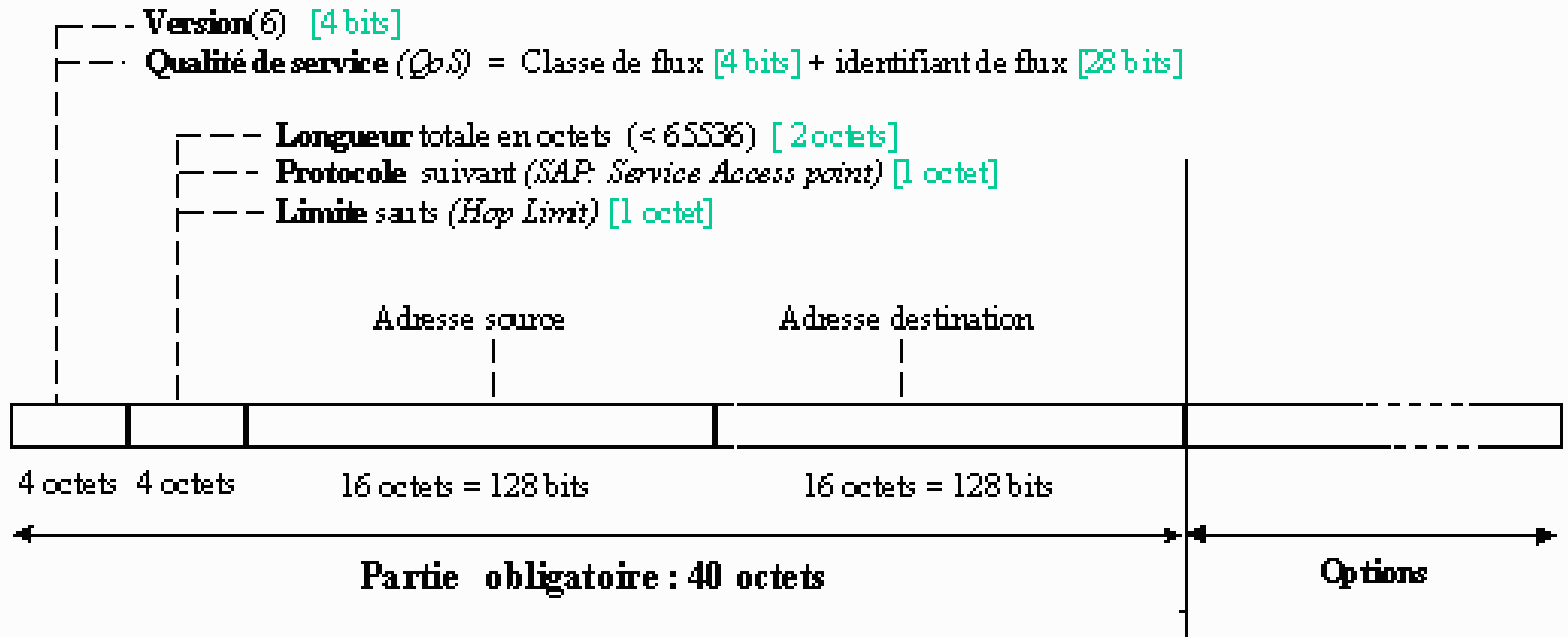
Champs de l'en-tête IPv4

- **Version** (4 bits) : valeur = 4.
- **Header Lg** (4 bits) : longueur de l'en-tête en mots de 32 bits.
- **Type of Service** ou champ DS (DiffServ) : LBE, BE, BBE, etc.
- **TTL « Time To Live »** (1 octet) : nombre maximum de routeurs que le paquet est autorisé à traverser, décrétementé par chaque routeur traversé.
- **Protocol** : identifiant du protocole en charge du champ Information (ce qu'il y a dans le paquet IP !) :
ICMP = $(01)_{16}$, TCP = $(06)_{16}$, UDP = $(17)_{16}$.
- **Source Address** : adresse IP de la station émettrice du paquet.
- **Destination Address** : adresse IP de la station réceptrice du paquet.

Les limites d'IPv4

- Adressage sur 32 bits $\rightarrow 2^{32}$ adresses disponibles (~ 4 milliard).
- Attribution des « lots d'adresses » et des noms de domaines de plus haut niveau par l' « Internet Corporation for Assigned Names and Numbers » (**ICANN**) de droit privé. Délégation aux **RIR** (Registres Internet Régionaux) comme **RIPE-NCC** en Europe.
- Depuis février 2011, l'ICANN n'a plus de lots nouveaux d'adresses disponibles...
- \rightarrow nécessité de passer à IPv6 : déploiement par les opérateurs, technologie des routeurs à faire évoluer.
- Déploiement d'IP V6 : **statistiques mesurées par google**

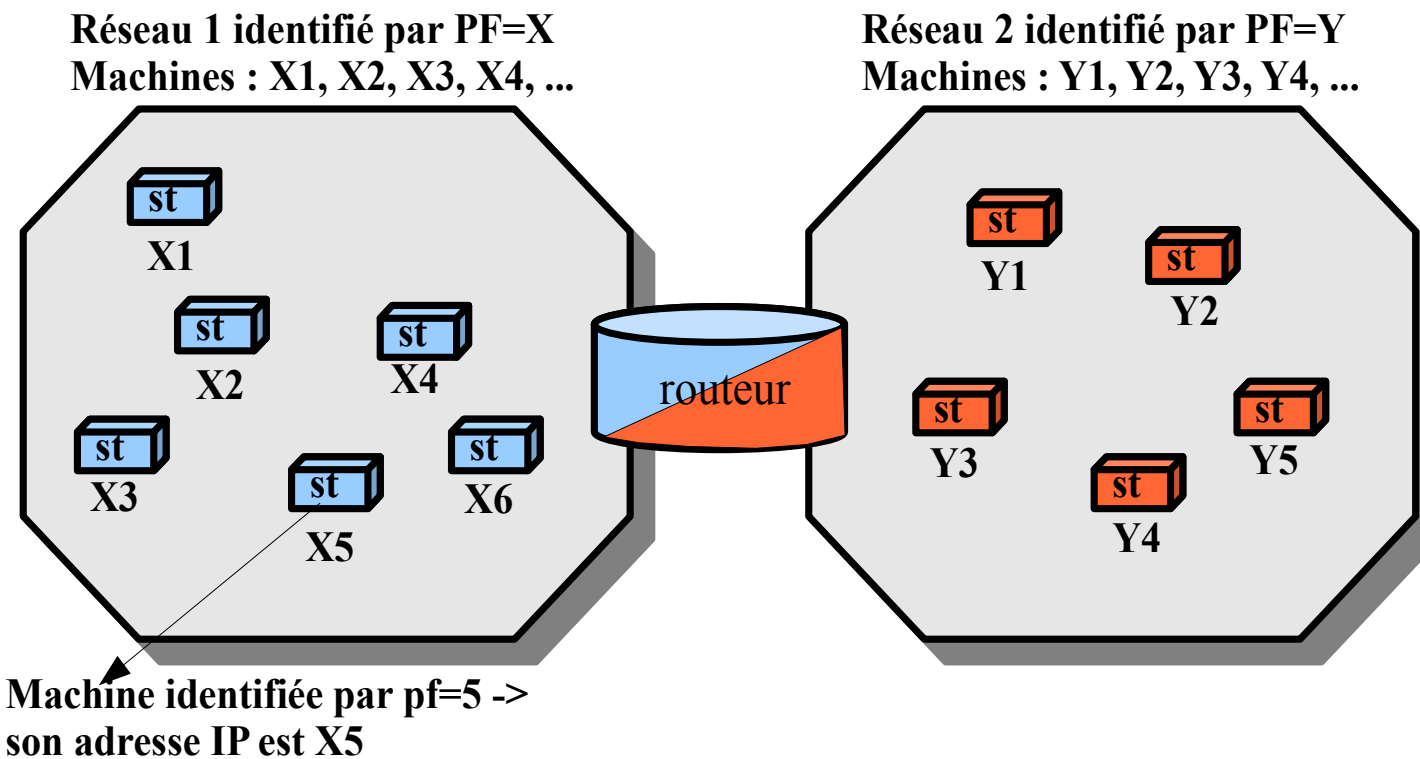
Format des paquets IPv6



- Standard depuis 1999, mais déploiement important depuis 2010 : <http://en.wikipedia.org/wiki/File:Rir-ipv6-allocation-rate.svg>
- Adressage sur 128 bits, soit $2^{128} = 3,4 \times 10^{38}$ adresses.
- Pas de fragmentation, pas de checksum de l'en-tête.
- Définition de plusieurs niveaux de qualité de service (QoS).

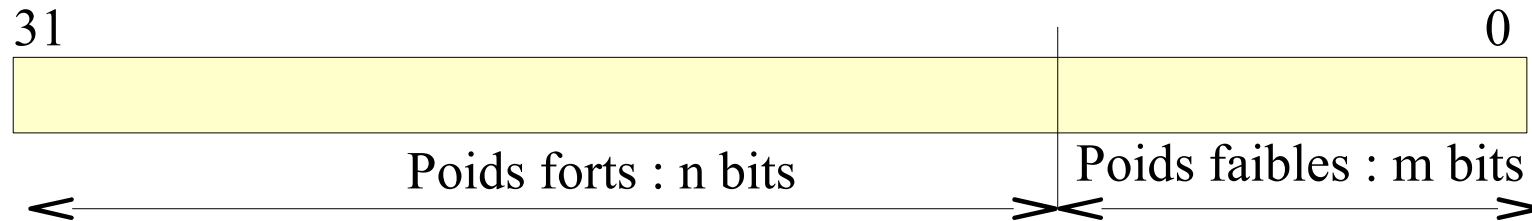
Principe de l'adressage IP V4

- Adressage **hiérarchique** de base :
 - Identification du réseau -> **poids forts** (PF) de l'adresse IP
 - Identification de chaque machine dans le réseau -> **poids faibles** (pf) de l'adresse IP
- **Réseau IP** : défini par une suite d'adresses **contiguës**, donc avec la même valeur des bits de poids forts



Adressage IP V4

- **Format d'adresse** : suite de $32 = n + m$ bits
 n bits pour identifier le réseau + m bits pour identifier la machine dans ce réseau.



- Un réseau IP, identifié par ses n bits de poids forts, possède 2^m valeurs appelées « **plage d'adresses** », réparties en :
 - l'adresse IP du réseau : les m bits sont tous à **0**
 - les adresses des machines : au maximum $2^m - 2$ machines
 - une adresse de diffusion : les m bits sont tous à **1**
- **Masque de réseau** :
 - Identifie la séparation entre la partie réseau (n premiers bits) et la partie machine (les m derniers bits)
 - **Masque** = tous les n bits sont à 1 et tous les m bits sont à 0

Exemple d'adresses dans un réseau IP

- Réseau de 11 stations :
 - $2^4 = 16 \rightarrow$ 4 bits nécessaires pour identifier chaque station
 - Nombre de bits de la partie réseau : $32 - 4 = 28$ bits
(11000000 100000011 00001111 0001)
 - Masque de ce réseau : 11111111 11111111 11111111 11110000

	Partie réseau				Partie machine
Adresse du réseau	11000000	10000011	00001111	0001	0000
Adresse station 1	11000000	10000011	00001111	0001	0001
Adresse station 2	11000000	10000011	00001111	0001	0010
Adresse station 11	11000000	10000011	00001111	0001	1011
Adresse non utilisée	11000000	10000011	00001111	0001	1101
Adresse de diffusion	11000000	10000011	00001111	0001	1111

Notations des adresses IP

- Notation des adresses sous forme « décimale pointée » : les 32 bits sont découpés en 4 octets et chaque octet est codé en décimal :
 - Ex: 11000000 100000011 00001111 00010001
192 . 131 . 15 . 17
- Notation CIDR (Classless Inter-Domain Routing) :
 - Définition : Adresse IP / nombre de bits du préfixe réseau.
 - Cas d'une adresse de réseau IP : 192.18.131.0/24, 24 bits de préfixe réseau
 - Il reste 8 bits pour la partie adresse machine : $2^8 - 2$ machines
 - Adresse de diffusion dans ce réseau : 192.18.131.255
 - La notation CIDR d'une adresse de réseau est **équivalente** à celle qui consiste à donner l'adresse du réseau et la valeur du **masque de ce réseau**.
- Classification historique: classe A (/8) classe B (/16) classe C (/24)
- Adresses de réseaux privés : 192.168.x.0/24 et 10.0.0.0/8

Sous-réseau IP

- Possibilité de répartir les adresses d'un réseau IP ... pour créer de nouveaux réseaux IP... plus petits!
- Un sous-réseau IP **est un** réseau IP -> respect de la **contiguïté** des adresses allouées.
- Découpage en déplaçant « vers la droite » la limite de répartition partie réseau / partie machine. Exemple :
 - Réseau initial en /24 -> répartition : 24+8
 - Pour faire 4 sous-réseaux, on prend les 2 bits de poids forts de la partie machine : 24+2=26, 8-2=6, 26+6=32.
 - Les 4 valeurs différentes de ces 2 bits définissent 4 sous-réseaux :
 - Sous-réseau 1 : **00** 000000 à **00** 111111
 - Sous-réseau 2 : **01** 000000 à **01** 111111
 - Sous-réseau 3 : **10** 000000 à **10** 111111
 - Sous-réseau 4 : **11** 000000 à **11** 111111

Lien entre adresse IP et adresse MAC : le protocole ARP

- Quand un paquet IP doit être acheminé d'une station vers une autre du même réseau physique, il faut déterminer l'adresse MAC du destinataire pour former la trame (contenant ce paquet) avec la bonne adresse MAC destination : **@IP => @MAC ?**
- **ARP : Address Resolution Protocol**
 - ARP permet d'associer une adresse MAC à l'adresse IP correspondant à la même (carte de) machine.
 - **Protocole ARP :**
 - Émission d'une **requête ARP** en **Broadcast** demandant l'adresse MAC de la machine dont l'adresse IP est donnée en paramètre.
 - La **réponse ARP** est renvoyée par la station qui a cette adresse MAC.
 - Stockage de ce couple (**@IP, @MAC**) pour une durée limitée dans une table appelée « **cache ARP** ».
 - Accès au cache ARP par la commande : **ip neigh** (pour neighbour). 17

Glossaire

- Adresse de diffusion
- Architecture TCP/IP
- ARP
- Best-effort
- CIDR
- Classe de réseaux (A, B, C)
- DHCP
- DNS
- FTP
- HTTP
- ICMP
- ICANN
- IMAP
- Interface
- IPV4
- IPV6
- Masque de réseau
- MTU
- Plage d'adresses
- Préfixe réseau
- POP
- SMTP
- Sous-réseau
- TTL

Module M2102

Architecture des réseaux

Chapitre 3

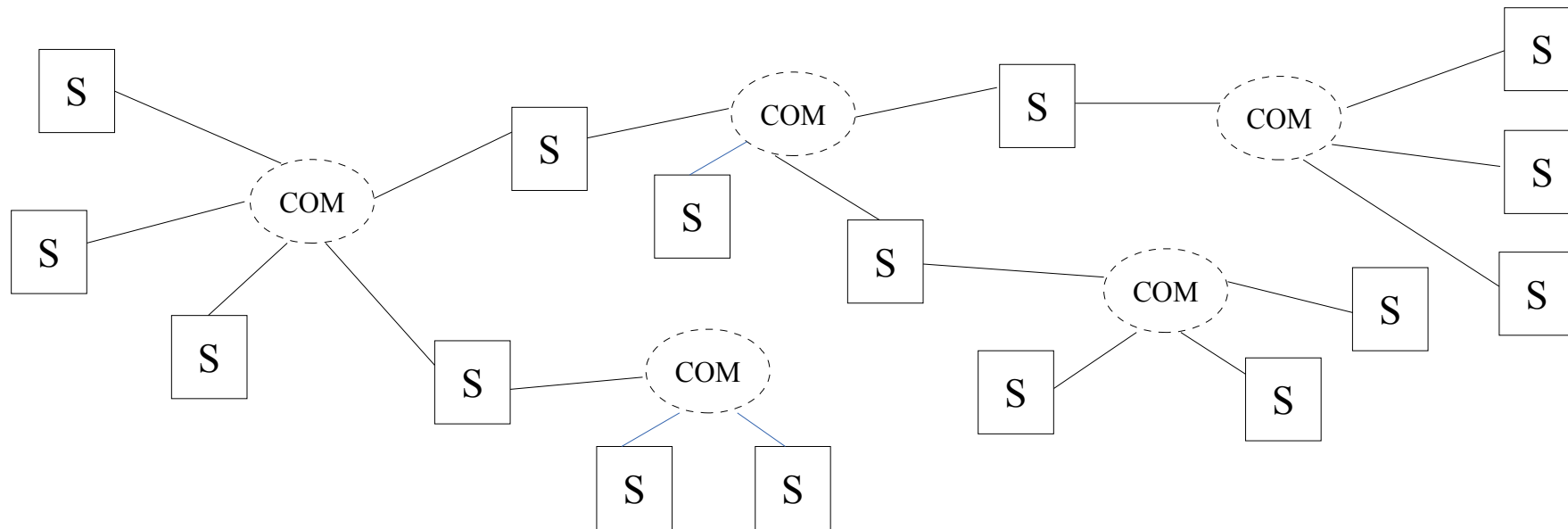
Protocole Internet IP : routage IP

Lectures préalables :

- [Routage sur Wikipédia](#)
- [Routage IP sur FrameIP](#), [Routage IP sur wikibooks](#)

Définition du routage

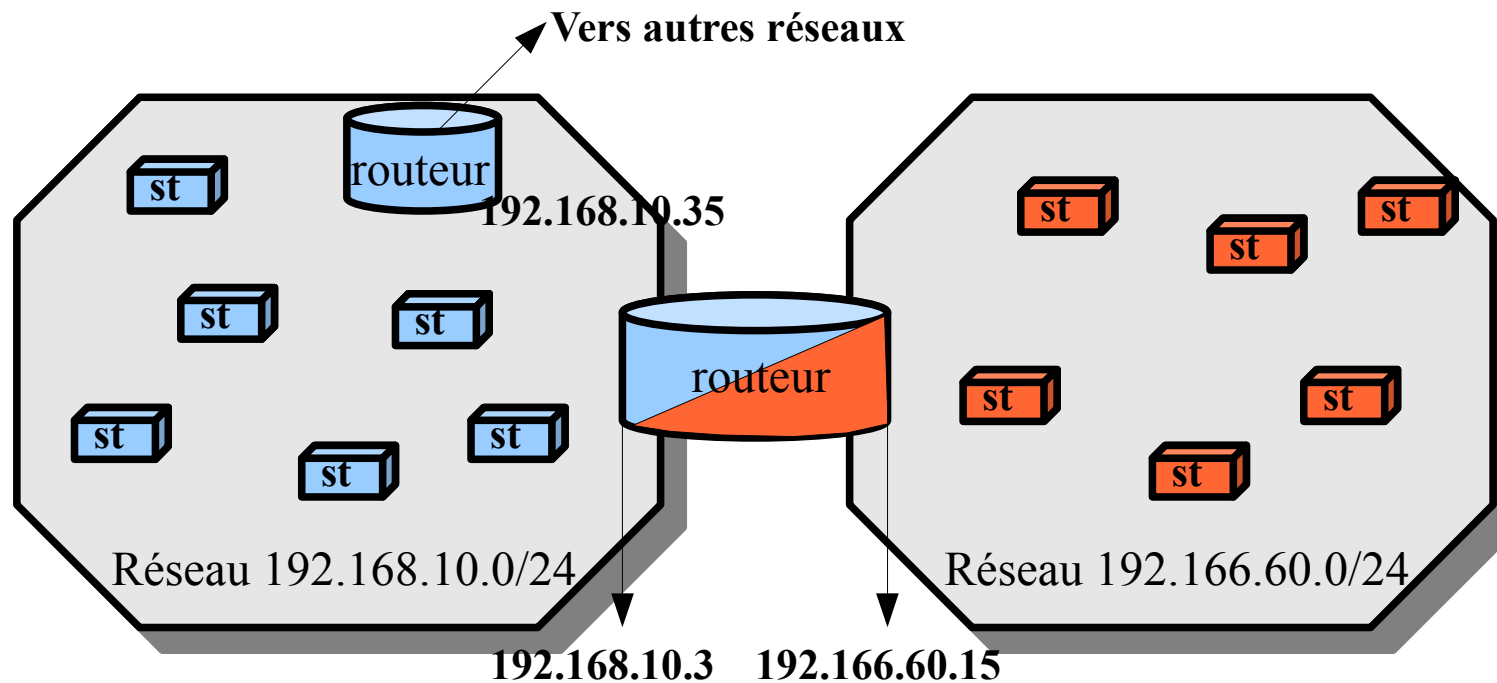
- Dans l'Inter-réseau Internet, la sélection d'un chemin partant de la source vers la destination est appelée **le routage**.



- Un chemin passe par 3 types de stations : la source, un nombre variable de routeurs (y compris 0) et la destination.
- La fonction de routage démarre dès la source.

Routeur IP

- Un routeur IP est un équipement connecté à plusieurs réseaux IP pour permettre l'acheminement des paquets d'un réseau à l'autre :
 - Il a une adresse logique (IP) dans chacun des réseaux auquel il est connecté.
 - Il a une adresse physique (MAC) dans chacun des réseaux auquel il est connecté.



Routage IP

- Principe : lorsqu'un paquet IP arrive dans un routeur, celui-ci retransmet le paquet :
 - Soit **directement à la station** destinataire si celle-ci est connectée au routeur (elle est dans un même réseau)
 - Soit **vers un autre routeur** auquel il est directement connecté... le routage se fait « de proche en proche »
- La détermination de la route suivante se fait par une **table de routage** :
 - Table de correspondance entre adresse de réseau destinataire et **routeur suivant** (avec **interface** d'envoi de la trame).
- Ce principe s'applique à toute station, **même si elle n'est pas routeur** : toute station d'un réseau IP a une table de routage, en particulier la station source.

Table de routage d'un routeur

- **Structure de la table** : tableau d'autant de lignes que de réseaux destinataires identifiés + 1 ligne « défaut » (Destination = 0.0.0.0) désignant tous les autres réseaux :

Colonnes principales : **Destination Gateway Genmask Iface (Interface)**

- **Destination & Genmask** : pour identifier le **réseau** auquel appartient la machine **destinataire** du paquet
- **Gateway & Iface** : pour déterminer vers quelle direction et quelle trame envoyer : vers un routeur (Gateway) ou vers le destinataire final si Gateway est vide (noté 0.0.0.0 ou noté *).

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.10.35	0.0.0.0	eth0
192.168.10.0	0.0.0.0	255.255.255.0	eth0
192.166.60.0	0.0.0.0	255.255.255.0	eth1

- Attention : la colonne destination indique des **réseaux de destination** (ensemble de machines) mais non des adresses de machines.

Algorithme de routage

Principe : pour chaque paquet à envoyer, chaque ligne est essayée successivement jusqu'à trouver une correspondance entre l'adresse IP destinataire et une adresse réseau de la colonne **Destination**.

Si (adrIP-dest && Genmask) == adrDestination alors Trouvé

(&& = ET logique)

- **adrIP-dest** est l'adresse IP de la **machine** destinatrice contenue dans le champ *@destination* du paquet à acheminer.
- **adrDestination** est la valeur de la colonne *Destination* de la ligne de la table de routage (c'est une adresse de **réseau**).
- Quand le champ *Destination* est à « 0.0.0.0 », c'est pour indiquer le routeur à utiliser pour toutes les adresses non identifiées dans les autres lignes (routage par « défaut »).

Routage depuis une station pc-dg-xxx-yy

Commandes : **netstat -rn** ou **/sbin/route**

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.141.19	0.0.0.0	eth0
192.168.141.0	0.0.0.0	255.255.255.0	eth0

- Si le destinataire du paquet est une machine du réseau 192.168.141.0/24, c'est une station du **même réseau** que la station pc-dg-xxx-yy :
 - La station pc-dg-xxx-yy envoie le paquet IP par l'interface *eth0* **directement** au destinataire : il n'y a donc pas de routeur à utiliser (Gateway = 0.0.0.0).
 - L'*@MAC* destination de la trame envoyée est obtenue à partir de l'adresse IP du destinataire en faisant appel au protocole **ARP**.
- Dans tous les autres cas (le destinataire du paquet est une machine d'un autre réseau), le paquet sera redirigé vers le routeur d'*@IP* : 192.168.141.19 (nom : sw-dg-040d-1-tx), par la même interface *eth0*.

Exemple de tables de routage

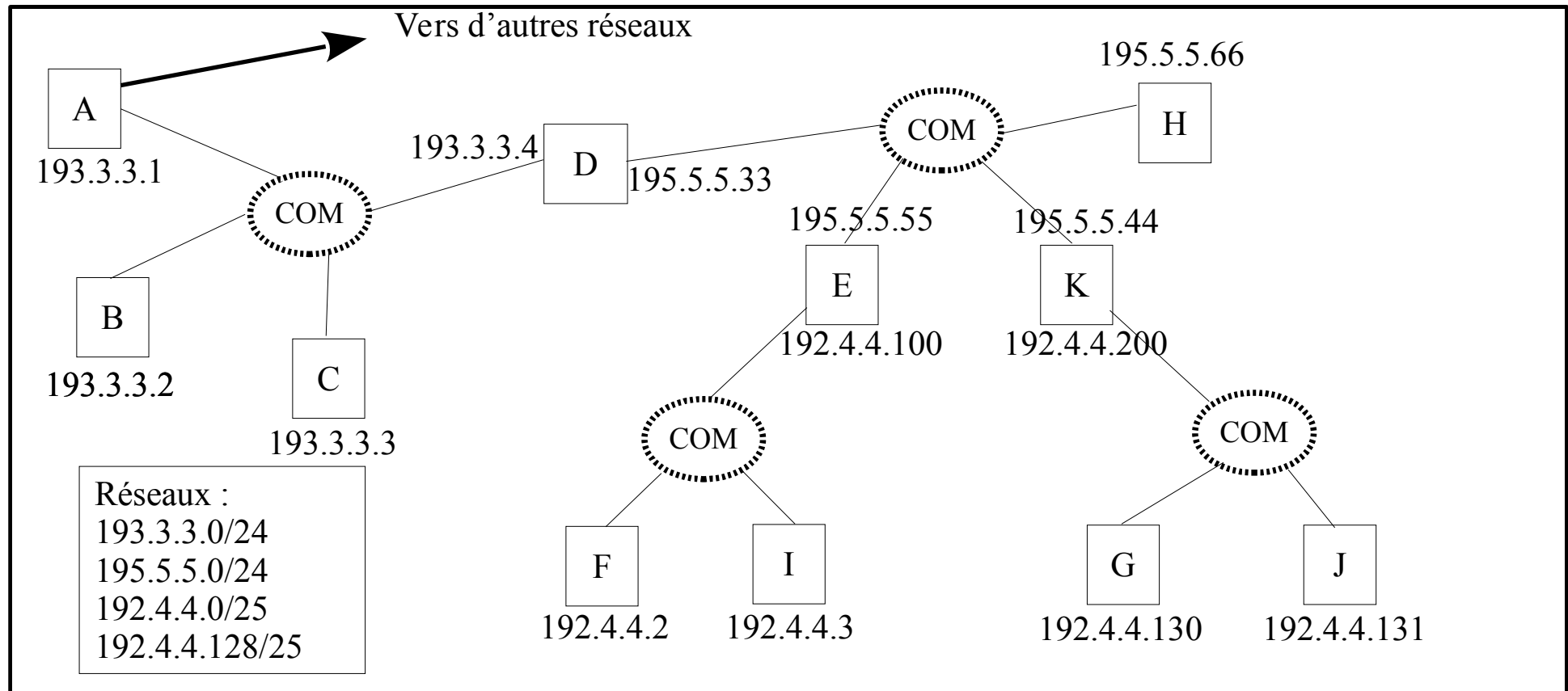


Table de routage de la **machine B** :

Destination	Gateway	Genmask	lface
0.0.0.0	193.3.3.1	0.0.0.0	eth0
193.3.3.0	0.0.0.0	255.255.255.0	eth0
195.5.5.0	193.3.3.4	255.255.255.0	eth0
192.4.4.0	193.3.3.4	255.255.255.0	eth0

Table de routage de la **machine D** :

Destination	Gateway	Genmask	lface
0.0.0.0	193.3.3.1	0.0.0.0	eth0
193.3.3.0	0.0.0.0	255.255.255.0	eth0
195.5.5.0	0.0.0.0	255.255.255.0	eth1
192.4.4.0	195.5.5.55	255.255.255.128	eth1
192.4.4.128	195.5.5.44	255.255.255.128	eth1

Routage dans la station D

- **Cas d'un paquet émis par B vers H (@IP= 195.5.5.66) :**
 - $195.5.5.66 \ \&\& \ 255.255.255.0 = 195.5.5.0 \rightarrow \text{Gateway} = 0.0.0.0$
 - C'est un acheminement **direct** de D au destinataire H puisqu'ils sont sur un même réseau : 195.5.5.0/24.
- **Cas d'un paquet émis par B vers F :**
 - $192.4.4.2 \ \&\& \ 255.255.255.128 = 192.4.4.0 \rightarrow \text{Gateway}=195.5.5.55$
 - C'est un acheminement vers un autre **routeur** (station E sur le réseau 195.5.5.0/24) car le destinataire F n'est pas situé sur un même réseau que D.
- **Exercices :**
 - **routage d'un paquet émis par E vers A, de A vers G**
 - **faire la table de routage de la station E**

Module M2102

Architecture des réseaux

Chapitre 4

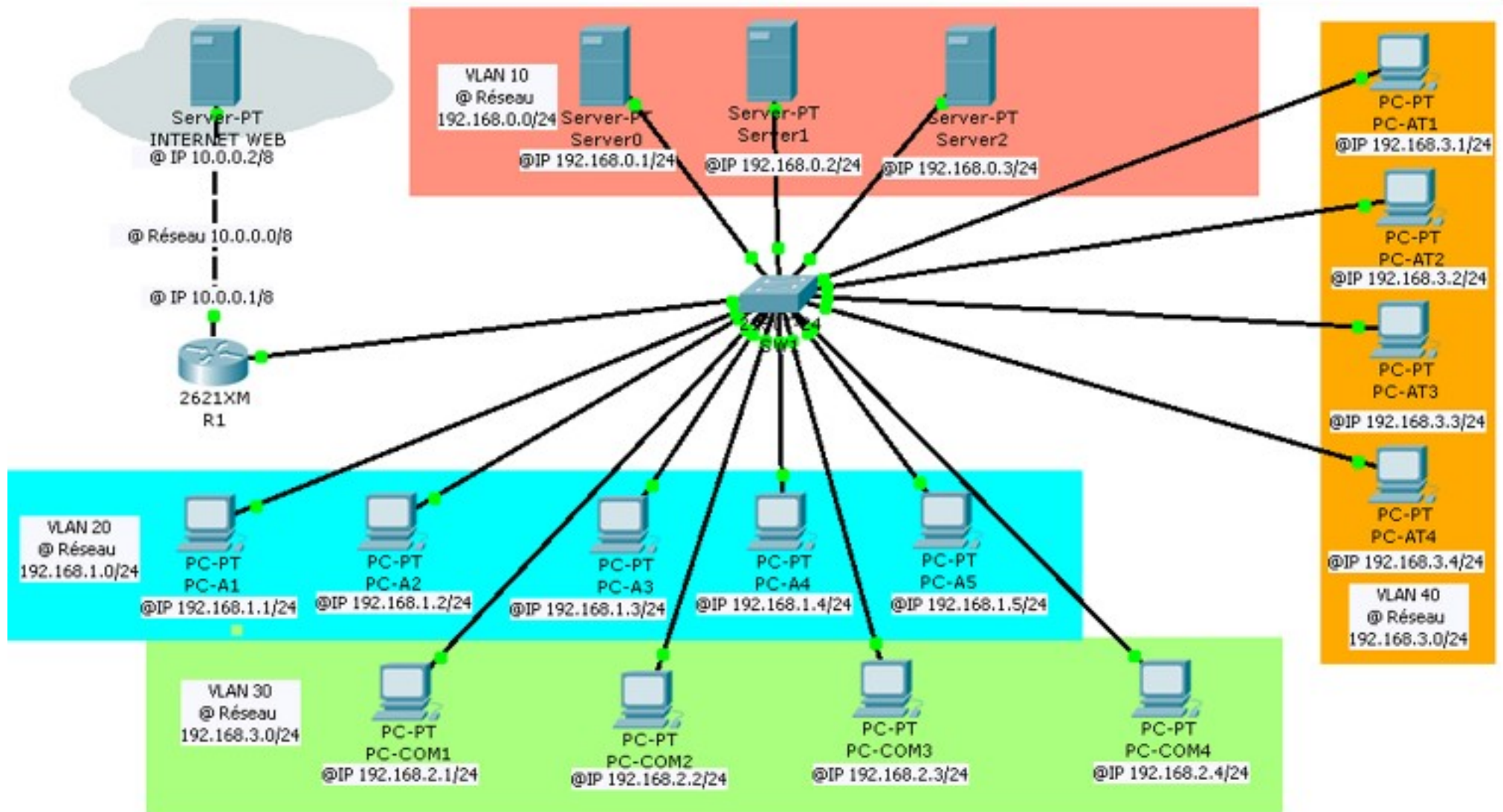
Réseaux locaux virtuels

VLAN

Lectures préalables :

- [VLAN sur wikipedia](#)
- [VLAN sur wikibooks](#)

Exemple : 4 VLANs et un switch2-3

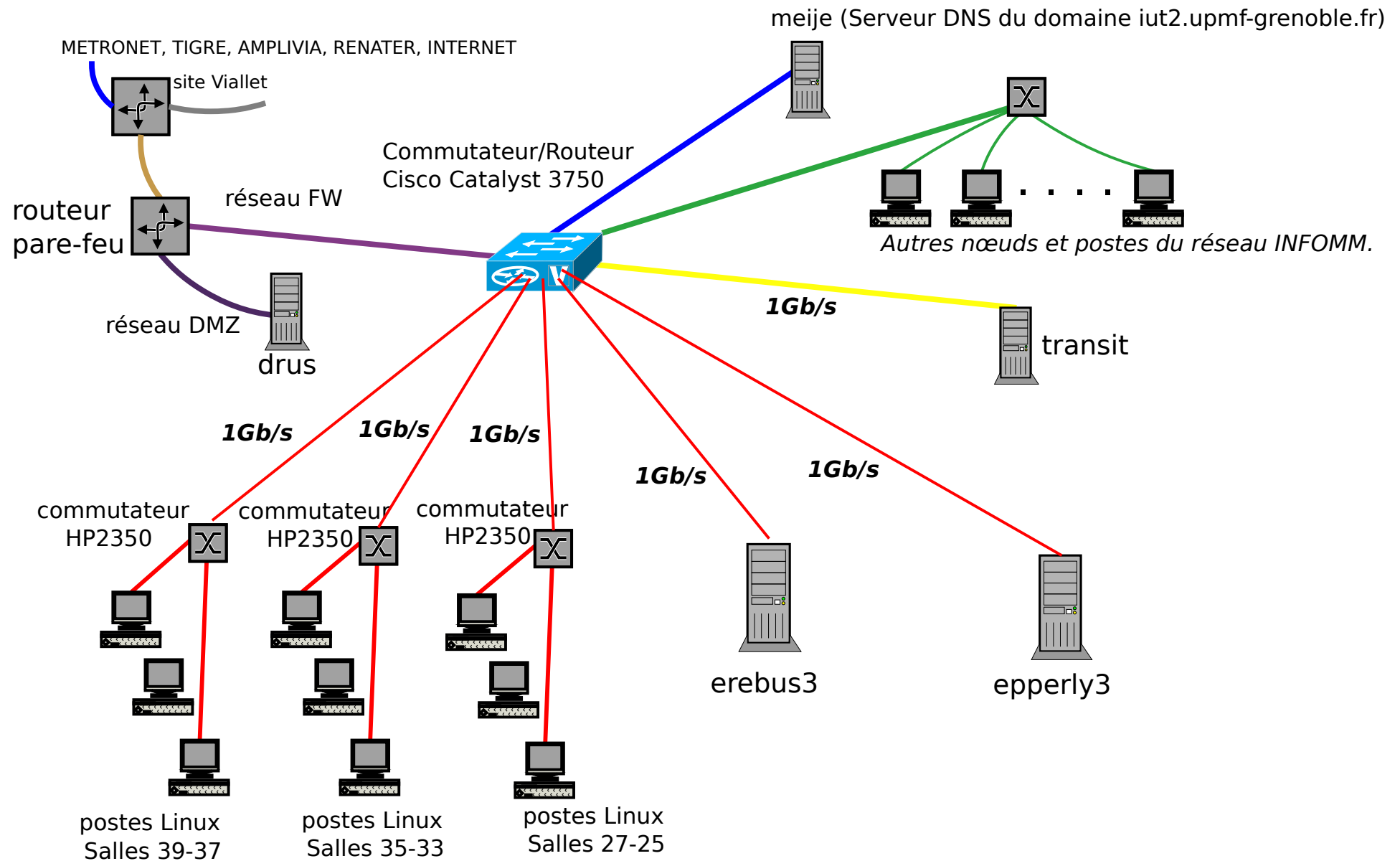


Source : <http://www.tech.agopyan.fr/Cisco/Images/im-pac-tr.png>

Vocabulaire

- **Réseau local virtuel (VLAN : Virtual Local Area Network) :**
 - Réseau local : technologie Ethernet (ou Wi-Fi).
 - Virtuel : dissociation entre la structure matérielle du réseau et la définition de réseaux IP.
 - Principe : diviser un réseau local (physique) en plusieurs réseaux logiques (IP) appelés VLAN.
 - Équipement qui permet cette organisation en VLAN : le switch2-3 ou commutateur-routeur.
- **Switch2-3 (ou commutateur-routeur, ou switch multi-niveaux).** Il assure à la fois :
 - Une fonction de commutation Ethernet (niveau liaison ou niveau « MAC » des réseaux locaux = niveau 2).
 - Une fonction de routage IP (niveau réseau = niveau 3).

Le switch2-3 de l'IUT2



Description du Cisco Catalyst 3750



- 24 (48) port Ethernet 100Mb/s, 2 (4) ports Gigabit Ethernet.
- Facilité d'utilisation, de déploiement et d'évolution (interface web, auto-configuration, auto-négociation, empilement).
- Redondance pour assurer le service en cas de défaillance.
- Qualité de service : gestion de trafic différenciée selon QoS (4 files de sortie par port), limitation adaptative du débit.
- Fonctions de sécurité pour l'ensemble du réseau.

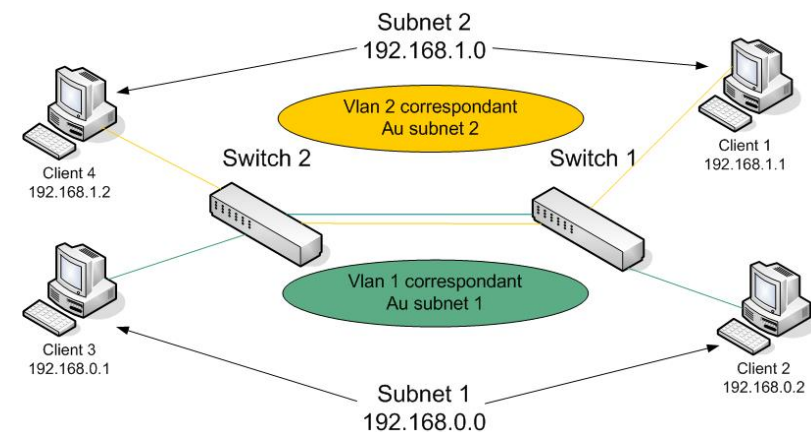
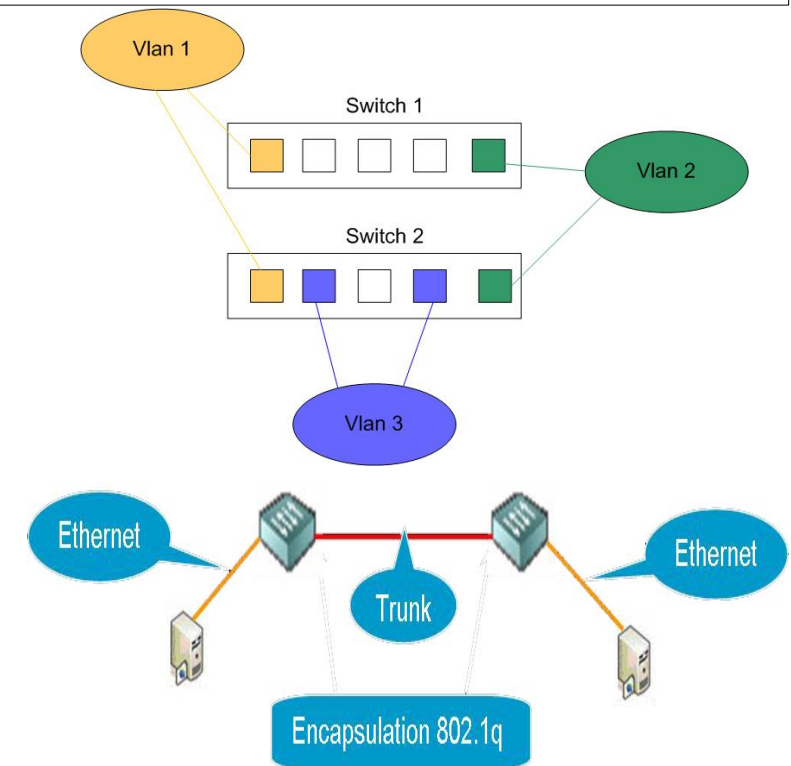
Principe de fonctionnement

- Un switch2-3 permet de répartir les stations qui lui sont connectées en plusieurs réseaux IP **virtuellement** indépendants (VLANs) :
 - Un VLAN fonctionne comme un réseau local Ethernet : les stations d'un même VLAN font partie du même réseau local Ethernet (et donc du même réseau IP).
 - Chaque VLAN étant un réseau IP, il a une adresse de réseau IP et un espace d'adresses IP avec une @IP par station qui en fait partie, **plus une @IP pour le switch2-3**.
 - Le switch2-3 utilise la **commutation Ethernet** pour faire communiquer les stations d'un même VLAN (table de commutation : N° de ports du switch ↔ adresses MAC).
 - Pour les échanges entre stations de VLANs différents, le switch2-3 utilise le **routage IP** (table de routage, @ IP).
- Avantages : administration centralisée des réseaux, évolutivité plus grande, isolation des trafics (sécurité).

Types de VLANs

Source : <http://www-igm.univ-mlv.fr/~dr/XPOSE2006/SURZUR-DEFRANCE/vlan.html>

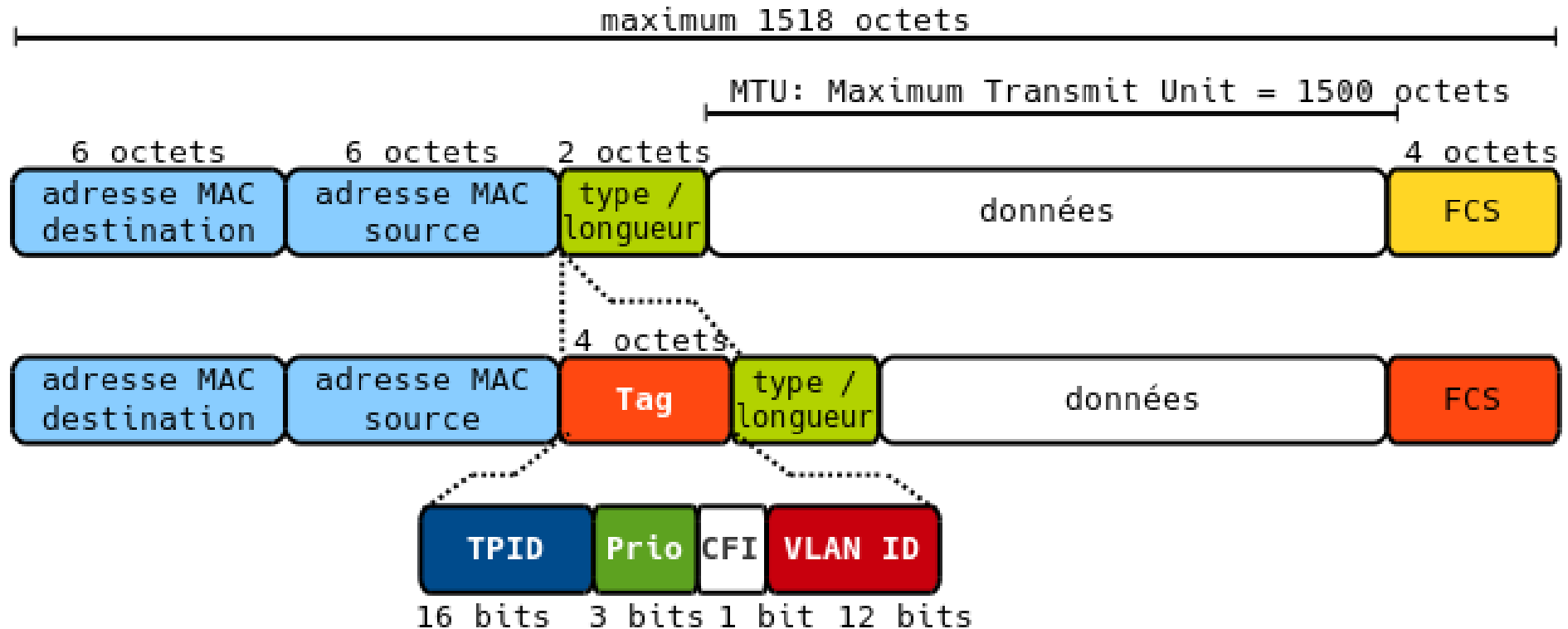
- VLAN de niveau 1 : répartition des stations dans les VLANs en fonction des ports des switch2-3 :
 - Mise en place simple sauf si les VLANs sont sur plusieurs switches (utiliser 802.1q).
 - Très bonne sécurité.
- VLAN de niveau 2 : chaque VLAN est défini par la liste des @MAC des stations :
 - Configuration centralisée entre switches.
 - Sécurité moyenne (usurpation d'@MAC)
- VLAN de niveau 3 : chaque VLAN est défini par son @IP de réseau :
 - Appartenance automatique d'une station par son @IP (mais plus lent car niveau 3).
 - Sécurité faible (usurpation d'@IP).



Répartition des stations dans les VLANs

- Répartition statique de niveau 1 : un VLAN est défini comme l'ensemble des stations reliées par un **ensemble donné de ports** d'un switch2-3 :
 - Les stations d'un même port font toujours partie du même VLAN.
 - Les trames échangées entre les stations d'un même VLAN sont des trames Ethernet standard.
- Répartition dynamique de niveau 1 avec un **identifiant**, dans le cas d'un inter-réseau formé de plusieurs switch2-3 :
 - Les ports des switch2-3 sont affectés chacun à un VLAN.
 - Les stations d'un même VLAN sont librement réparties.
 - Chaque VLAN est identifié par un VLAN ID (VID) sur 12 bits.
 - Le protocole 802.1q est activé entre les switch2-3 pour que les trames échangées soient des « tagged frames » comprenant dans l'en-tête le champ d'identification de VLAN (VID) permettant aux switch2-3 de rediriger correctement les trames.

Format de trame 802.1q



Le champ **TPID** a pour valeur 0x8100 pour identifier le mode « tagged frame » du protocole 802.1q, et différencier les trames Ethernet simples qui ont juste le champ **Type**.

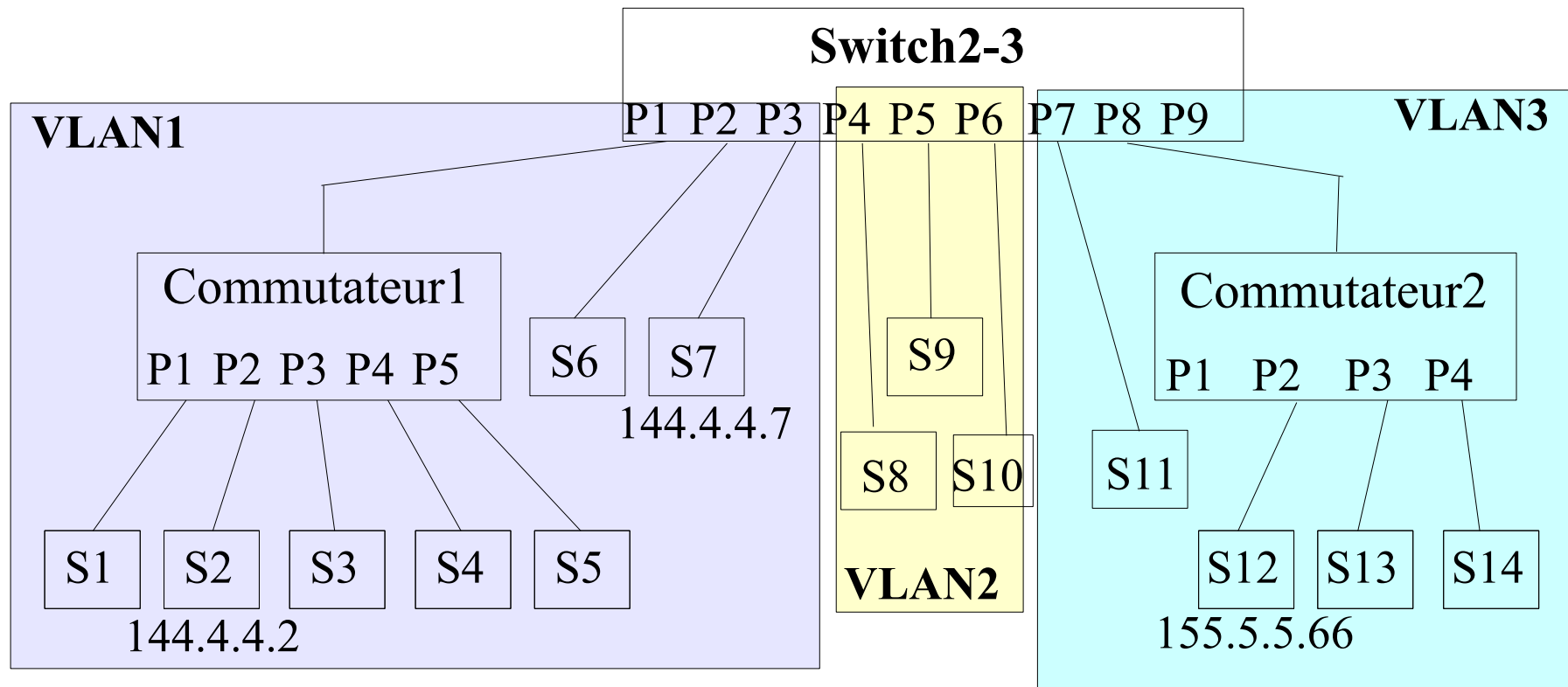
Source :

<https://inethoc.net/articles/inter-vlan-routing/inter-vlan-routing.vlan.html#inter-vlan-routing.vlan.dot1q>

Voir aussi : https://en.wikipedia.org/wiki/IEEE_802.1Q

Mise en œuvre de VLANs

Exemple de configuration statique



Trois VLANs :

VLAN1 : (P1, P2, P3) @IP:144.4.4.0/24

VLAN2 : (P4, P5, P6) @IP:155.5.5.32/27

VLAN3 : (P7, P8, P9) @IP: 155.5.5.64/26

Adresses du switch2-3

- C'est un routeur IP : il a donc autant d'adresses IP que de réseaux VLAN IP qu'il définit :
 - @IP dans le VLAN1 : 144.4.4.32
 - @IP dans le VLAN2 : 155.5.5.48
 - @IP dans le VLAN3 : 155.5.5.65
- À ces adresses IP sont associées des adresses MAC :
 - @MAC (P1, P2, P3) : 00:0D:29:E3:63:44
 - @MAC (P4, P5, P6) : 00:0D:29:E3:63:45
 - @MAC (P7, P8, P9) : 00:0D:29:E3:63:46

Tables du switch2-3

- **Table de commutation** utilisée pour tous les échanges entre stations d'un **même** VLAN (équivalente à 3 tables de commutation).

@MAC dest	n° port
@MAC S1 à S5	P1
@MAC S6	P2
@MAC S7	P3
@MAC S8	P4
@MAC S9	P5
@MAC S10	P6
@MAC S11	P7
@MAC S12 à S14	P8

- **Table de routage** pour les autres échanges :

Destination	Mask	Gateway	Interface
144.4.4.0	255.255.255.0	0.0.0.0	eth0
155.5.5.32	255.255.255.224	0.0.0.0	eth1
155.5.5.64	255.255.255.192	0.0.0.0	eth2

Tables de routage des stations

- Les tables de routage des stations du VLAN1 sont de la forme :

Destination	Mask	Gateway	Interface
144.4.4.0	255.255.255.0	0.0.0.0	eth0
0.0.0.0	0.0.0.0	144.4.4.32	eth0

- Les tables de routage des stations du VLAN2 sont de la forme :

Destination	Mask	Gateway	Interface
155.5.5.32	255.255.255.224	0.0.0.0	eth0
0.0.0.0	0.0.0.0	155.5.5.48	eth0

- Les tables de routage des stations du VLAN3 sont de la forme :

Destination	Mask	Gateway	Interface

commutation ou routage ?

- Cas1: **S2** envoie un paquet à **S7** :
 - Sa table de routage indique que le « gateway » est elle-même.
 - S2 envoie donc directement une trame dont l'adresse destination Ethernet est l'adresse de **S7**.
 - Le switch2-3 reçoit une trame dont il n'est pas le destinataire : il utilise donc sa table de commutation pour envoyer cette trame sur le port 3 où est situé **S7**.
- Cas2 : **S2** envoie un paquet à **S12** :
 - Sa table de routage lui indique que le « gateway » est le switch2-3 d'adresse IP 144.4.4.32.
 - S2 envoie donc une trame Ethernet dont l'adresse destination est l'adresse MAC du switch2-3 sur le réseau 144.4.4.0.
 - Le switch2-3 va faire appel à sa table de routage IP pour pouvoir acheminer ce paquet vers **S12**.

Module M2102

Architecture des réseaux

Chapitre 5

Protocoles UDP et TCP

UDP : User Datagram Protocol

TCP : Transmission Control Protocol

Lectures préalables :

- [TCP sur wikipedia](#)
- [TCP sur comment ça marche](#)

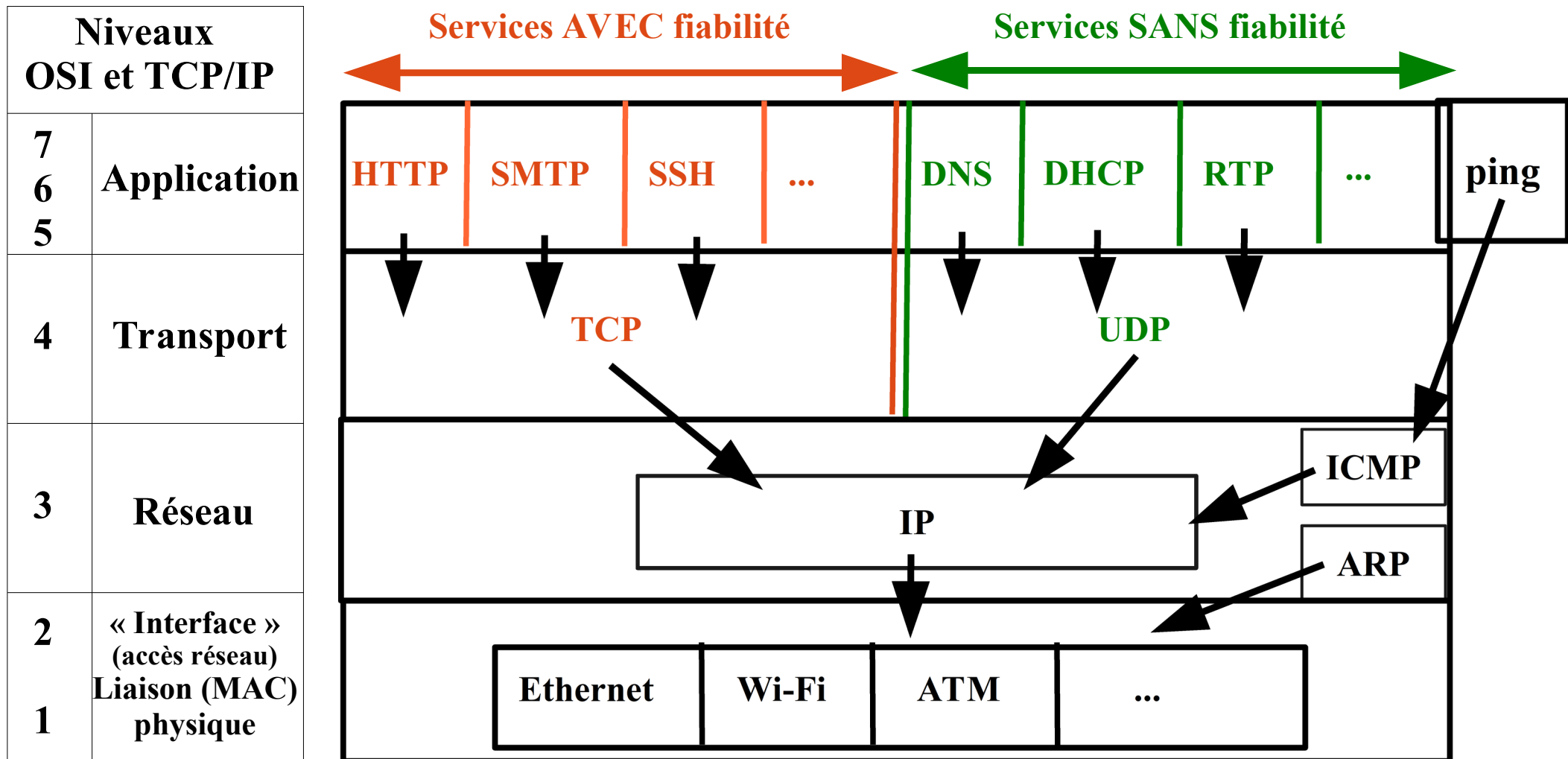
Niveau transport dans l'architecture TCP/IP

Niveau transport :

UDP : service de transport « simple » sans connexion

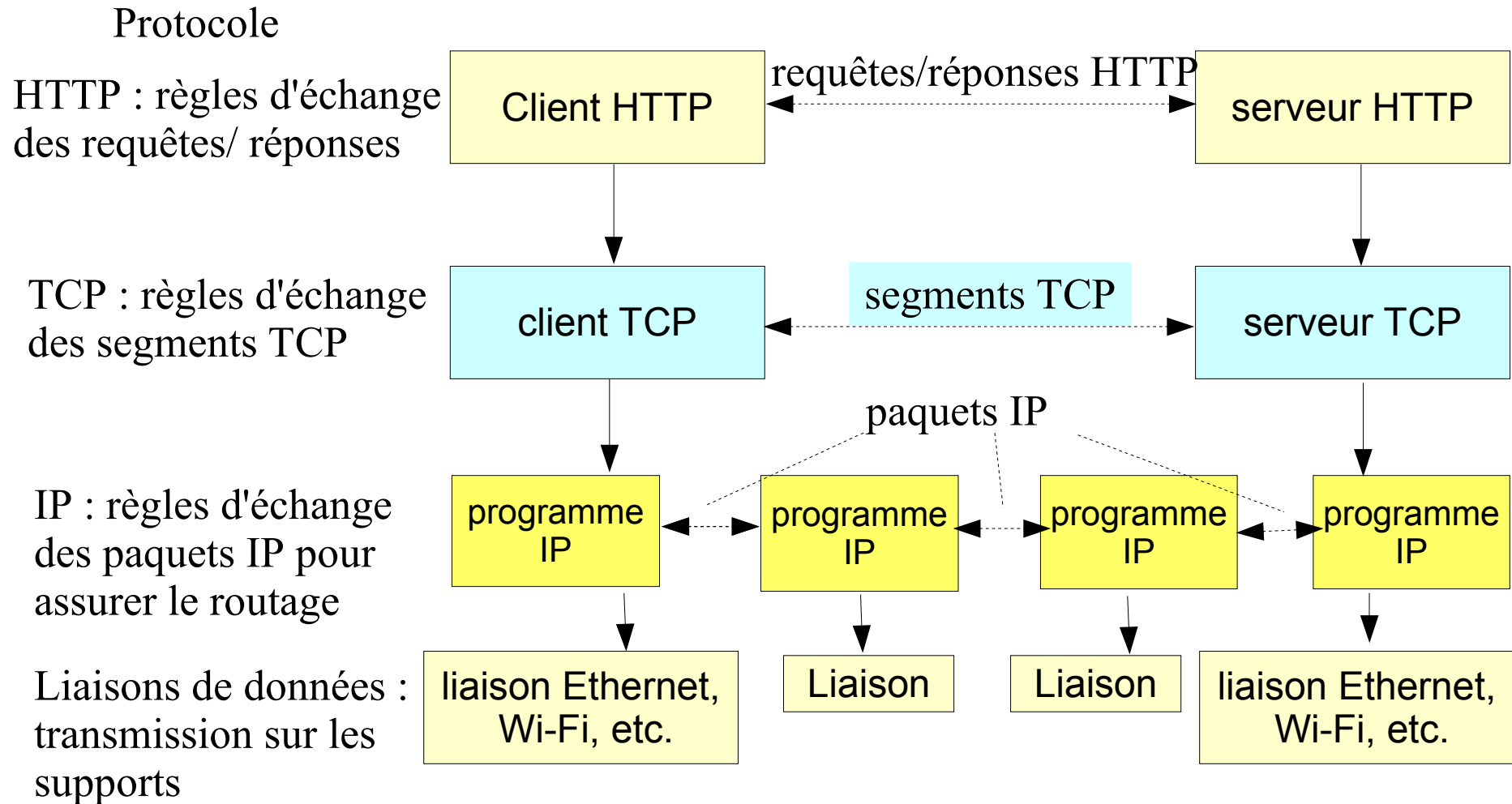
TCP : service de transport avec connexion (fiabilité des connexions)

Source : schéma adapté du cours M3102 - Yann Laurillau



Niveaux de protocole

Exemple des protocoles HTTP/TCP/IP



Mise en place du niveau transport

- **Transport des datagrammes ou des flots d'octets** entre un processus application client et un processus application serveur.
- **Identification des processus client et serveur :**
 - l'adresse IP ne suffit pas : plusieurs appli sur une même station.
 - le numéro de processus système ne convient pas car le « PID » est local et dépend du système utilisé.
 - > **numéro de port** : champ sur 16 bits de l'en-tête TCP ou UDP.
- **Modèle client/serveur :**
 - toute communication est **initialisée par un client**.
 - le numéro de port et l'adresse IP du serveur doivent être connus du (des) client(s) avant toute communication.
 - les échanges de données sont ensuite **symétriques**.

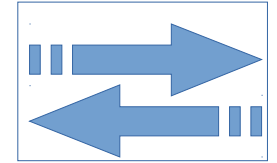
Protocole UDP

- Principe : service de transport minimum et simple ([RFC 768](#))
- Services offerts :
 - Communication directe, dite « sans connexion »
 - Encapsulation : dans un paquet IP (taille max = celle de IP).
 - Pas de fragmentation/réassemblage (mais fait par IP).
 - Multiplexage (plusieurs communications UDP en même temps) : possible en utilisant des n° de port différents.
 - **PAS** de contrôle d'erreur ni de flux.
- Utilisation : services NFS, DHCP, téléphonie, télémessure, jeux.
- Format de l'en-tête d'un **datagramme** UDP :

31	15	0
Source port	Destination port	
Total length (bytes)		Header Checksum

Protocole TCP

- Principes ([RFC 793](#)) :
 - couche logicielle qui masque aux applications les contraintes du réseau (hors les délais induits!).
 - service de **transport fiable en mode flot d'octets**.
- Notion de **connexion TCP** associée au couple constitué du processus client et du processus serveur :
 - < @IP serveur, N° port serveur, @IP client, N° port client >
- Réalisation du **mode flot** :
 - Ouverture de connexion, préalable à tout échange de données.
 - Numérotation des octets de données à émettre.
 - Émission et réception des octets en blocs de **segments**, indépendamment des dépôts et retraits faits par les programmes appli -> stockage en mémoire (tampon) par TCP.

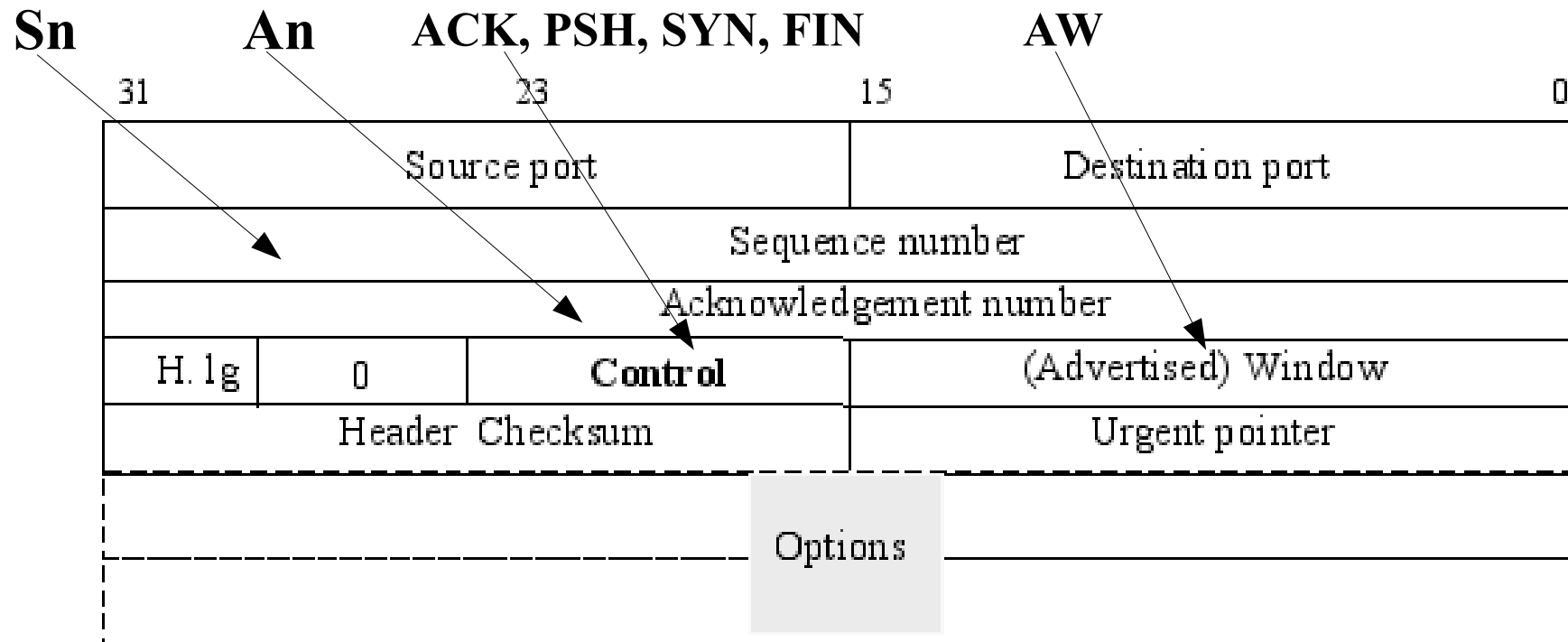


Format des paquets (segments) TCP

20 octets (+ options)



Longueur déterminée par le récepteur grâce au champ Total Length de l'en-tête IP



Champs de l'en-tête TCP

- **Sn : Sequence number** : n° du premier octet contenu dans le champ info (n° dans le flot de données d'émission).
- **An : Acknowledge number** : n° du prochain octet attendu dans le flot de données reçues, acquitte les octets de n° inférieurs.
- **AW : Advertised Window** : fenêtre d'émission (notée ici **W**).
- **H.lg : Header Length** : longueur de l'en-tête, en mots de 32 bits (si pas d'option, H.lg=5).
- **Control (Flags) : <0, 0, URG, ACK, PSH, RST, SYN, FIN>**
 - **SYN** : demande d'ouverture de connexion (O).
 - **FIN** : demande de fermeture de connexion (F).
 - **ACK** : le paquet acquitte des données ou une demande O/F.
 - **PSH** : le segment contient des données qui peuvent être délivrées à l'application.

Étapes de la transmission de données

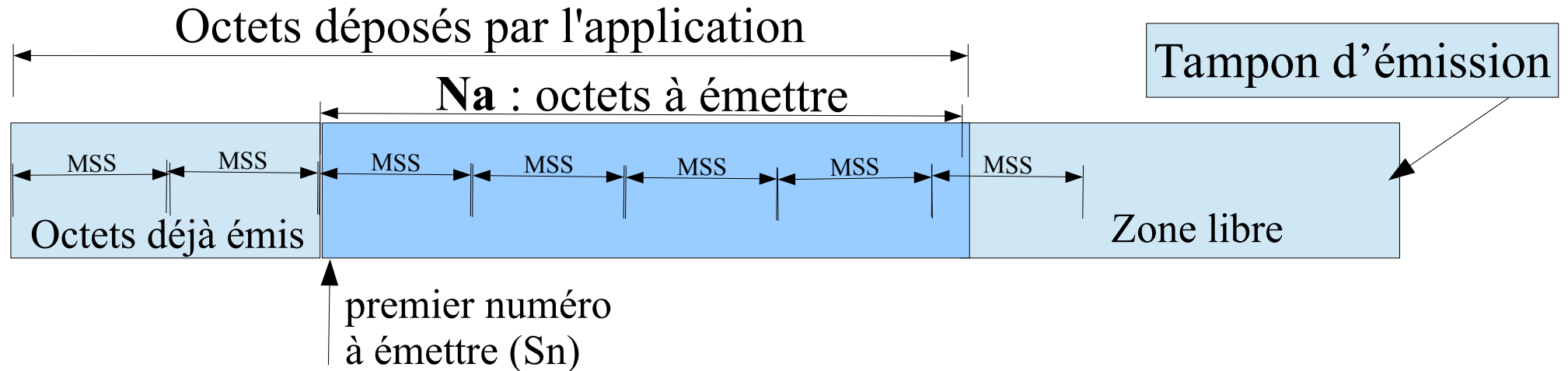
- 1) Le programme application dépose ses données dans le tampon émission.
- 2) Le programme TCP émet ces données en blocs appelés « segments ».
- 3) Le programme TCP côté réception :
 - a) Récupère et stocke ces segments dans le tampon réception.
 - b) Envoie à l'émetteur un acquittement à chaque segment reçu.
- 4) Le programme application récupère les données dans le tampon réception.
- 5) Le programme TCP côté émission libère l'espace du tampon émission des données acquittées par le récepteur.
- 6) Le programme TCP côté réception libère l'espace du tampon réception des données récupérées par l'application.

Émission en TCP-1

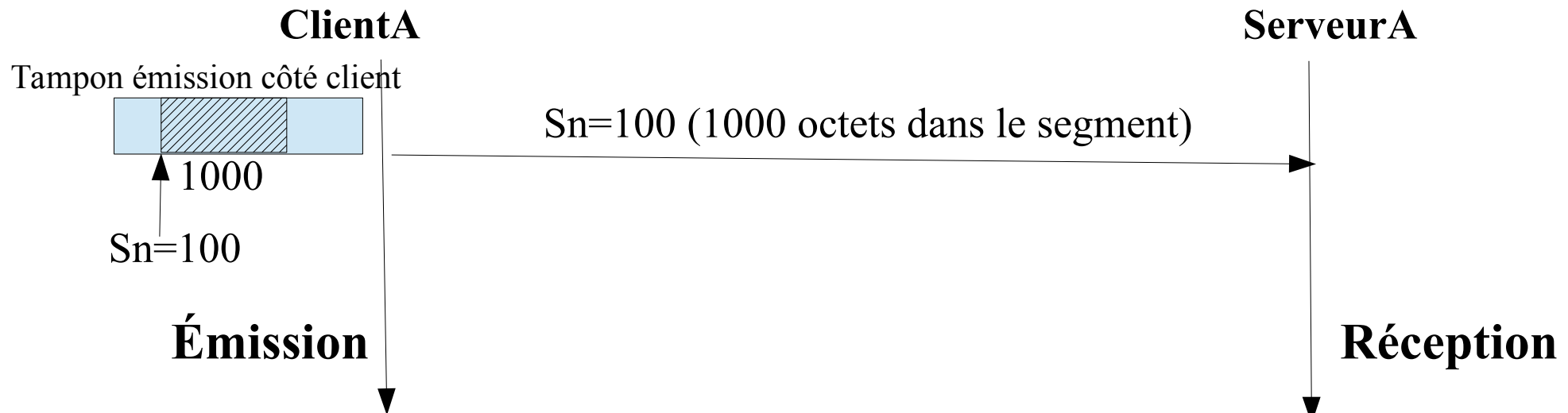
- Le programme application dépose ses données dans un tampon : c'est le « flot » d'émission, l'ordre dans le tampon sera celui de la transmission.
- **Le programme TCP envoie ce flot par segments** : il découpe les données du tampon (flot) en segments.
- TCP émet des octets du flot **dès qu'il le peut** : s'il y a des octets non encore émis et si la connexion le lui permet. La formule qui donne la taille de chaque segment émis est : $\text{MIN} (N_a, \text{MSS}, W)$:
 - **N_a** : Nb d'octets « application » à émettre, stockés dans le tampon d'émission.
 - **MSS** : Maximum Segment Size, qui dépend de la taille max de la trame (MTU).
 $\text{MSS} = \text{MTU} - \text{en-têtes IP et TCP}$.
 - **W** : fenêtre = volume autorisé par le programme TCP réception.

Émission en TCP-2

- Représentation du tampon d'émission (flot de données à émettre) :

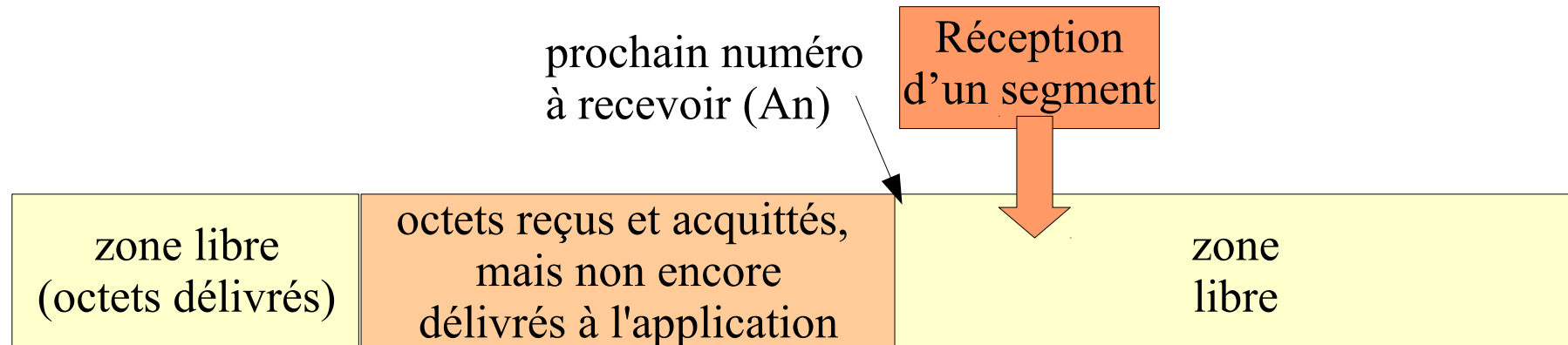


- Exemple d'émission de données ($MSS = 1000$)

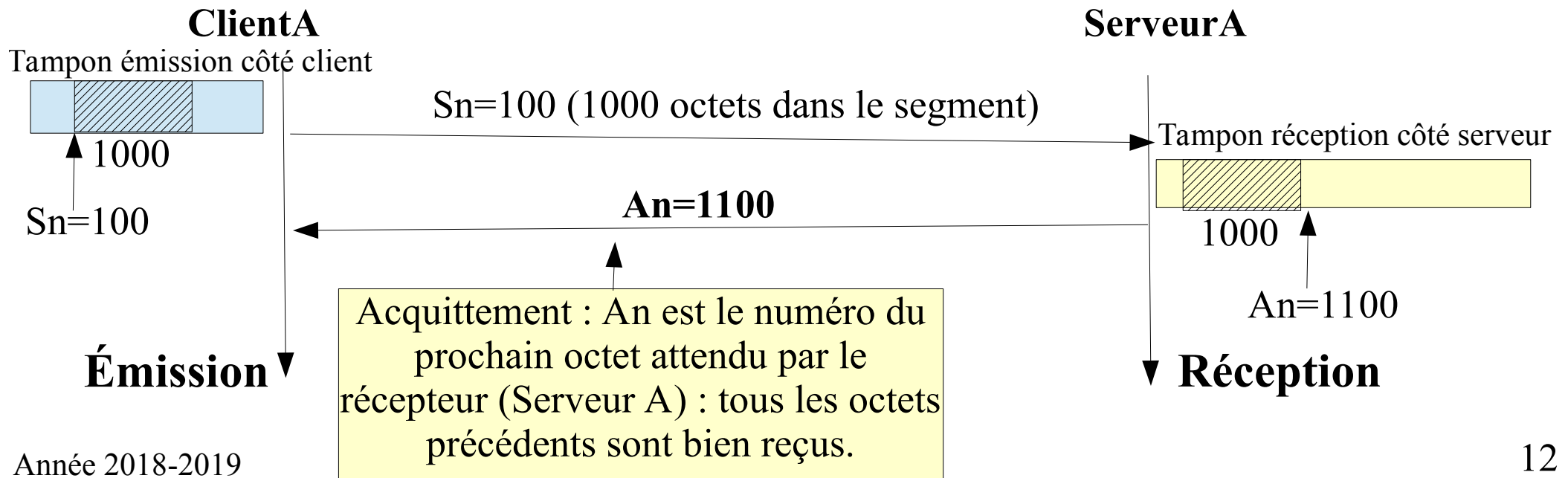


Réception et acquittement en TCP

- Stockage des données reçues dans un tampon réception :

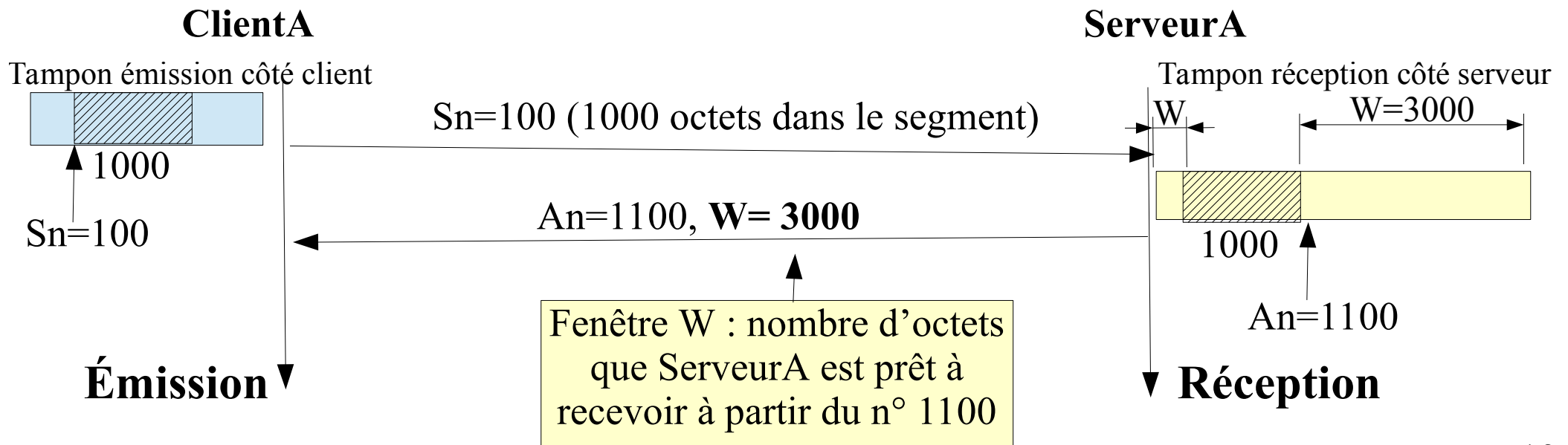


- Acquittement **dès** réception : le champ A_n indique **toujours** le n° du prochain octet à recevoir (= les n° précédents sont reçus sans erreur) :



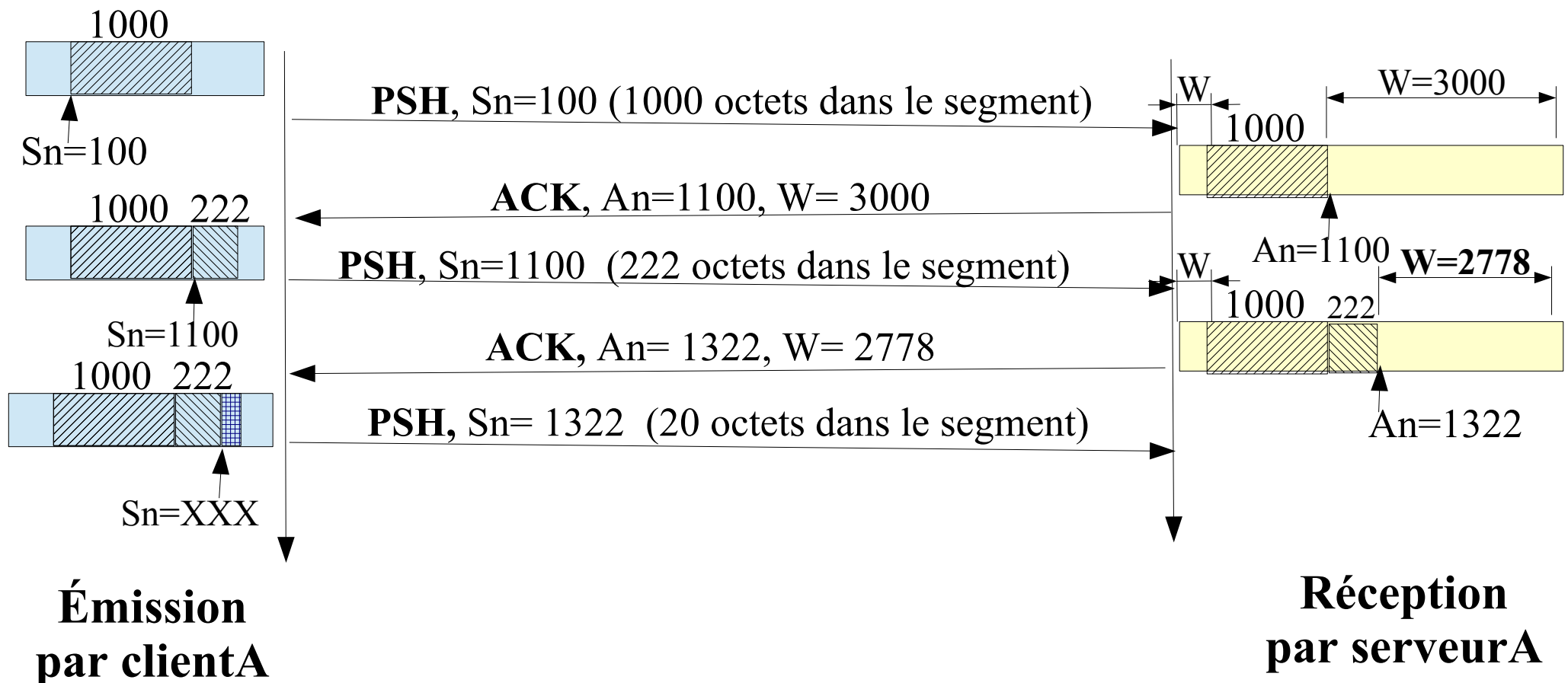
Fiabilisation des échanges en TCP

- **Contrôle d'erreur** : numérotation des octets, acquittement des octets reçus et utilisation du délai de réémission **T_{max}** pour réémettre les données non acquittées.
 - **S_n** : numéro du premier octet émis dans le segment.
 - **A_n** : prochain numéro d'octet attendu (tous les octets de numéro inférieur sont correctement reçus).
- **Conservation de l'ordre** des octets déposés par l'application.
- **Contrôle de flux** : le récepteur envoie **W**, place réception disponible.



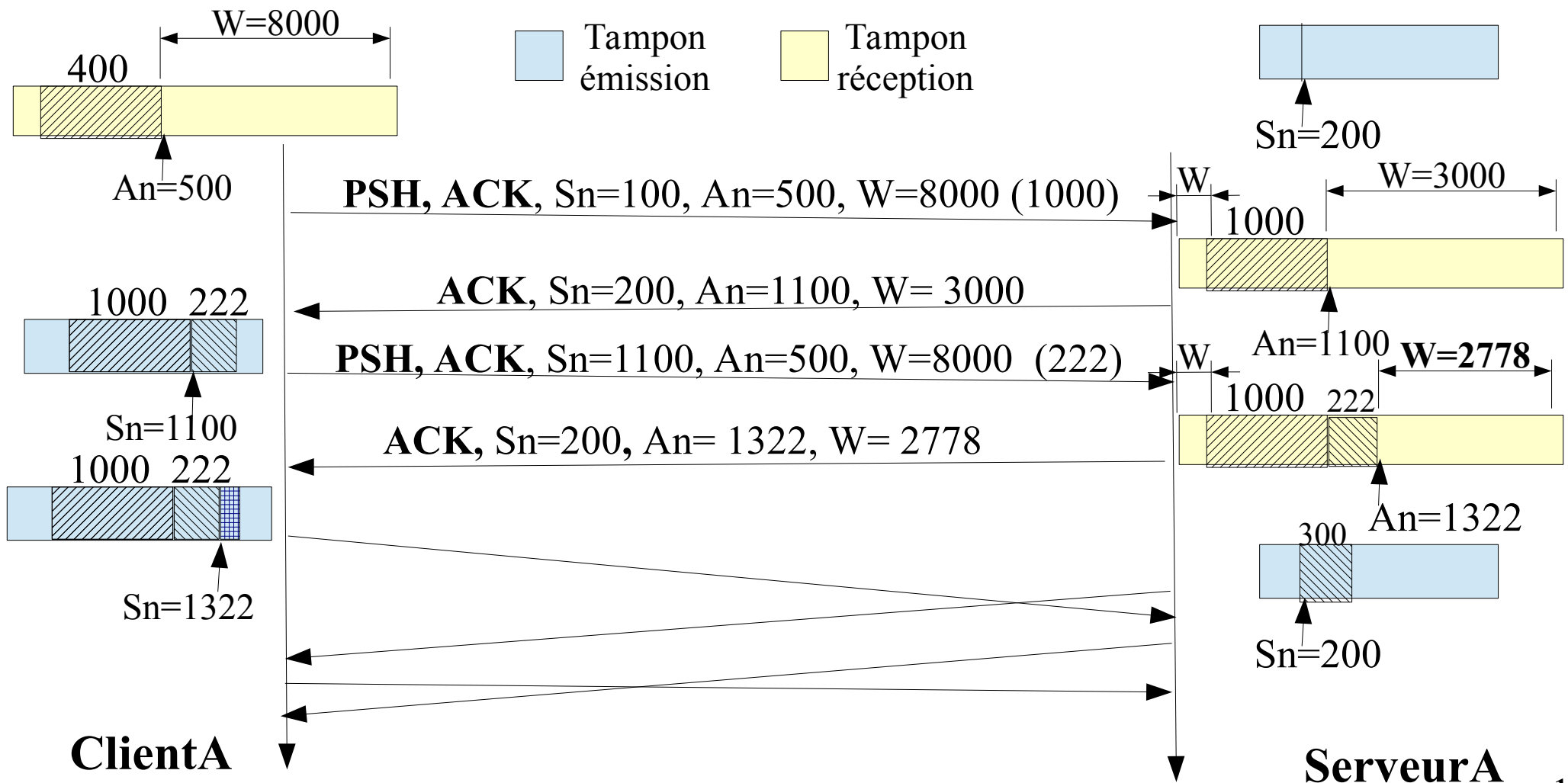
Champ « Control » et fenêtrage W

- **Control (Flags) : <0, 0, URG, ACK, PSH, RST, SYN, FIN>**
 - **ACK** : le paquet acquitte des données (indiqué par la valeur An).
 - **PSH** : le segment contient des données qui peuvent être délivrées à l'application.
- **Fenêtrage W** : le récepteur indique combien d'octets il peut encore recevoir.



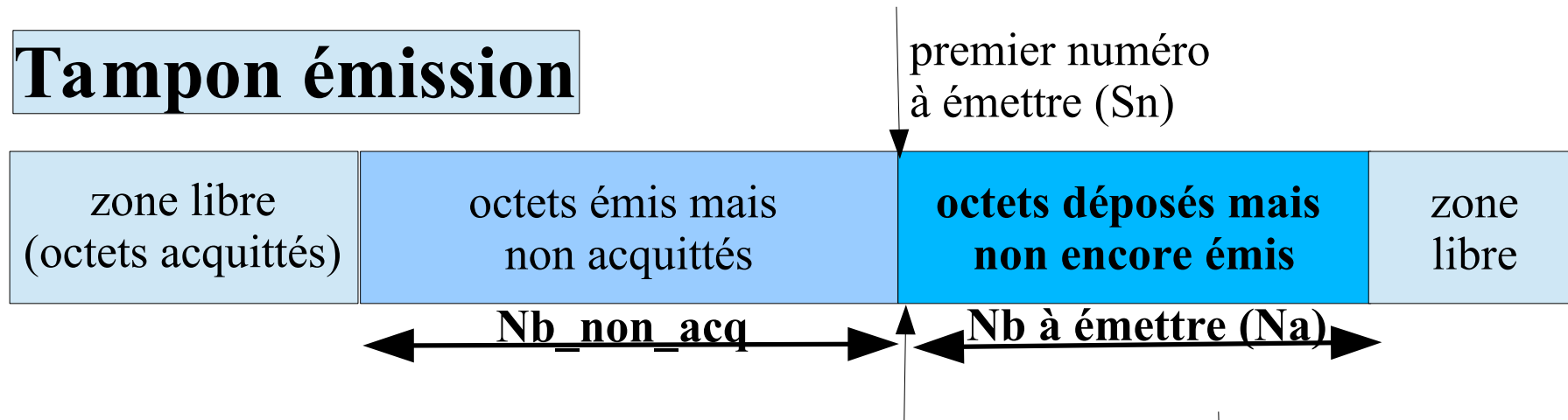
Simultanéité des échanges de données

- Les données sont émises et reçues dans les 2 sens de la connexion et les segments peuvent se « croiser » dans l'(inter)-réseau.
- Les flags et numéros S_n , A_n , W sont dans chaque segment !

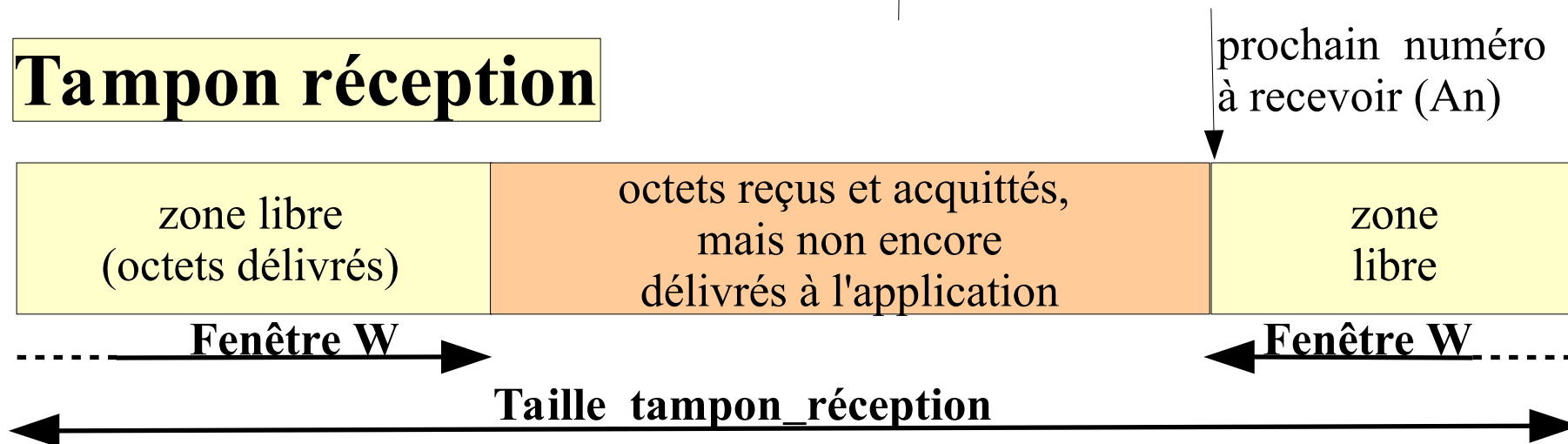


État des tampons émission et réception

Tampon émission



Tampon réception



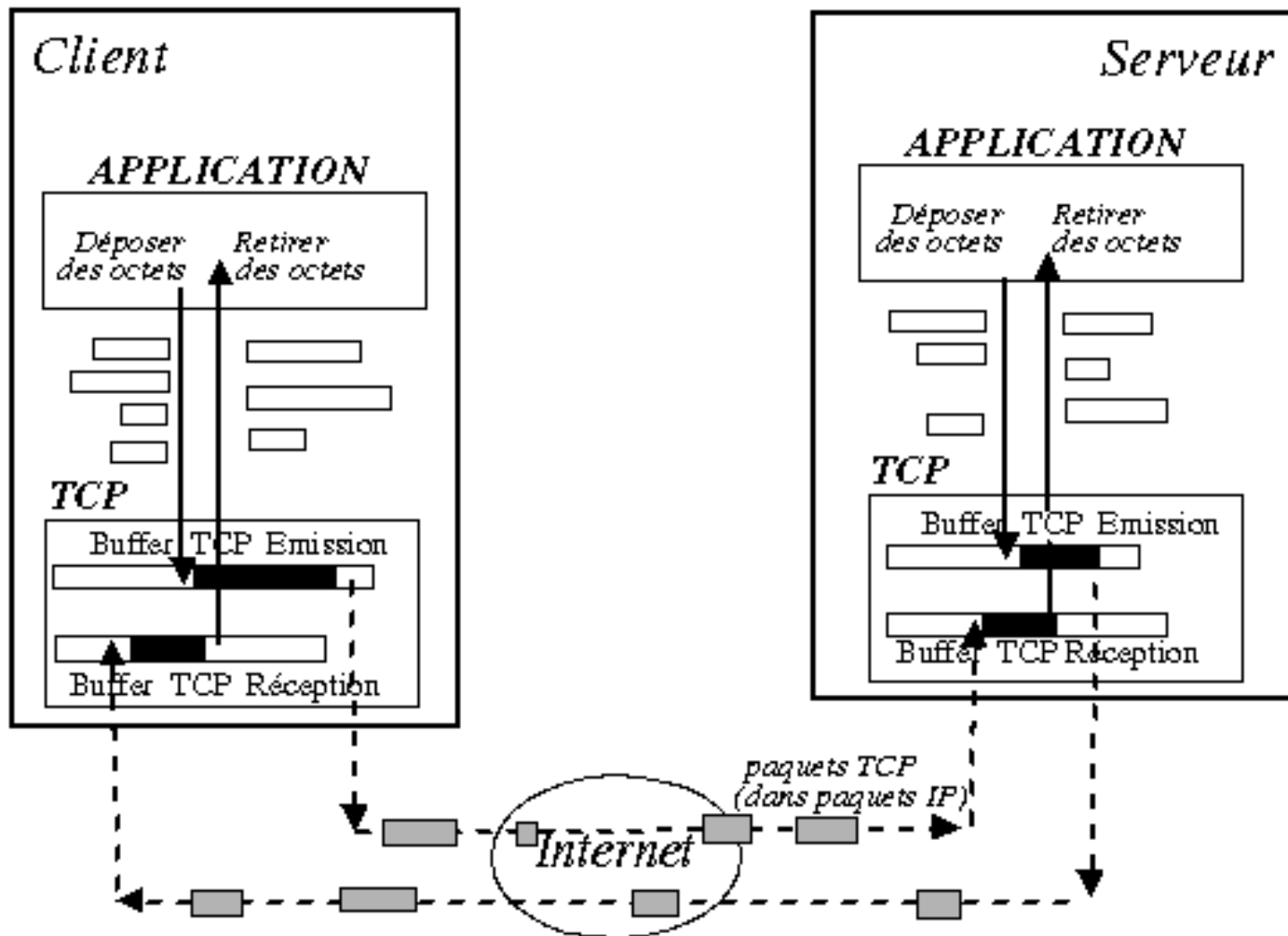
Valeur de la fenêtre W à émettre par chaque programme TCP :

C'est la zone libre de son tampon réception :

$W = \text{Taille_tampon_réception} - \text{octets reçus et non délivrés.}$

Exemple : tampon réception de 10000 octets dont 3000 occupés $\rightarrow W = 7000$

Rôle des tampons TCP

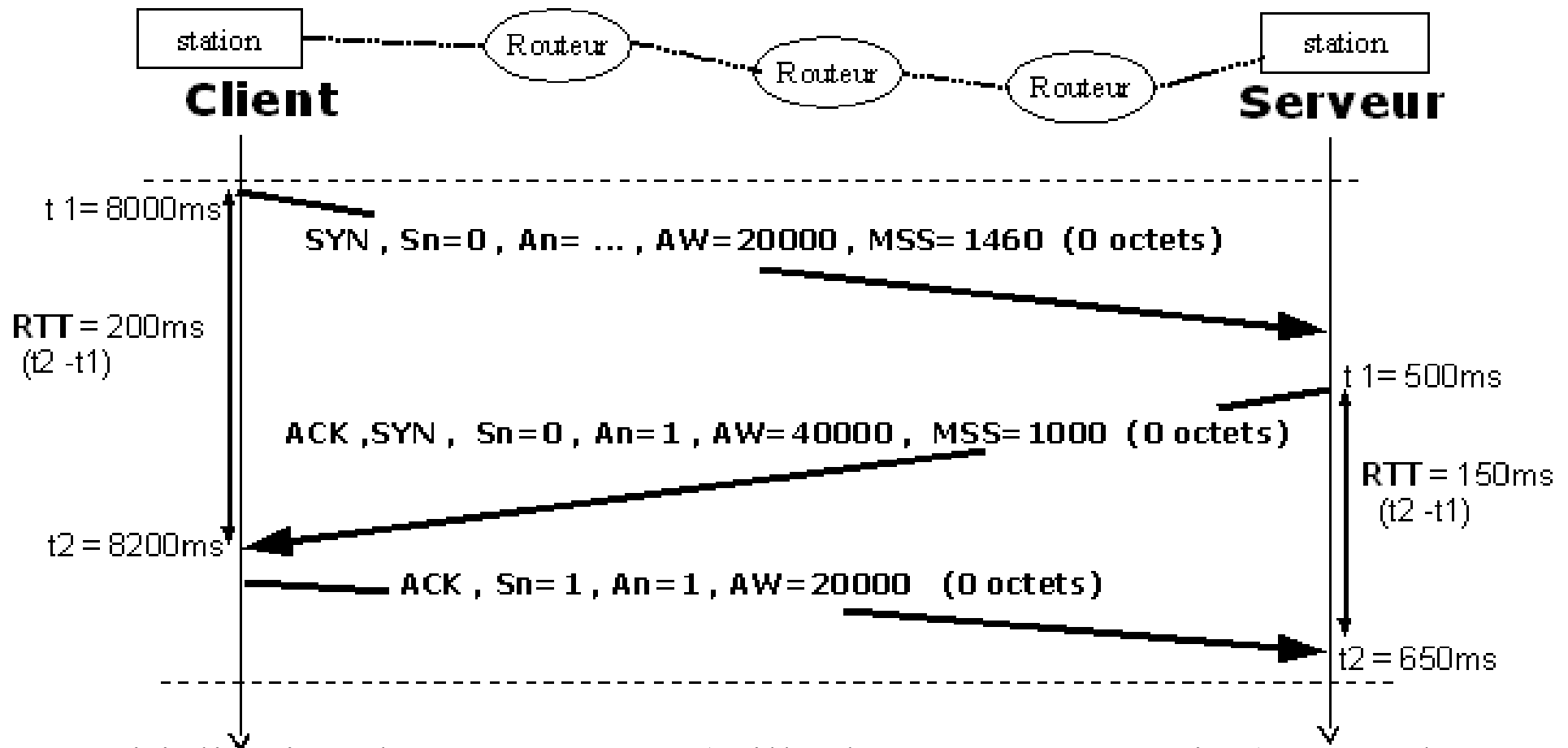


Chaque programme TCP a **deux** tampons (buffer) :

- Un à l'émission
- Un à la réception

- Désynchroniser le dépôt des données et l'envoi d'une part et la réception et la délivrance des données d'autre part.
- Permettre la mise en place des contrôles d'erreur et de flux.

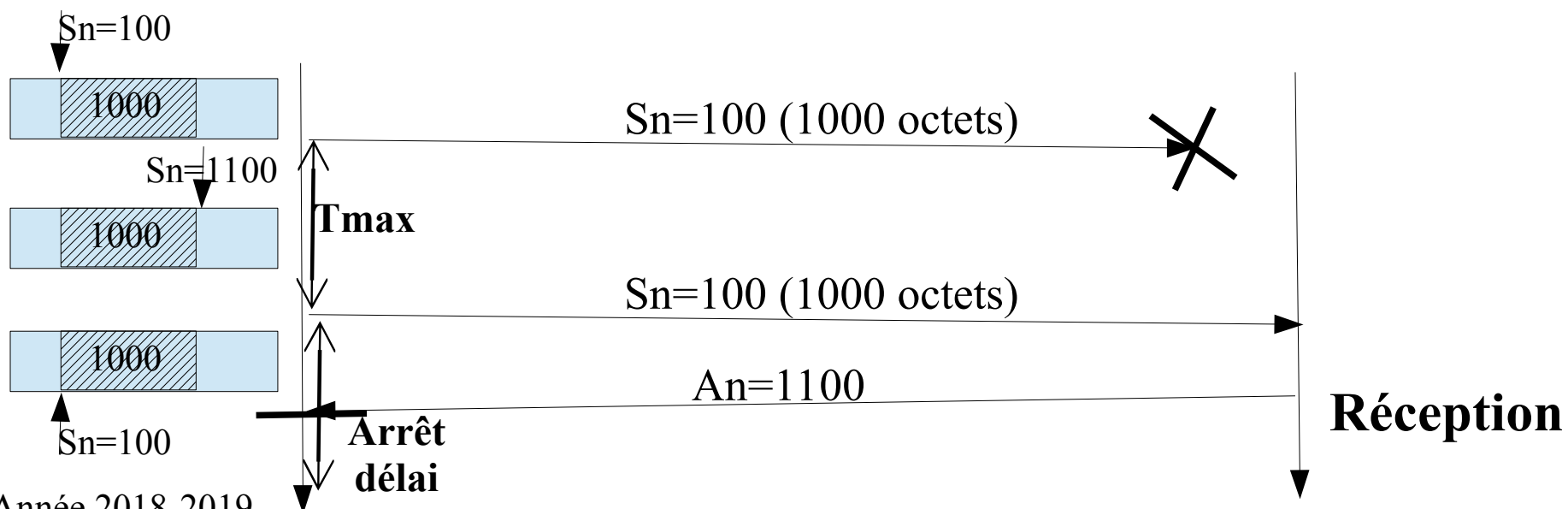
Échanges à l'ouverture d'une connexion



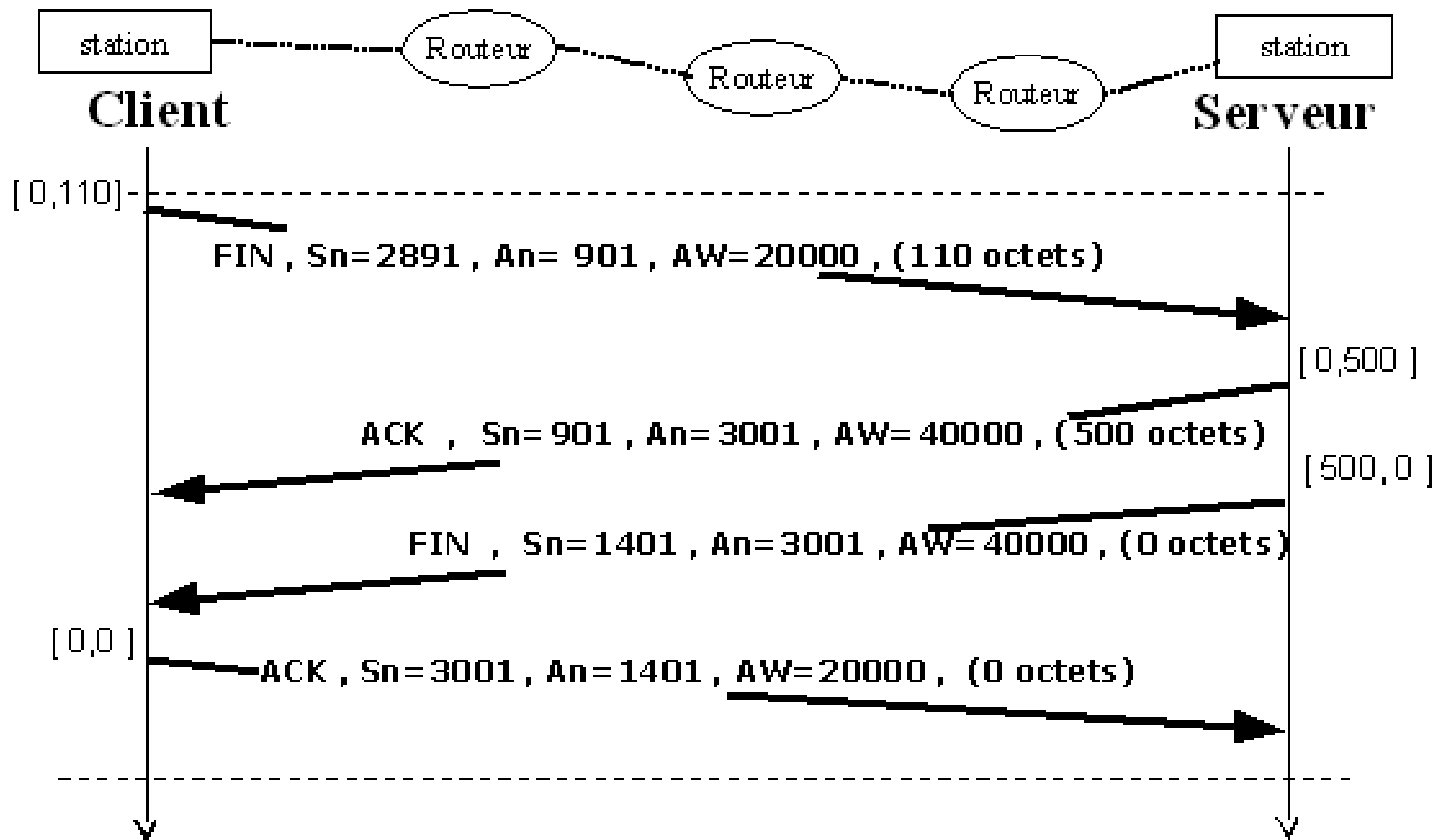
- Initialisation de S_n , A_n , AW (taille du tampon réception) pour chaque côté de la connexion.
- Valeur de MSS négociée : minimum des valeurs échangées.
- Initialisation du délai de réémission $T_{max} = 2 * RTT$, avec $RTT = \text{Round Trip Time}$ (délai d'aller-retour sur la connexion).

Échange avec perte de données

- **Détection d'erreur** : si l'acquittement de données n'arrive pas au bout du délai **T_{max}**, les données sont considérées comme perdues.
- **Correction d'erreur** : les données sont réémises.
- **Mise en oeuvre** :
 - Tampon émission, S_n, A_n.
 - **Délai de garde** initialisé à chaque segment de données émis.
 - En réception, **tout** segment reçu est aussitôt **acquitté**.



Échanges à la fermeture d'une connexion



- Après une demande FIN, les tampons sont vidés, puis la connexion est arrêtée.
- De nombreux cas sont à considérer : double envoi de FIN, etc.

Glossaire

- ACK
- An
- AW
- connexion TCP
- datagramme UDP
- Flags TCP
- mode flot
- MSS
- port
- PSH
- RTT
- Sn
- socket
- SYN
- Tampon
- Tmax
- W
- WS

Module M2102

Architecture des réseaux

Chapitre 6

Architecture Internet et architecture OSI (Open System Interconnection)

Lectures préalables :

- [Internet sur wikipedia](#)
- Introduction à Internet [par Oracle](#), [par Microsoft](#)

Fonctions générales d'un réseau

- Transport des informations : **transmission physique** et **acheminement** (routage, commutation)
- **Encapsulation** et fragmentation des données à transmettre
- **Contrôle d'erreur** :
 - détection d'erreur physique ou logique (données manquantes)
 - correction d'erreur : automatique ou par **retransmission**.
- **Contrôle de flux** : adaptation de l'émission aux capacités de réception.
- **Contrôle de congestion** : gestion au mieux des ressources internes du réseau pour assurer la transmission des flux de façon fluide et selon la qualité de service requise.
- **Partage du/des liens** : gestion des accès en fonction des demandes et/ou multiplexage des flux.

Fonctions réalisées selon les niveaux d'architecture

Niveau général	Fonctions	Unité de données Échangées
Application	Réalisation des échanges entre les composants de l' application . ex: serveur web et client navigateur	Message (<i>mail, requête /réponse HTTP</i>)
Acheminement/ Transport	Transport de bout en bout des données des applications avec la qualité de service requise (fiabilité , sécurité, Synchronisation) -> transport TCP Acheminement à travers le réseau -> routage IP	Paquet IP, Datagramme UDP, Segment TCP
Transmission physique	Transmission sur chaque lien . Détection des erreurs , gestion du partage et de l' accès aux liens. ex: Ethernet, Wifi, WDM	Trame Ethernet, Trame Wi-Fi, Cellule ATM, Trame PPP

Architecture normalisée

Open Systems Interconnection

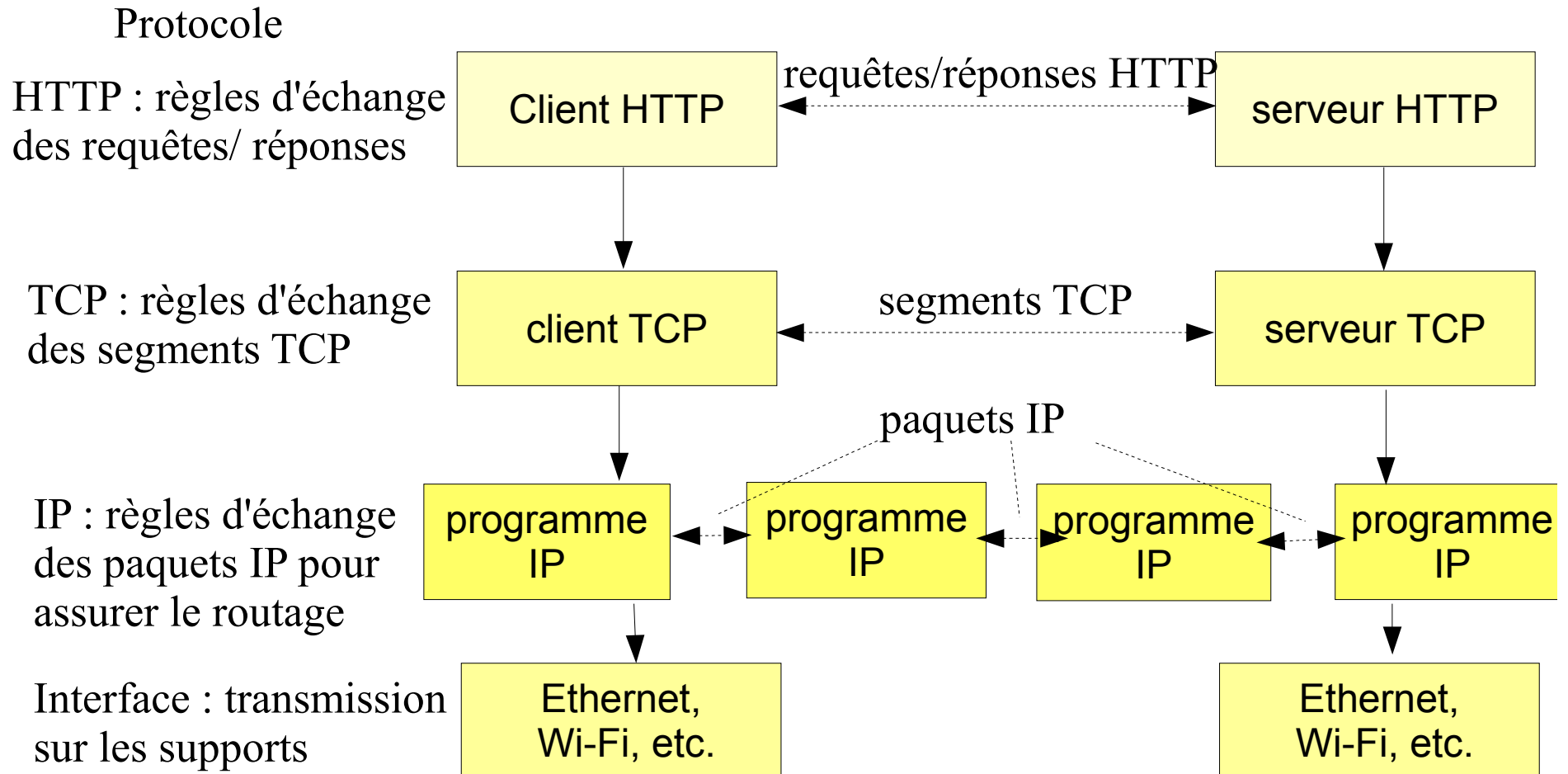
	niveau	nom	unité de donnée	services
<i>Application</i>	7	Application	Message	messagerie, transfert de fichiers, connexion à distance, accès
	6	Présentation		Gestion des formats de données : codage, compression, cryptage
	5	Session		Gestion des sessions : dialogue, reprise
<i>Acheminement</i>	4	Transport	Paquet Transport (segment TCP, datagramme UDP)	Acheminement de processus à processus : points d'accès, fiabilisation de bout en bout
	3	Réseau	Paquet Réseau (datagramme IP)	Acheminement de station à station : adresses réseau, routage, commutation ATM
<i>Transmission</i>	2	Liaison	Trame Liaison	Logique de la transmission sur un lien : adresses physiques, accès, fiabilisation
	1	Physique	Trame physique <i>Signal</i>	Physique de la transmission sur un lien : matériel : câblage, cartes réseau, commutateurs signaux (formes, émission, réception)

Architecture TCP/IP et niveaux OSI

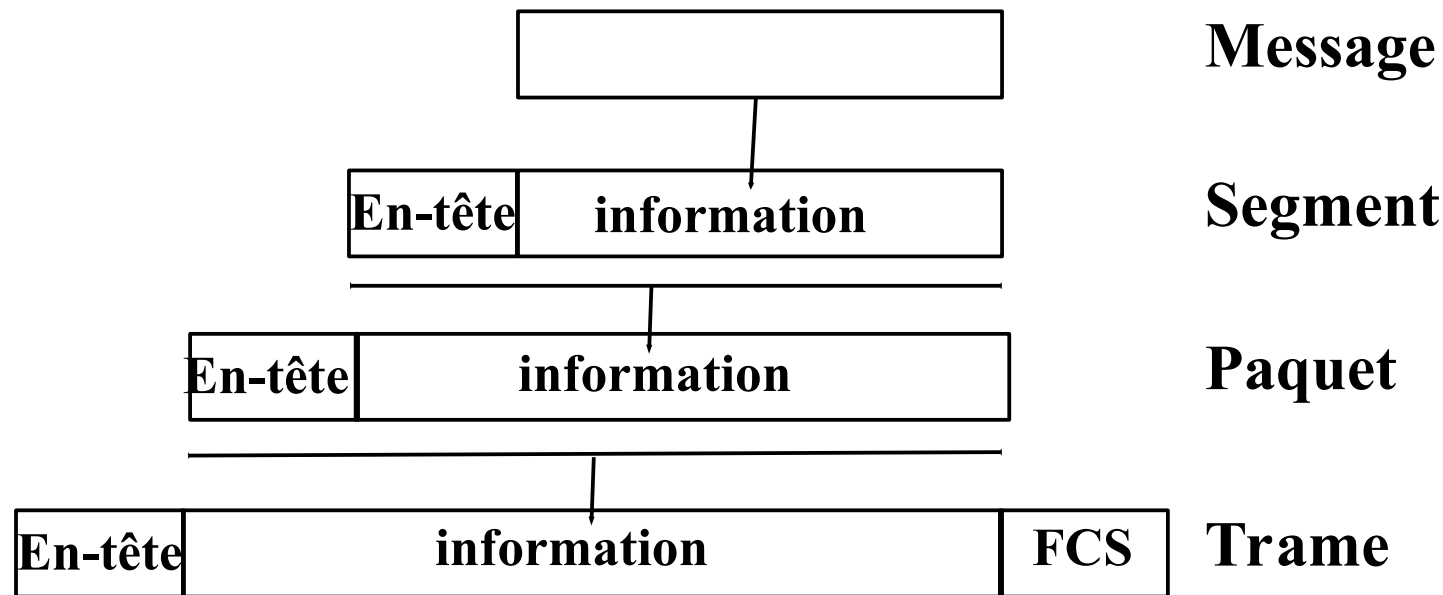
	Niveau OSI	Niveau TCP/IP	Unité de données	Principaux services et protocoles
<i>Application</i>	7 (5-6)	Application	Message	<i>Messagerie (SMTP, POP, IMAP), Transfert de fichiers (FTP, SSH/SFTP), Connexion à distance (TELNET, SSH), Web (HTTP), Bases d'Infos (LDAP, Postgres, MySQL), Service de nom (DNS), d'adresse (DHCP)</i>
<i>Acheminement</i>	4	Transport	Paquet de transport (segment)	<i>Acheminement de processus à processus, Communication port à port (TCP, UDP)</i>
	3	Réseau	Paquet de réseau (datagramme)	<i>Acheminement de station à station (routage IP), Contrôle des routes (ICMP)</i>
<i>Transmission</i>	1-2	Interface	Trame	<i>Ethernet, Wi-Fi, ATM, etc.</i>

Appels entre niveaux de protocole

Exemple des protocoles HTTP/TCP/IP

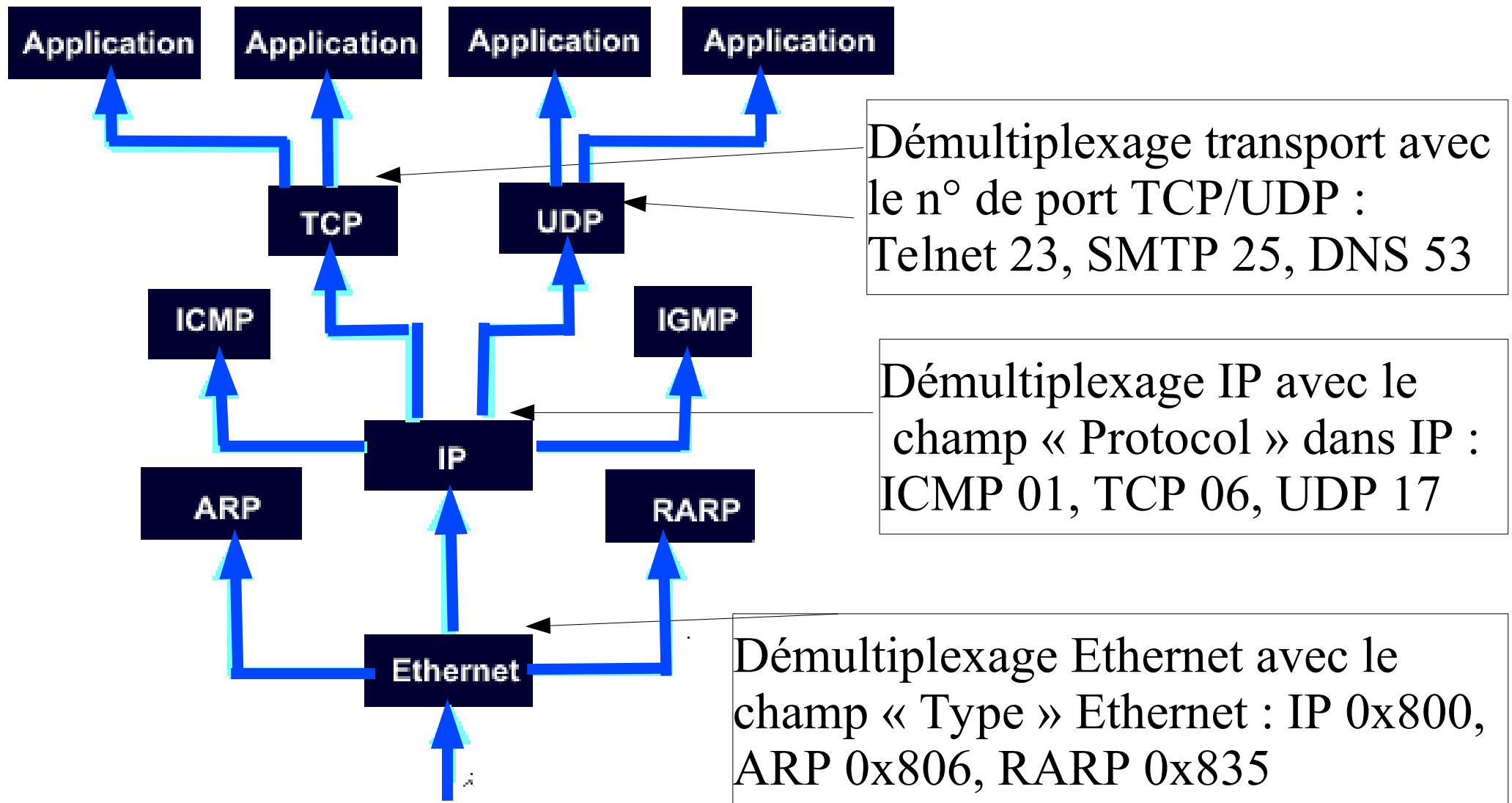


Encapsulation des données



- **UD : Unités de Données** de chaque niveau (trame, paquet IP, segment TCP, message).
- Le champ « **information** » contient l'Unité de Données du niveau supérieur.
- L'**en-tête** de chaque UD contient les données supplémentaires nécessaires à la réalisation du protocole : adresses, numéros, commandes, etc.

Démultiplexage dans TCP/IP/Ethernet

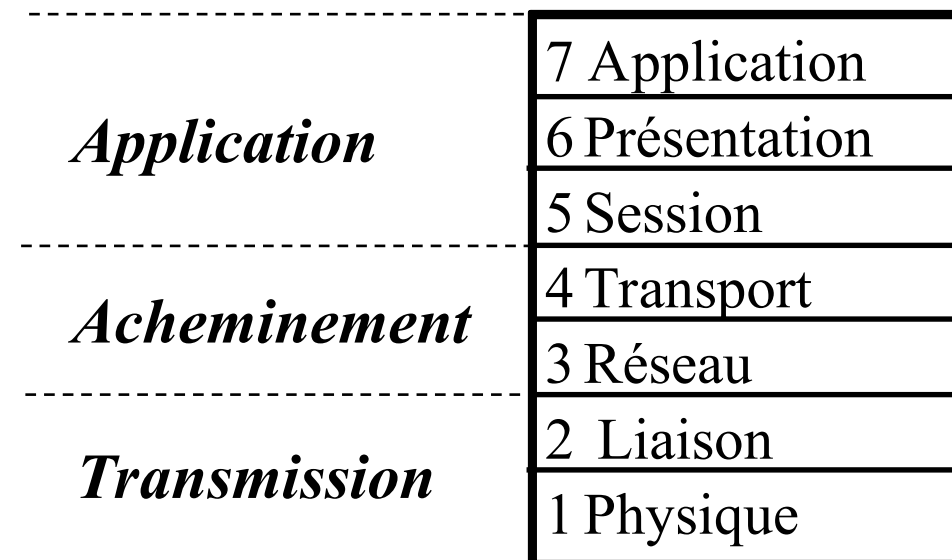


Source : <http://www.htr.ups-tlse.fr/pedagogie/cours/tcp-ip/introduction/index.html>

Organismes de normalisation

- Importance : pour communiquer, il faut s'entendre...
- Complexité technologique et convergence de métiers différents : informatique, télécommunication, téléphonie, télévision, audio...
- Organisations internationales de normalisation :
 - **IEEE** : Institute of Electrical and Electronics Engineers
 - **IETF** : Internet Engineering Task Force
 - **ISO** : International Organization for Standardization

-> architecture
de référence **OSI** :
Open
Systems
Interconnection



Normalisation des protocoles de l'Internet : l'IETF

- Internet Engineering Task Force, <http://www.ietf.org>
 - ouvert à tous, mais avoir de l'influence se mérite.
- Le lieu où tous les protocoles de référence ont été et continuent d'être standardisés, par exemple :
 - TCP, UDP, IPv4, IPv6, ICMP, IGMP, MLD, ARP, DHCP, DHCPv6, RTP/RTCP, RTSP, SIP, etc.
 - plus de 6000 standards et 124 groupes de travail actifs.
- Deux principes fondateurs :
 - « *We believe in rough consensus and working code.* »
 - « *Be conservative in what you send and liberal in what you accept.* »

Autres structures de standardisation

- Associations professionnelles :
 - Le consortium **W3C** (www.w3.org) : protocoles et directives pour le développement du Web.
 - La structure de coopération 3GPP (3rd Generation Partnership Project (www.3gpp.org) : spécifications pour les réseaux mobiles 3G et 4G.
 - Le forum **WiMAX** (www.wimaxforum.org)
 - Le forum **DSL** (www.adsl.com) : lignes d'accès haut débit.
- Agences de réglementation :
 - **ARCEP** : (www.arcep.fr) Autorité de Régulation des Communications Électroniques et des Postes.
 - **CNIL** : (www.cnil.fr) Commission Nationale de l'Informatique et des Libertés

ARCEP

- Missions de l'ARCEP :
 - Assurer le bon fonctionnement des réseaux téléphoniques, mobiles et Internet, en particulier en matière de qualité de service, interconnexion de données et transition vers IPv6 ;
 - Protéger contre les atteintes possibles à la neutralité d'internet.
- Mesures de la qualité du service d'accès à internet :
 - Avec des outils de crowdsourcing