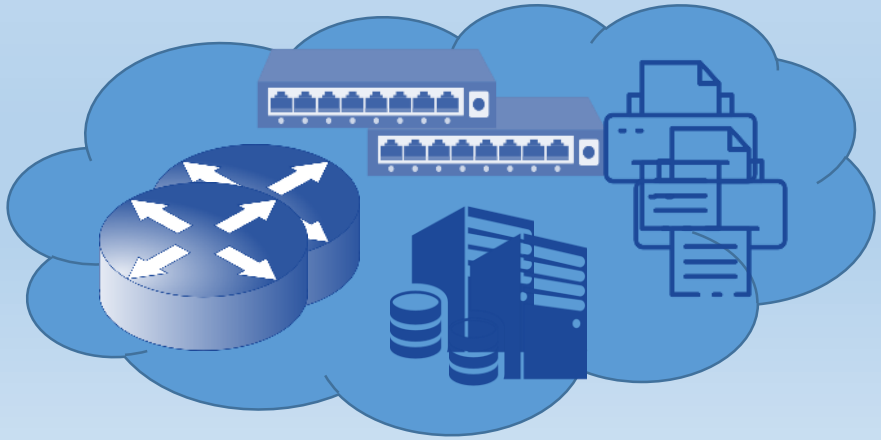
Université Sorbonne Paris Nord: IUT Villetaneuse

Dr. Mohamed Amine Ouamri

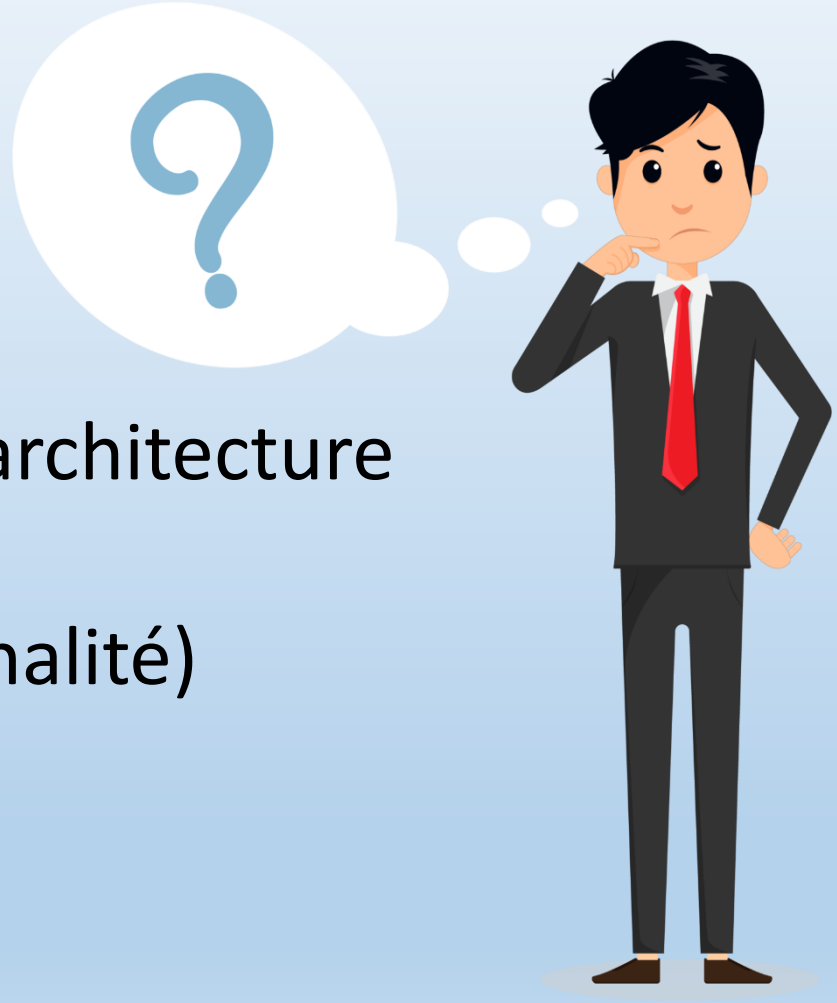
Matière :M51 Réseaux

Chapitre 1:Pile de protocoles TCP/IP et Adressage IPv4



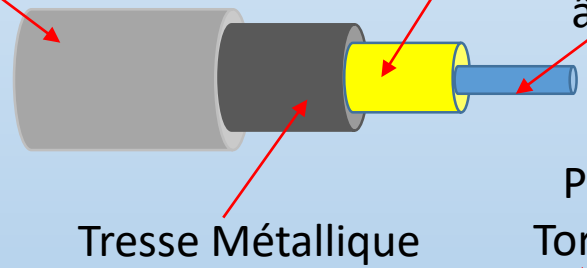
Contenu du chapitre

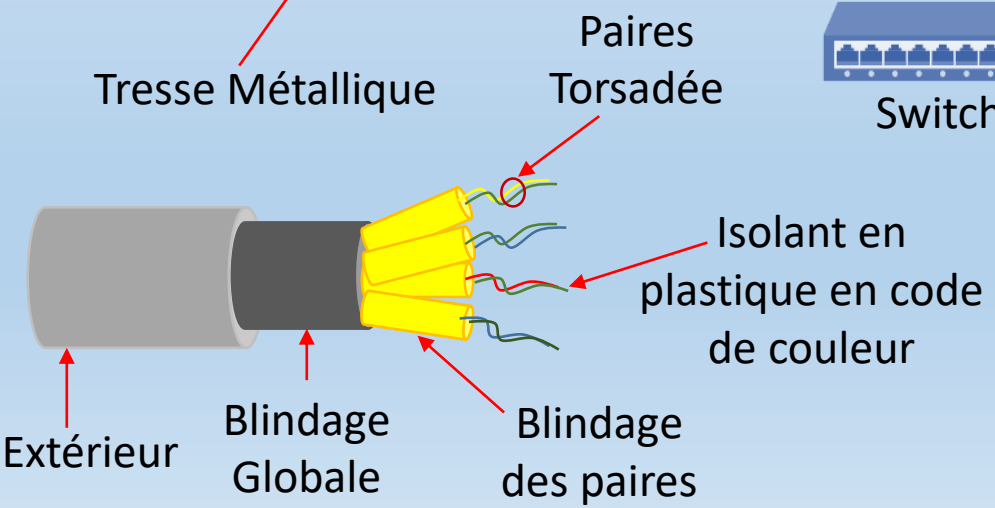
- Les éléments de communication
- Le concept de réseau
- Les Réseaux à Commutation
- Notion de protocole
- Principe de fonctionnement d’une architecture en couches
- Protocole TCP (Principe et fonctionnalité)
- Protocole IP et Adressage IPv4
- Principe de Fragmentation
- Performance Réseau



❖ Les éléments de communication

La communication démarre avec des informations qui doivent être envoyées d'un périphérique à un autre.





Eléments et Composants Réseaux Info

Les Postes de Travail
Ordinateur

Le Serveur
Fournie les ressources partagées aux clients

Les éléments d'interconnexion
Il permet de connecter deux segments réseaux

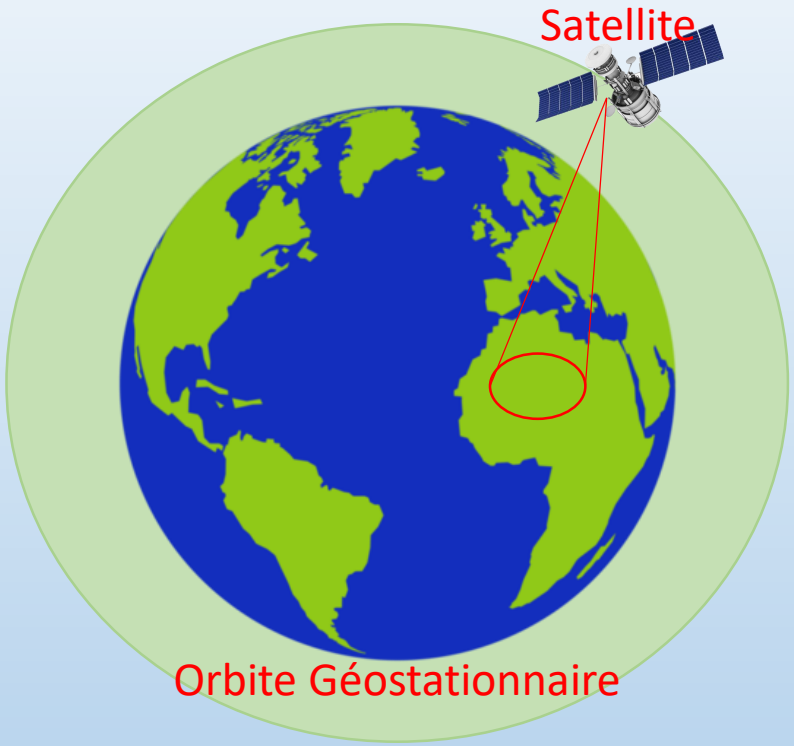
Switch


Hub

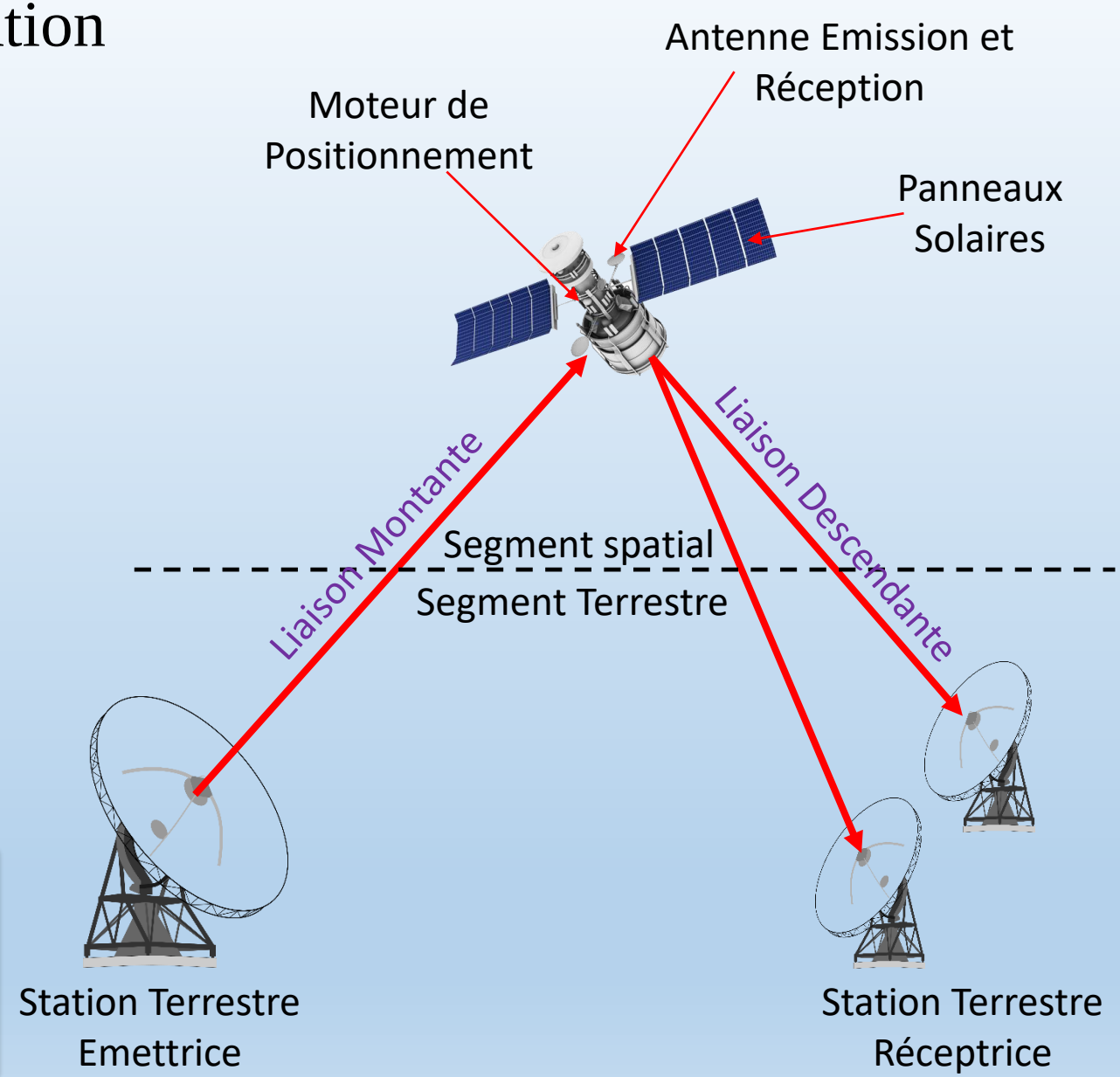
Les Périphériques
Eléments partagés par les clients

Le Routeur
Permet de diriger les données dans le réseau

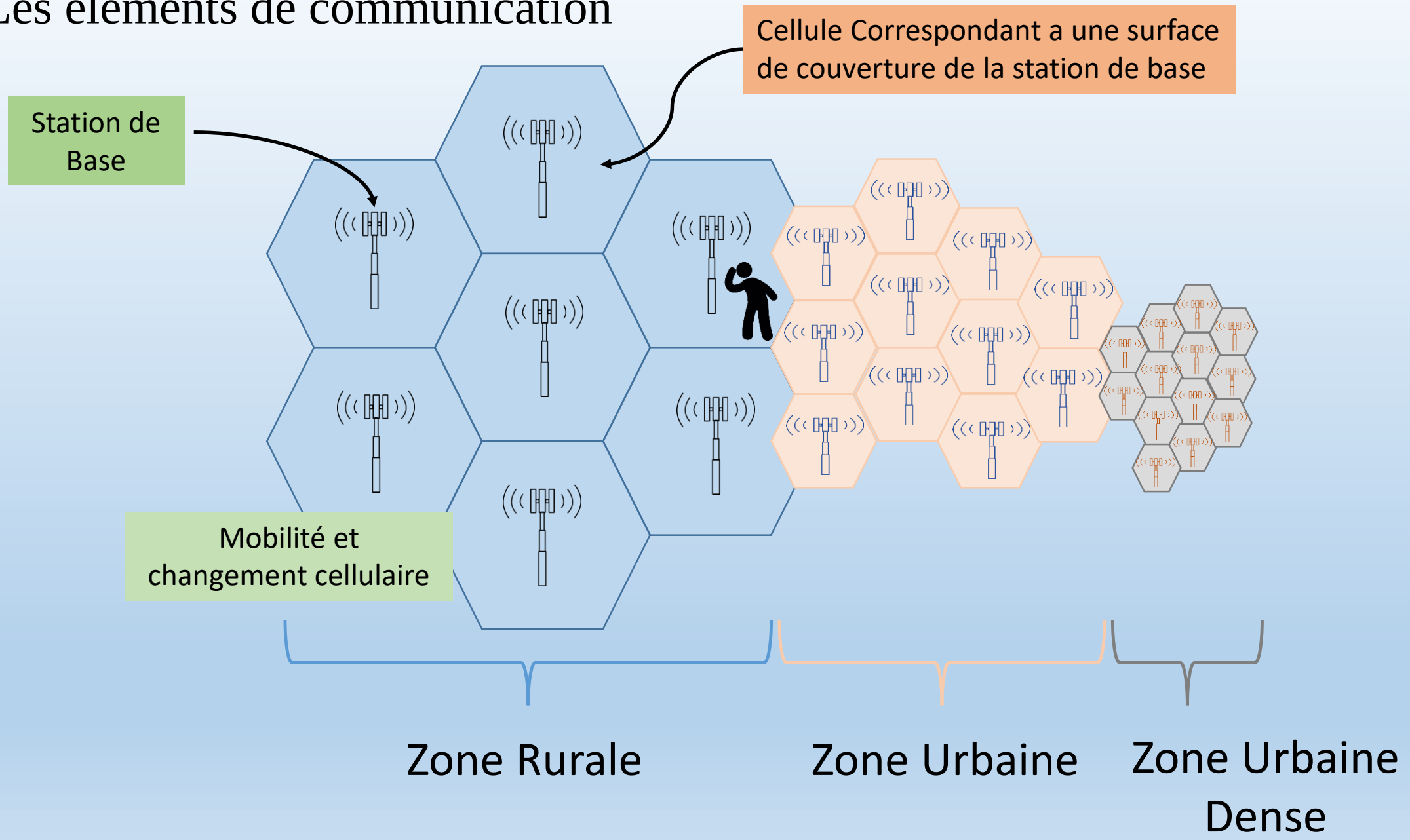
❖ Les éléments de communication



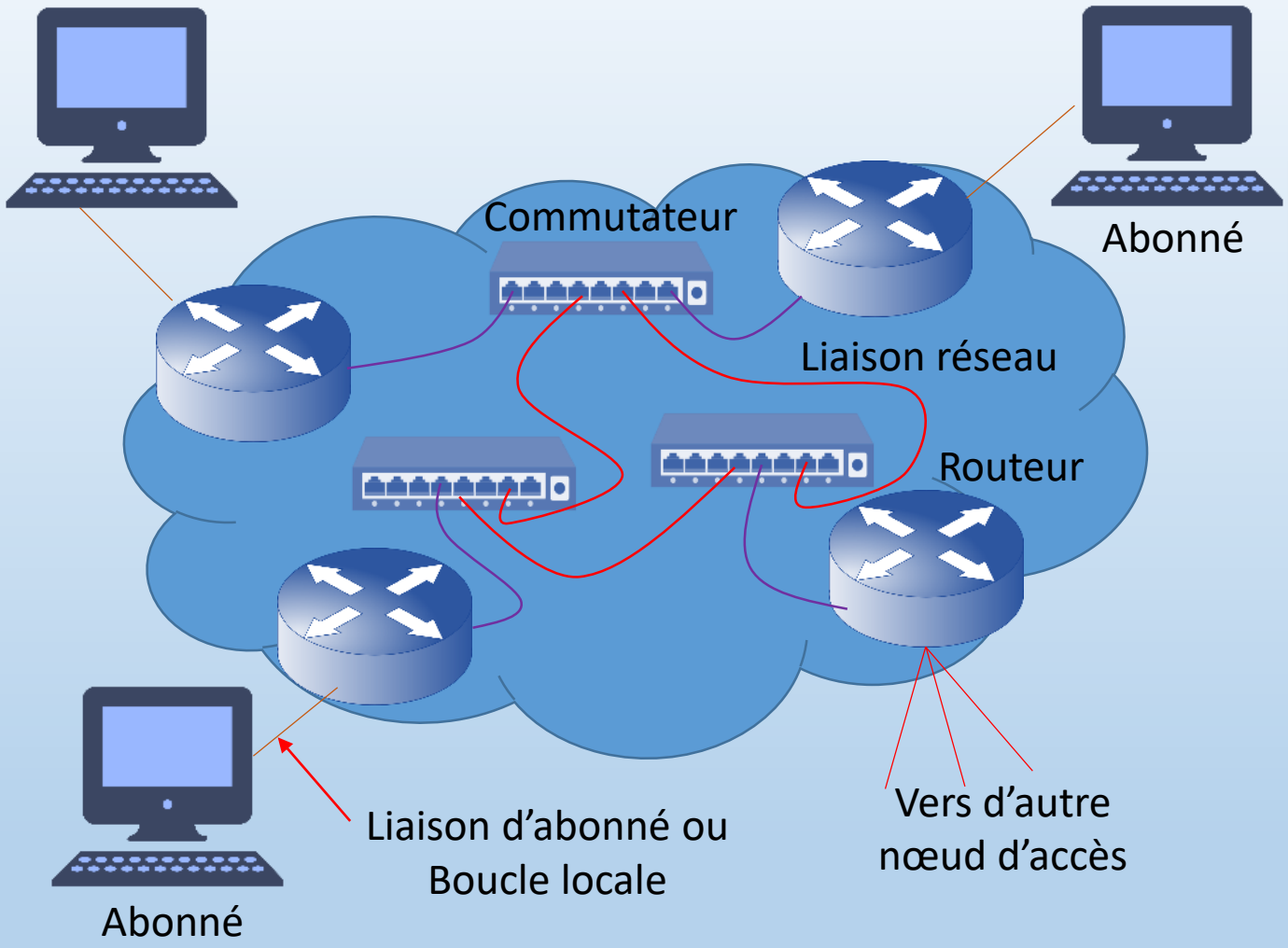
Une station terrestre émet vers le satellite un flux d'information. Le satellite n'est qu'un simple répéteur, il régénère les signaux reçus et les réémet en direction de la Terre



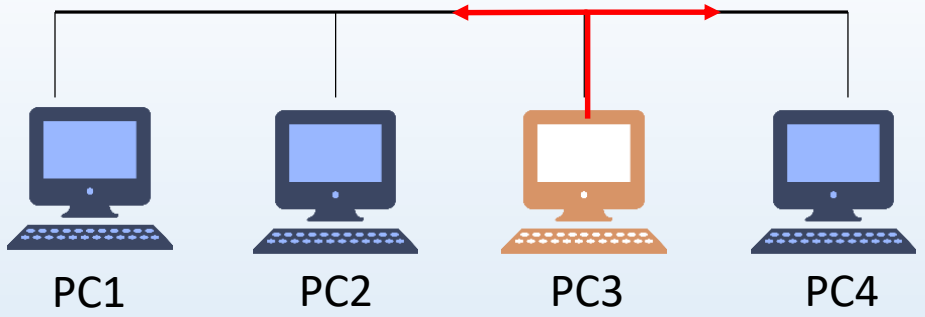
❖ Les éléments de communication



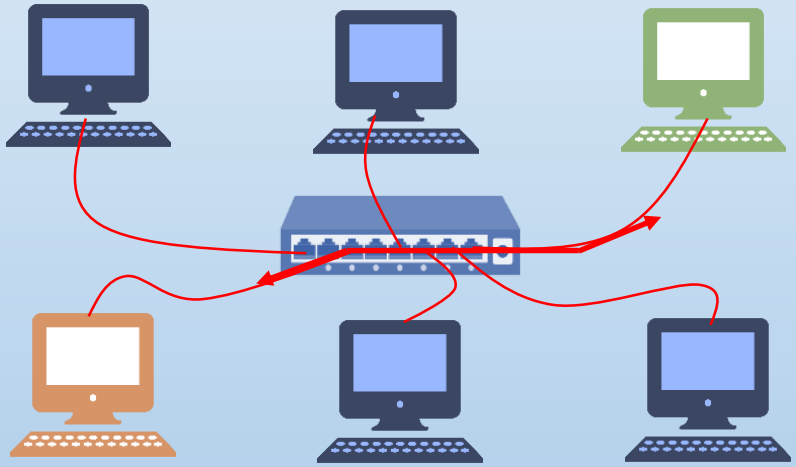
❖ Le concept de réseau



Un réseau est un assemblage de ressources matérielles et logicielles géographiquement réparties, destiné à fournir un service, ou à transporter des données.

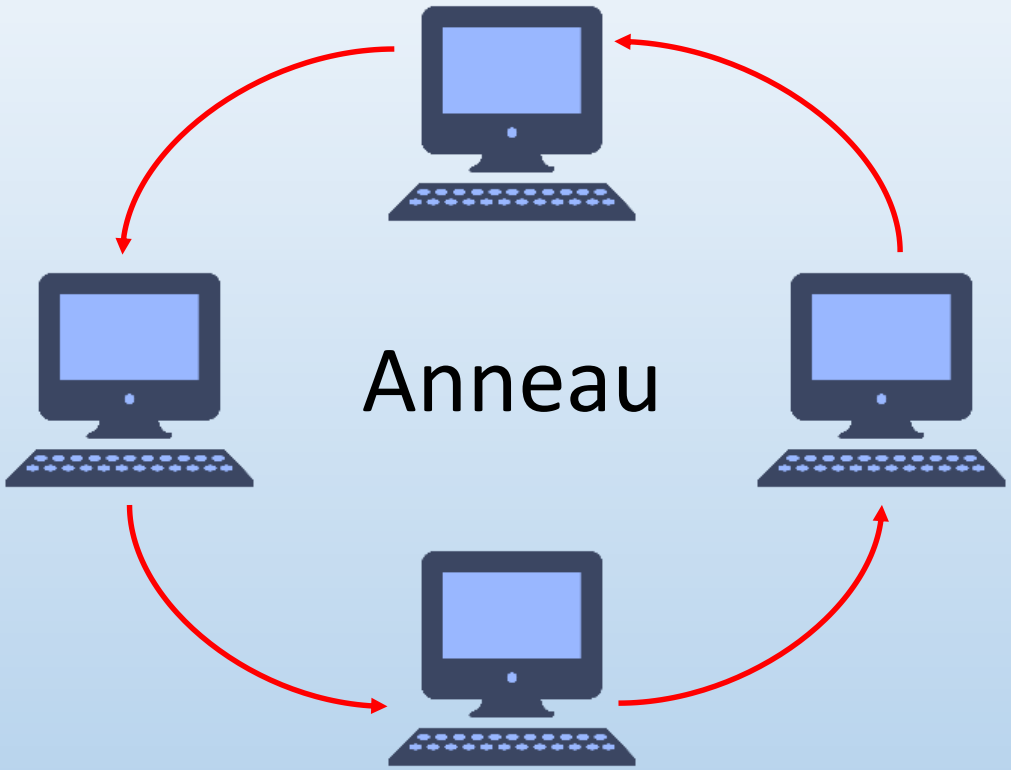


- ✓ Le bus (réseau diffusion) variante de la liaison multipoint.
- ✓ L'information émise est diffusée sur tout le réseau.
- ✓ Problèmes de conflit d'accès (contentions ou collisions)
- ✓ Ils autorisent des débits importants (>100 Mbit/s sur 100 m).

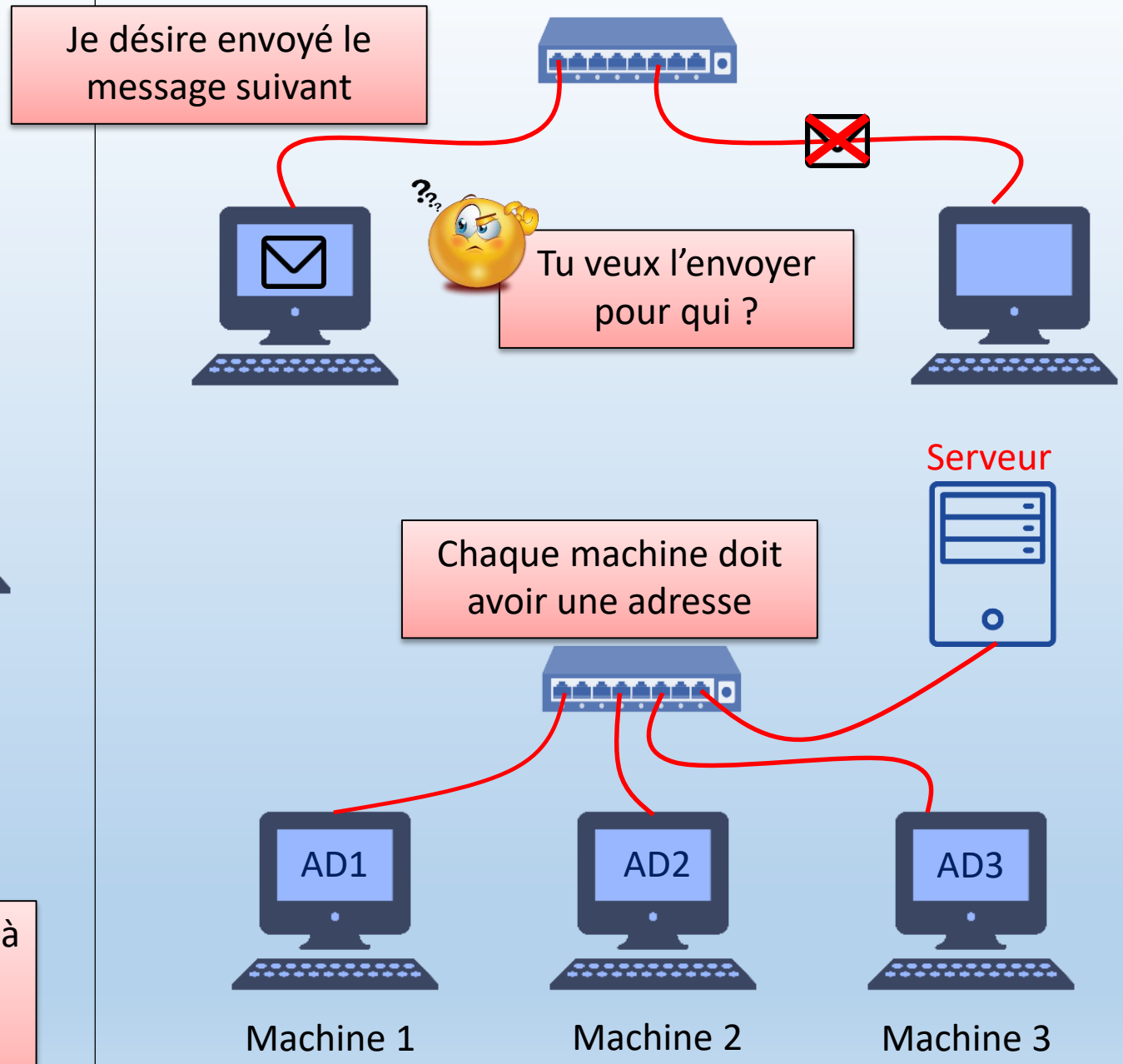


- ✓ L'étoile variante de la topologie en point à point.
- ✓ Tous les nœuds du réseau sont reliés à un nœud central.
- ✓ Tous les messages transitent par ce point central.
- ✓ Chaque message reçu est examiné et retransmet qu'à son destinataire.
- ✓ La défaillance d'une liaison n'entraîne pas celle du réseau.

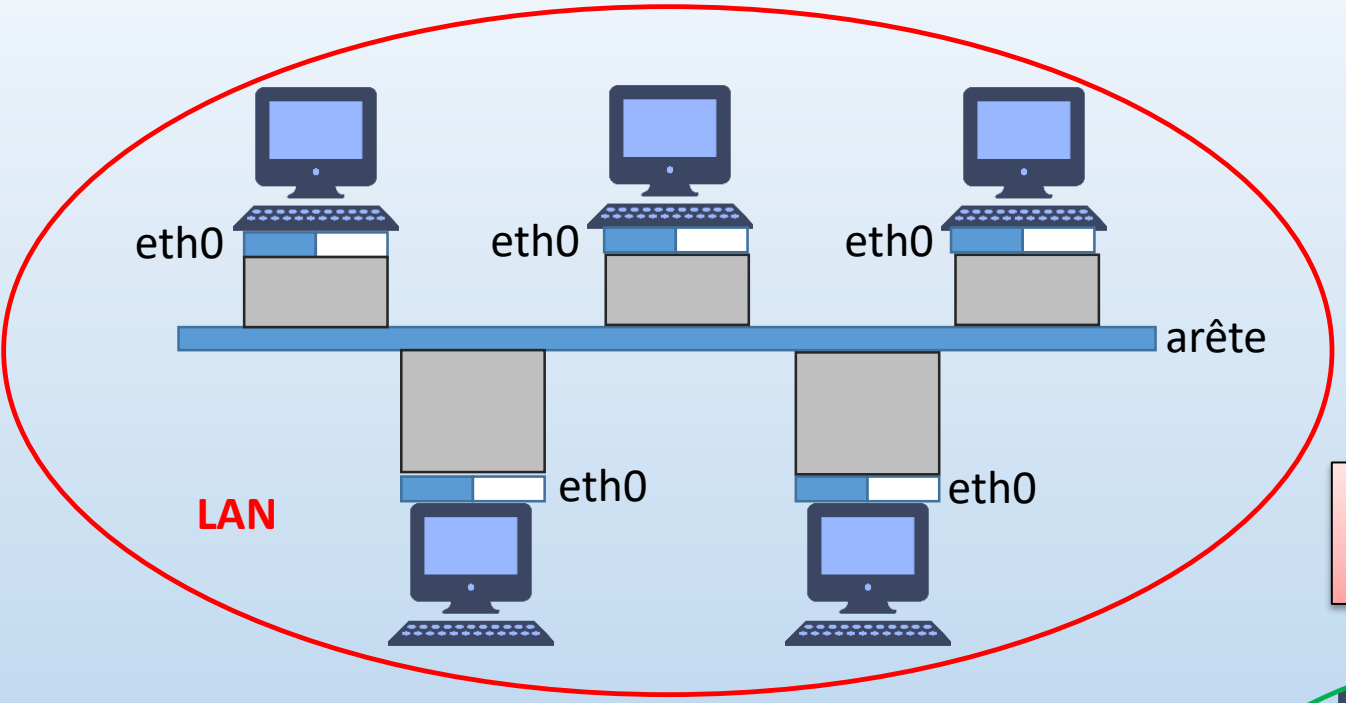
❖ Le concept de réseau



- ✓ Chaque poste est connecté au suivant en point à point.
- ✓ L'information circule dans un seul sens.
- ✓ chaque station reçoit le message et le régénère.

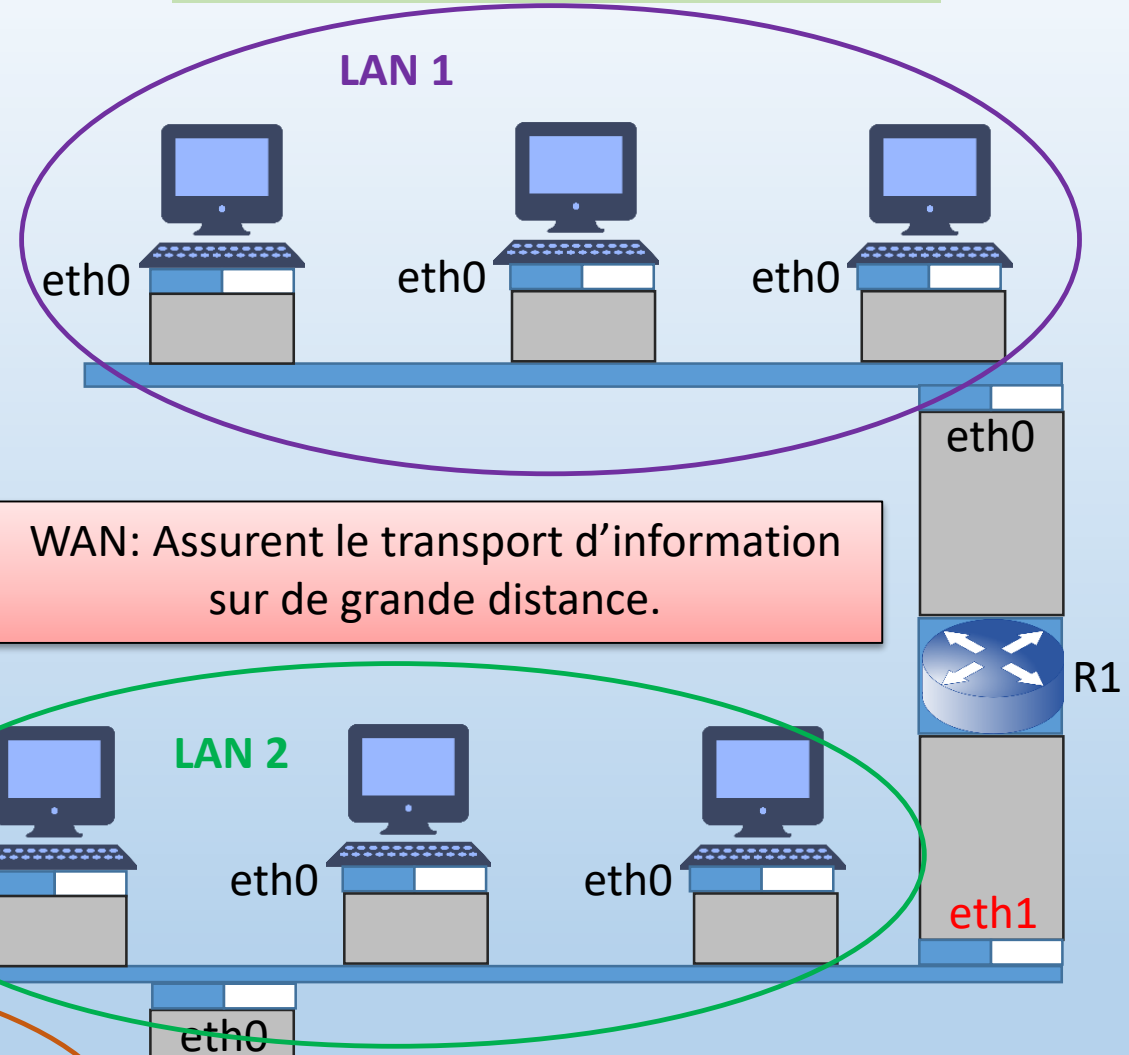


Un réseau local (plusieurs nœuds, une seule hyper-arête)



LAN: limitée à une circonscription géographique réduite (bâtiment...)

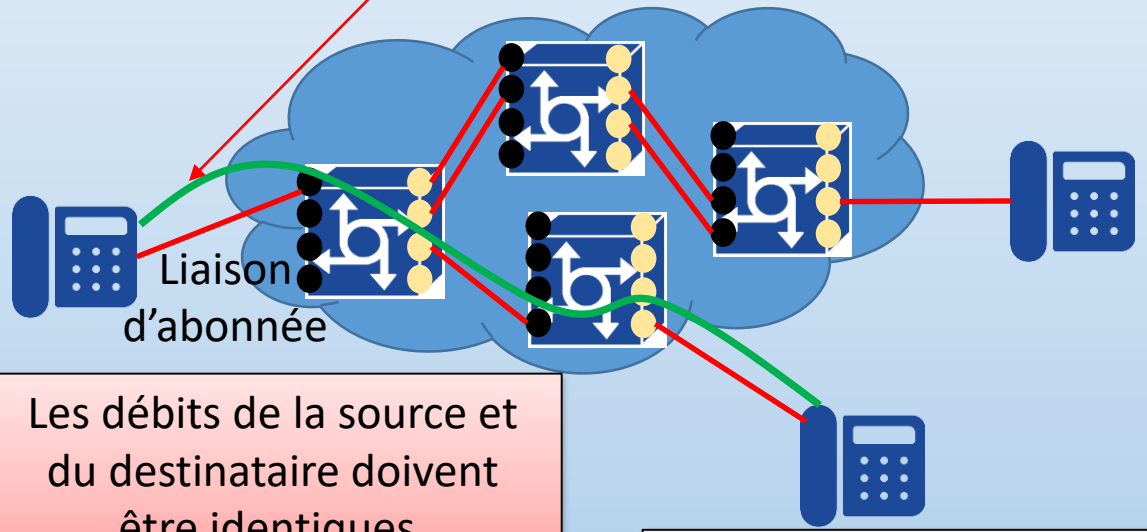
Un réseau étendu (plusieurs nœuds, une plusieurs hyper-arête)



WAN: Assurent le transport d'information sur de grande distance.

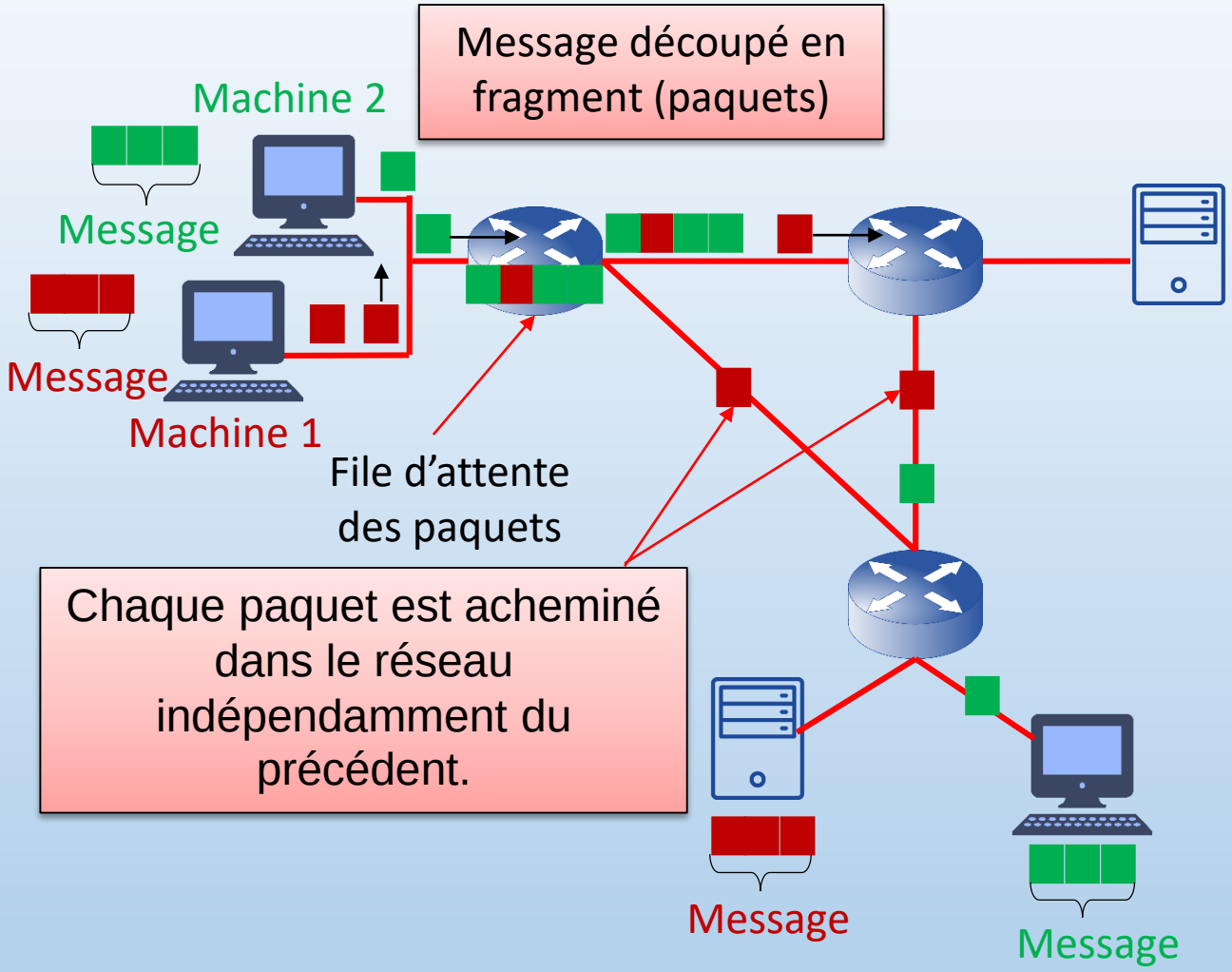
❖ Les Réseaux à Commutation

Lien physique est établi par juxtaposition afin de constituer une liaison de bout en bout.

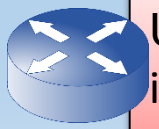


Les débits de la source et du destinataire doivent être identiques.

Les informations sont reçues dans l'ordre où elles ont été émises.

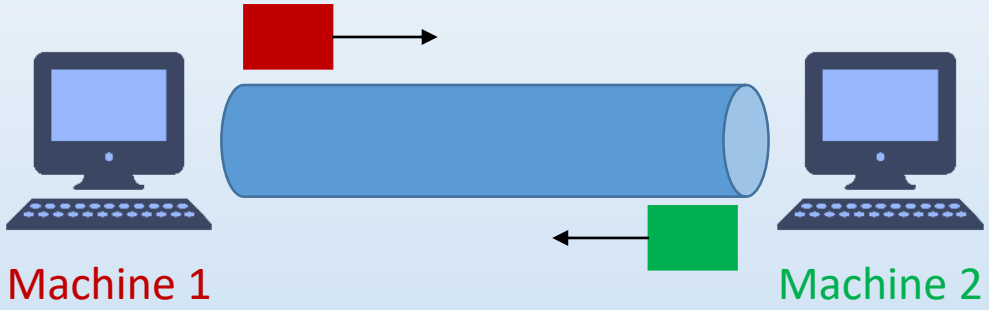


Chaque paquet est acheminé dans le réseau indépendamment du précédent.



Un routeur reçoit un paquet le réémet immédiatement sur la voie optimale

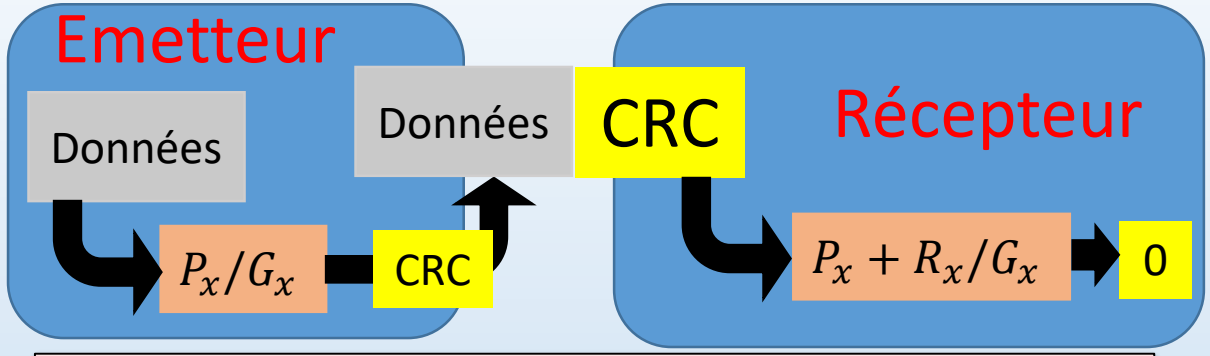
❖ Notion de protocole



Ensemble de conventions préétablies pour réaliser un échange fiable

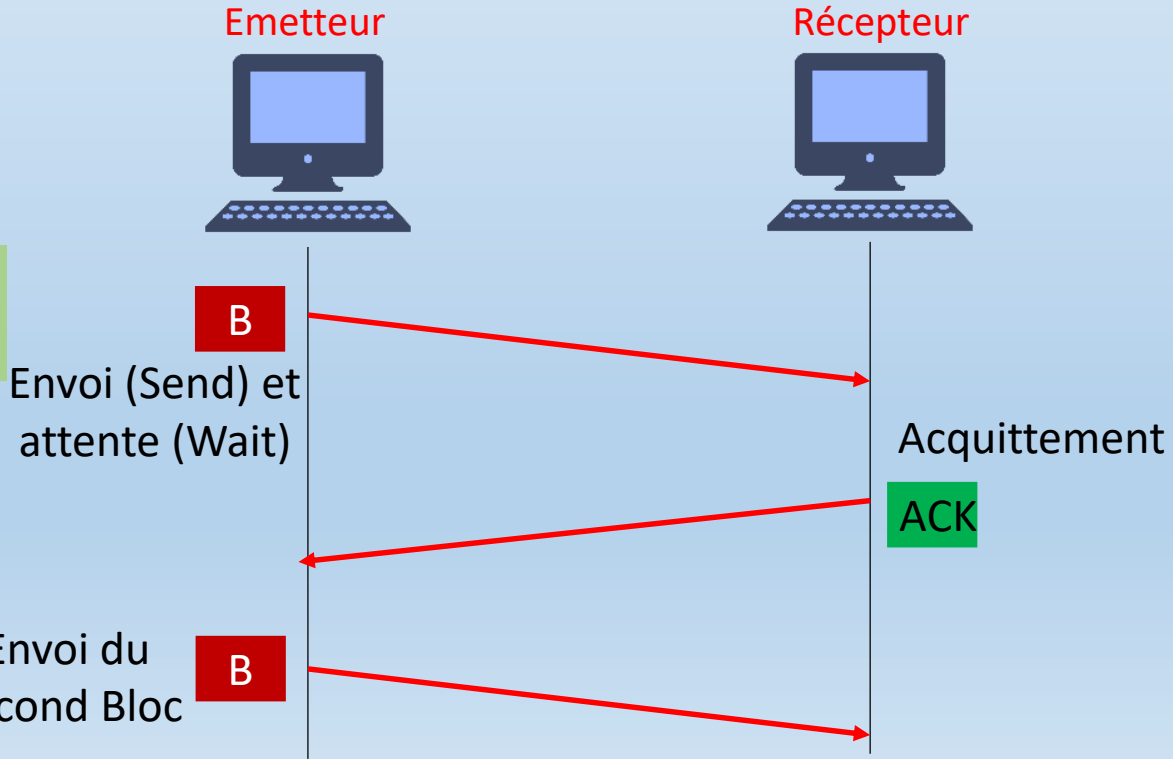
- Délimitation des blocs de données échangés
- Organisation, contrôle de l'échange et de liaison
- Contrôle de l'intégrité des données reçues1

❑ Contrôle de l'intégrité

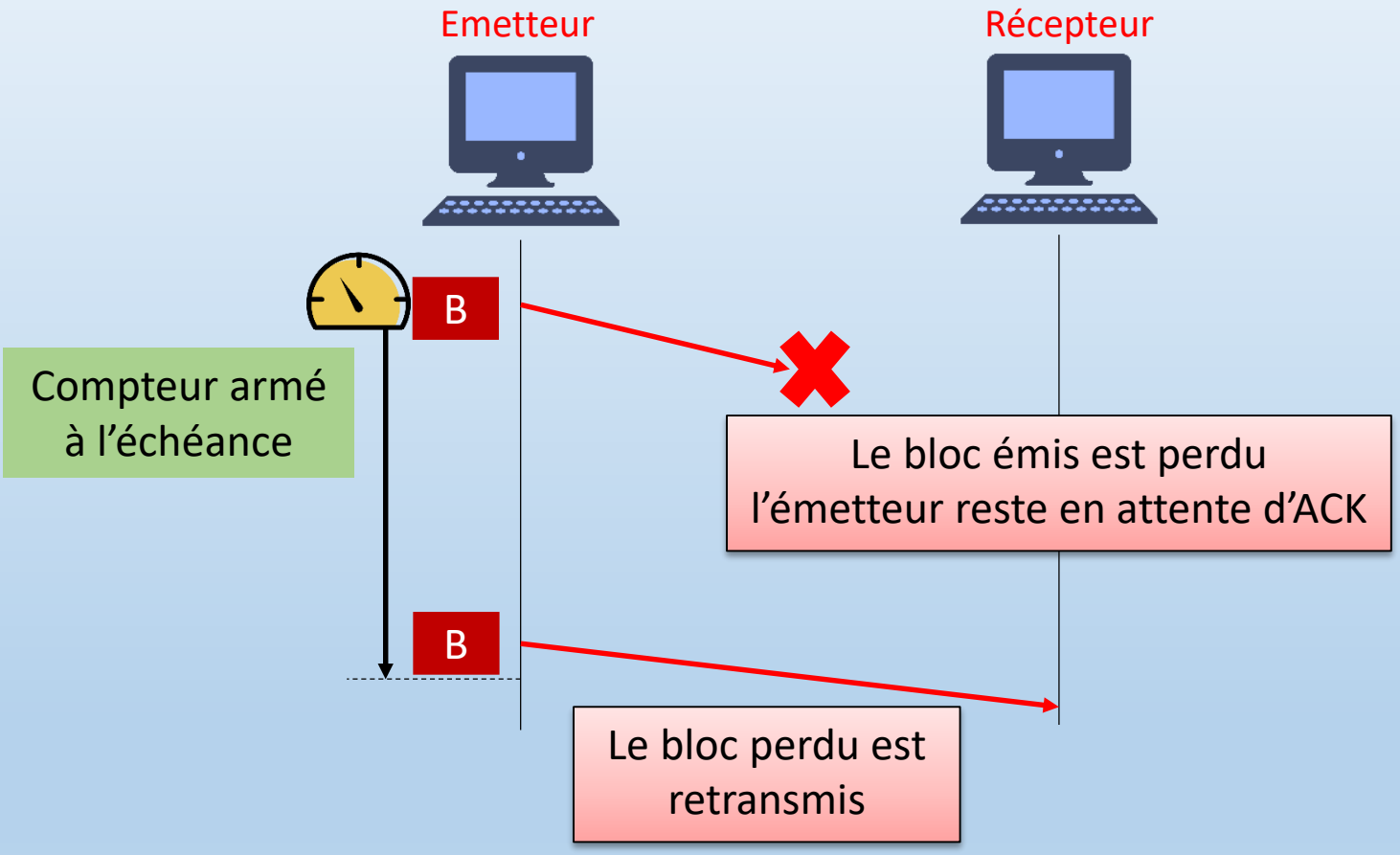


Les codes cycliques ou détection par clé calculée

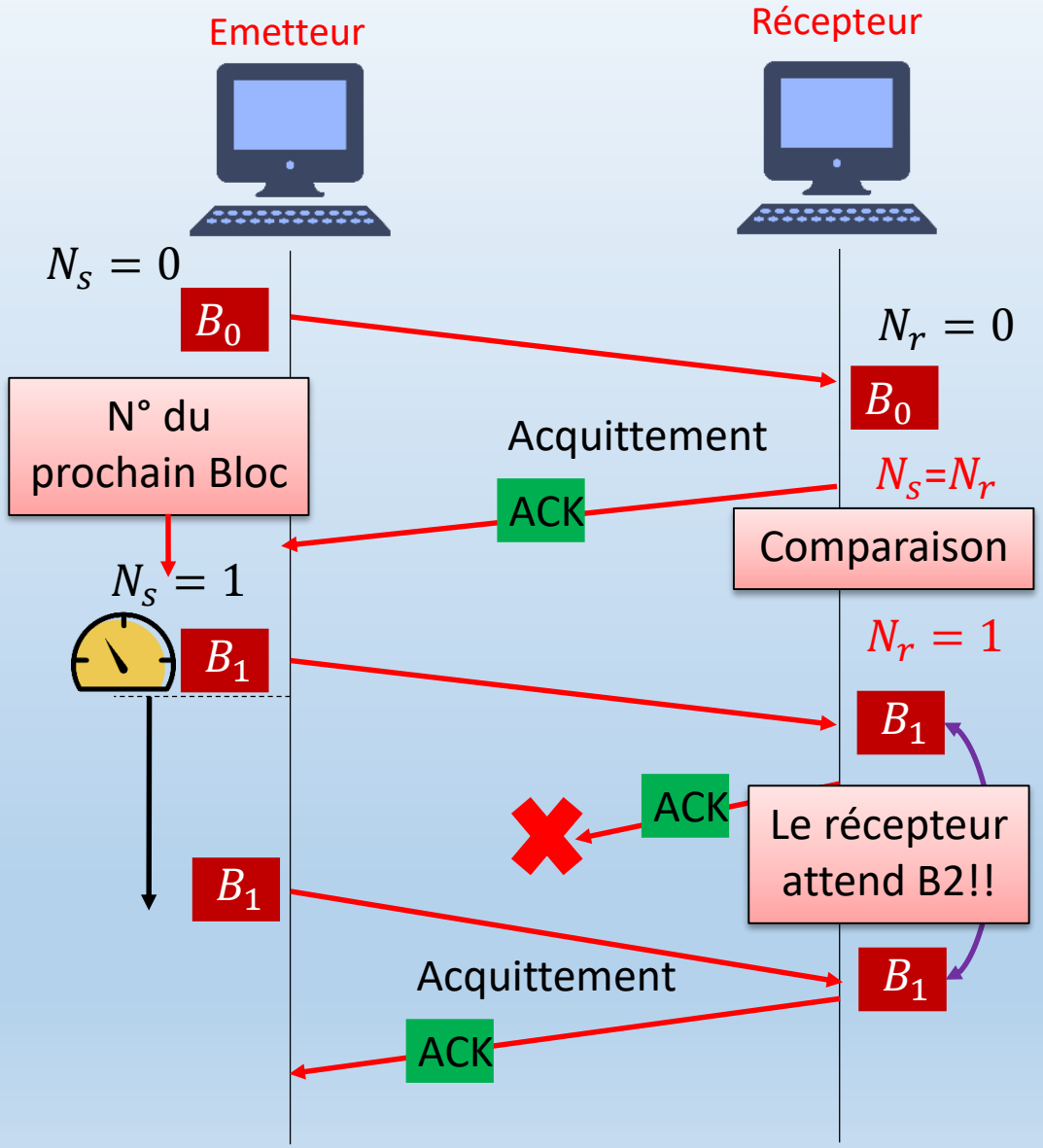
❑ Contrôle de l'échange



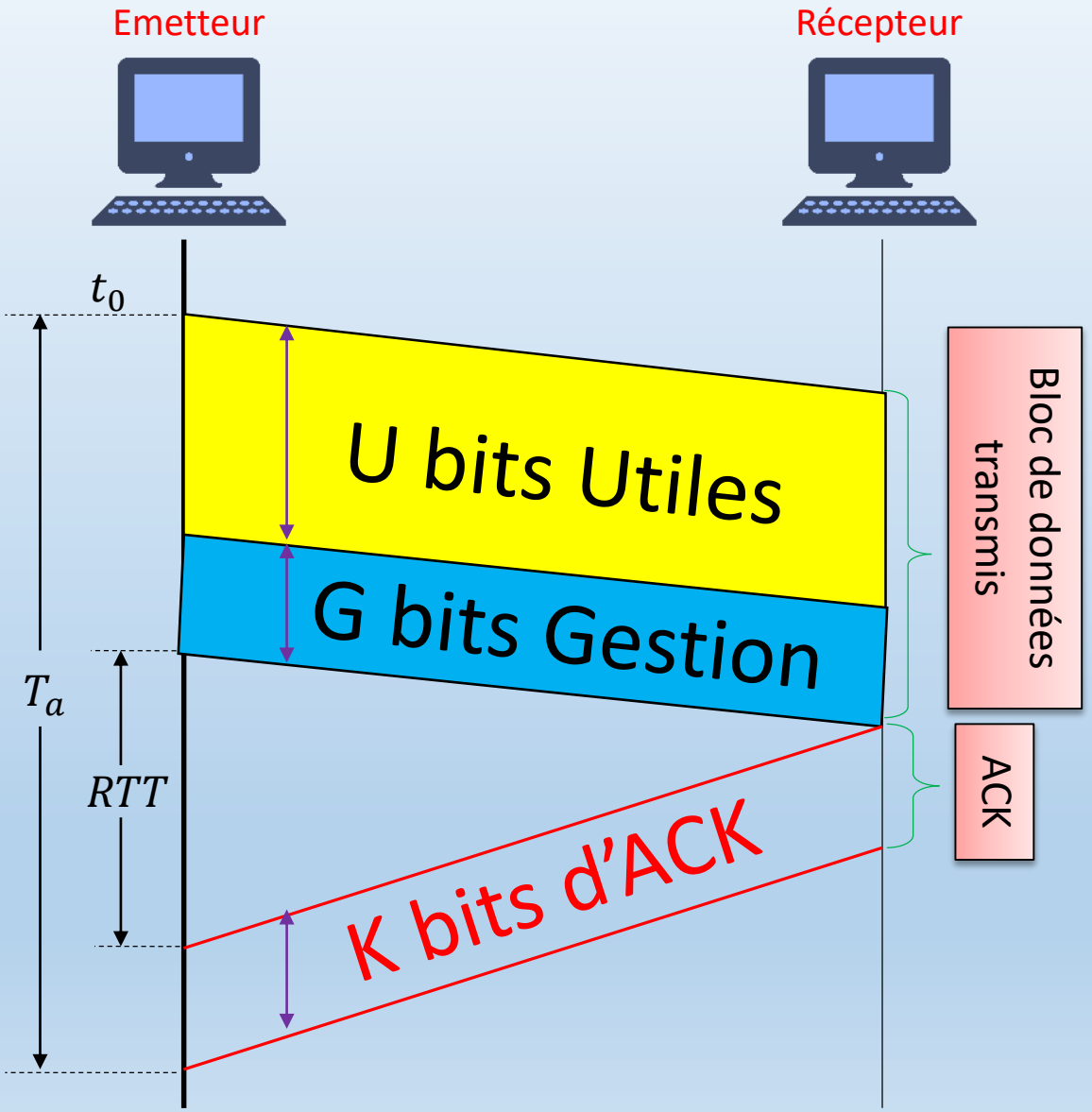
❑ Contrôle de l'échange



❑ Numérotation des blocs de données



❑ Efficacité du protocole de base



- L'efficacité sans erreur est donnée donc :

$$E_0 = \frac{U}{U + S}$$

$$S = G + K + D * RTT$$

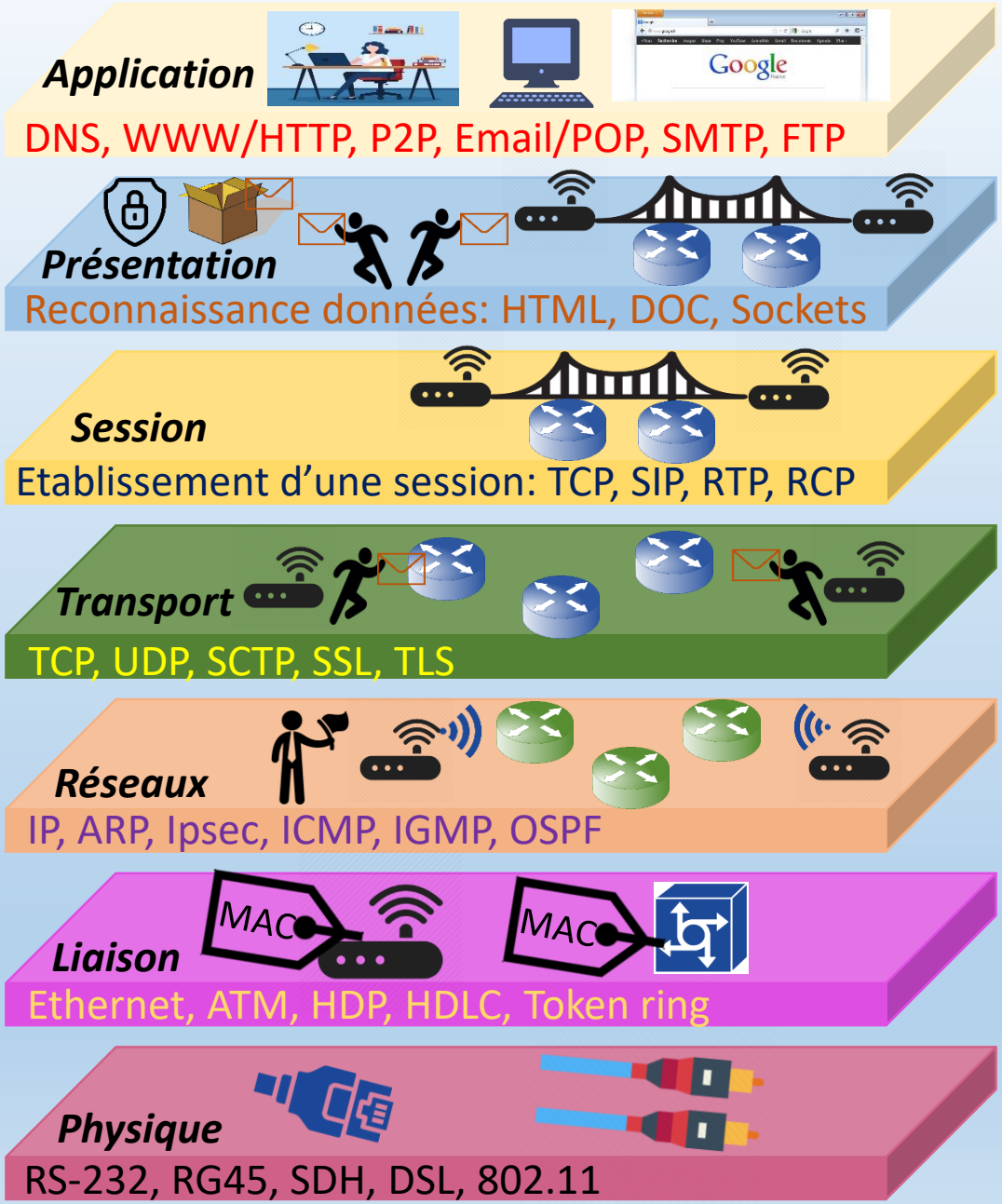
- L'efficacité erreur est donnée donc

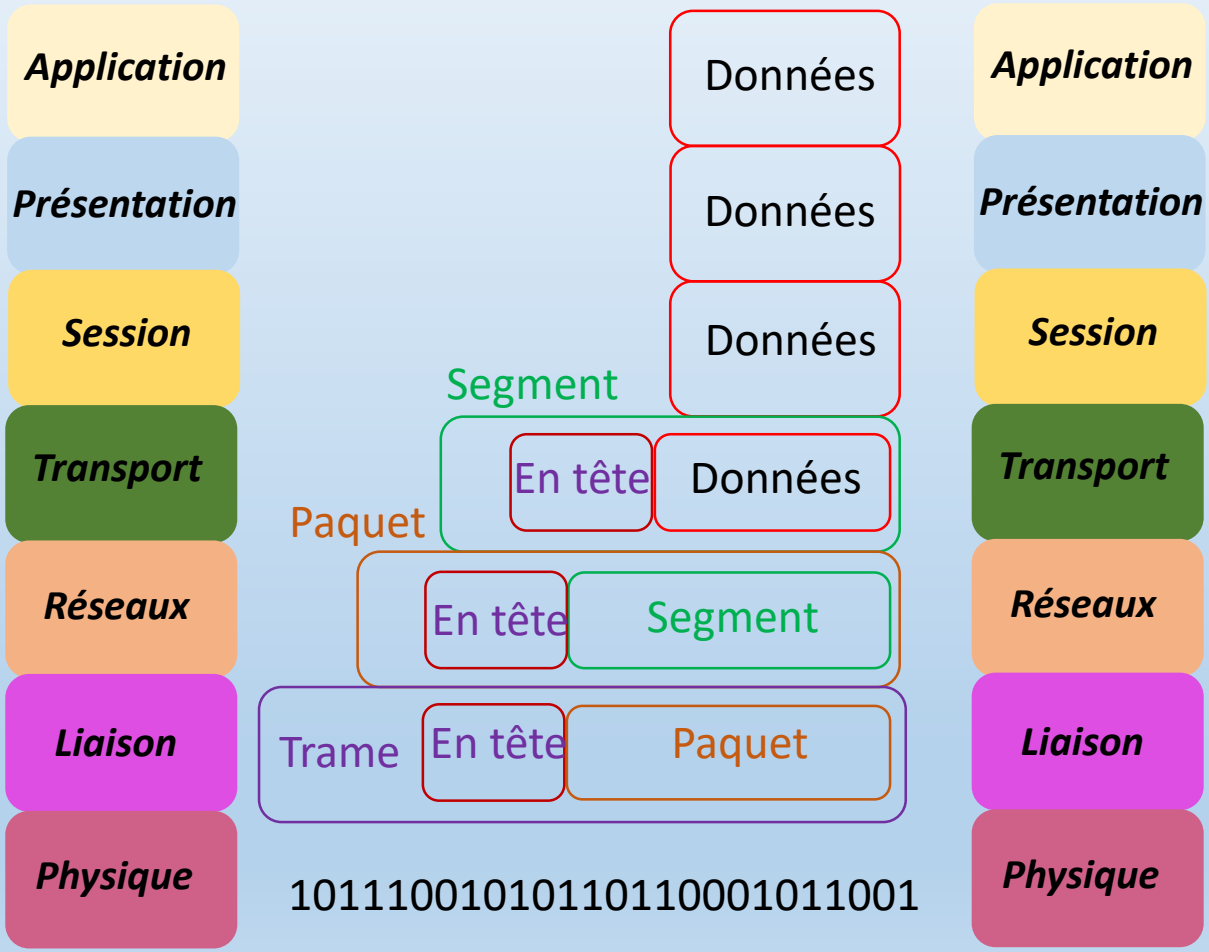
$$E_{err} = E_0 \times (1 - t_e)^N \times (1 - t_e)^K$$

En négligeant $(1 - t_e)^K$, l'efficacité peut être calculé par

$$E_{err} = E_0 \times (1 - t_e)^N$$

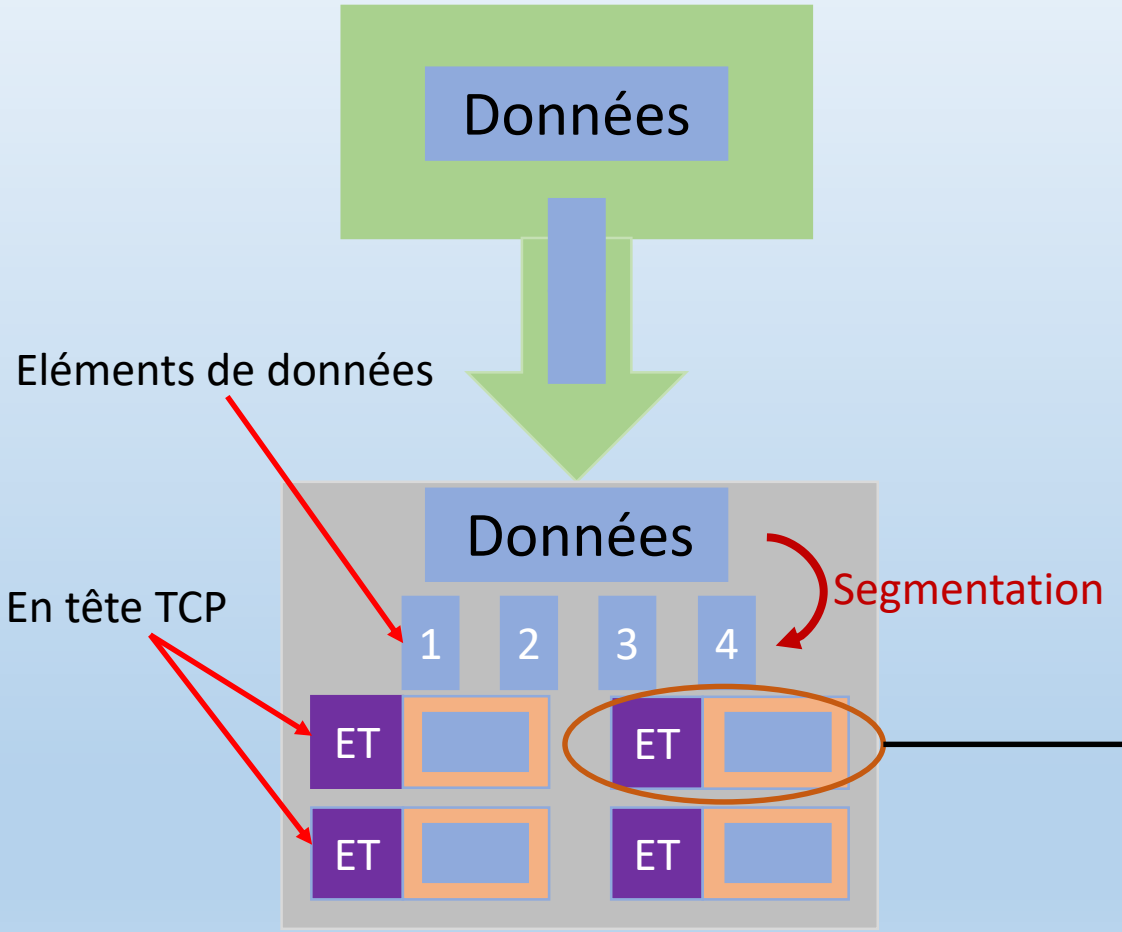
❖ Principe de fonctionnement d'une architecture en couches

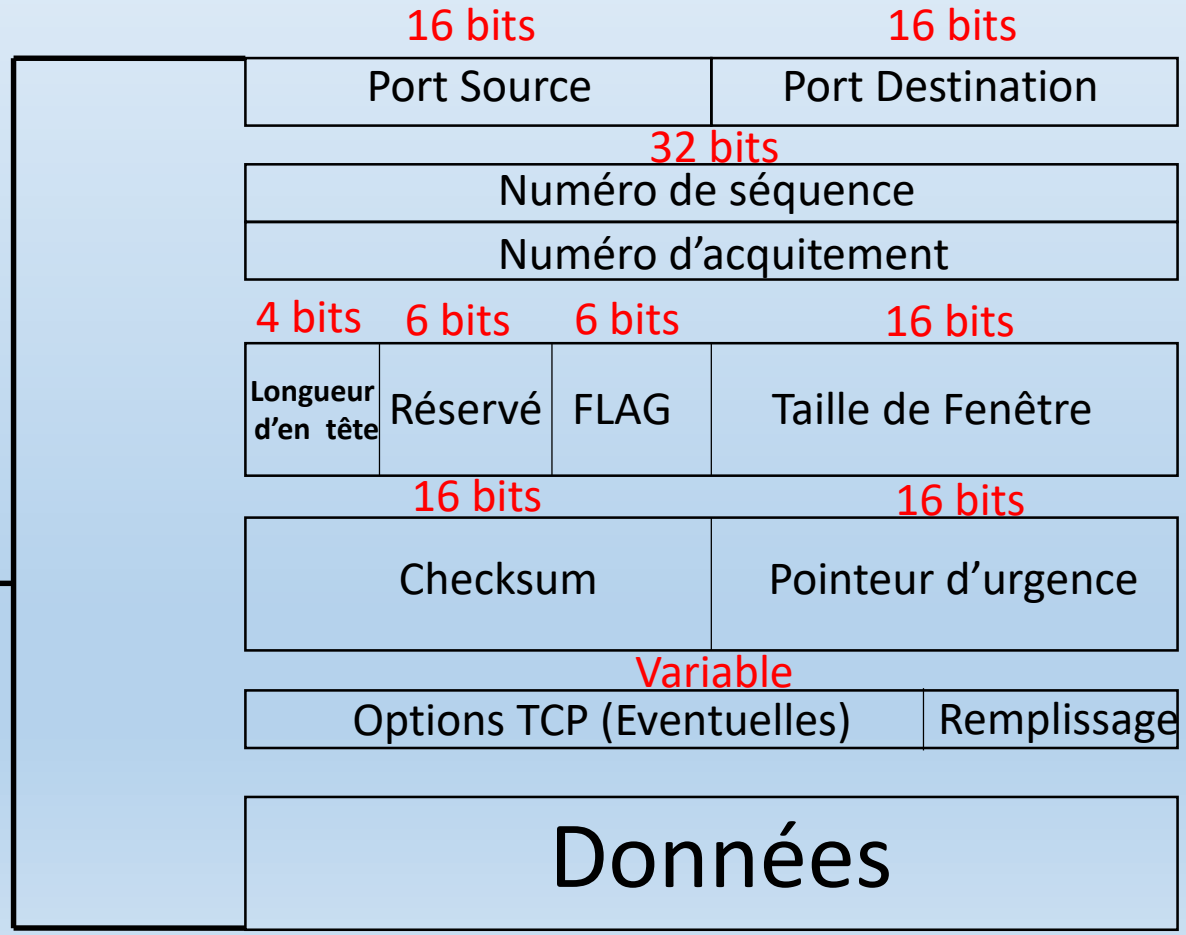




❖ Protocole TCP (Principe et fonctionnalité)

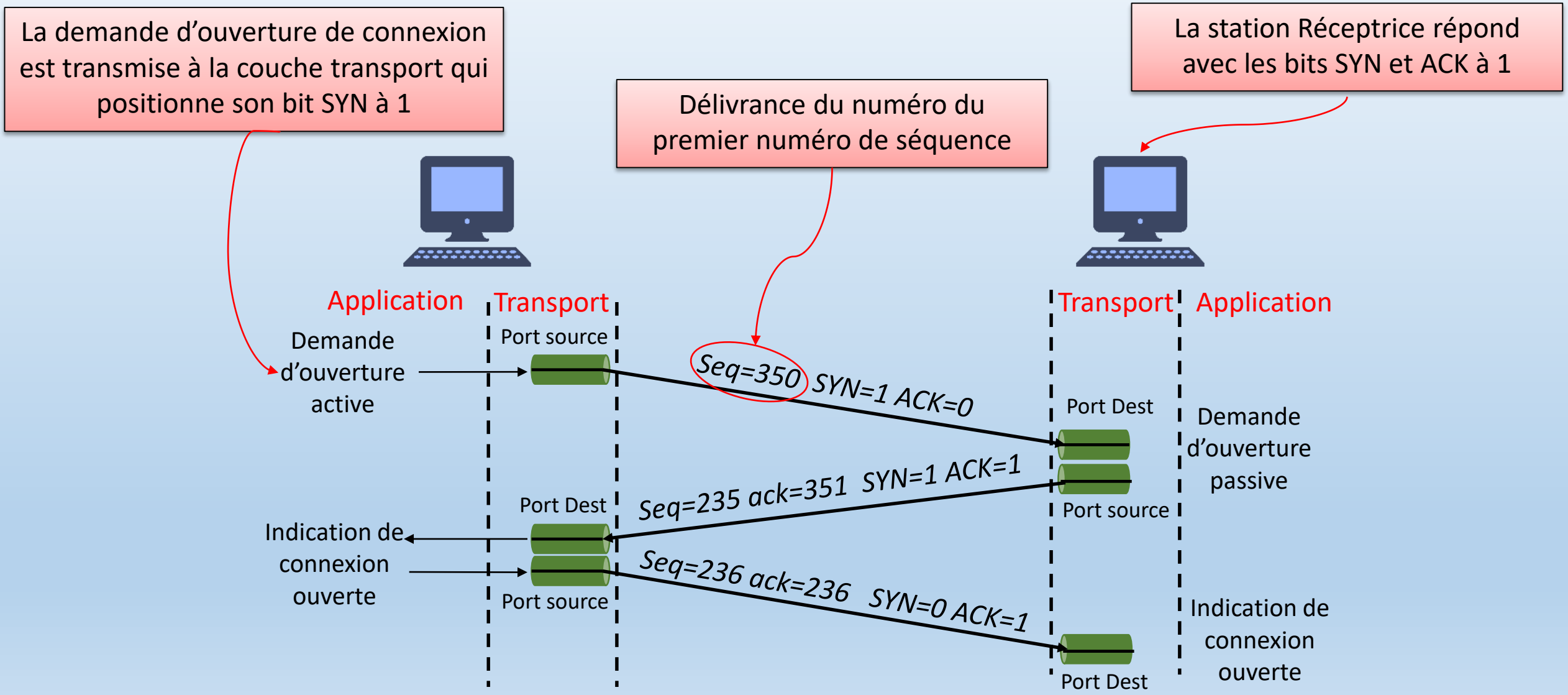
Ses principales caractéristiques sont:
- ✓ Etablissement et fermeture de connexion
- ✓ Segmentation et réassemblage
- ✓ Acquittement des datagrammes et retransmission
- ✓ Contrôle de flux et multiplexage des données



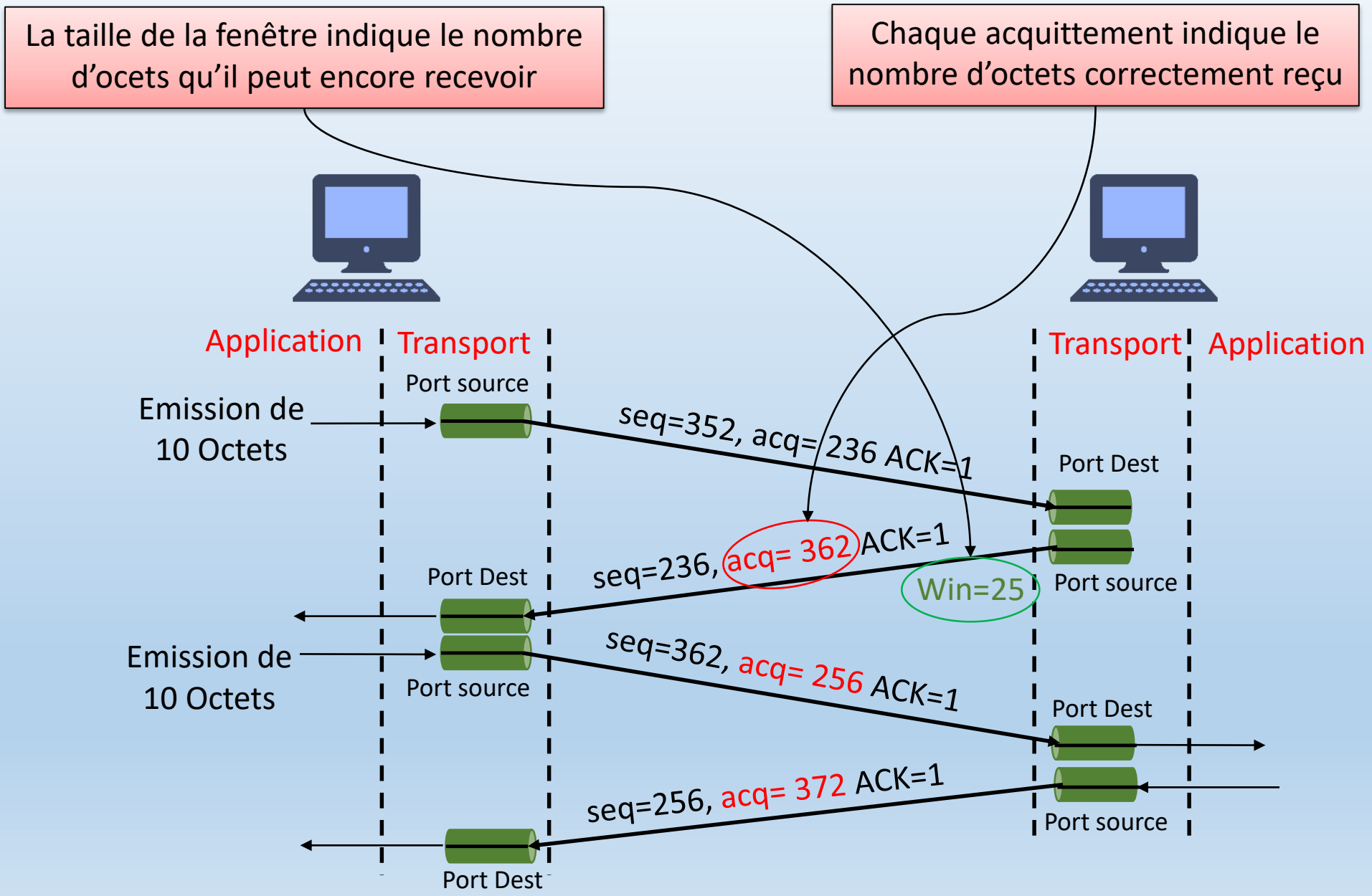


Champ TCP	Description
Ports Source et Destination	Identifier le processus source et le processus de destination.
Numéro de séquence	Le numéro de séquence indique le numéro du premier octet transmis dans le segment
Numéro d'acquittement	Contient le numéro de séquence du prochain octet attendu par le récepteur
La longueur de l'en tête	Donne le nombre de mots de 32 bits
Les bits de contrôle (FLAG)	Permettent de définir la fonction du message
Fenêtre	Indique le nombre d'octets que le récepteur peut encore accepter à partir du dernier numéro d'acquitement
Checksum	Correspond à une somme de contrôle de l'en tête de message
Le champ priorité	Contient un pointeur sur les octets de données à traité en priorité lorsqu'une interruption est enregistrée
Le champ option	Définie la taille maximale d'un Segment

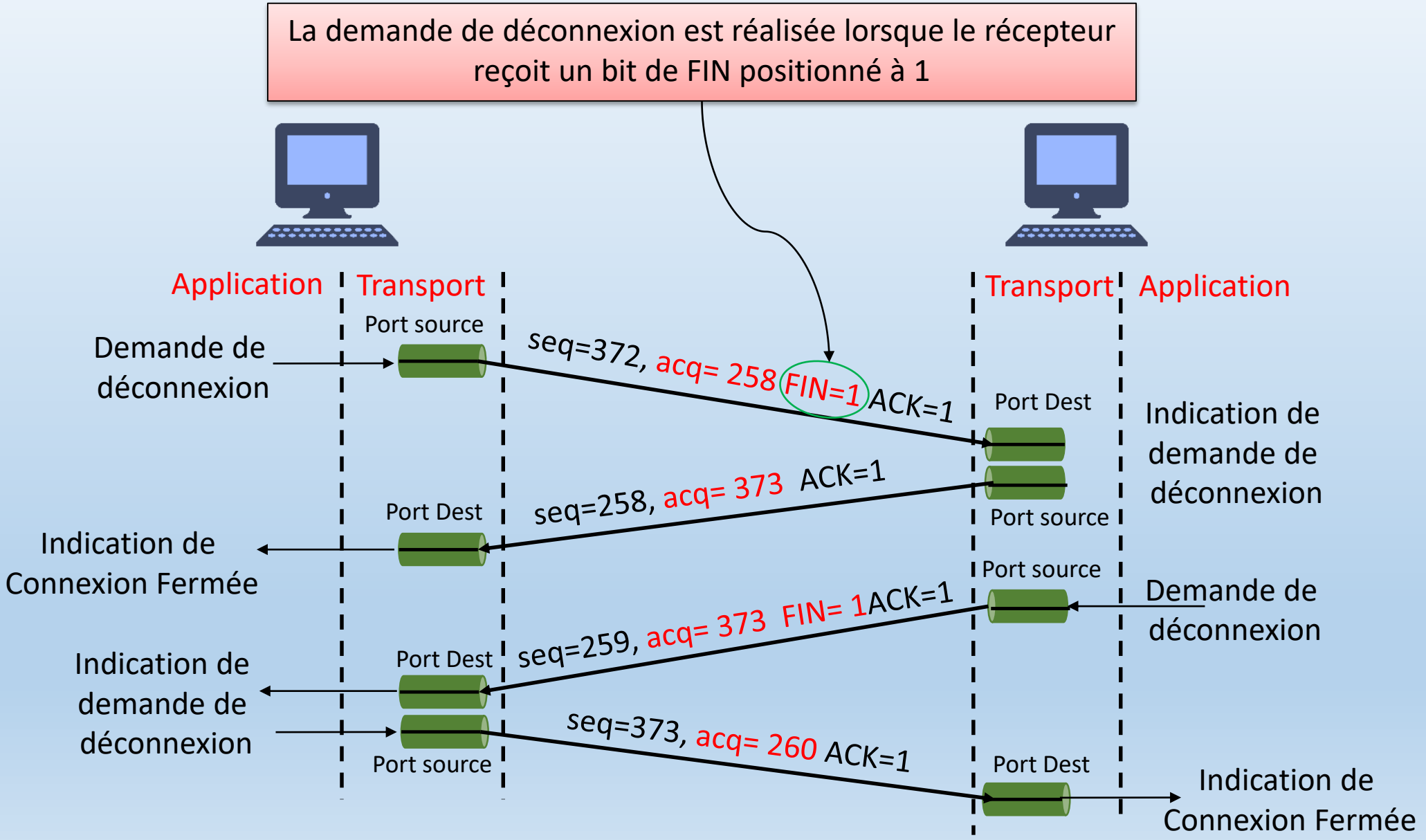
❑Ouverture d'une connexion TCP



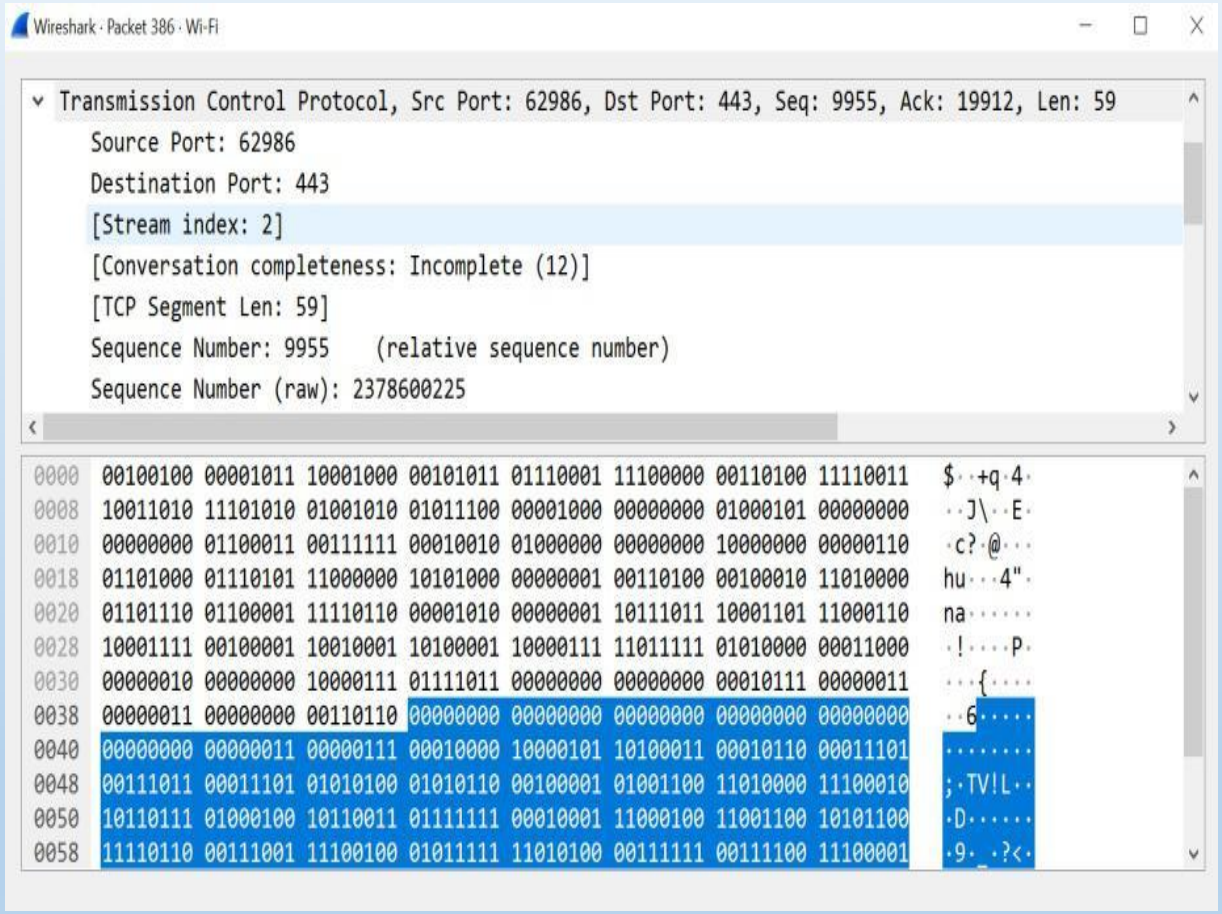
❑ Transfert de données TCP

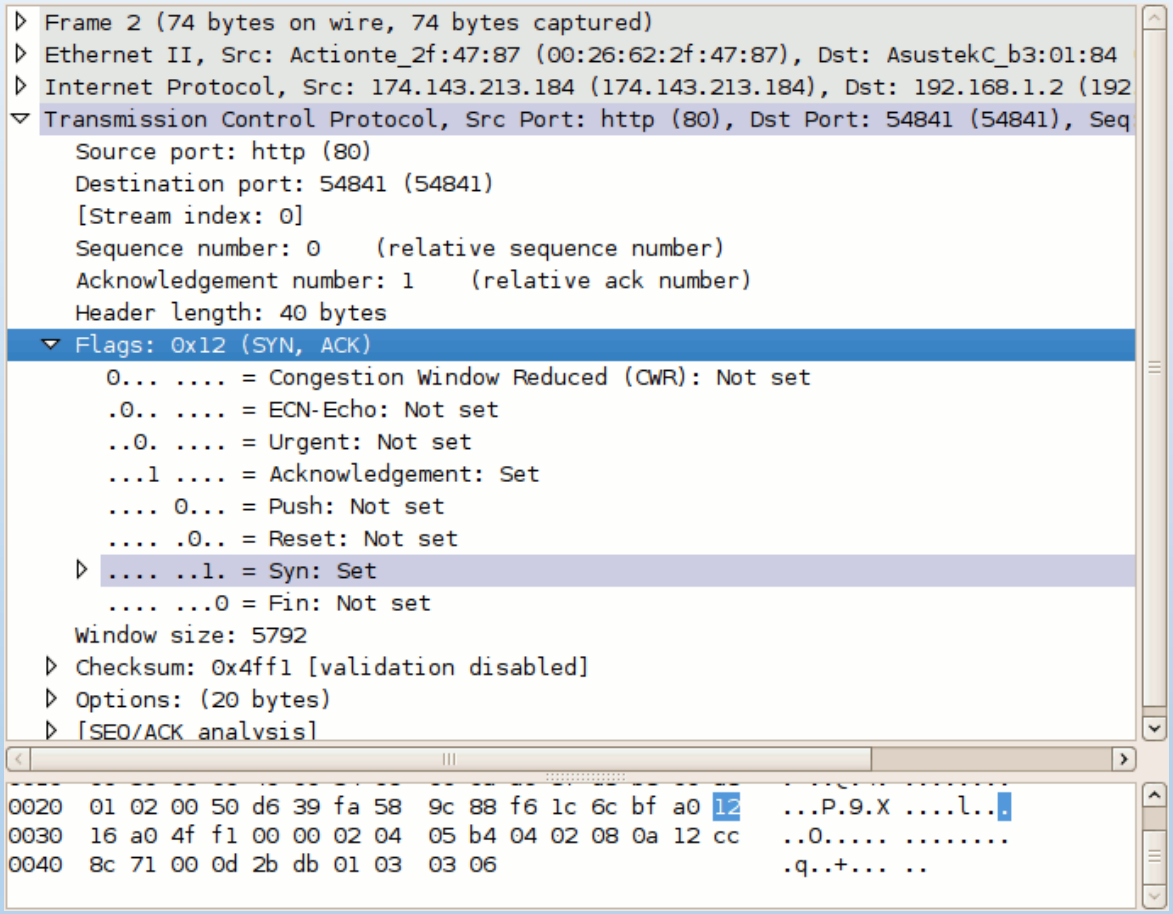


❑ Fermeture d'une connexion TCP



❑ Exemple d'analyse TCP avec wireshark





❖ Protocole IP et Adressage IPv4

Le protocole IP est un protocole de niveau réseau

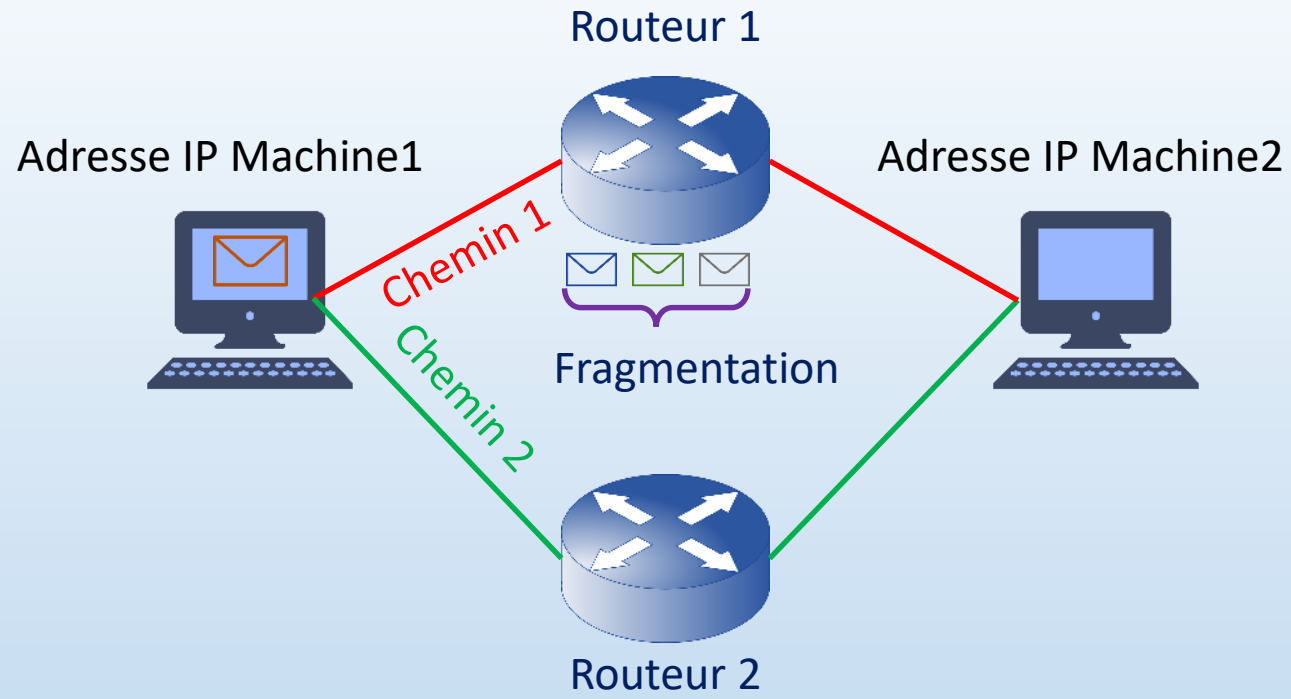
Objectif

Lors de l'émission

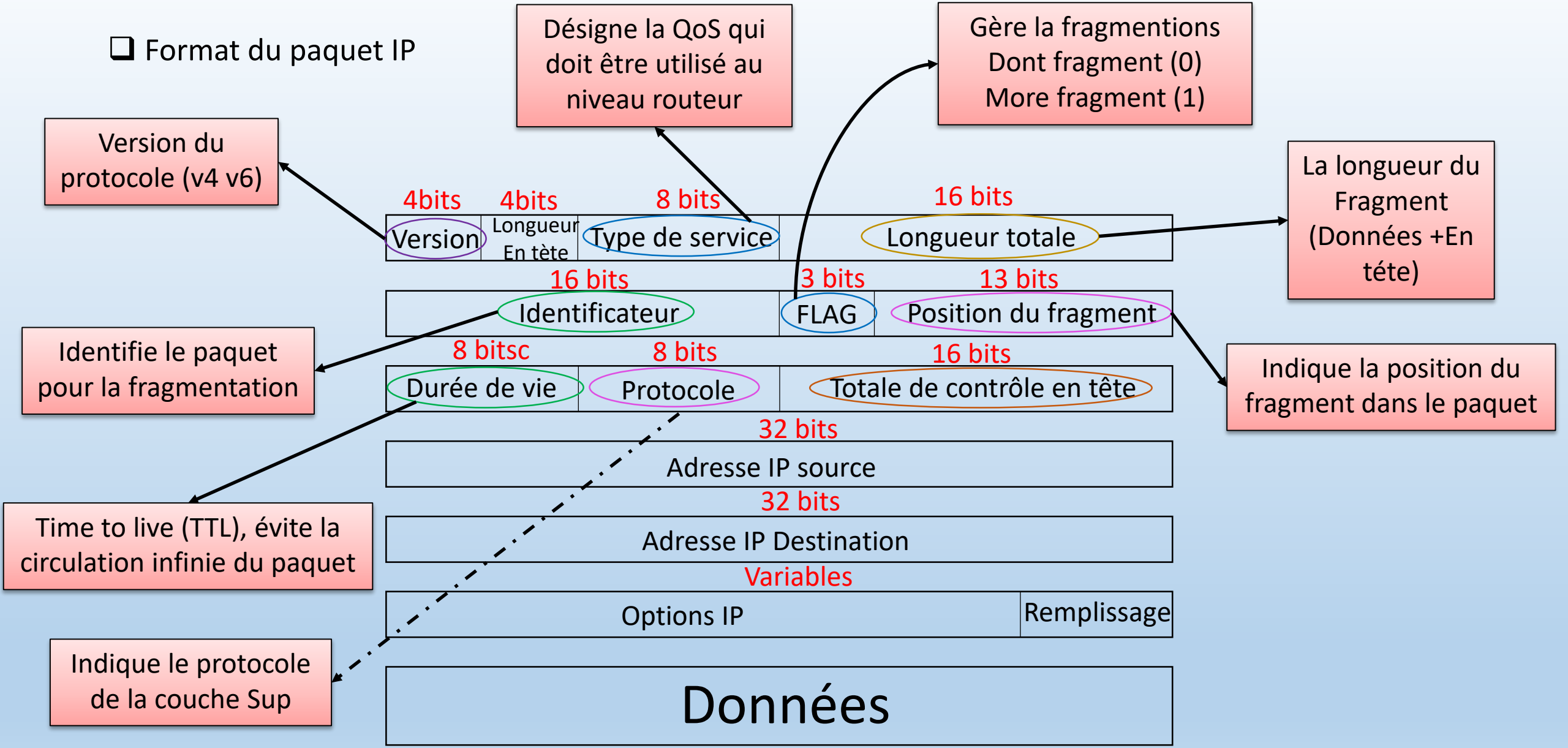
- Identification des paquets
- Détermination des chemins (Routage)
- Vérification du type d'adressage
- Fragmentation des paquets

Lors de la réception

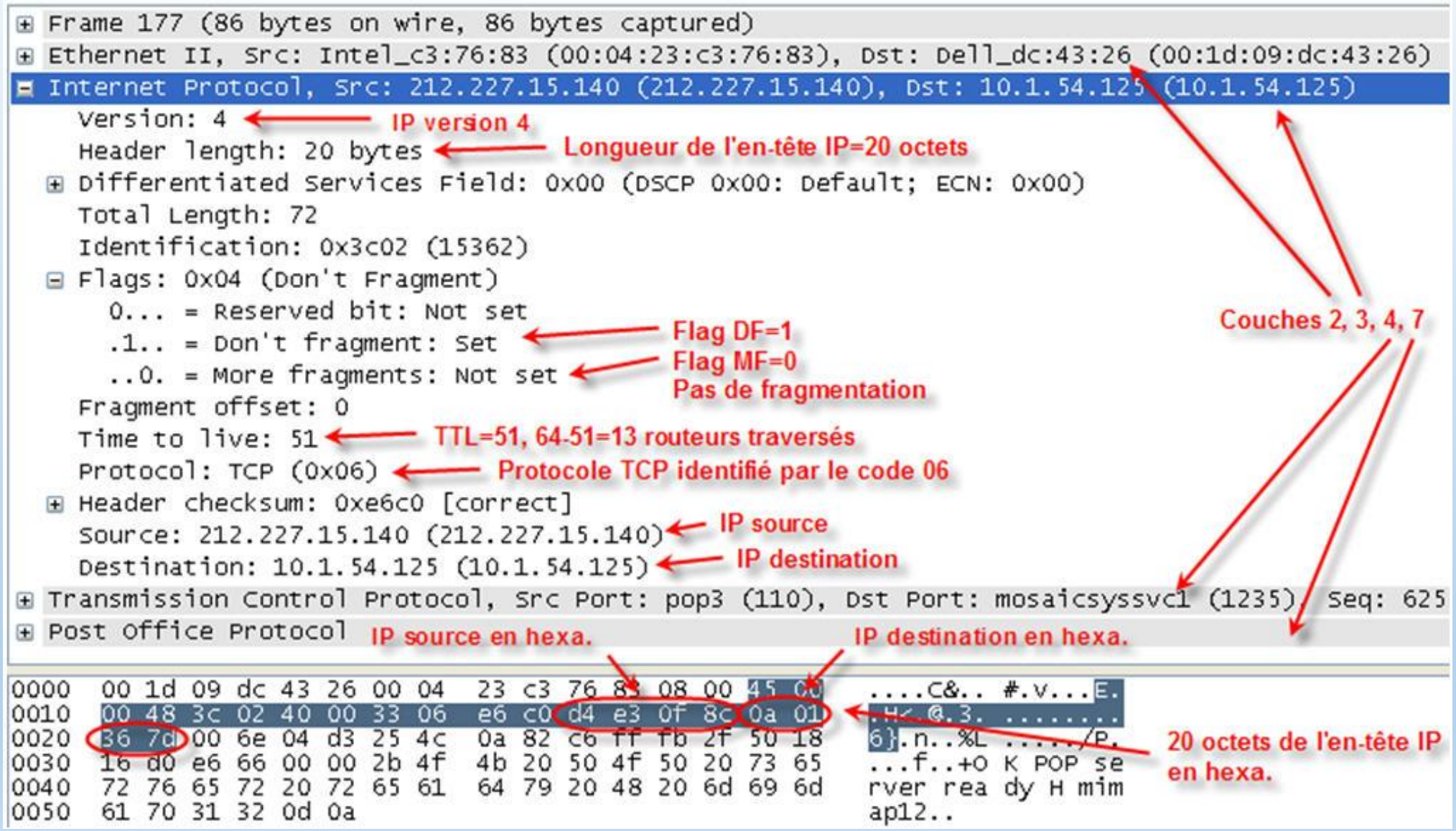
- Vérification de la longueur de paquet
- Contrôle d'erreurs
- Transmission de paquet réassemblé en au niveau Sup
- Réassemblage des paquets en cas de fragmentation



❑ Format du paquet IP

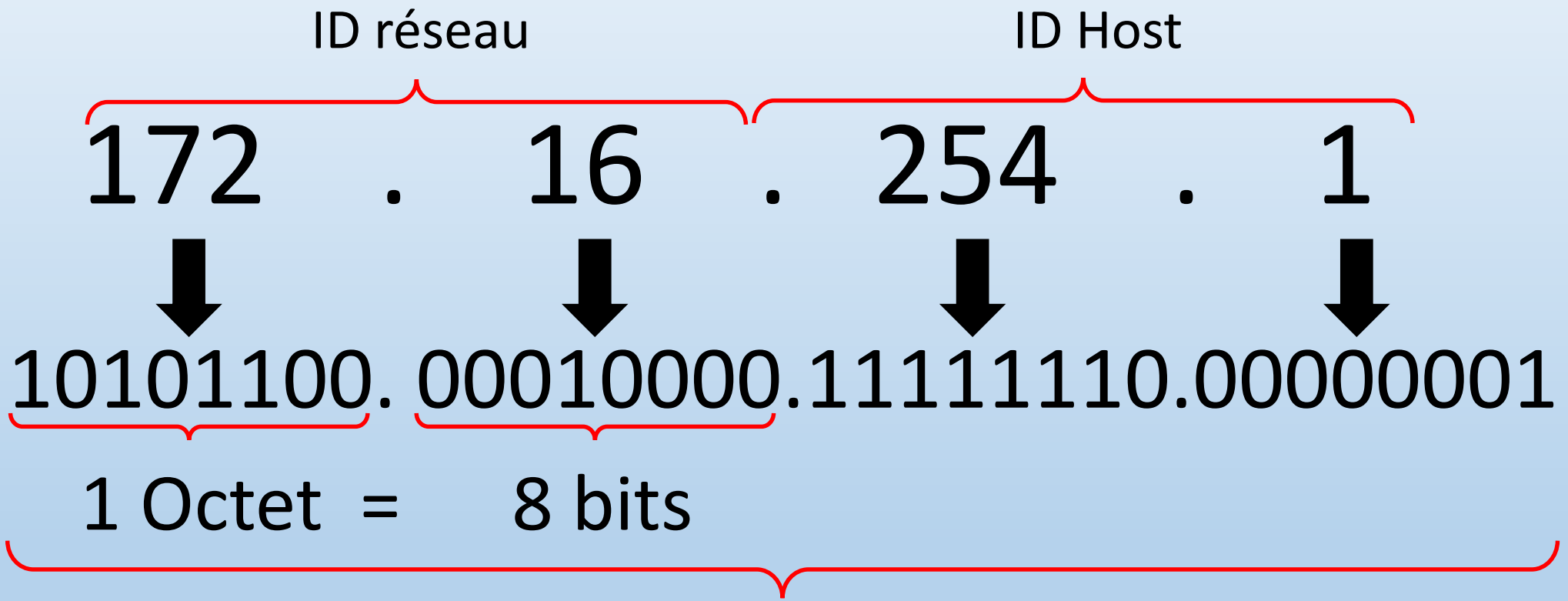


❑ Exemple d'analyse de datagramme IP avec wireshark

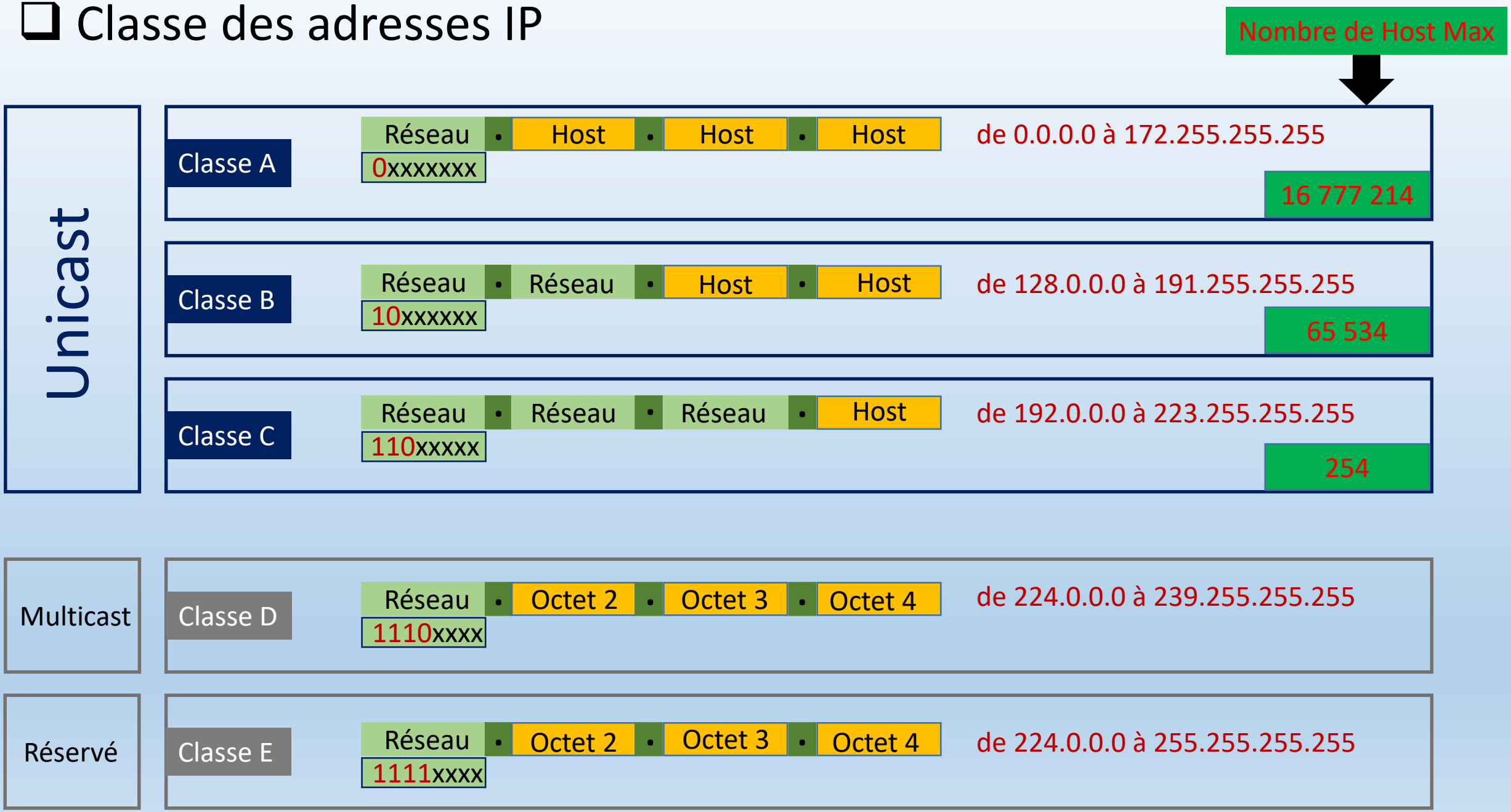


❑ Adressage IPv4

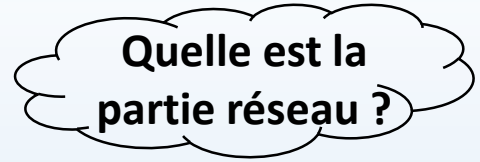
Adresse IP = ID réseau + ID Host



❑ Classe des adresses IP



❑ Masque de sous réseau



	Réseau	Réseau	Réseau	Host
Adresse IP machine 1	192	168	1	1
Masque sous réseau	255	255	255	0

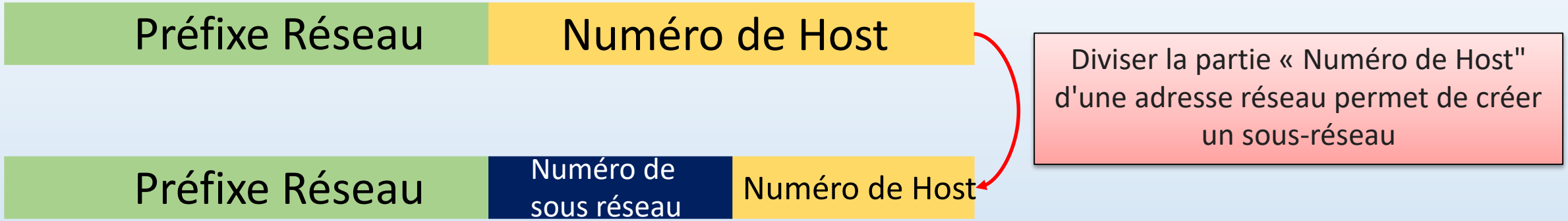
Adresse IP machine 1	11000000	1010100	00000001	00000001
Masque sous réseau	11111111	11111111	11111111	00000000

Identifie le Réseau — Identifie les Hosts

Le nombre Max de Hôtes est de 254 (256 – 1 **Adresse réseau** -1 **adresse de diffusion**)
Adresse réseau: 192.168.1.0 (adresse de départ) ou bien 192.168.1.**/24**
Adresse de diffusion: 192.168.255.255 (Dernière adresse)

→ CIDR

❑ Calcule des sous réseaux (Segmentation)



Exemple de calcule

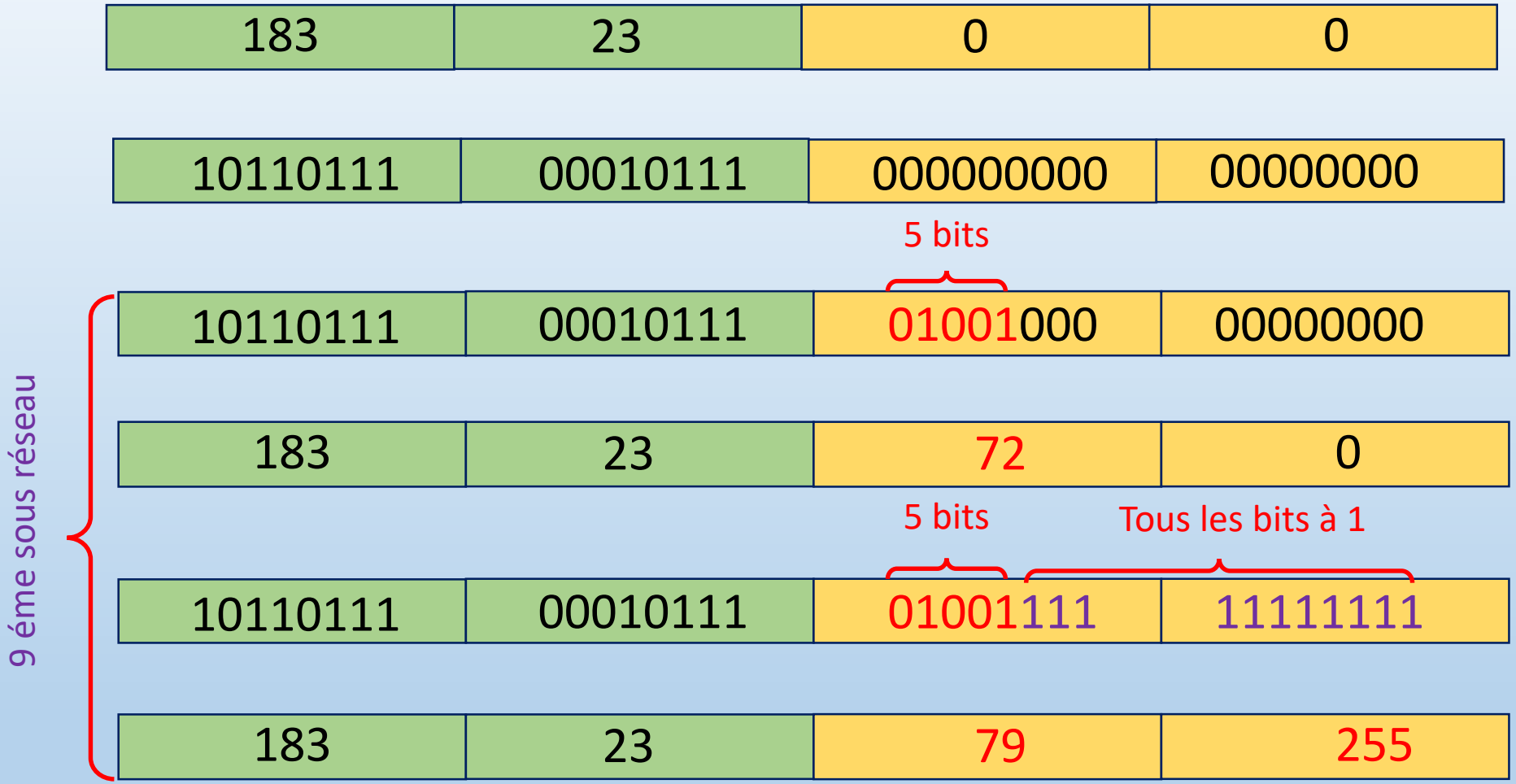
Soit le réseau 183.23.0.0/16 à diviser en 27sous-réseaux

$27=2^5$ En ajoute 5 bit au 16 bit de réseau (16+5=21)

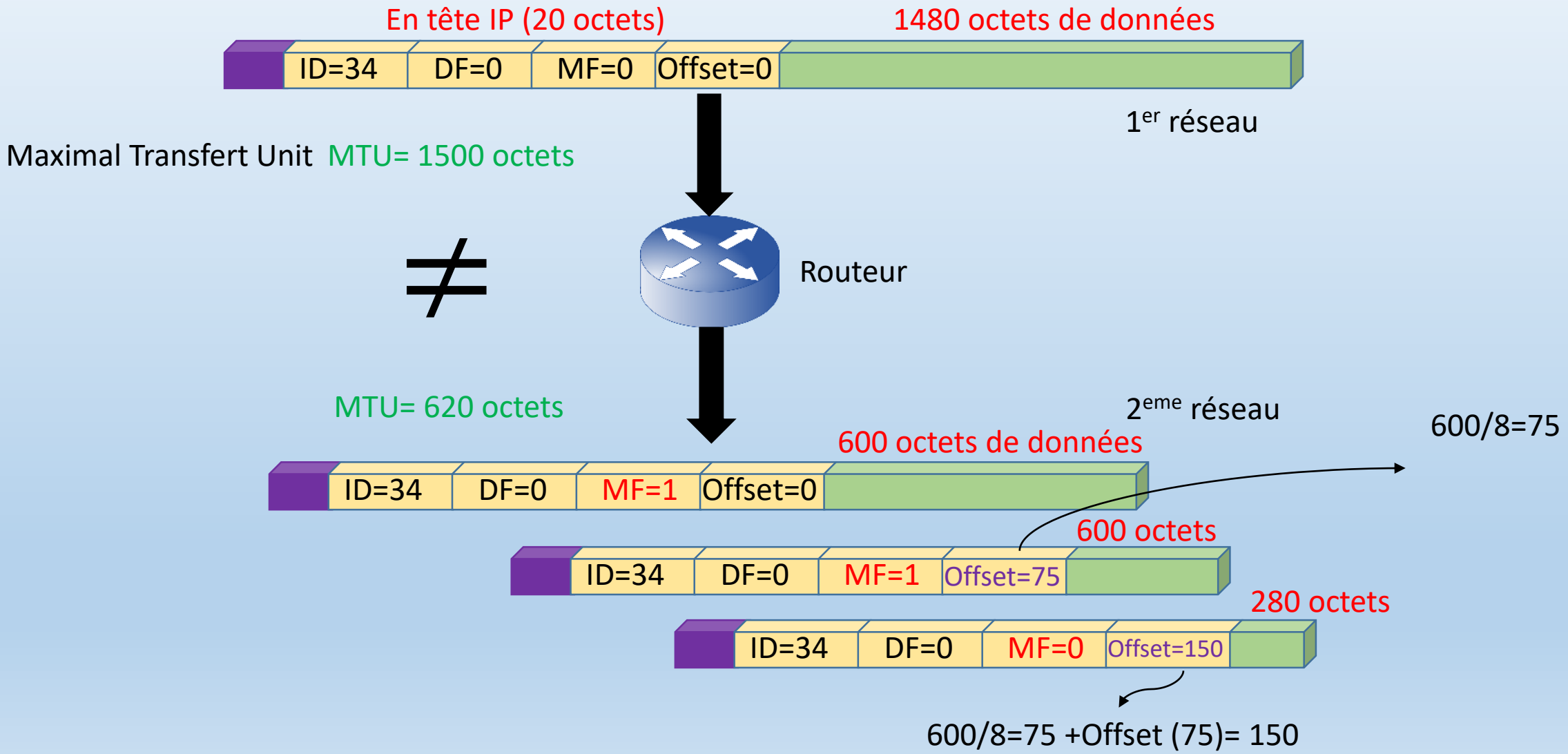
Le nouveau masque sous réseau est alors /21

11111111	11111111	1111100	00000000

❑ Calcule des sous réseaux (Segmentation)

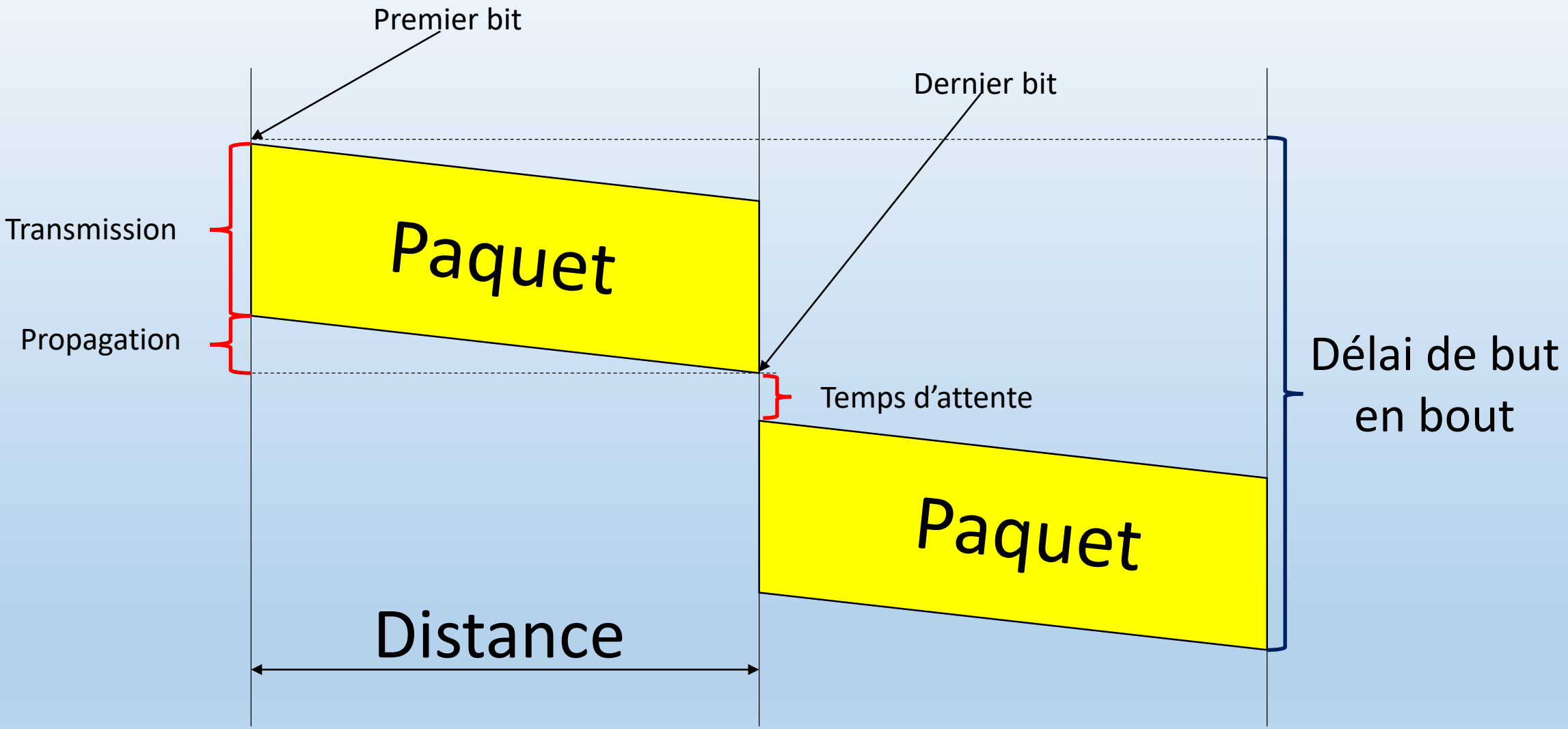


❖ Principe de Fragmentation



❖ Performance Réseau

temps de propagation = Distance/vitesse de propagation



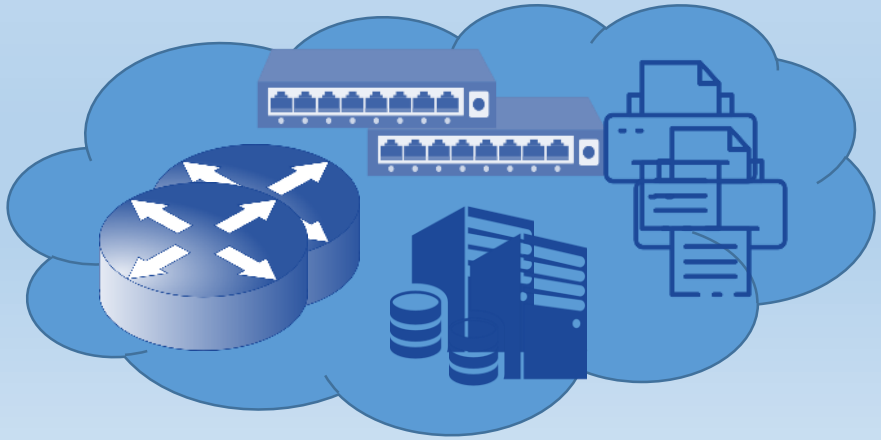
Délai= temps de propagation + temps de Transmission + temps d'attente (Négligeable)

Université Sorbonne Paris Nord: IUT Villetaneuse

Dr. Mohamed Amine Ouamri

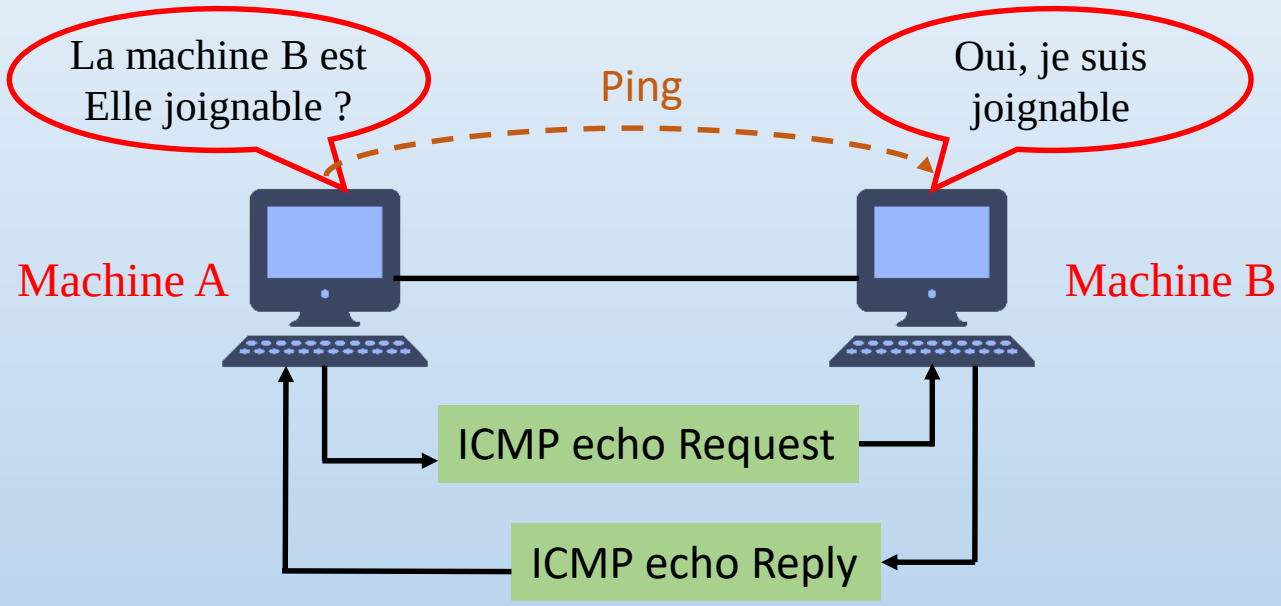
Matière :M51 Réseaux

Chapitre 2: Protocoles ICMP et ARP

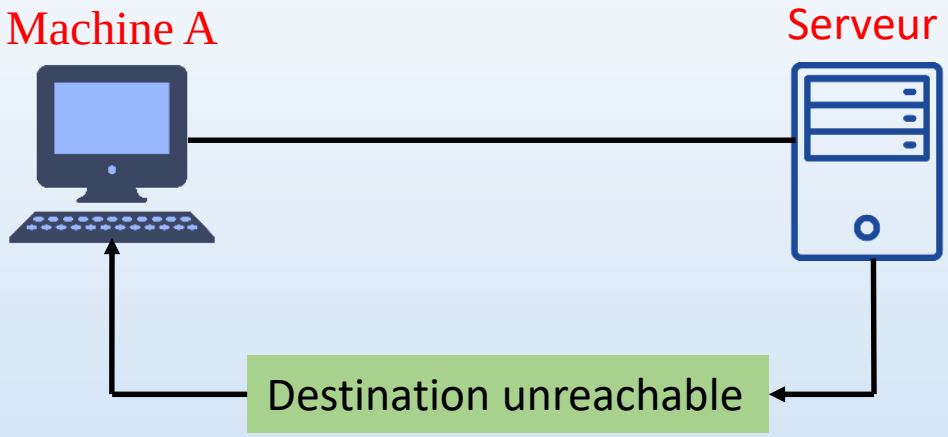


❖ Protocole ICMP

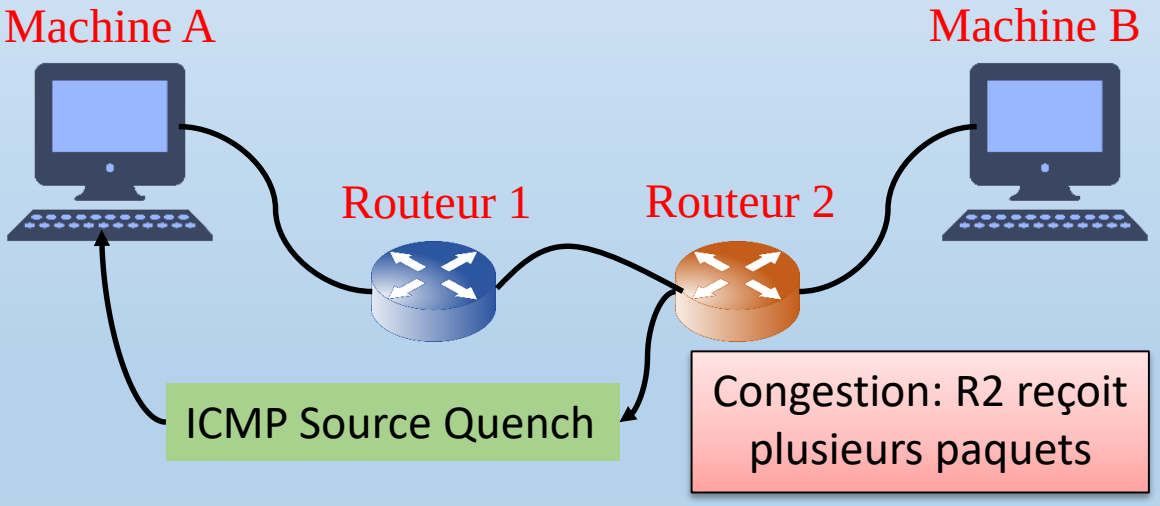
Le protocole ICMP est employé pour gérer le trafic IP.



- ✓ Consiste à vérifier si les données atteignent leur destination au bon moment.
- ✓ Annoncer les erreurs et la congestion des réseau



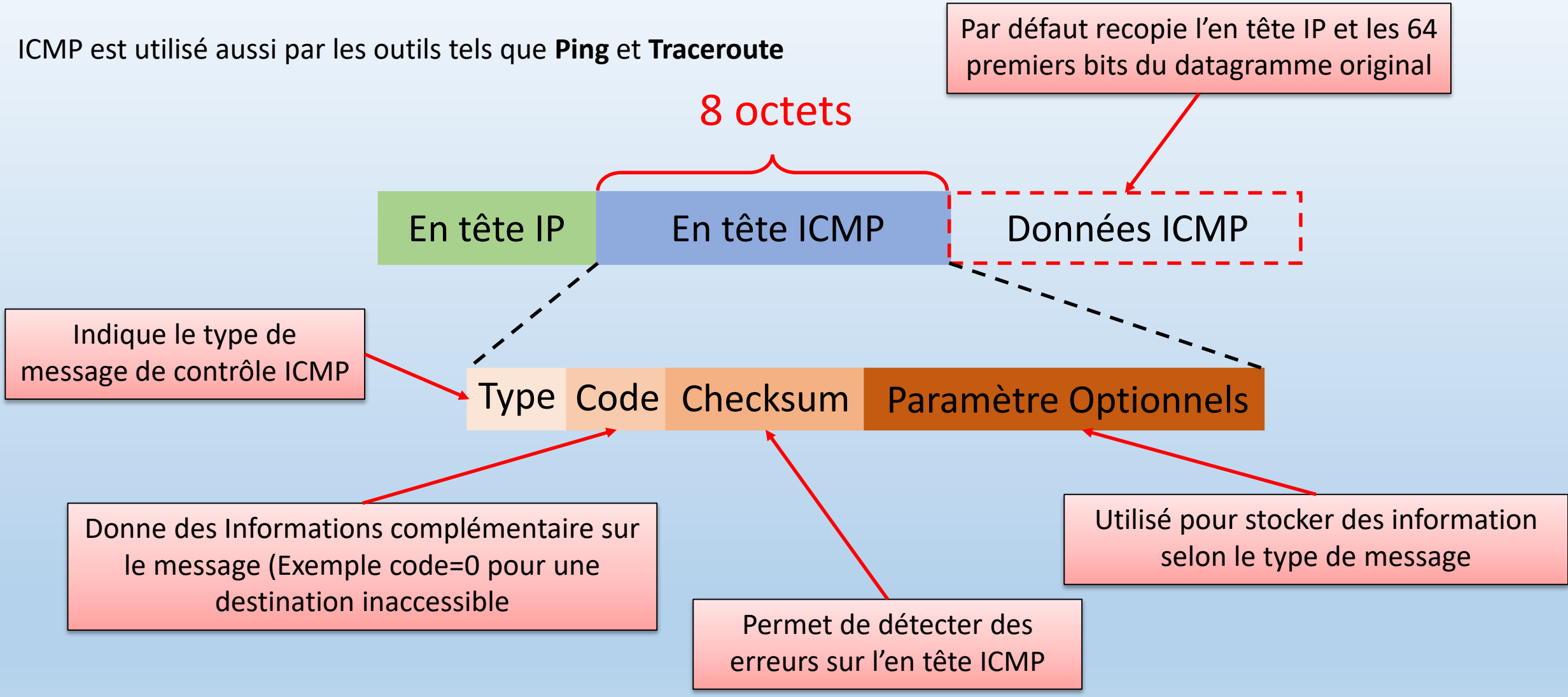
La destination (vers le serveur) est inaccessible



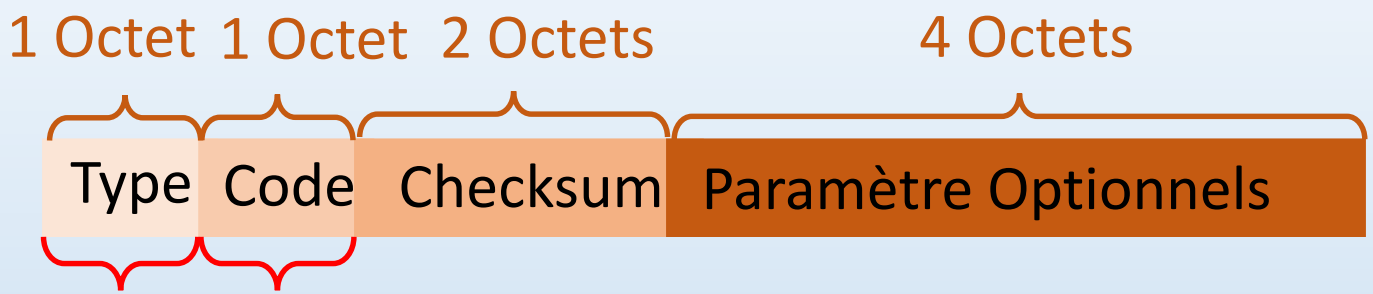
Le messages (ICMP Source Quench) entraîne un ralentissement du rythme de transmission des paquets

❑ Format des paquets ICMP

ICMP est utilisé aussi par les outils tels que **Ping** et **Traceroute**



❑Type de message et code ICMP



0	0	**Echo reply:** le hote répond au message ICMP echo request
3	0-15	**Destination Unreachable:** le paquet ne peut être délivré
4	0	**Source Quench:** Incite la source à ralentir la vitesse de transmission
5	0-3	**Redirect:** Demande au routeur de rediriger le paquet par un autre chemin
8	0	**Echo request:** Demande a une machine si elle est présente et opérationnelle
11	0-1	**Time exceeded:** Le champ Time to live (TTL) dans l'en tête IP est arrivé à 0
12	0-2	**Parameter Problem:** Champ non valide dans l'en tête IP
13	0	**Timestamp Request:** Identique à echo request avec un Horodatage
14	0	**Timestamp Reply:** Identique à echo reply avec un Horodatage

❑ Messages de redirection ICMP

RA# show ip route
Network X, ubest/mbest: 1/0
**via 192.168.1.3, [1/0], 10:12:20, static*

2 Le Routeur A vérifie la table de routage en direction du réseau X

3 Le message de redirection ICMP est envoyé à la Machine A. Le message conseil d'envoyer son trafic pour le réseau X

Routeur A

192.168.1.2/24

4 Le Routeur A Transmet le paquet de données d'origine à sa destination

ICMP Redirect

Données

Données

192.168.1.1

192.168.1.3/24

Réseau X

Switch

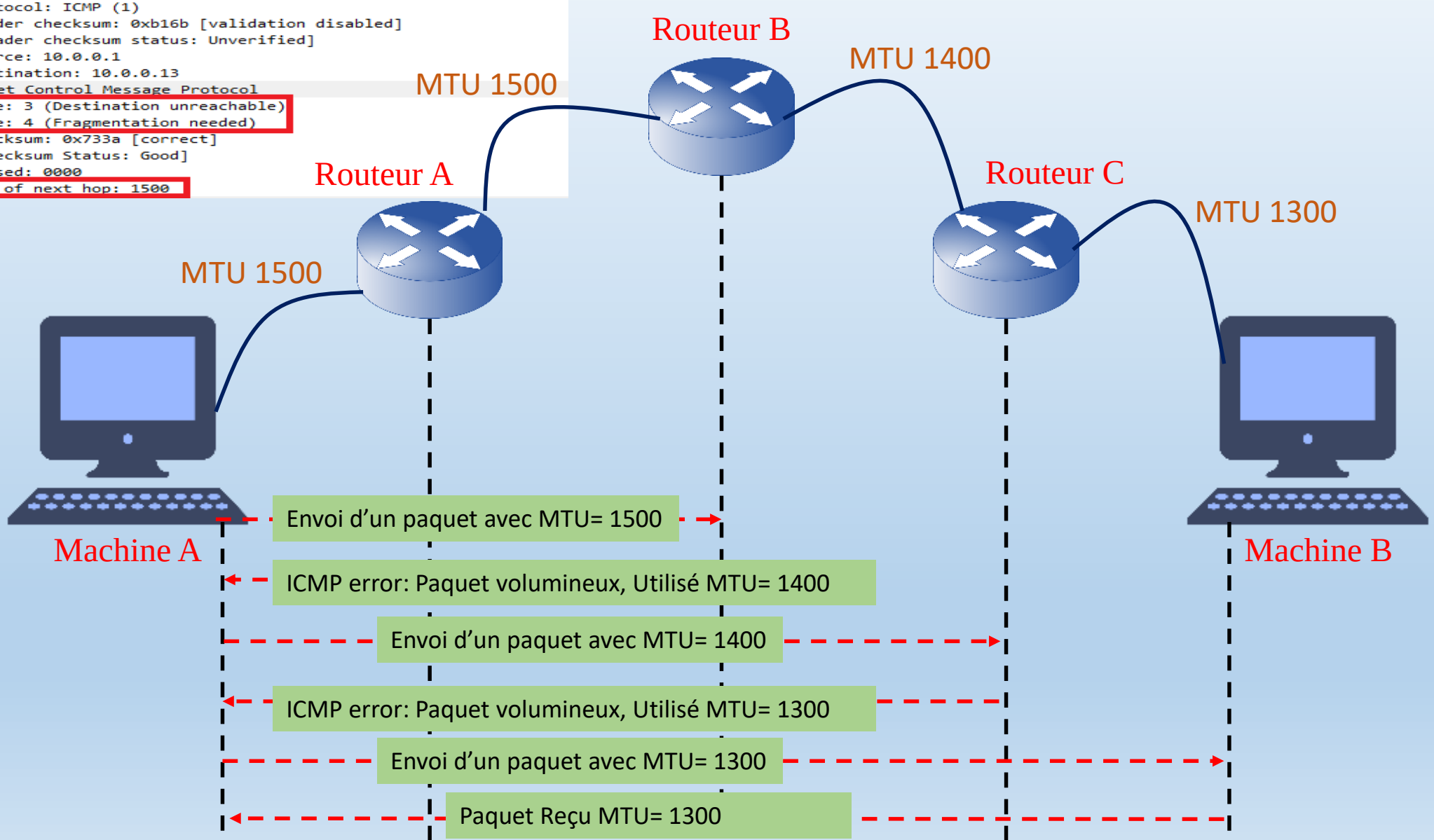
Routeur B

Machine A

1 Le Routeur A reçoit un paquet de données en provenant de la Machine A

5 La Machine A utilise le message redirection ICMP pour ajuster son cache de routage et commence à envoyer les paquets de données directement à Routeur B

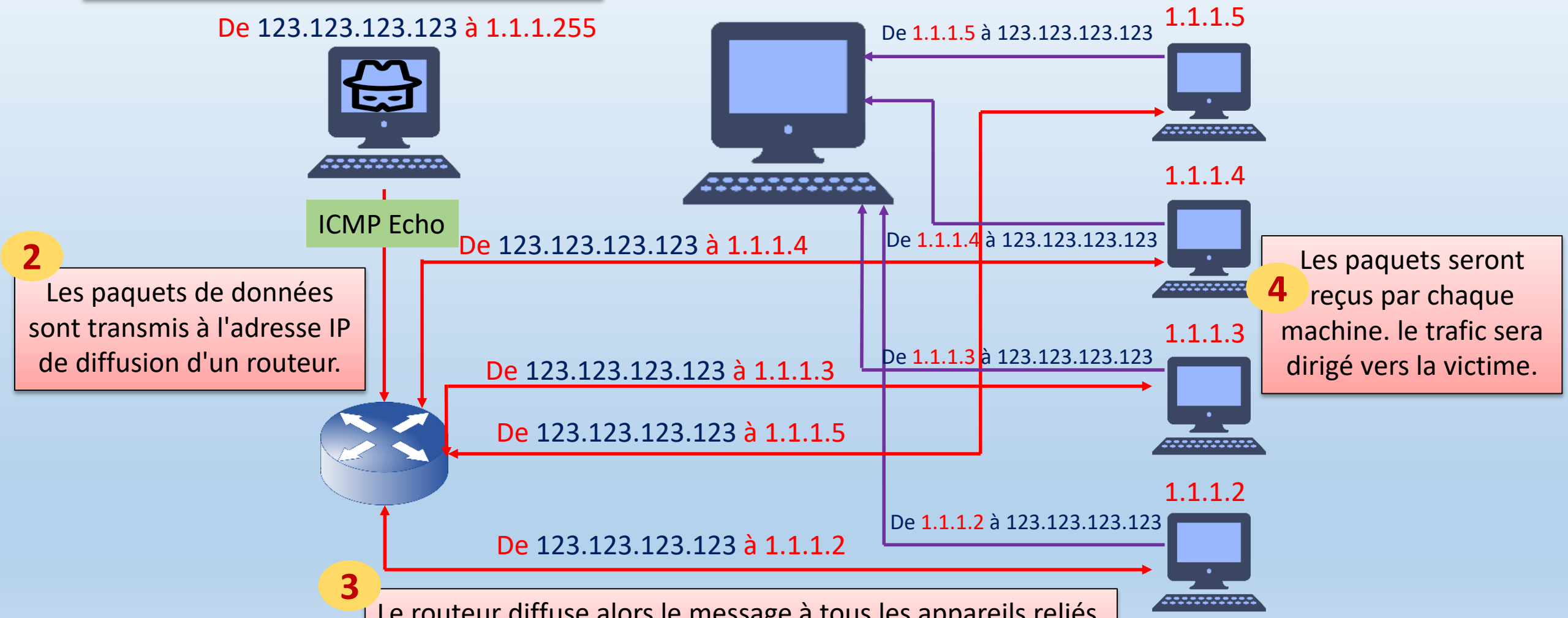
```
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xae4c (44620)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 71
    Protocol: ICMP (1)
    Header checksum: 0xb16b [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.1
    Destination: 10.0.0.13
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 4 (Fragmentation needed)
    Checksum: 0x733a [correct]
    [Checksum Status: Good]
    Unused: 0000
    MTU of next hop: 1500
```



❑ Les attaques par ICMP (Smurf ICMP)

1 Un programme malveillant usurpe IP des paquets avec l'adresse IP de la victime.

5 La cible commence à recevoir des paquets de données qu'elle n'a pas demandés. Ces paquets se succèdent et, s'ils sont trop nombreux, la cible commence à avoir du mal à les digérer.



2 Les paquets de données sont transmis à l'adresse IP de diffusion d'un routeur.

3 Le routeur diffuse alors le message à tous les appareils reliés au sein de ce réseau de diffusion, ce qui multiplie l'attaque.

4 Les paquets seront reçus par chaque machine. le trafic sera dirigé vers la victime.

❖Protocol ARP (Address Resolution Protocol)

1 La machine A désire communiqué avec la machine C (elle connait son @IP). Elle envoi un **ARP request** avec @MAC de diffusion afin de connaitre @MAC de la machine C

@IP: 192.168.1.4/24
@MAC: dd.dd.dd.dd.dd.dd
Machine D

2 Toutes les machines sur le réseau reçoivent cette requête ARP

C'est pas moi

3 Seul la machine C répondra à la requête par un **ARP reply** et envoi son @MAC

@IP: 192.168.1.1/24
@MAC: aa.aa.aa.aa.aa.aa
Machine A

@IP: 192.168.1.3/24
@MAC: cc.cc.cc.cc.cc.cc
Machine C

ARP reply

C'est moi

ARP request

Switch

C'est pas moi

Machine B
@IP: 192.168.1.2/24
@MAC: bb.bb.bb.bb.bb.bb

ARP request

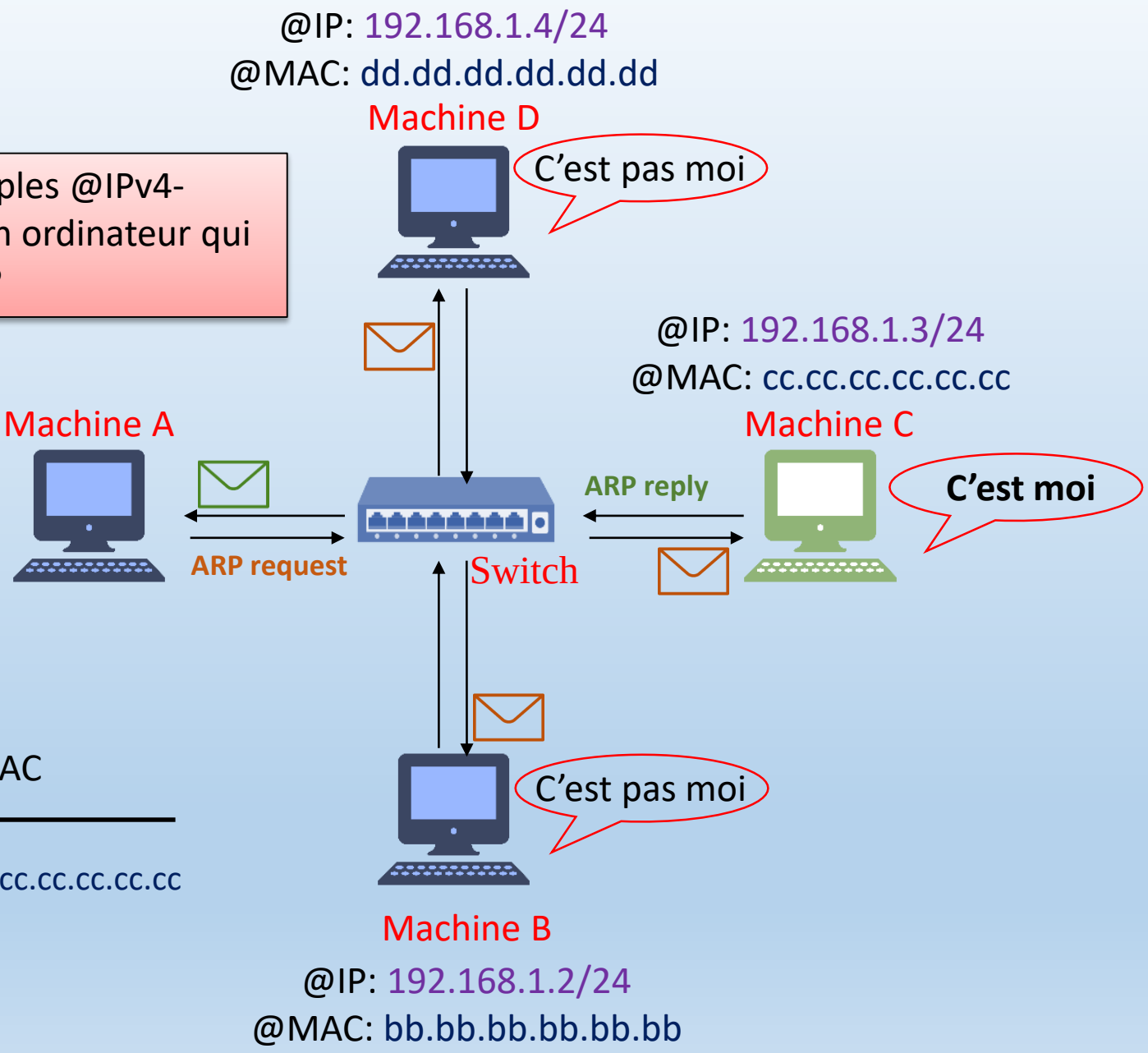
Source: Machine A	Destination: Machine C
@IP: 192.168.1.1/24 @MAC: aa.aa.aa.aa.aa.aa	@IP: 192.168.1.2/24 @MAC: FF.FF.FF.FF.FF.FF

ARP reply

Source: Machine C	Destination: Machine A
@IP: 192.168.1.3/24 @MAC: cc.cc.cc.cc.cc.cc	@IP: 192.168.1.1/24 @MAC: aa.aa.aa.aa.aa.aa

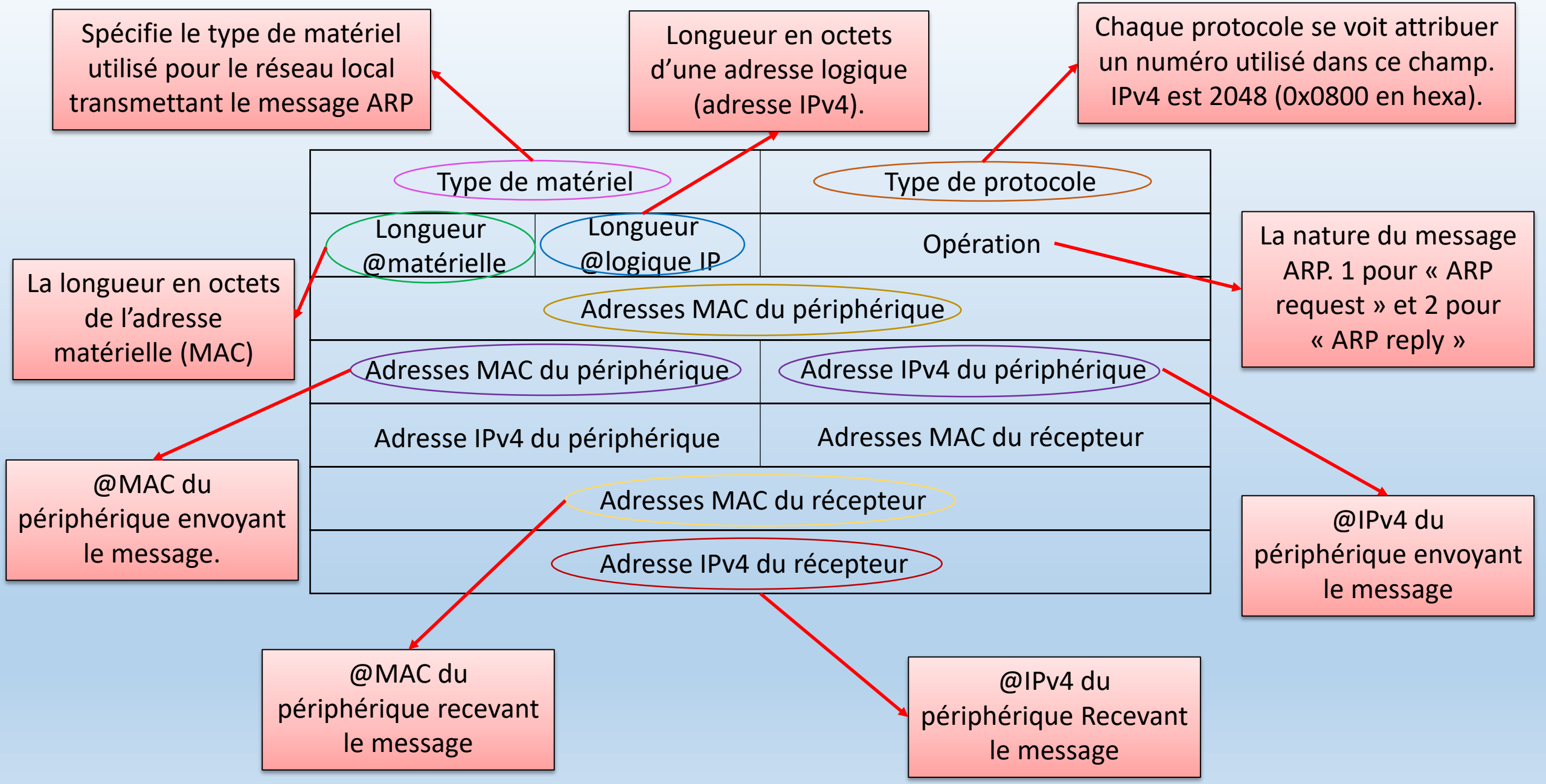
❑Cache ARP

Le cache ARP est une table de couples @IPv4-@MAC contenue dans la mémoire d'un ordinateur qui utilise le protocole ARP



ARP cache

@IP	@MAC
@IP: 192.168.1.2/24	@MAC: cc.cc.cc.cc.cc.cc


Spécifie le type de matériel utilisé pour le réseau local transmettant le message ARP
Longueur en octets d'une adresse logique (adresse IPv4).
Chaque protocole se voit attribuer un numéro utilisé dans ce champ. IPv4 est 2048 (0x0800 en hexa).
Type de matériel
Type de protocole
Longueur @matérielle
Longueur @logique IP
Opération
La longueur en octets de l'adresse matérielle (MAC)
La nature du message ARP. 1 pour « ARP request » et 2 pour « ARP reply »
Adresses MAC du périphérique
Adresses MAC du périphérique
Adresse IPv4 du périphérique
@MAC du périphérique envoyant le message.
Adresse IPv4 du périphérique
Adresses MAC du récepteur
@IPv4 du périphérique envoyant le message
Adresses MAC du récepteur
Adresse IPv4 du récepteur
@MAC du périphérique recevant le message
@IPv4 du périphérique Recevant le message

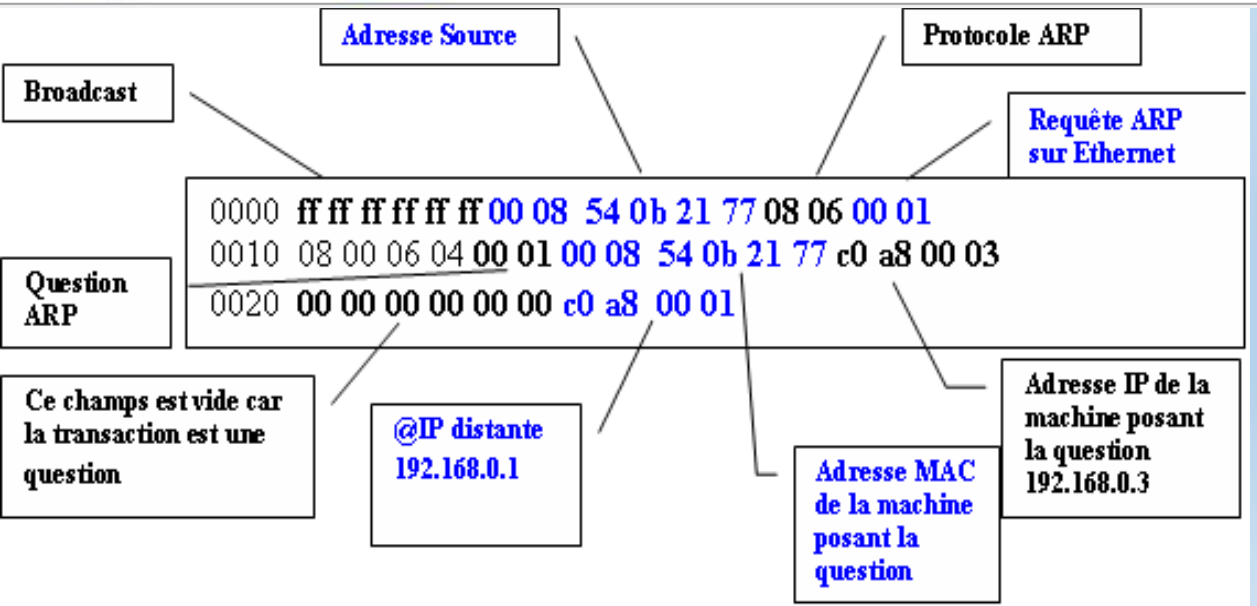
❑ Exemple de message ARP sur wireshark

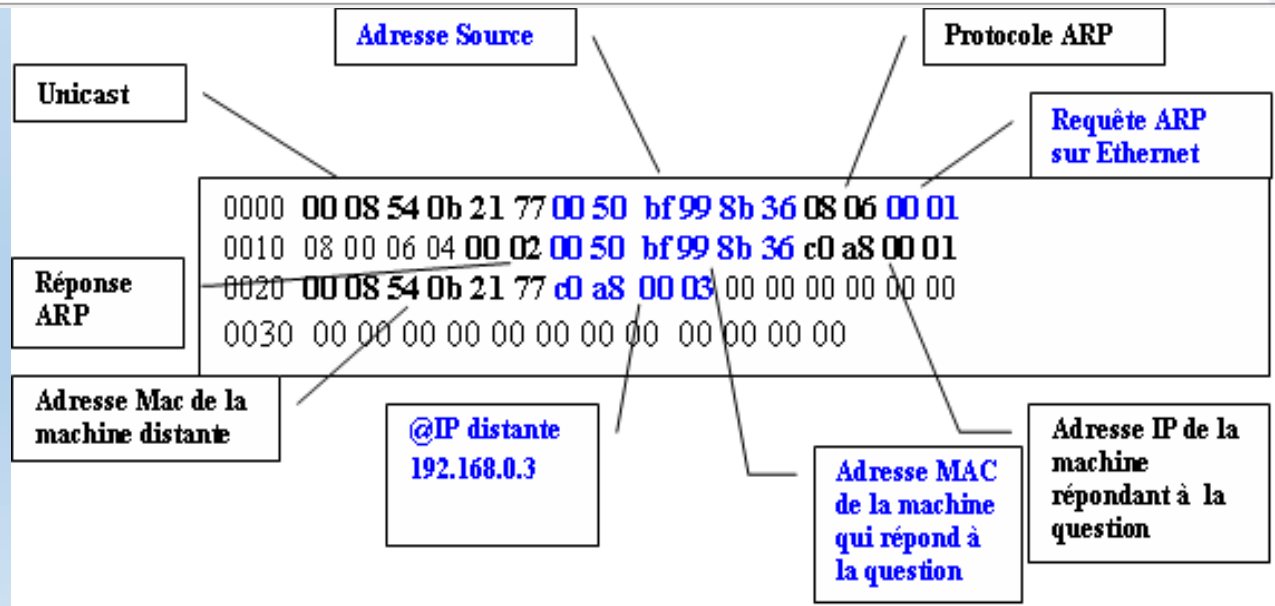
Capturing from - [PC2 Ethernet0 to Switch1 Ethernet1]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

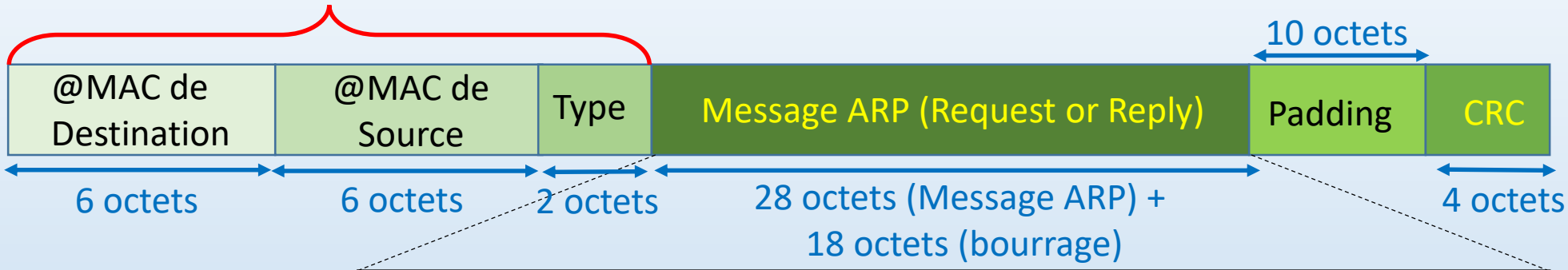
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:01	Broadcast	ARP	64	Who has 10.0.0.1? Tell 10.0.0.2
2	0.000969	Private_66:68:00	Private_66:68:01	ARP	64	10.0.0.1 is at 00:50:79:66:68:00
3	0.002961	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) request id=0xb3eb, seq=1/256, ttl=64 (reply in 4)
4	0.004024	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) reply id=0xb3eb, seq=1/256, ttl=64 (request in 3)
5	1.008272	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) request id=0xb4eb, seq=2/512, ttl=64 (reply in 6)
6	1.008272	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) reply id=0xb4eb, seq=2/512, ttl=64 (request in 5)
7	2.061677	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) request id=0xb5eb, seq=3/768, ttl=64 (reply in 8)
8	2.062452	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) reply id=0xb5eb, seq=3/768, ttl=64 (request in 7)
9	3.063776	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) request id=0xb6eb, seq=4/1024, ttl=64 (reply in 10)
10	3.064772	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) reply id=0xb6eb, seq=4/1024, ttl=64 (request in 9)
11	4.066126	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) request id=0xb7eb, seq=5/1280, ttl=64 (reply in 12)
12	4.067091	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) reply id=0xb7eb, seq=5/1280, ttl=64 (request in 11)

```
    Padding: 00000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
    Sender IP address: 10.0.0.2
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 10.0.0.1
```





Message ARP encapsulé dans une Trame Ethernet



Type de matériel	Type de protocole
Longueur @matérielle / Longueur @logique IP	Opération
Adresses MAC du périphérique	
Adresses MAC du périphérique	Adresse IPv4 du périphérique
Adresse IPv4 du périphérique	Adresses MAC du récepteur
Adresses MAC du récepteur	
Adresse IPv4 du récepteur	

Université Sorbonne Paris Nord: IUT Villetaneuse

Dr. Mohamed Amine Ouamri

Matière :M51 Réseaux

Chapitre 3: Virtuel Local Area Network