

CH5 Transmettre des informations - Les réseaux

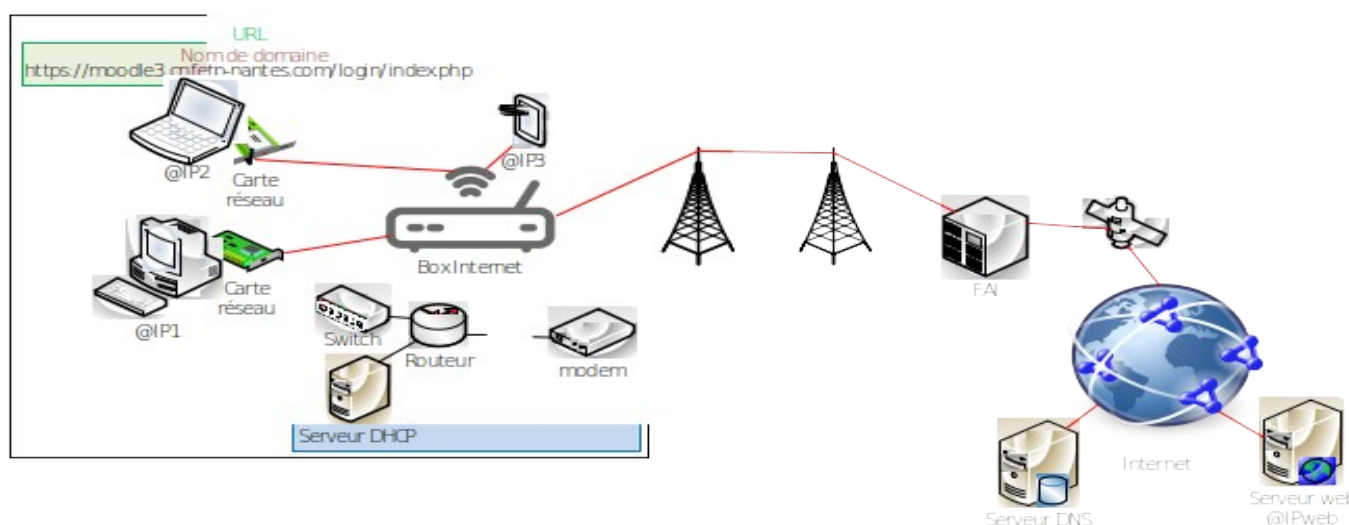
ACT 1 Un réseau débranché

A voir : https://youtu.be/_0thnFumSdA

1. Un réseau usuel : internet

a. Internet

Internet est un ensemble de réseaux reliés par des câbles et des routeurs.



infrastructure réseau domestique permettant de se connecter au réseau Internet

Les constituants du réseau internet sont :

Switch	Interconnexion des équipements Ethernet (RJ45/Wifi) du réseau local (LAN)
Modem	Conversion du signal Ethernet en signal ADSL / fibre optique...
Firewall	Filtrage des ports TCP et/ou des applications
Routeur	Permet le passage du réseau local vers d'autres réseaux
FAI	« Fournisseur d'Accès Internet » : fourni une @IP publique et fait l'interface entre mon LAN et Internet
Serveur DHCP	« Dynamic Host Configuration Protocol » : attribution automatique de la configuration réseau aux stations du LAN (@IP, masque, passerelle, DNS...)
Serveur DNS	« Domain Name Server » : table de correspondance entre les noms de domaine et les @IP des serveurs

Description (simplifiée) de la communication permettant d'accéder à un site web :

1	à partir de l'URL, le PC client interroge son serveur DNS pour connaître l'@IP du serveur correspondant.	2	l'@IP du serveur web ne faisant pas partie du LAN, la station envoie la requête au routeur (passerelle).
3	le firewall vérifie que la requête ne fait pas l'objet d'une règle de filtrage.	4	le modem assure la translation NAT : c'est-à-dire qu'il remplace l'@IP privée de la station par l'@IP publique fournie par le FAI.
5	routage de la requête à travers les différents routeurs sur Internet	6	le serveur web renvoie la réponse à la station.

La **fonction d'un réseau** est de transmettre des informations (voix, données et images ou partager des ressources (logiciels et de fichiers...) sécurisés ou non entre un émetteur et un récepteur.

Les réseaux se répartissent en 2 grandes familles :

Type de réseau	Étendue du réseau	Exemple
LAN Local Area Network	Réseau local : confiné à un lieu particulier.	Réseau interne du lycée
WAN Wide Area Network	Réseau étendu : limité à un pays, un continent, voire la planète...	Internet

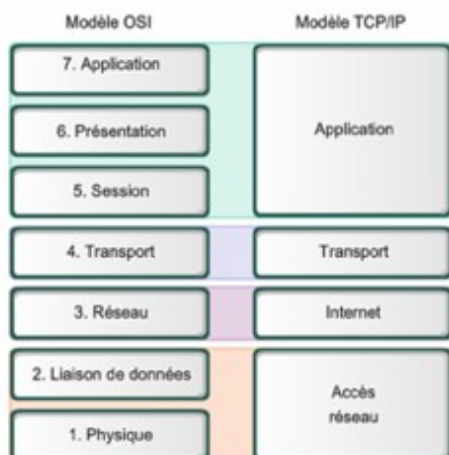
On pourra approfondir ces notions sur : <https://www.commentcamarche.net/contents/512-topologie-des-reseaux>

b. Modèle de fonctionnement

Les réseaux fonctionnent selon un modèle théorique, développé lors de la conception du premier réseau [Arpanet](#), ancêtre du réseau Internet : le **modèle OSI** (*Open Systems Interconnection*).

Ce modèle consiste en la circulation de l'information à travers différentes *couches*, chacune ayant un rôle particulier.

La version modernisée et simplifiée est le **modèle TCP/IP** utilisé actuellement. Il est constitué de 4 couches : **Application, Transport, Internet** et **Accès réseau**.



Couche Transport :

Officiellement, cette couche n'a que deux implémentations : le **protocole TCP** (Transmission Control Protocol) et le **protocole UDP** (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

Couche Internet :

Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants **sans connexion (en tout cas pour le protocole IP)**. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination.

Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le **contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures (TCP)**. Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le **routage**.

Voir cette animation pour visualiser le processus : <https://www.geogebra.org/m/vdyjcyzd>

2. Se repérer sur le réseau

ACT2 Simulation Filius

a. Adresse physique (couche *Accès Réseau*)

Chaque élément du réseau est identifié « physiquement » sur le réseau par son **adresse MAC** (*Media Access Control*). Elle est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret.

Par exemple, `5E : FF : 56 : A2 : AF : 15`

Les 3 premiers octets correspondent au code du fabricant de la carte réseau et les 3 derniers octets correspondent au numéro (identifiant) de la carte réseau.



carte ethernet



carte wifi

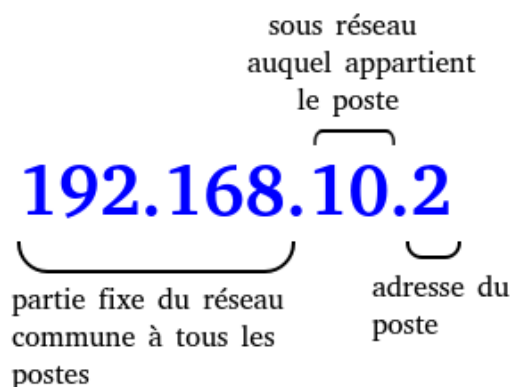
Remarques :

- L'adresse MAC est plus précisément l'adresse de la carte réseau : l'interface physique entre l'ordinateur et le câble du réseau. Cette carte a pour fonction de préparer, d'envoyer et de contrôler le flux de données sur le réseau.
- L'adresse MAC est unique ; elle est inscrite par le fabricant sur la puce de la carte.

b. Adresse IP (couche *Internet*)

A un autre niveau, les éléments du réseaux sont repérés par leur **adresse IP**, constitué de 4 blocs de 8 bits chacun, soit 32 bits (4 octets).

Dans un réseau on peut trouver l'adresse IPv4 ci-contre :



Pour s'adapter aux différentes tailles et structures de réseaux qui pourraient être créés et à une éventuelle évolution future, les adresses IP sont divisées en deux parties :

- l'adresse du réseau (*NetID*)
- l'adresse de diffusion (*HostID*), appelée *broadcast*

Le nombre d'adresses possibles réseaux est donc défini par la première partie *NetID* ; on parle de **classe de réseau**. 5 classes désignées par les lettres A, B, C, D et E ont été créées. Les deux dernières très spécifiques ne seront pas développées ici.

Classe	1 octet	1 octet	1 octet	1 octet
A	0xxx xxxx NetID (2 ⁷ réseaux)	HostID (2 ²⁴ - 2 périphériques)		
B	10xxxxxx NetID (2 ¹⁴ réseaux)	HostID (2 ¹⁶ -2 périphériques)		
C	110xxxxx NetID (2 ²¹ réseaux)	HostID (2 ⁸ -2 périphériques)		

Les premiers bits (en rouge) du NetID permettent de définir la classe du réseau.

Le tableau précédent conduit à l'attribution d'adresses :

- **Classe A** : de 0.0.0.1 à 127.255.255.254
- **Classe B** : de 128.0.0.0 à 191.255.255.254
- **Classe C** : de 192.0.0.0 à 223.255.255.254

Remarques : Adresses spécifiques

- **Adresse réseau** : adresse IP pour laquelle les bits de la partie hôte sont à 0.

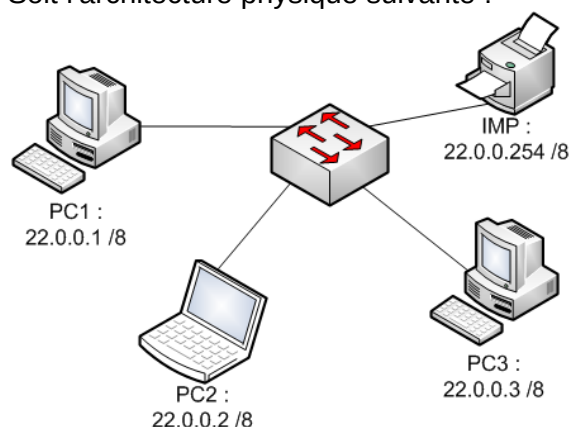
Réseau	Hôte		
22	0	0	0

- **Adresse de diffusion** : adresse IP pour laquelle les bits de la partie hôte sont à 1.

Réseau	Hôte		
22	255	255	255

- **Adresse de « loop-back »** : le bloc 127 est réservé et ne peut être utilisé, ainsi l'adresse 127.0.0.1 identifie la machine elle-même (*localhost*).

Soit l'architecture physique suivante :



(Note : « /8 » donne le nombre de bits sur lesquels est codé le HostID)

c. Masque de sous-réseau (couche Internet)

Pour identifier un sous-réseau, on utilise donc la partie *NetID* de l'adresse IP. L'objectif est de pouvoir différencier une adresse IP contenant un sous-réseau de celle n'en contenant pas. Pour cela, une information supplémentaire sera nécessaire aux matériels comme les routeurs, il s'agit du **masque de sous-réseau**.

Le masque de sous-réseau possède une adresse IP sur 4 octets soit 32 bits. Chacun de ces bits peut prendre la valeur 1 ou 0. Afin de différencier l'adresse machine de l'adresse réseau on appliquera comme masque l'adresse IP : 255.255.255.0. Le codage binaire de cette adresse conduira à avoir des 1 pour la partie réseau/sous-réseau et des 0 pour la partie machine.

Au final, en appliquant un **ET** logique, on masquera les bits servant d'identification des périphériques et on laissera visible l'adresse IP réseau/sous-réseau

Exemple :

Le périphérique a pour adresse IP 152.110.225.10 et le masque de sous-réseau 255.255.255.0

Adresse IP	Conversion binaire
152.110.225.10	10010111.01100110.11100001.00001010
255.255.255.0	11111111.11111111.11111111.00000000
<i>Résultat de l'opérateur logique ET</i>	10010111.01100110.11100001.00000000

On obtient ainsi le réseau et le sous-réseau car l'adresse initiale est une adresse IP de classe B.

Remarque :

L'utilisation est limitée aux classes A et B car il n'y a pas de possibilité de le faire sur la classe C. Le masque par défaut pour la classe A est 255.0.0.0 et pour la classe B 255.255.0.0.

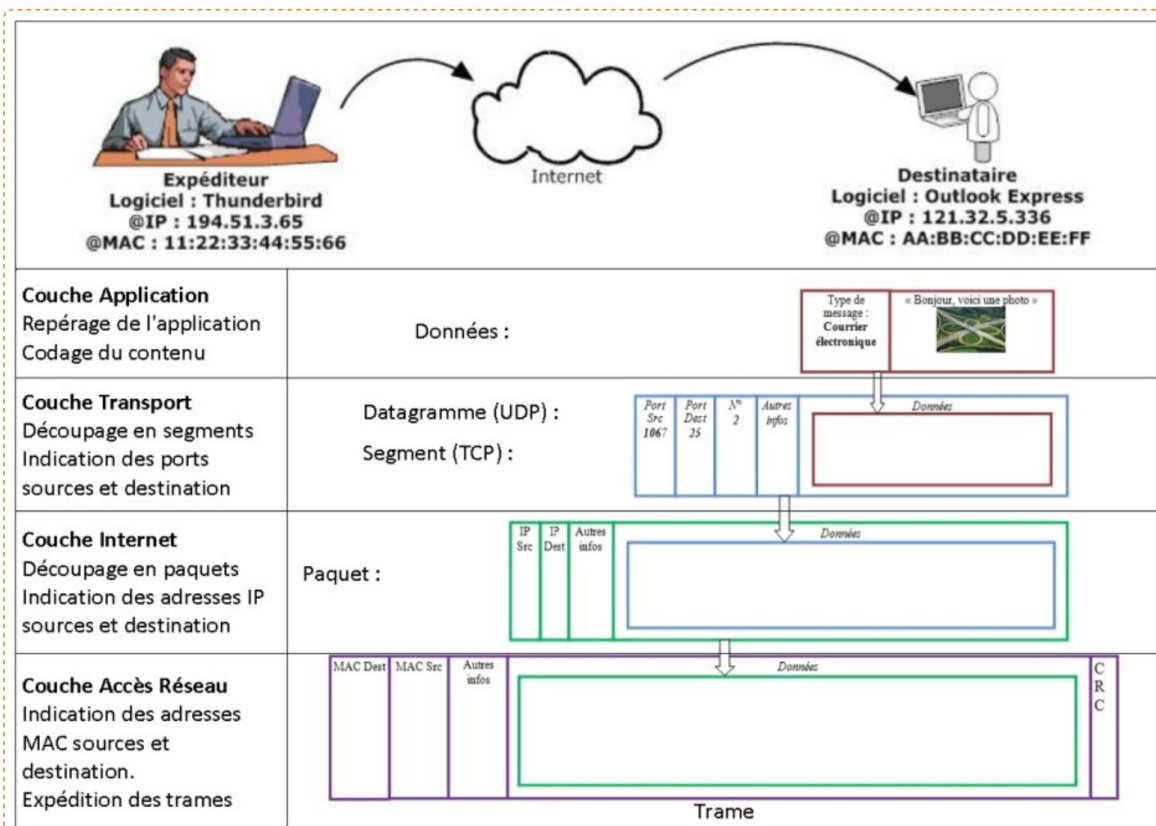
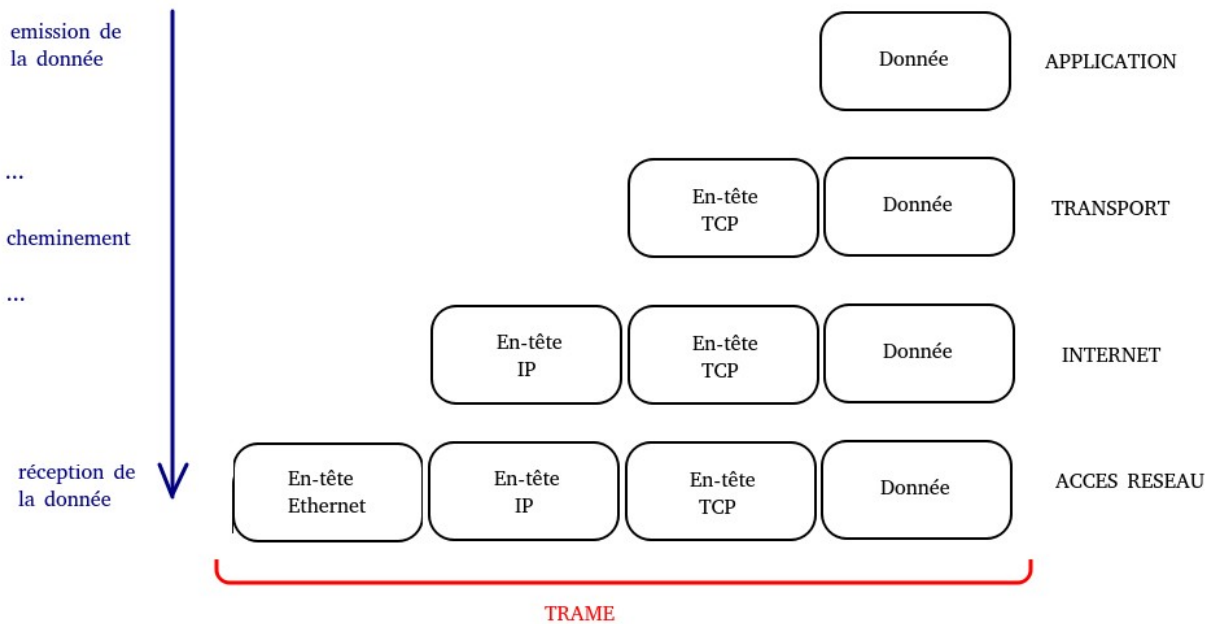
3. Transmettre des informations

Pour échanger des informations, on utilise un réseau de communication sur lequel un mode de communication commun est défini et utilisé : pour l'ensemble des règles concernant un mode de communication, on parle de **protocole**.

Couche modèle TCP/IP	Protocoles Usuels		Utilisation
Application	HTTP	<i>HyperText Transfer Protocol</i>	Accéder aux pages web
	SMTP	<i>Simple Mail Transfer Protocol</i>	Courrier électronique
	FTP	<i>File Transfer Protocol</i>	Echange de fichiers

Transport	TCP	<i>Transfert Control Protocol</i>	Source / Destinataire : Transport des données avec vérification de la réception
	UDP	<i>User datagram Protocol</i>	Source / Destinataire : Transport des données sans vérification de la réception
Internet	IP	<i>Internet Protocol</i>	Routage sur le réseau
Accès Réseau	ARP	<i>Address Resolution Protocol</i>	Associe adresse MAC à adresse IP

Chaque protocole est donc associé à une couche, et il rajoute à chaque étape de la transmission de la donnée des informations. On parle de **paquet**, car la donnée n'est pas brute mais **encapsulée** dans une **trame**.

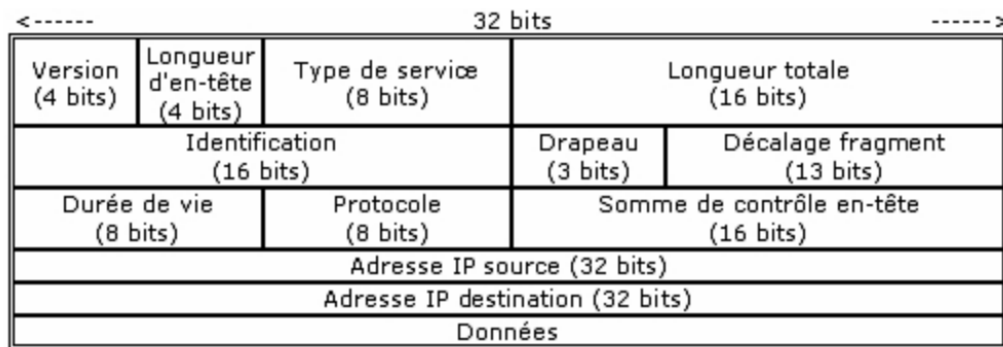


Exemples :

- Trame complète d'un paquet transmis via le modèle TCP/IP

<https://view.genial.ly/5f674e7451337070914e437a/interactive-image-datagramme-ip>

- Détail de la trame liée au protocole IP de la couche Internet



Remarque :

Une animation pour expliquer la gestion du bit alterné qui vérifie la bonne réception des paquets (*acquittement* ou *acknowledgement*) dans le protocole TCP

<https://www.geogebra.org/m/kcmqxrjc>

d. Différencier deux adressages

Le protocole TCP permet de le transfert des de s'assurer du transfert correct des données entre deux machines. Mais comment faire pour transférer 2 données à partir d'une même machine ?

Pour cela, à chaque donnée issue d'une application exécutée par la machine est affecté un numéro unique appelé **port**, codé sur 16 bits. Le numéro de port permet alors de diriger les données reçues, via la carte réseau, vers la bonne application.

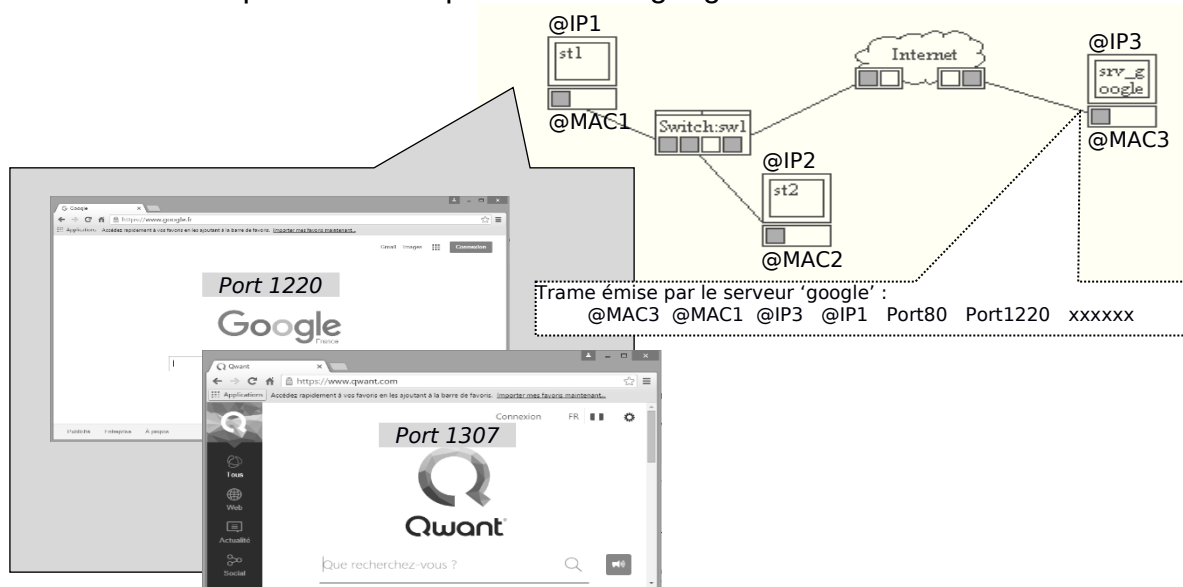
On trouve les ports usuels suivants :

- port 80 : protocole HTTP
- port 25 : protocole SMTP
- port 20 ou 21 : protocole FTP

Exemple :

Supposons qu'on ouvre 2 onglets sur le navigateur web de la machine **st1** . Chacun des 2 onglets se voit attribuer un numéro de port (par exemple 1220 et 1307).

À partir de l'onglet de port 1220, on saisit l'url « <https://www.google.fr> » ; ci-dessous, on schématise la réponse fournie par le serveur google :



Lorsque le machine **st1** reçoit la trame ci-dessus, elle vérifie que les adresses **MAC** et **IP** correspondent bien à sa configuration, puis dirige les données « xxxxxx » vers l'application possédant le port 1020. Ainsi la page d'accueil de 'google' apparaît dans le bon onglet.