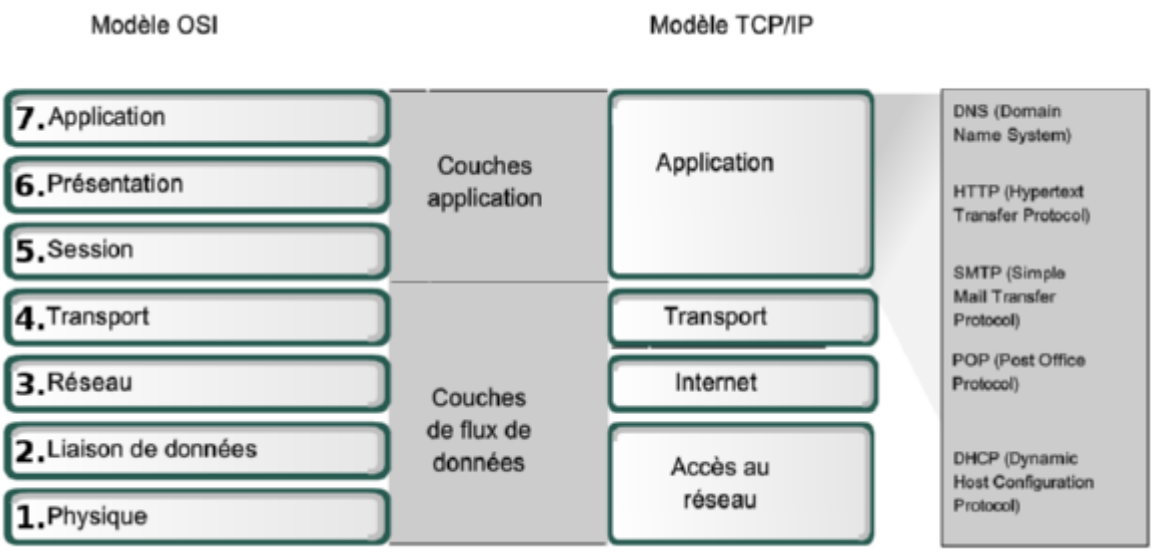
RAPPEL SUR LES MODELES OSI ET TCP/IP

LES 2 MODELES COMPARES



2 modèles :

- le modèle OSI (Open Systems Interconnection) normalisé par l'ISO (européen)
- le modèle TCP/IP ou modèle DoD (américain).

Ces 2 modèles sont très proches et ne sont pas à opposer… Ils décrivent la même réalité et fonctionnent de la même façon (modèles en couches).

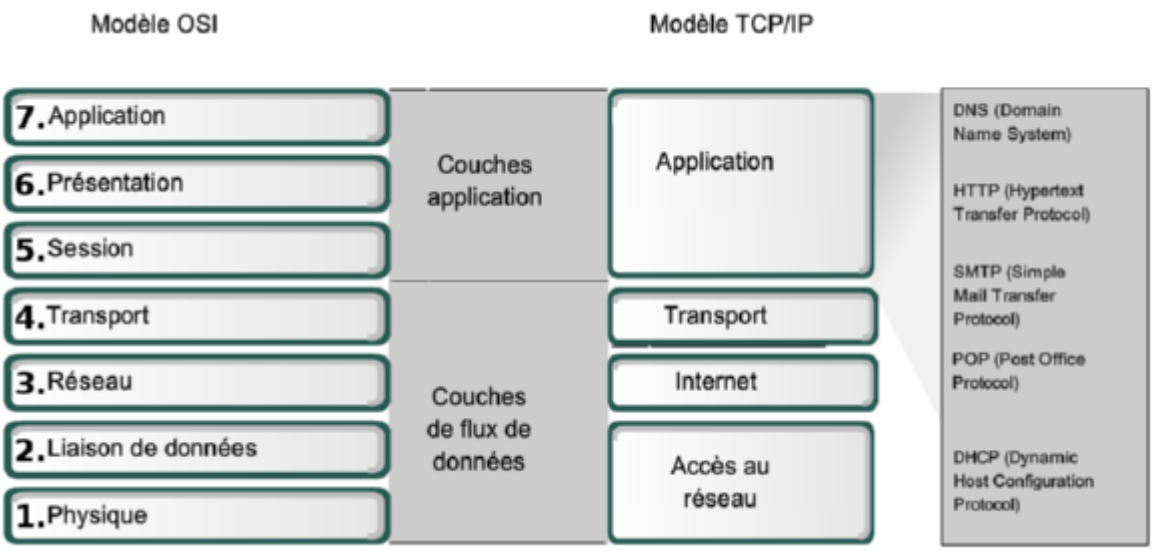
Ces 2 modèles sont ouverts et ne sont liés à aucun constructeur.

Les idées directrices ayant conduit à l'élaboration du modèle OSI sont les suivantes :

- ne pas créer un nombre de couches tel que la description des fonctionnalités et l'intégration de celles-ci au moment du développement d'un projet deviendraient difficiles.
- Créer des couches distinctes pour traiter les fonctions qui sont manifestement différentes sur le plan du traitement exécuté et de la technologie mise en oeuvre.
- Rassembler les fonctions similaires dans une même couche, placer des frontières en des points particuliers (les Sap : Services Acces Points).
- Permettre des changements de fonctions ou de protocoles dans une couche sans en affecter les autres.
- Créer, pour chaque couche, des interfaces avec la couche immédiatement supérieure et la couche immédiatement inférieure et seulement avec celle-là.

L'ENCAPSULATION

Ce mécanisme est essentiel. Il vous aidera à mieux comprendre comment fonctionne un réseau informatique et vous permettra d'analyser les trames capturées par des logiciels d'analyse type Wireshark.



Cisco définit le terme de **PDU** (**P**acket **D**ata **U**nit) pour désigner segment, paquet ou trame en fonction de la couche étudiée.

ANIMATION POUR FAIRE COMPRENDRE

Source : Université Montpellier.

Animation modèle OSI

MISE EN EVIDENCE DES COUCHES AVEC L'ANALYSEUR DE TRAMES WIRESHARK

Le produit open source multi-plateformes WIRESHARK

Wireshark est un analyseur de protocoles (analyseur de trames) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. Avant juin 2006, Wireshark répondait au nom d'Ethereal.

Un analyseur de paquets (ou analyseur de réseaux ou de protocoles) est un logiciel permettant d'intercepter et de consigner le trafic des données transférées sur un réseau de données. L'analyseur « capture » chaque PDU des flux de données circulant sur le réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications RFC ou autres appropriées.

Wireshark est programmé pour reconnaître la structure de différents protocoles réseau. Vous pouvez l'utiliser pour afficher l'encapsulation et les champs spécifiques aux PDU, puis interpréter leur signification.

Cet outil est utile pour toutes les personnes intervenant au niveau des réseaux. Vous pouvez vous en servir dans le cadre de la plupart des travaux pratiques des cours SIO, à des fins d'analyse de données et de dépannage, voire de hacking (sur votre propre réseau bien sûr!!).

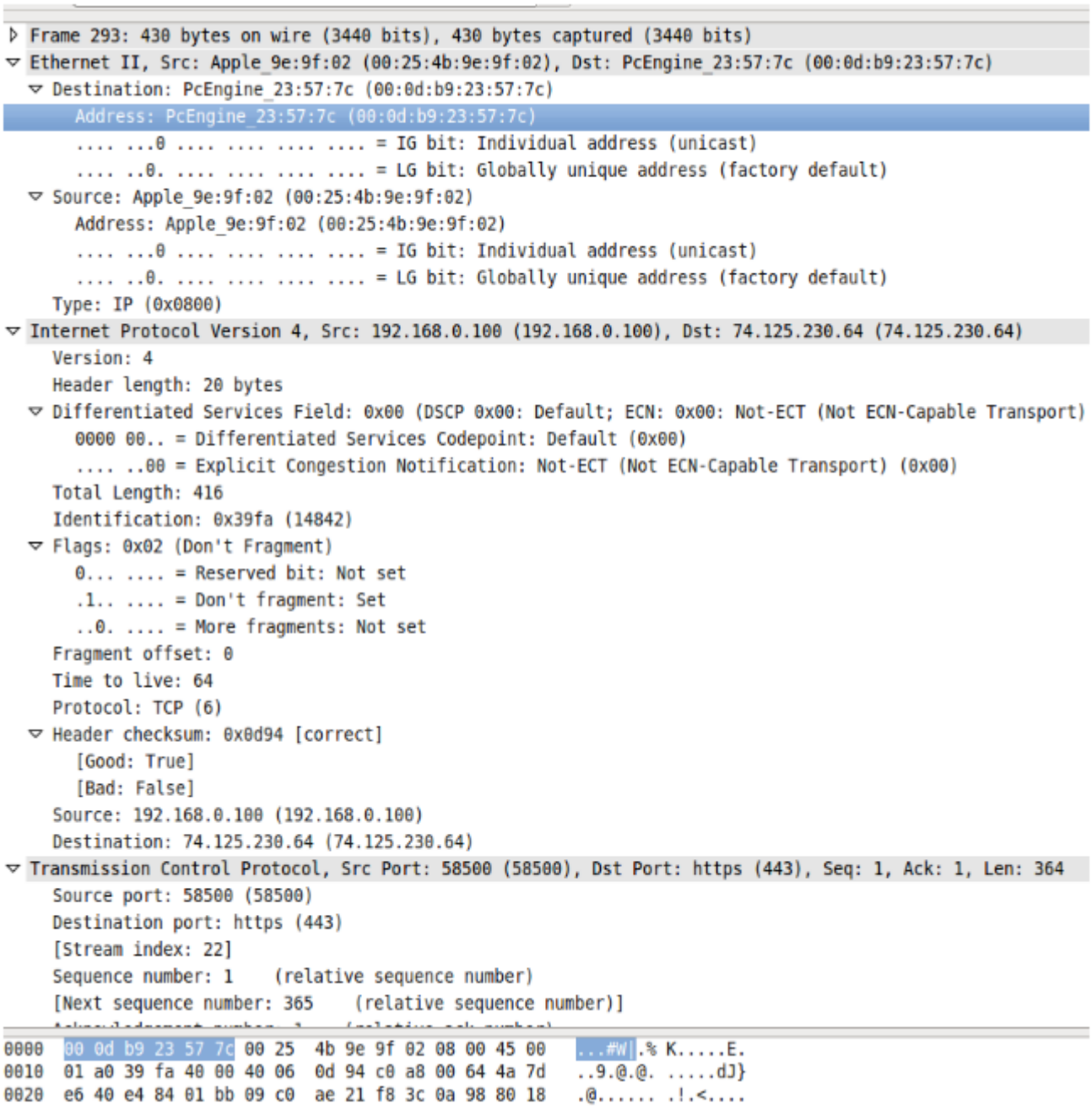
Tous les logiciels de ce type comportent 2 modules :

- module de capture
- module d'analyse

En règle générale, on va donc dans un premier temps capturer (une ou plusieurs trames) pour ensuite, dans un deuxième temps, analyser.

Pour en savoir plus sur cet analyseur et télécharger le programme correspondant, accédez au site https://www.wireshark.org/

Analyse de la trame capturée et repérage des couches du modèle OSI



PETIT EXERCICE POUR FAIRE COMPRENDRE !

En France, la **DGSE** (**D**irection **G**énérale de la **S**écurité **E**xtérieure) se compose de 2 « Directions » (Direction Stratégique et Direction du Renseignement) et de 2 « Divisions » (Division Technologique et Division des Opérations).

Les 2 Divisions sont découpées chacune en trois niveaux hierarchiques : Renseignement, Cryptage et Transmission.

Entre les 2 Divisions, des échanges d'informations s 'effectuent, toujours de manière cryptée, entre les niveaux « Renseignement » de l'une et le niveau « Renseignement » de l'autre. Seuls les niveaux « Transmission » peuvent utiliser les canaux de communications (filaire, hertzien ou autres).

Le tableau infra permet de reconstituer l'organigramme simplifié de ces 2 Divisions :

	RESPONSABLES DIVISION DES OPERATIONS	**RESPONSABLES DIVISION TECHNOLOGIQUE**
RENSEIGNEMENT	Colonel TERRIERE	Lieutenant-Colonel SANTAMPONNE
CRYPTAGE	Lieutenant-Colonel Nathalie VESOUL	Lieutenant-Colonel RAMPOUX
TRANSMISSION	CAPITAINE Mélanie ZERROUR	COMMANDANT CAPSUD

QUESTION 1 :

- Rappelez de manière concise le principe du modèle OSI.

- Les échanges entre les 2 Divisions respectent-ils le modèle OSI ? Pourquoi ?

Une note de service confidentielle émanant du service de sécurité interne laisse supposer que des relations euh... disons... intimes semblent exister entre, d'une part, les responsables des services « Transmission » et, d'autre part entre le Lieutenant-Colonel Nathalie VESOUL et son homologue RAMPOUX.

QUESTION 2 :

Les informations contenues dans cette note de service, si elles s'avèrent exactes, remettent-elles en cause les principes du modèle OSI? Dites très précisément pourquoi.

TP ASSOCIE

UTILISATION DE WIRESHARK POUR AFFICHER DES UNITÉS DE DONNÉES DE PROTOCOLE ET METTRE EN EVIDENCE LES COUCHES DU MODELE OSI