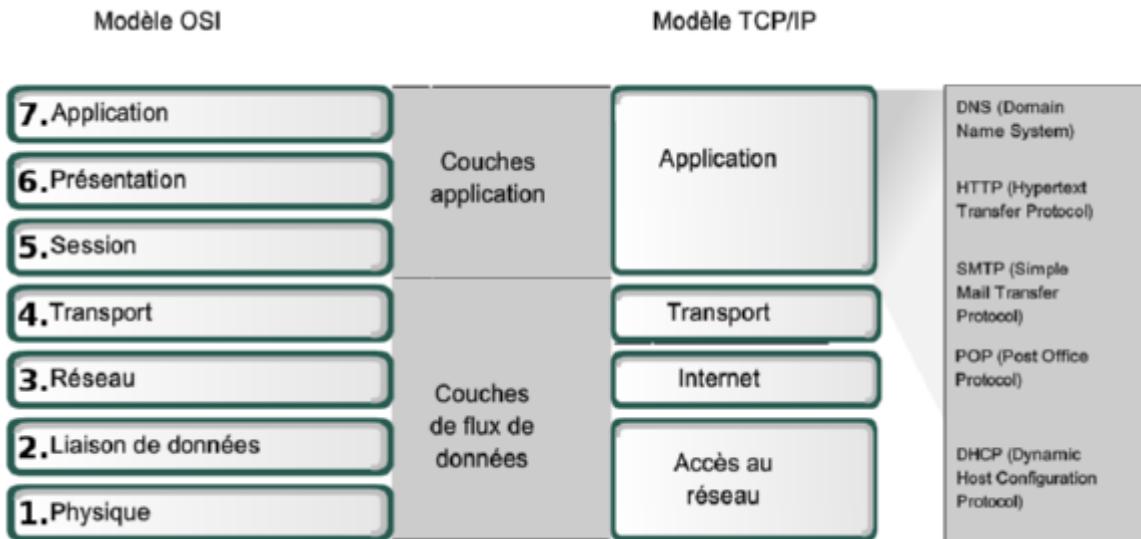


## RAPPEL SUR LES MODELES OSI ET TCP/IP

### 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).

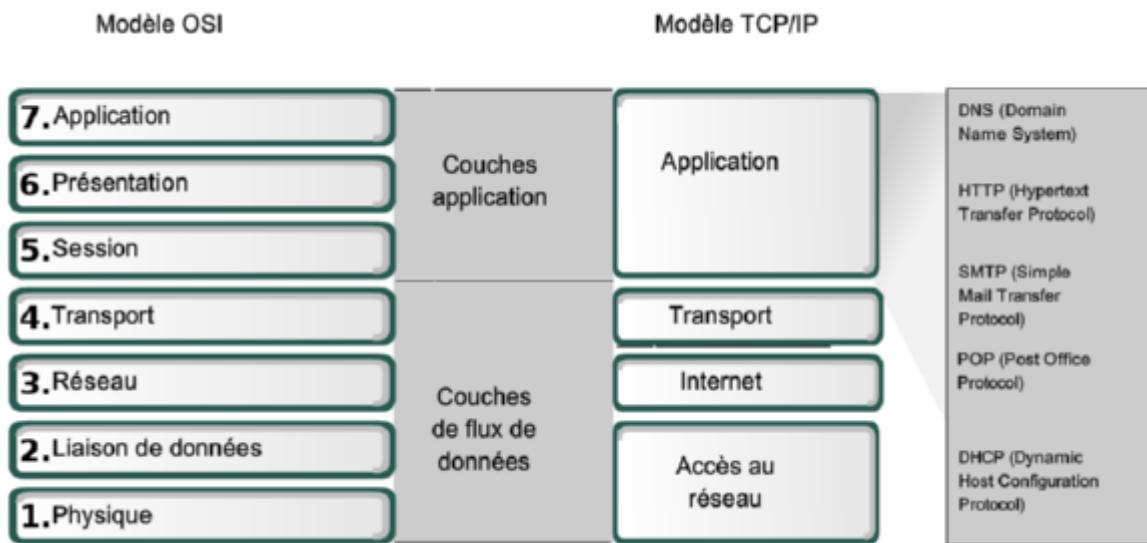
Ces 2 modèles sont ouverts et ne sont liés à aucun constructeur.

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 Accès 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** (Packet Data Unit) pour désigner segment, paquet ou trame en fonction de la couche étudiée.

## ANIMATION POUR FAIRE COMPRENDRE

Source : Université Montpellier.

[Animation modèle OSI](#)

## MISE EN ÉVIDENCE 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

```

❯ Frame 293: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits)
❯ Ethernet II, Src: Apple_9e:9f:02 (00:25:4b:9e:9f:02), Dst: PcEngine_23:57:7c (00:0d:b9:23:57:7c)
  Destination: PcEngine_23:57:7c (00:0d:b9:23:57:7c)
    Address: PcEngine_23:57:7c (00:0d:b9:23:57:7c)
      .... .0 ..... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
  Source: Apple_9e:9f:02 (00:25:4b:9e:9f:02)
    Address: Apple_9e:9f:02 (00:25:4b:9e:9f:02)
      .... .0 ..... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
❯ Internet Protocol Version 4, Src: 192.168.0.100 (192.168.0.100), Dst: 74.125.230.64 (74.125.230.64)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 416
  Identification: 0x39fa (14842)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x0d94 [correct]
    [Good: True]
    [Bad: False]
  Source: 192.168.0.100 (192.168.0.100)
  Destination: 74.125.230.64 (74.125.230.64)
❯ Transmission Control Protocol, Src Port: 58500 (58500), Dst Port: https (443), Seq: 1, Ack: 1, Len: 364
  Source port: 58500 (58500)
  Destination port: https (443)
  [Stream index: 22]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 365 (relative sequence number)]
  ...
  0000  00 0d b9 23 57 7c 00 25 4b 9e 9f 02 08 00 45 00  ...#W%.K....E.
  0010  01 a0 39 fa 40 00 40 06 0d 94 c0 a8 00 64 4a 7d  ..9.@@. ....dJ}
  0020  e6 40 e4 84 01 bb 09 c0  ae 21 f8 3c 0a 98 80 18  .@..... .!.<....
```

## PETIT EXERCICE POUR FAIRE COMPRENDRE !

En France, la **DGSE** (Direction Générale de la Sécurité Extérieure) 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 hiérarchiques : 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 :

	<b>RESPONSABLES DIVISION DES OPERATIONS</b>	<b>RESPONSABLES DIVISION TECHNOLOGIQUE</b>
<b>RENSEIGNEMENT</b>	Colonel TERRIERE	Lieutenant-Colonel SANTAMONNE
<b>CRIPTAGE</b>	Lieutenant-Colonel Nathalie VESOUL	Lieutenant-Colonel RAMPOUX
<b>TRANSMISSION</b>	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 ÉVIDENCE LES COUCHES DU MODÈLE OSI**

From:

[/ - Les cours du BTS SIO](#)

Permanent link:

[/doku.php/sisr2/osi](#)

Last update: **2013/11/27 21:39**

