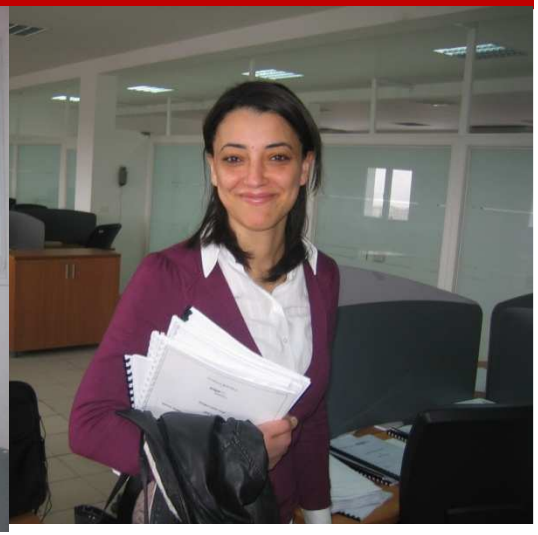
Ecole Supérieure Privée
d'Ingénierie et de Technologies

www.esprit.ens.tn

Sécurité des réseaux informatiques

Ramzi Ouafi
Assistant Technologue – Esprit
e-mail : Ramzi.ELOUAFI@esprit.ens.tn



Plan

- Objectifs du cours
- Rappel sur la pile protocolaire TCP/IP
- La sécurité des réseaux
- Filtrage, NAT, Firewall
- Les moyens cryptographiques.
- Les protocoles de sécurité.
- Les réseaux VPN.
- Les serveurs d’authentification.
- La sécurité des réseaux wi-fi.
- Les systèmes IDS.
- Les normes d’audit de sécurité.

Introduction

- Problématique
- Le modèle OSI
- Le modèle TCP/IP

Problématique de conception & d'interopérabilité

Problème

Comment réduire la **complexité de conception** *d'un système de communications ?*

Solution

Utilisation d'une **architecture en couches** *très structurée pour séparer les sous-problèmes (diviser pour mieux régner)*

Problème

Comment assurer la **compatibilité** *des équipements, leur* **durée de vie**, *et permettre l'***interconnexion** *des réseaux ?*

Solution

Besoin de **normalisations** *dans les réseaux*

Définition

Une **couche** est un ensemble homogène destiné à accomplir une tâche ou un service

Normalisation

- Un organisme international:
  - l'ISO (International Standardization Organization)
    - Dépend de ONU, regroupe organismes nationaux, utilisateurs, industriels
    - Ex :ANSI – American National Standards Institute
    - Modèle de référence appelé aussi modèle OSI (Open System Interconnexion)
- Un institut :
  - L'IEEE (**Institute of Electronic and Electricity Engineers**)
    - Réseaux locaux : notamment norme 802.3 (Ethernet), 802.5 Token Ring Rédigées à l'initiative d'experts techniques, puis revues par la communauté Internet dans son ensemble
  - RFC (**Request For comments**), site officiel www.rfc-editor.org
  - Ex : IP (RFC 791), DNS (RFC 1034), HTTP (RFC 1945),…

Le modèle de référence

Définition

Appelé **modèle de référence** ou **modèle OSI (Open System Interconnexion)**, ce modèle a été proposé par l'ISO (International Standardization Organization) pour décrire une architecture des réseaux, permettant l'interconnexion de systèmes ouverts à la communication avec d'autres systèmes

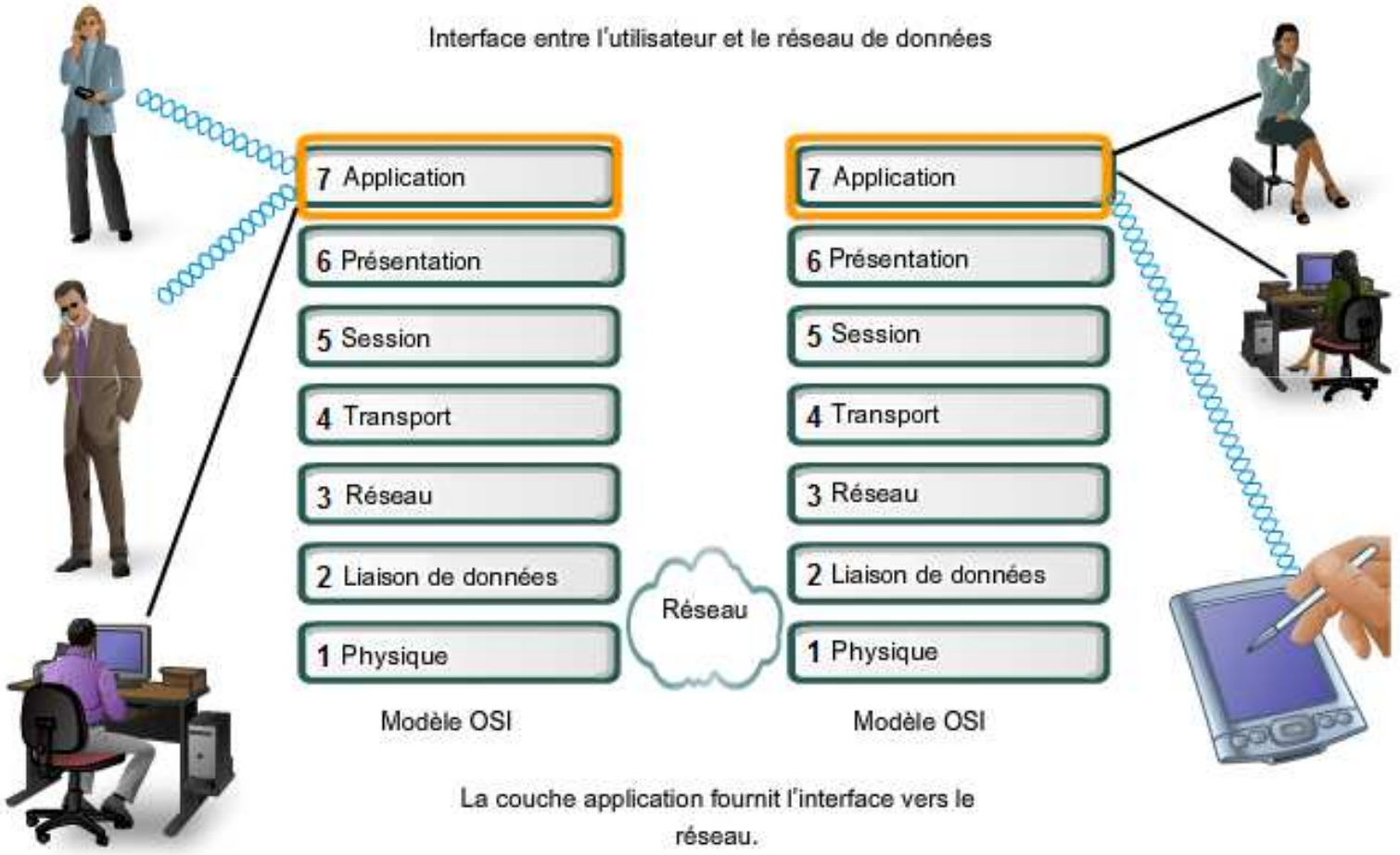
Le modèle de référence

Principe

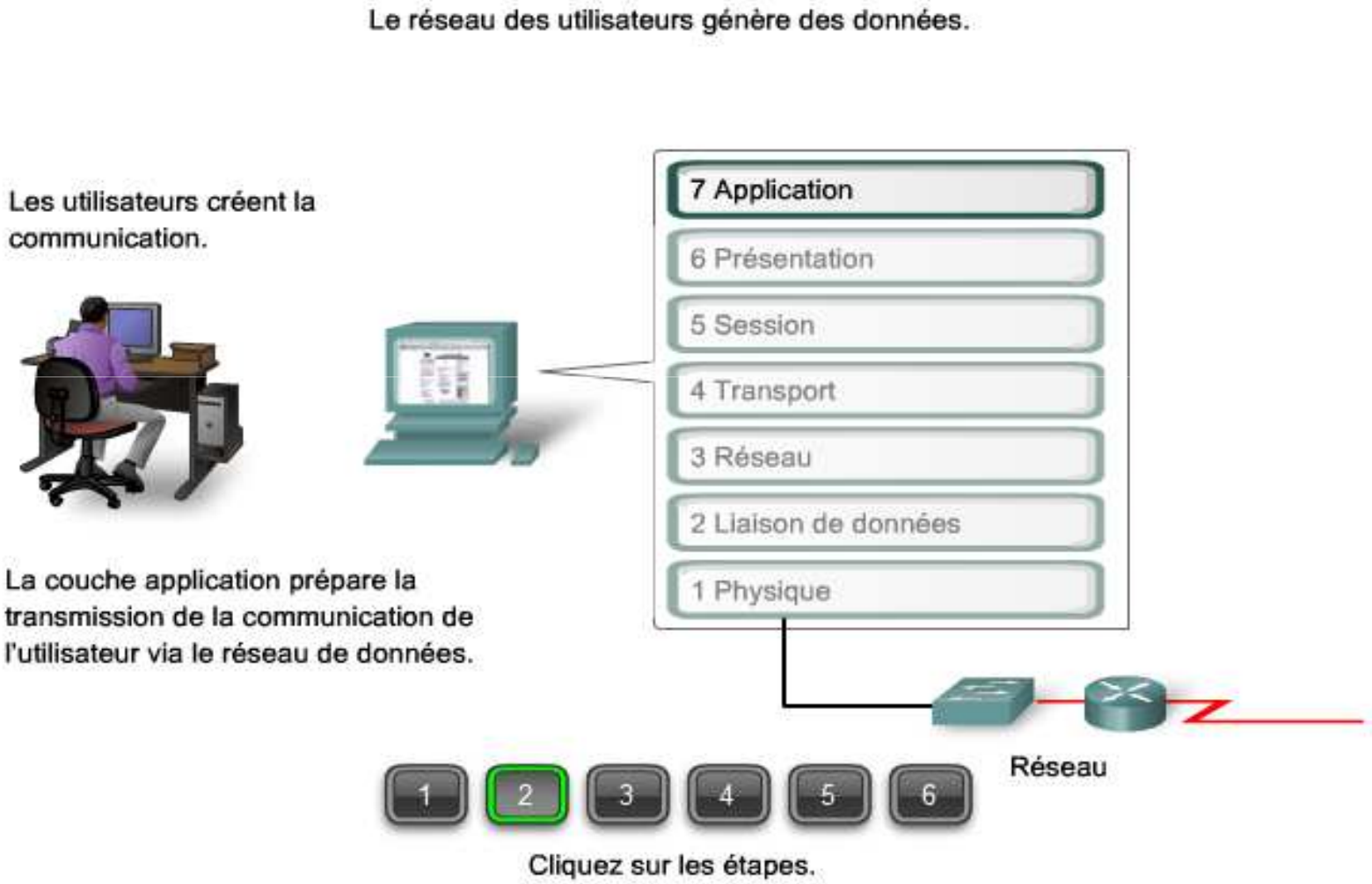
- *une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire*
- *chaque couche exerce une fonction bien définie*
- *les fonctions de chaque couche doivent êtres choisies en pensant à la définition de protocoles normalisés internationaux*
- *le choix des frontières entre les couches doit minimiser le flux d'informations aux interfaces*
- *le nombre de couches doit être suffisamment*
  - *grand pour éviter la cohabitation dans une même couche de fonctions très différentes*
  - *et petit pour éviter que l'architecture ne devienne difficile à maîtriser*

[Tanenbaum]

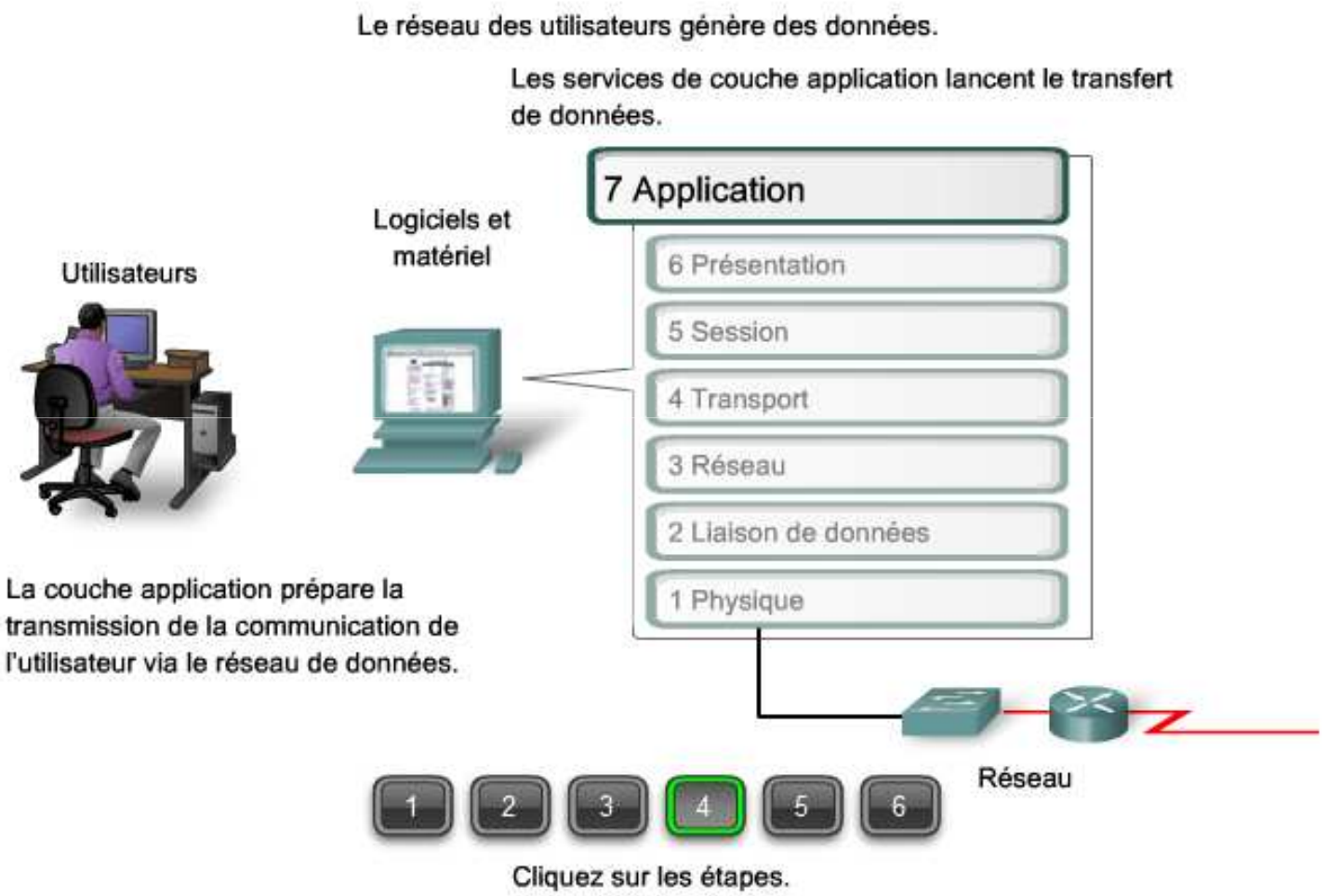
Le modèle de référence OSI



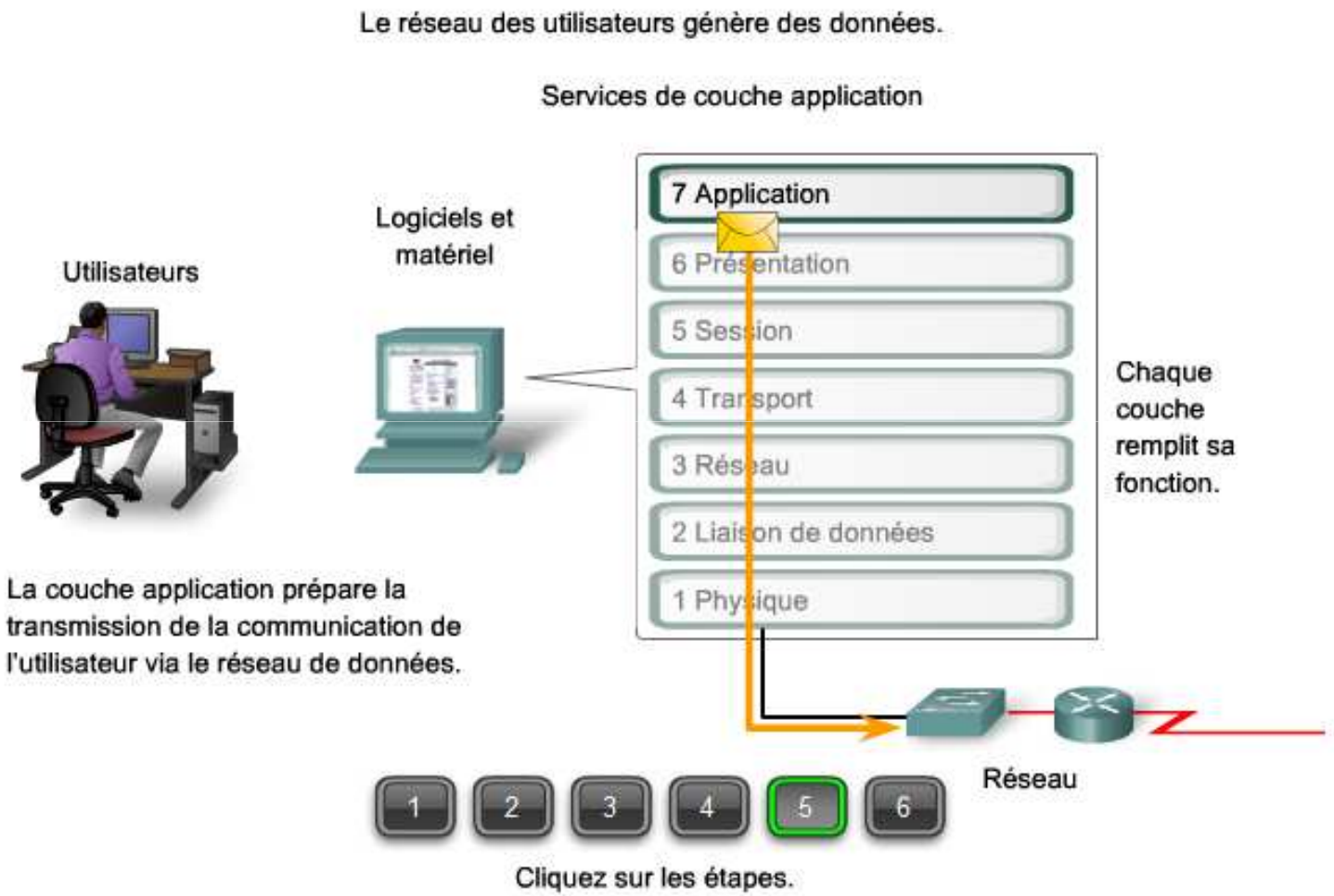
Le modèle de référence OSI



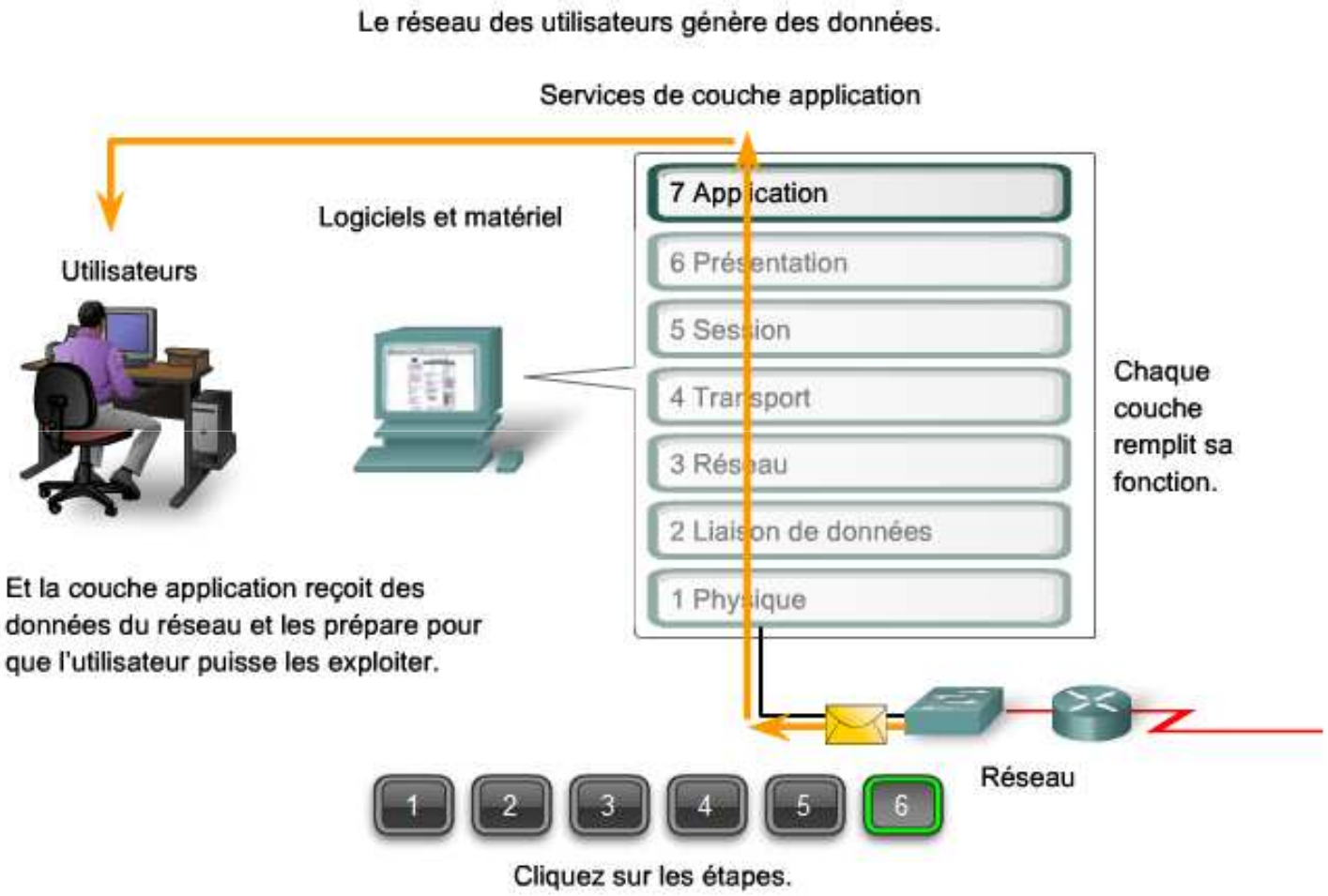
Le modèle de référence OSI



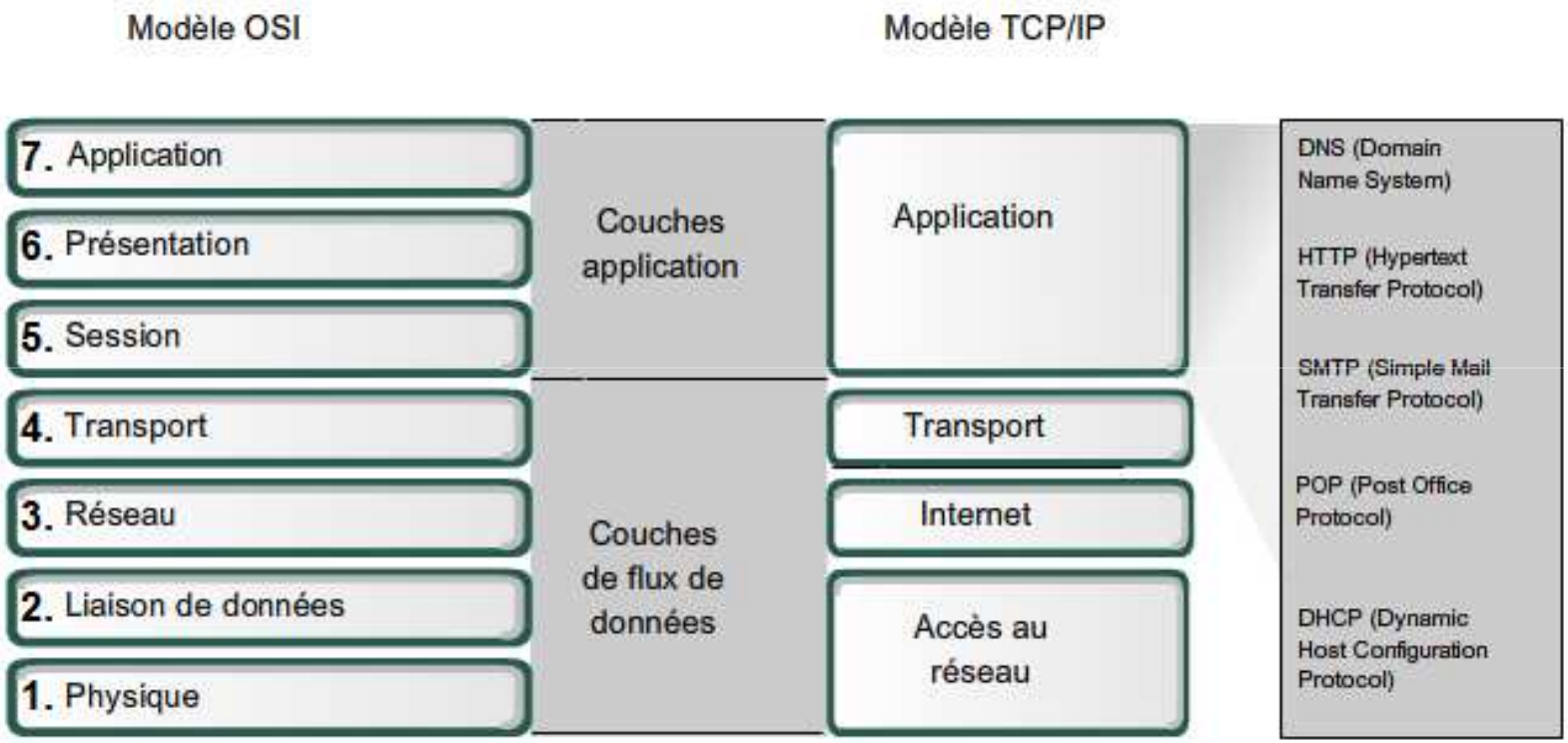
Le modèle de référence OSI



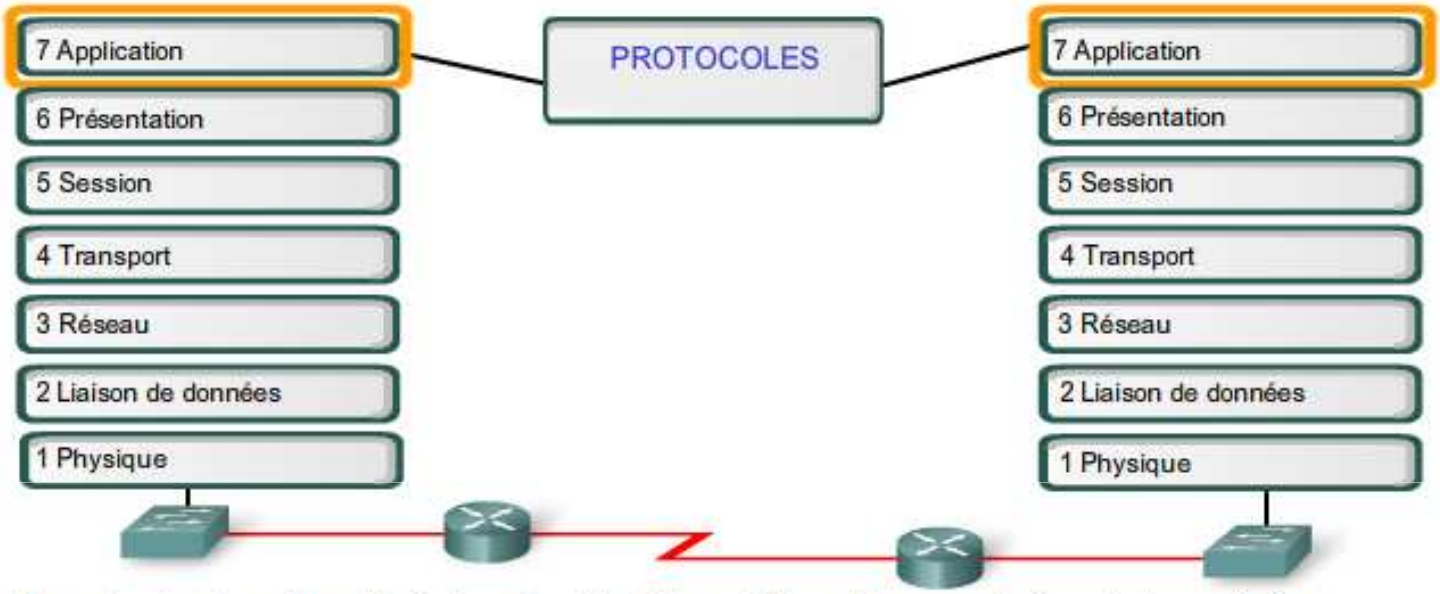
Le modèle de référence OSI



Le modèle de référence OSI vs TCP/IP



Le modèle de référence OSI et TCP/IP



Les protocoles de couche application fournissent les règles spécifiques à la communication entre les applications.

Les protocoles :

définissent les processus s'exécutant en début et en fin de communication ;
définissent les types de messages ;
définissent la syntaxe des messages ;
définissent la signification des champs d'information ;
définissent la manière dont les messages sont envoyés et la réponse attendue ;
définissent l'interaction avec la couche inférieure suivante.

La couche physique

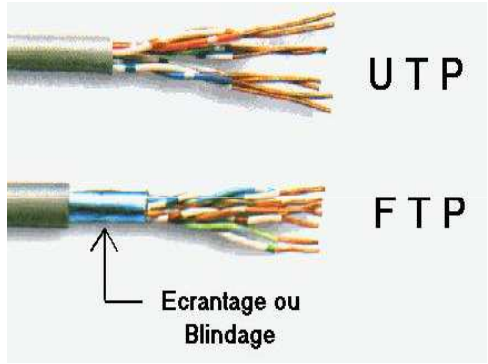
1 Physique

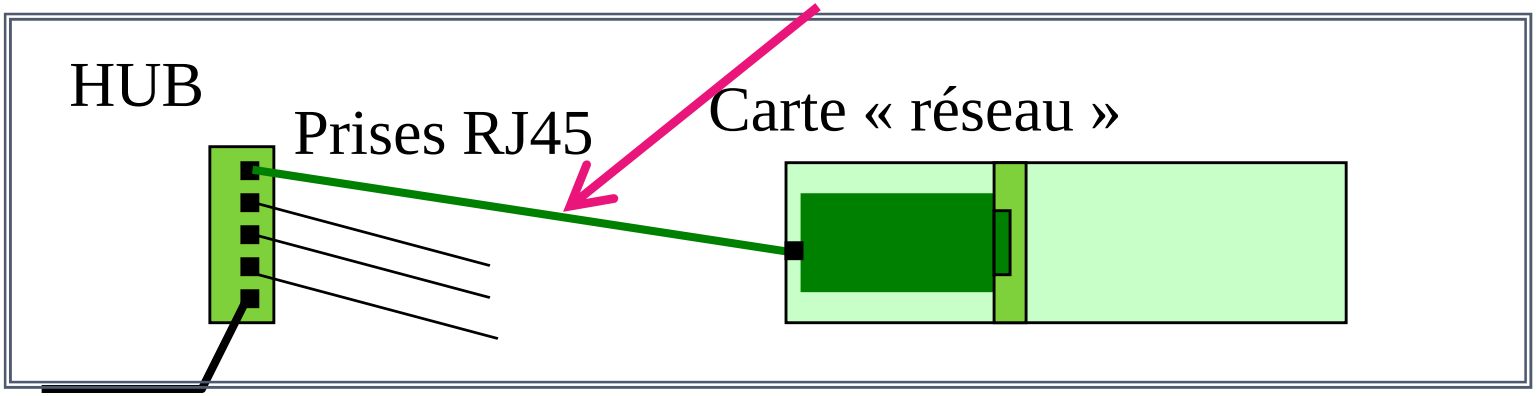
Medium

Les protocoles de connexion au niveau **bit**. Il s'agit des caractéristiques électriques, fonctionnelles et procédurales pour activer, maintenir et désactiver les liaisons physiques. Elle assure la transmission d'un flux de bits de manière la plus transparente possible.

La couche physique

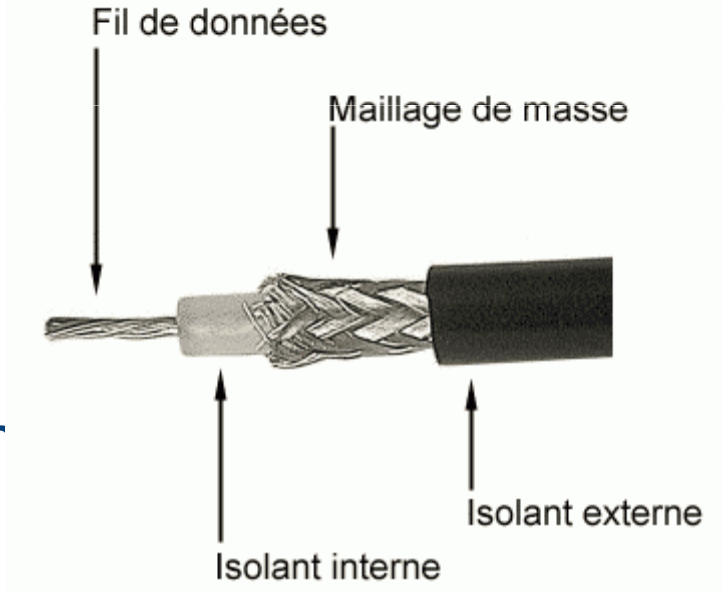
- Définit les supprots de transmission
- Paires Torsadées
  - fils métalliques (de type téléphonique)
  - bandes passant variant à l'inverse de la distance
    - limites à 72 kbits/s sur quelques kilomètres
    - jusqu'à 155 Mbits/s sur 100 m en catégorie 5
  - utilisé de plus en plus en réseau local (100baseT)





La couche physique

- **Câbles coaxiaux :**
  - Propriétés de bande passante et de faible bruit
  - Difficultés de mise en place
  - Deux grandes familles :
    - le fin (diamètres 4.4mm)
    - le gros (diamètres 9.5mm

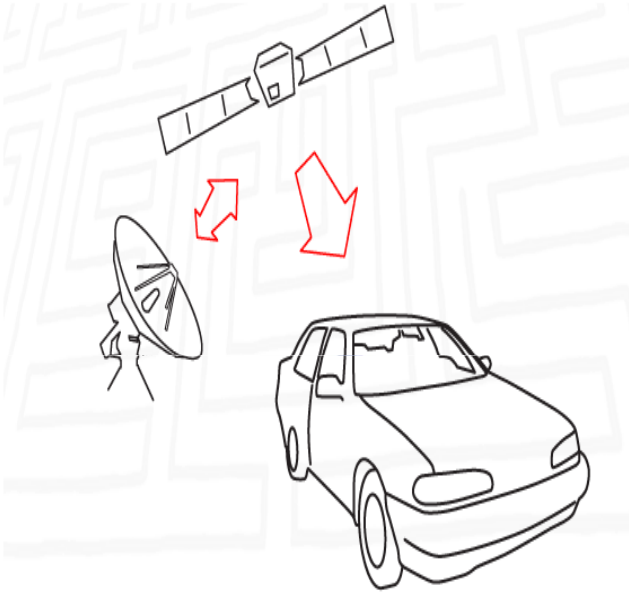


La couche physique

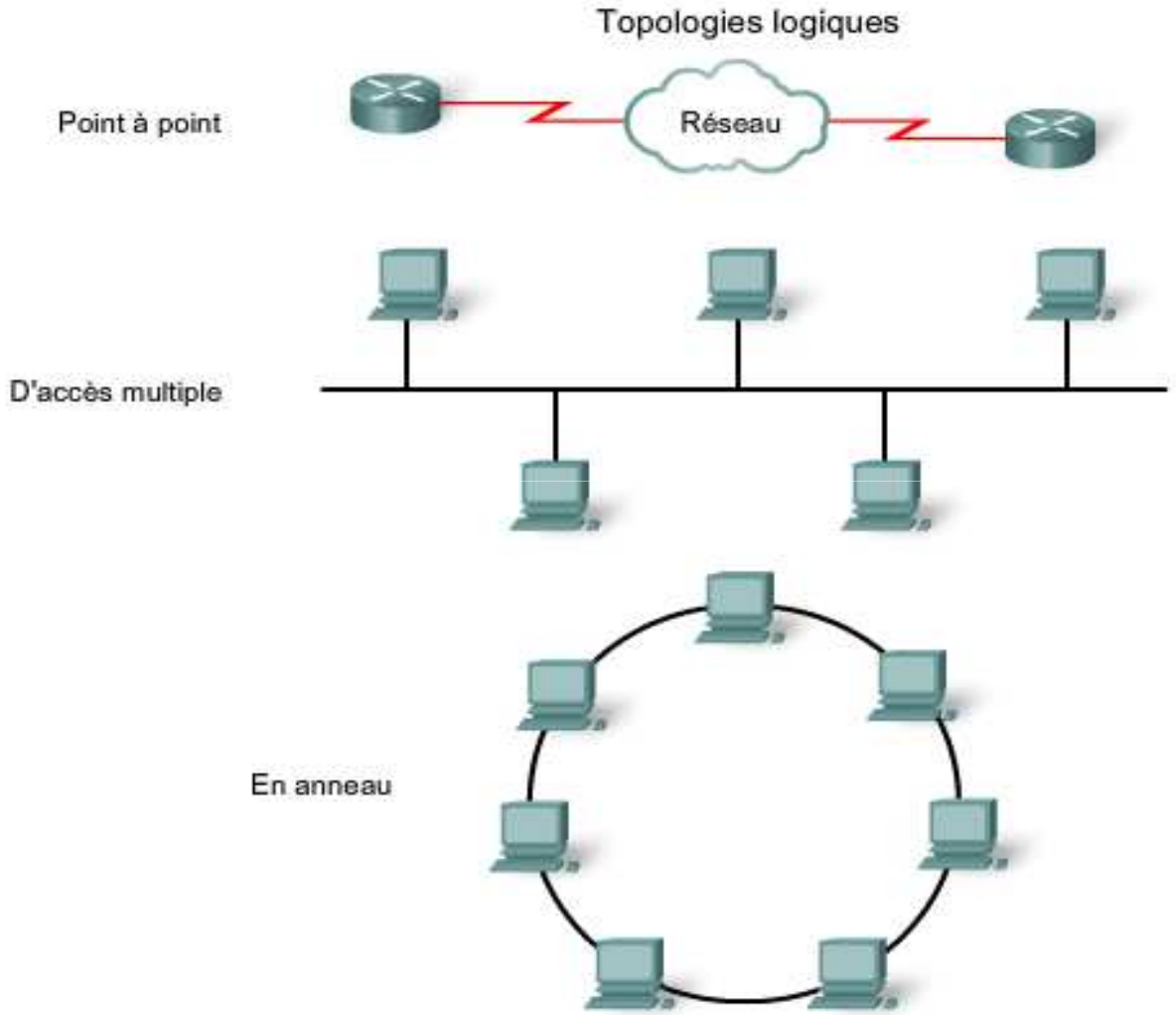
- Fibres Optiques
  - faible atténuation
  - insensibilité au bruit électromagn
  - très haut débits (>2Gbit/s)
  - banalisation de la connectique

La couche physique

- Faisceaux « sans fils »
  - Hertziens
    - Radios
    - Satellites
  - Infrarouges
- Vision Directe
- Hauts débits (selon les plages de fréquence)
- Re-configuration géographique aisée
- Economique



La couche physique

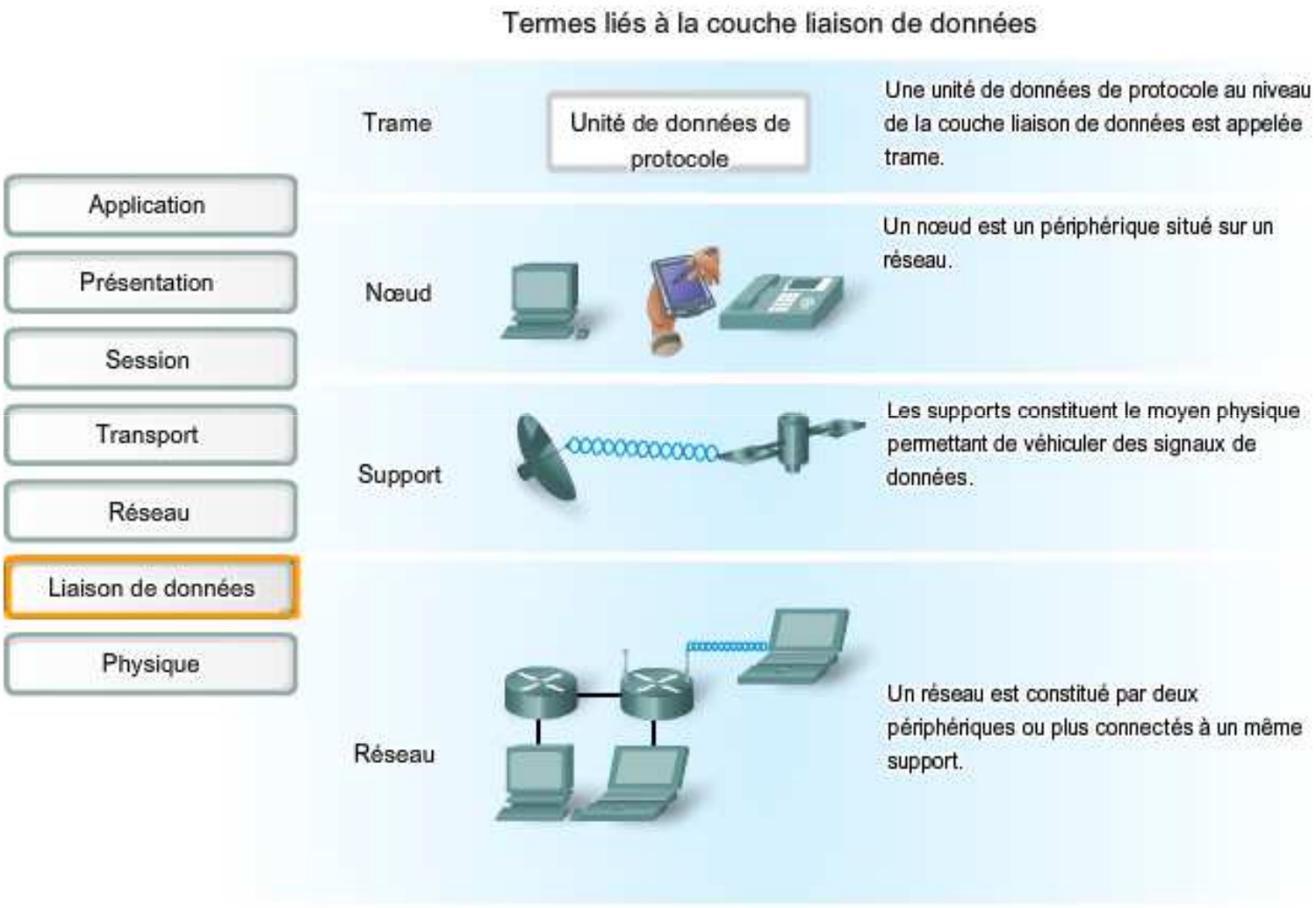


La couche Liaison de physique

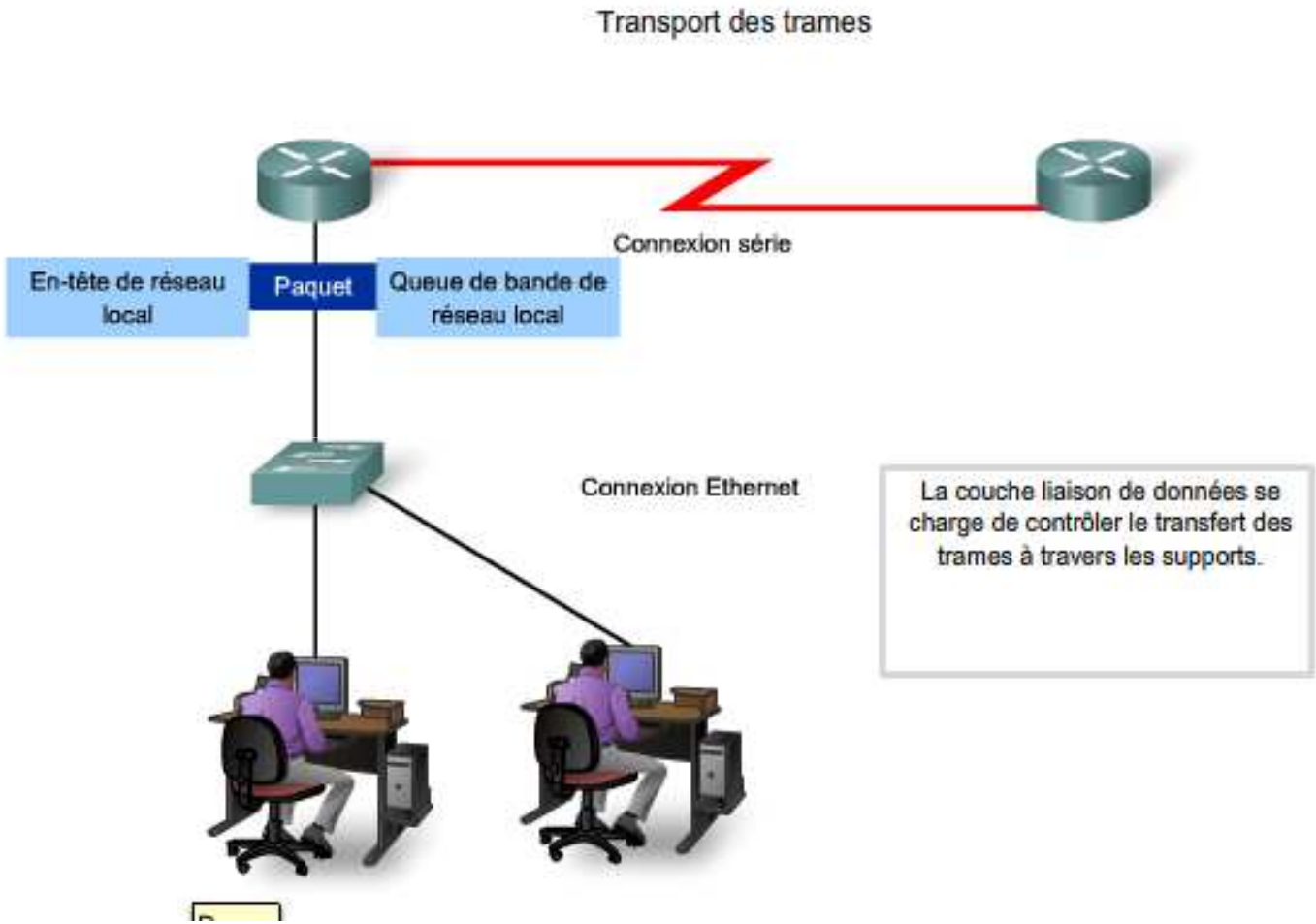
2 Liaison
Physique
Medium

les protocoles de liaison point à point . Groupe les bits en caractères et en trames. Synchronise les échanges et détecte (corrige) les erreurs de transmission ainsi que le contrôle de flux. Prend en charge une partie du contrôle d'accès au médium.

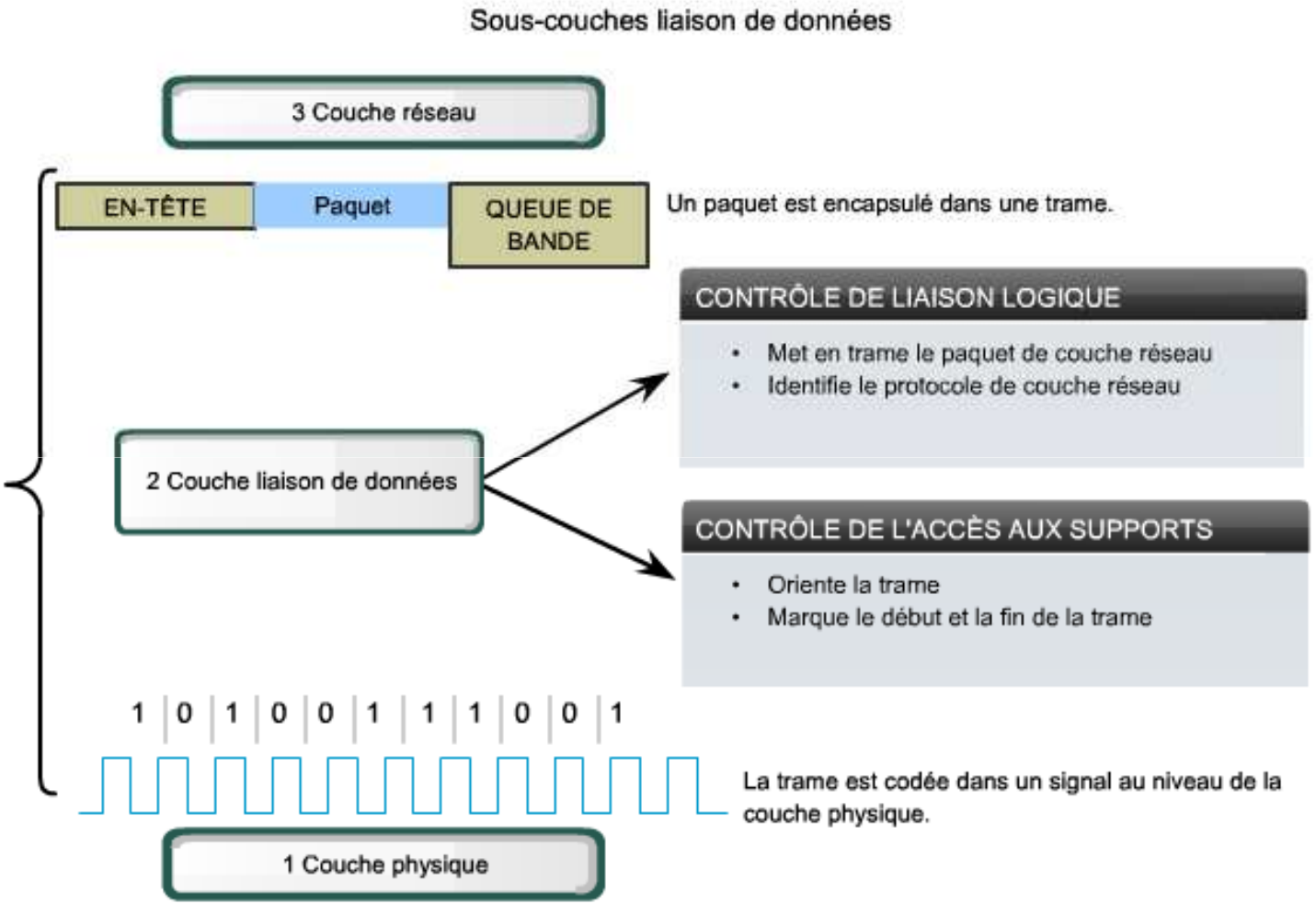
La couche Liaison de physique



La couche Liaison de physique



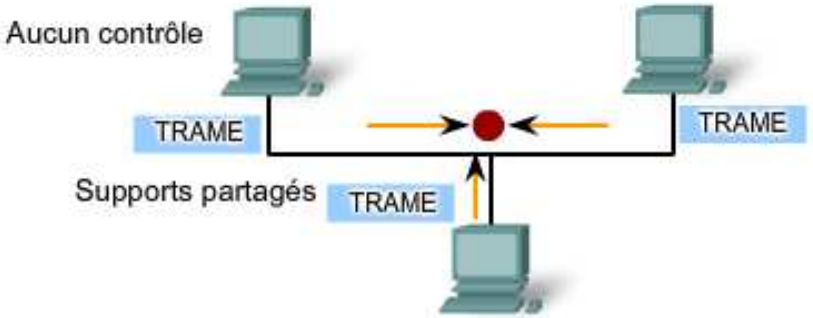
La couche Liaison de données



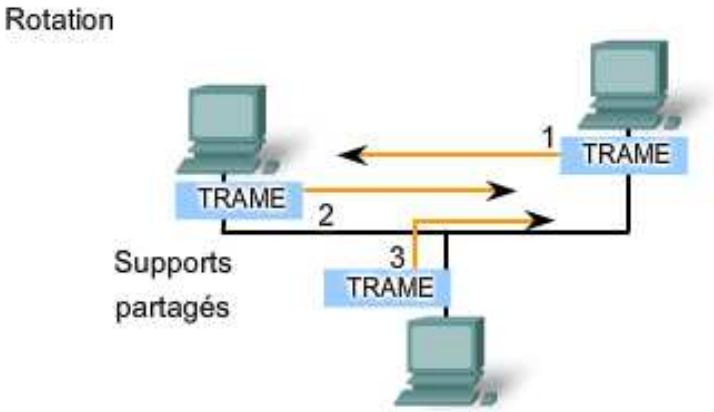
La couche Liaison de physique

Méthodes de contrôle d'accès au support

Aucun contrôle du tout donnerait lieu à de nombreuses collisions.
Les collisions génèrent des trames corrompues, qui doivent alors être ré-envoyées.

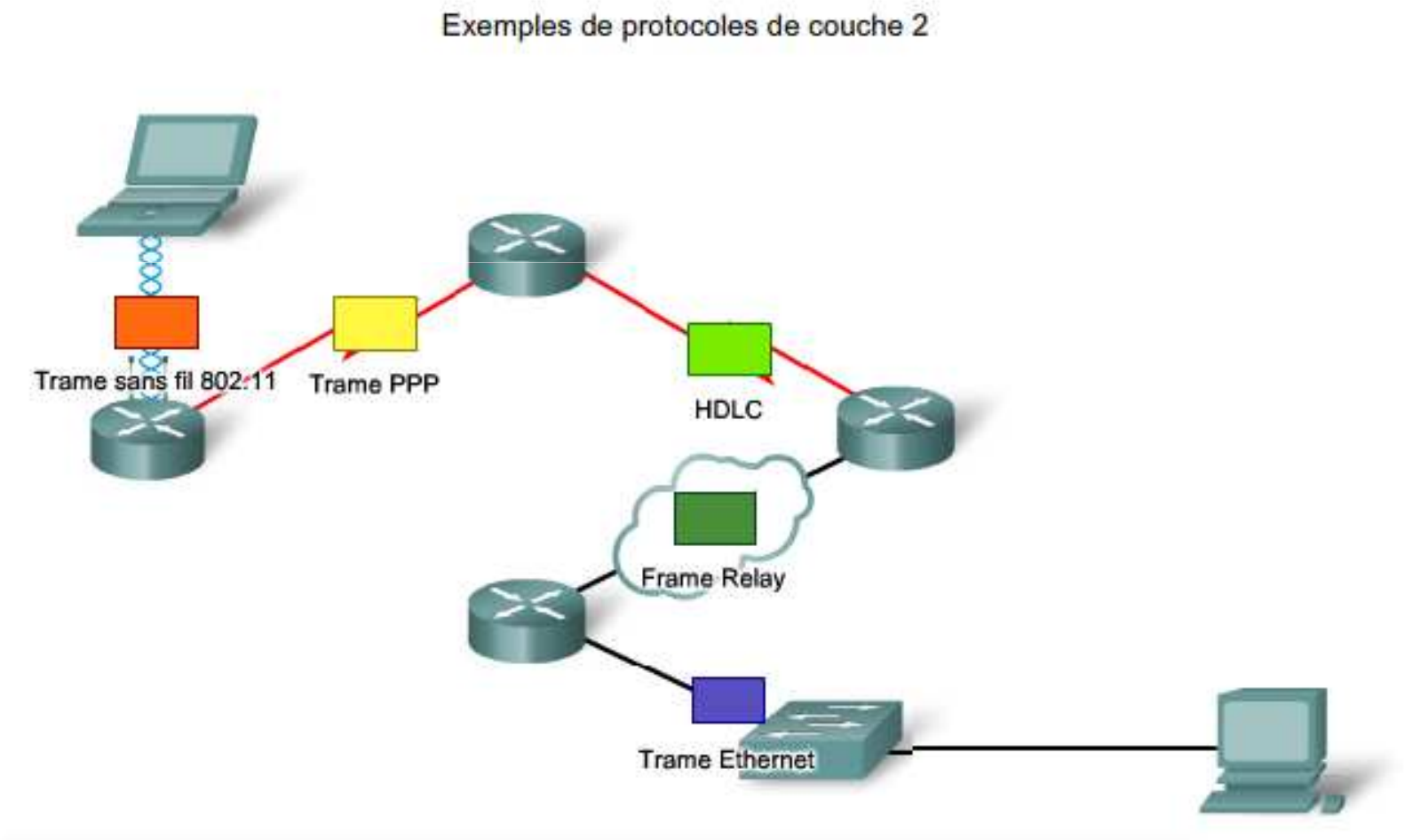


Les méthodes qui assurent un niveau élevé de contrôle empêchent les collisions mais le processus provoque une forte surcharge.
Les méthodes qui assurent un niveau faible de contrôle provoquent une surcharge basse mais les collisions sont plus fréquentes.



La couche Liaison de données

- Exemple de trames
  - Ethernet ; PPP (Point-to-Point Protocol) ; HDLC (High-Level Data Link Control) ; Frame Relay ;



La couche Liaison de données

Le champ **TYPE/ LONGUEUR** est un champ facultatif utilisé par certains protocoles pour indiquer le type de données qui arrive ou, éventuellement, la longueur de la trame.

Le champ **ADRESSE** stocke les adresses de liaison de données source et de destination.

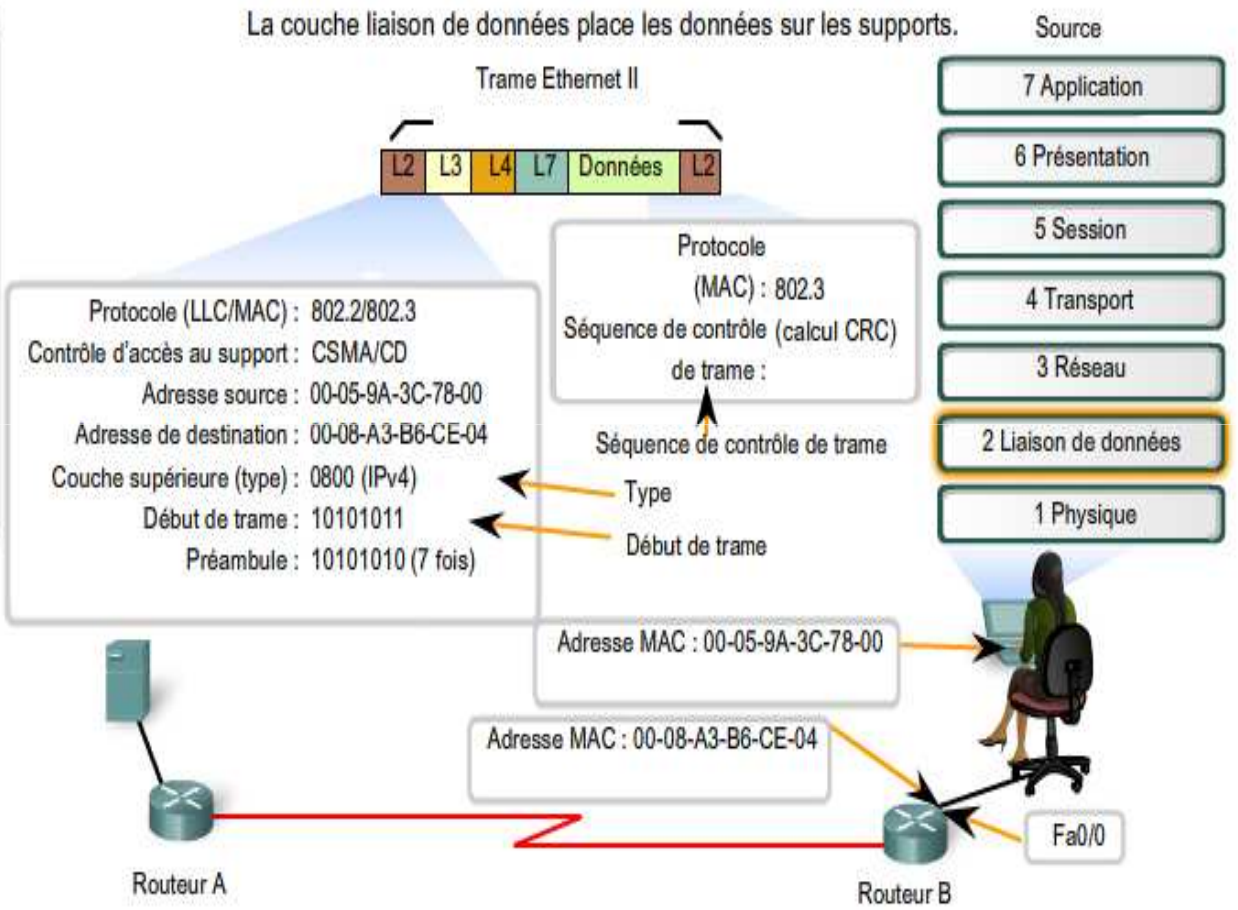
Le champ **DÉBUT DE TRAME** indique aux autres périphériques du réseau qu'une trame arrive sur le support.

Le champ **Séquence de contrôle de trame** est utilisé pour la vérification des erreurs. La source calcule un nombre en fonction des données de la trame et place ce nombre dans le champ de séquence de contrôle de trame. La destination recalcule alors les données pour voir si les séquences de contrôle de trame correspondent. Si elles ne correspondent pas, la destination supprime la trame.

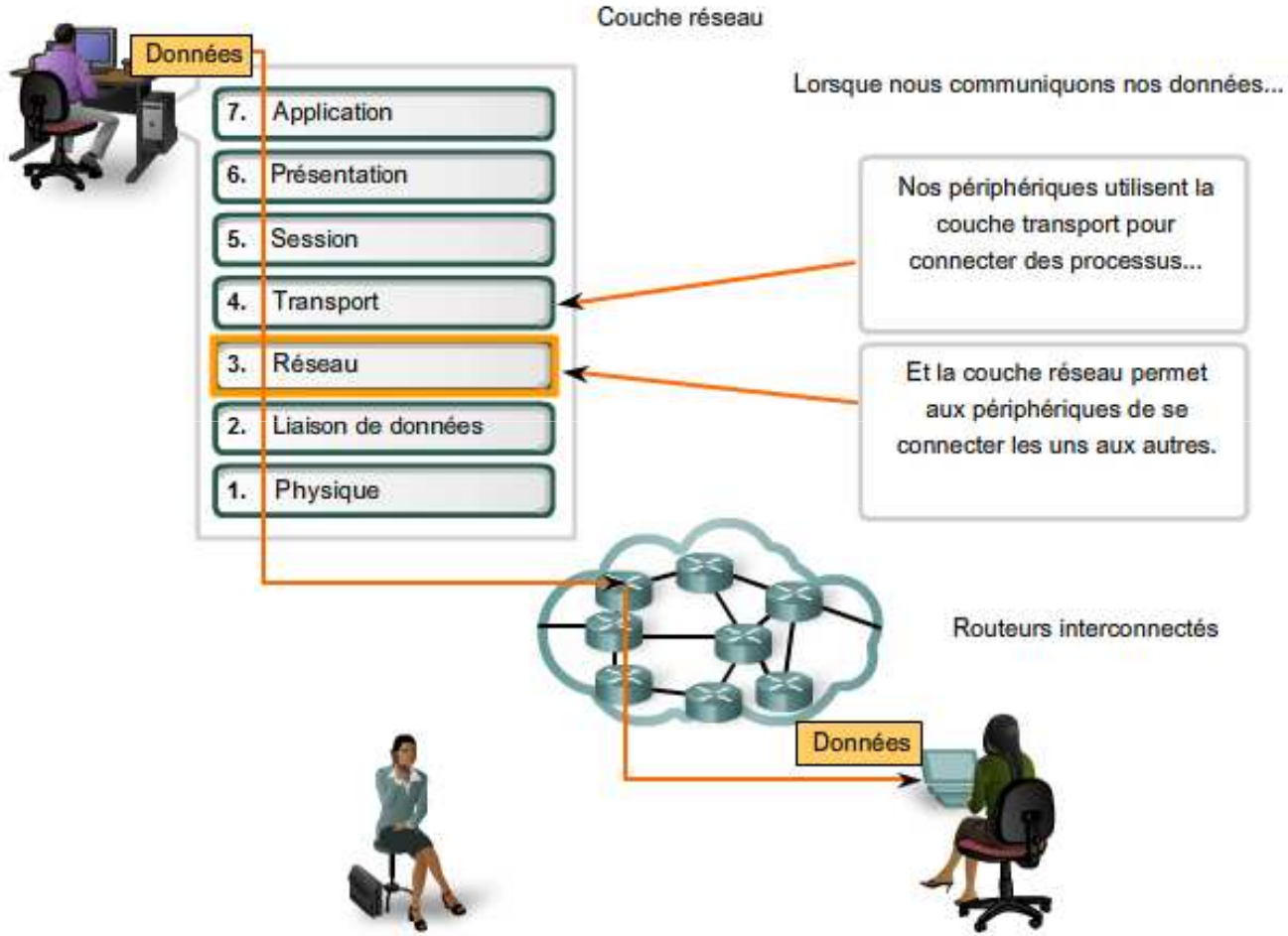
Le champ **Fin de trame**, également nommé queue de bande de trame, est un champ facultatif utilisé lorsque la longueur de la trame n'est pas spécifiée dans le champ Type/Longueur. Il indique la fin de la trame lorsque la trame est transmise.

La couche Liaison de données

La trame indique également le protocole de couche supérieure d'IPv4 avec la valeur 0800 dans le champ Type. La trame commence avec un préambule et un indicateur Start of Frame (SOF) et se termine avec un contrôle par redondance cyclique (CRC) dans la séquence de contrôle de trame, à la fin de la trame pour la détection d'erreur. Elle utilise ensuite CSMA/CD pour contrôler le placement de la trame sur les supports.

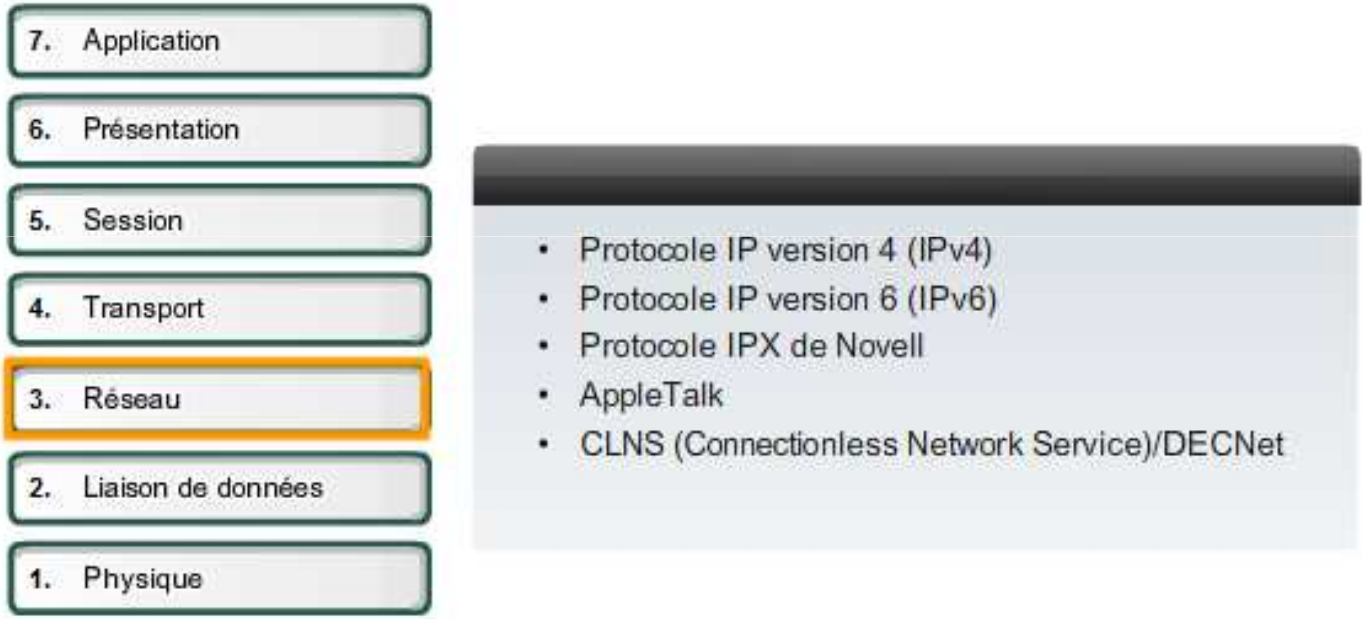


La couche réseau

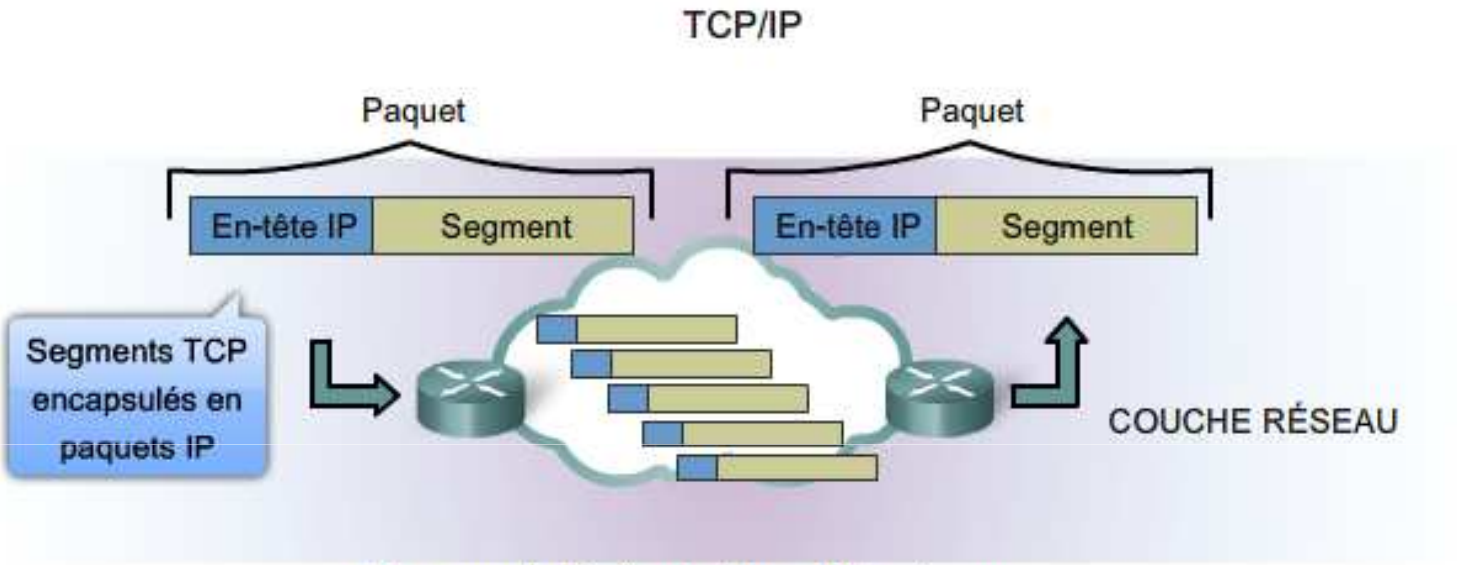


La couche réseau

Protocoles de couche réseau



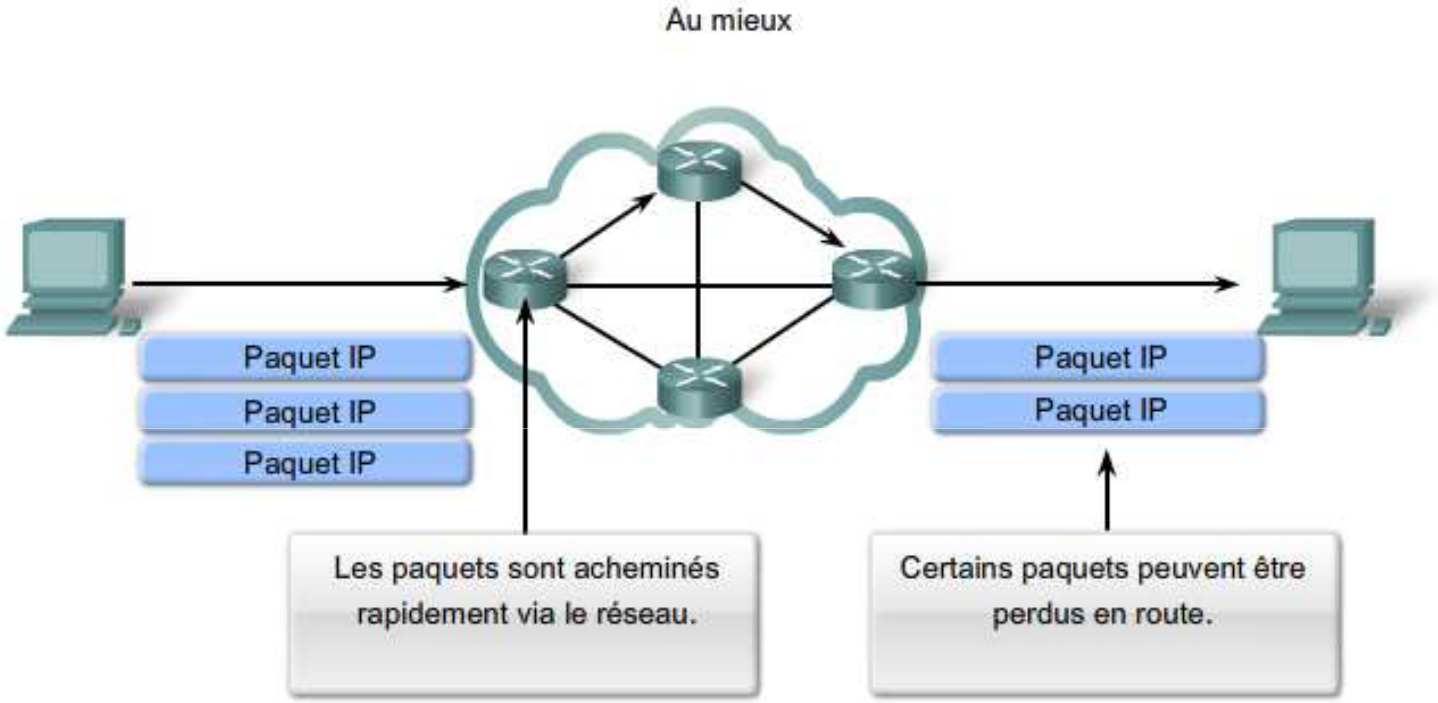
La couche réseau



Les paquets IP circulent dans l'interréseau.

- Sans connexion : aucune connexion n'est établie avant l'envoi des paquets de données.
- Au mieux (peu fiable) : aucune surcharge n'est utilisée pour garantir la transmission des paquets.
- Indépendant des médias : fonctionne indépendamment du média transportant les données.

La couche réseau



Protocole de couche réseau peu fiable, IP ne garantit pas que tous les paquets envoyés seront reçus.

D'autres protocoles gèrent le processus de suivi des paquets et garantissent leur acheminement.

La couche réseau

Génération de paquets IP

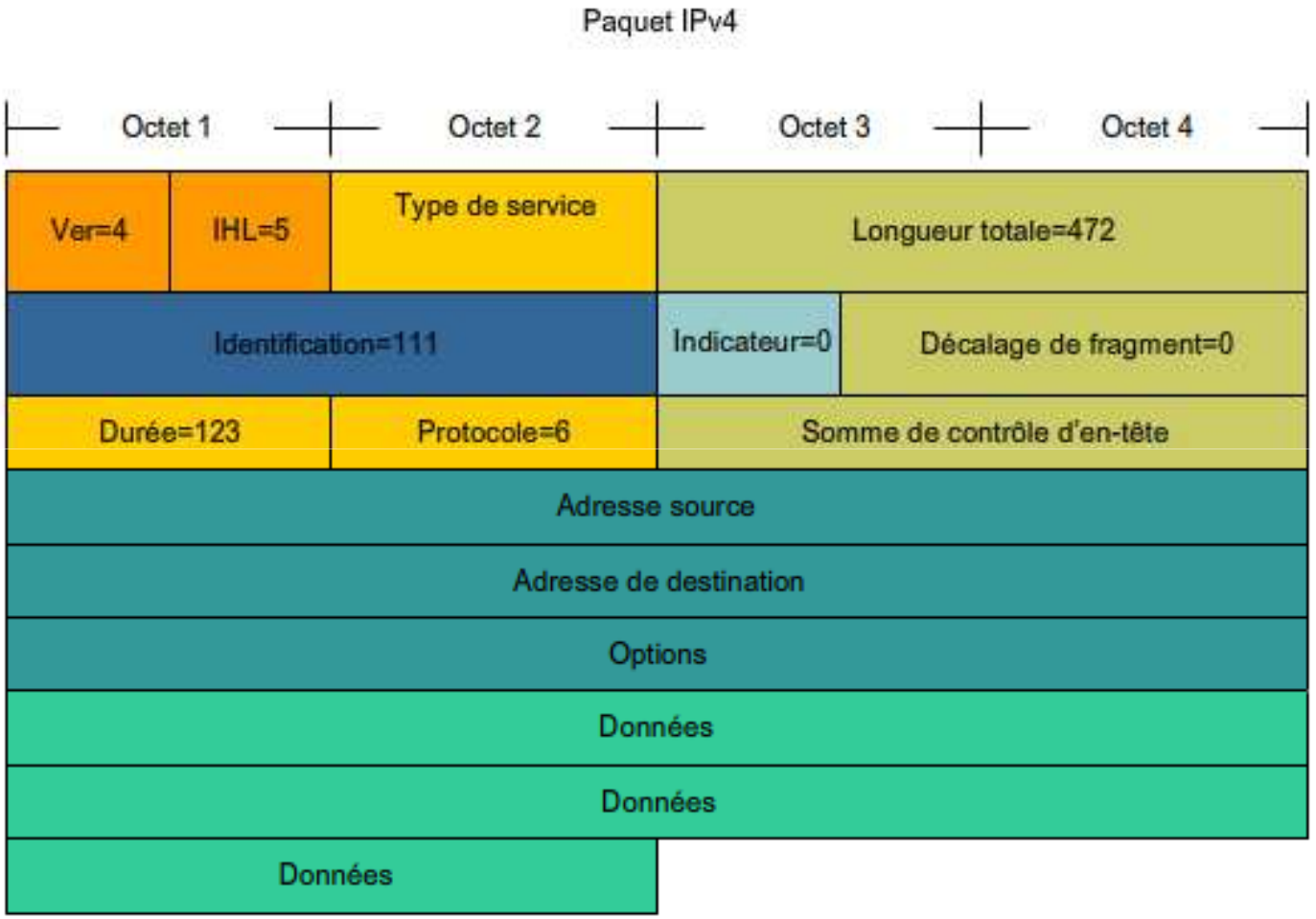
Encapsulation de la couche transport

Encapsulation de la couche réseau

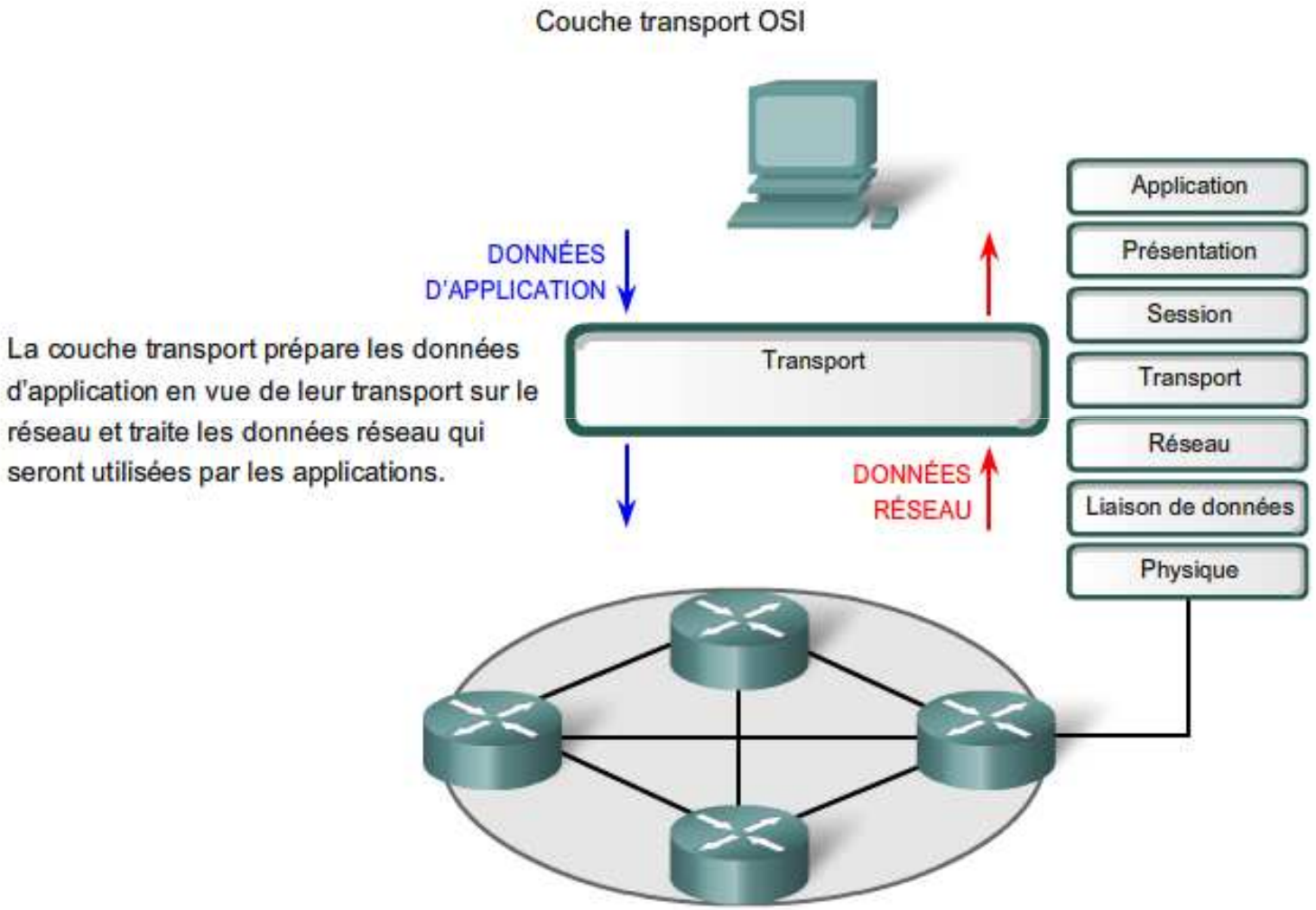
Paquet IP

Dans les réseaux TCP/IP, l'unité de données de protocole de la couche réseau est le paquet IP.

La couche réseau

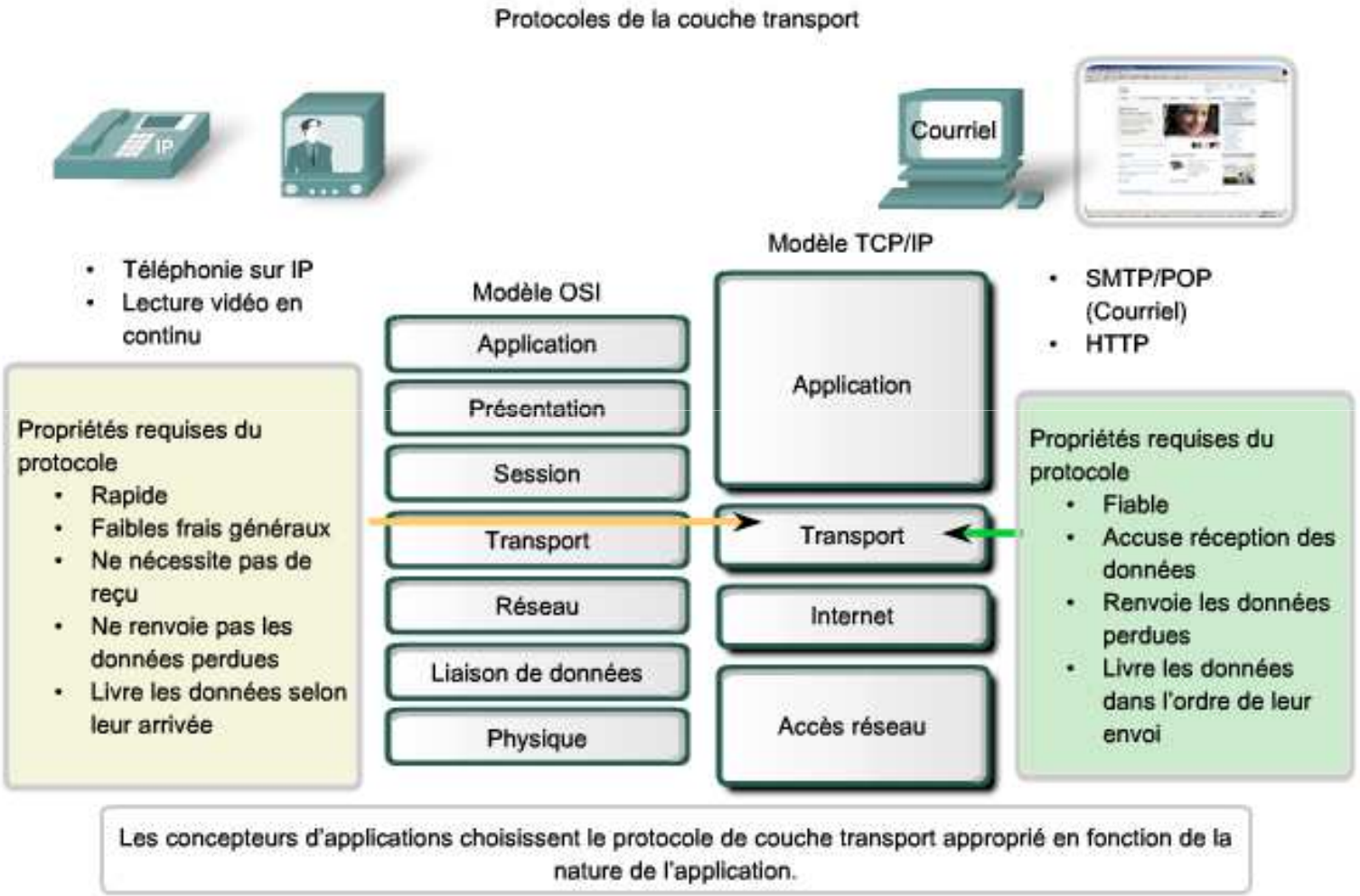


La couche Transport

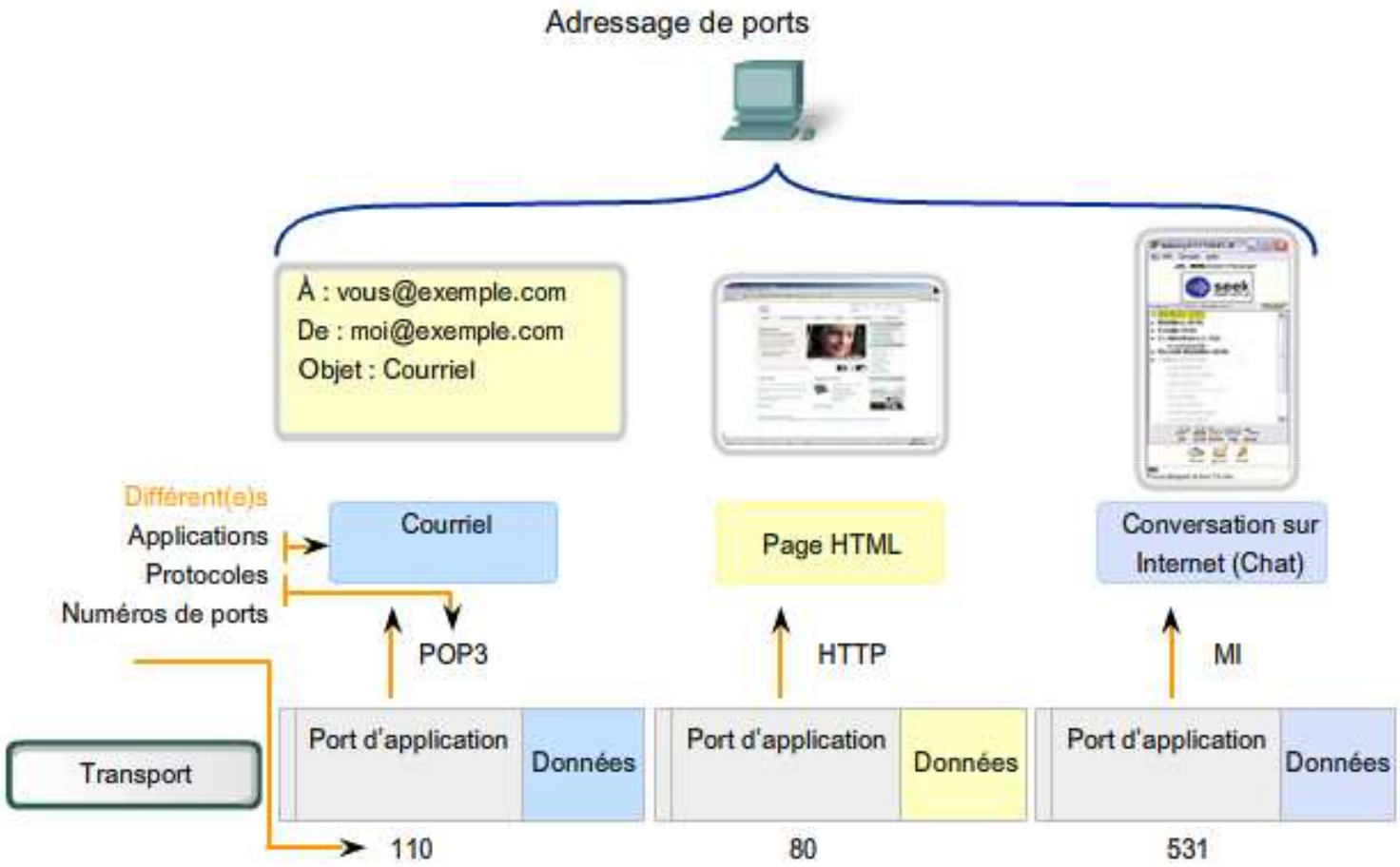


La couche transport prépare les données d'application en vue de leur transport sur le réseau et traite les données réseau qui seront utilisées par les applications.

La couche Transport



La couche Transport



Les données des différentes applications sont dirigées vers l'application adéquate car chaque application dispose d'un numéro de port unique.

La couche Transport

La couche Transport

Numéros de ports

Plage des numéros de ports	Groupe de ports
0 à 1023	Ports réservés (Contact)
1024 à 49151	Ports inscrits
49152 à 65535	Ports dynamiques et/ou privés

Ports UDP inscrits :
1812 Protocole d'authentification RADIUS
2000 Cisco SCCP (VoIP)
5004 RTP (Protocole de transport voix et vidéo)
5060 SIP (VoIP)

Ports UDP réservés :
69 TFTP
520 RIP

Ports UDP

La couche Transport

Numéros de ports

Plage des numéros de ports	Groupe de ports
0 à 1023	Ports réservés (Contact)
1024 à 49151	Ports inscrits
49152 à 65535	Ports dynamiques et/ou privés

Ports inscrits communs aux protocles TCP et UDP :
1433 MS SQL
2948 WAP (MMS)

Ports réservés communs aux protocoles TCP et UDP :
53 DNS
161 SNMP
531 Messagerie instantanée d'AOL, IRC

Ports communs aux protocoles TCP et UDP

La couche Transport

En-têtes TCP et UDP

Segment TCP

Bit (0)	Bit (15) Bit (16)	Bit (31)
Port source (16)	Port de destination (16)	
Numéro d'ordre (32)		
Numéro de reçu (32)		
Longueur de l'en-tête (4) Réservé (6) Bits de code (6)	Fenêtre (16)	
Somme de contrôle (16)	Urgent (16)	
Options (0 ou 32 le cas échéant)		
DONNÉES DE LA COUCHE APPLICATION (Taille variable)		

20 octets

Datagramme UDP

Bit (0)	Bit (15) Bit (16)	Bit (31)
Port source (16)	Port de destination (16)	
Longueur (16)	Somme de contrôle (16)	
DONNÉES DE LA COUCHE APPLICATION (Taille variable)		

8 octets

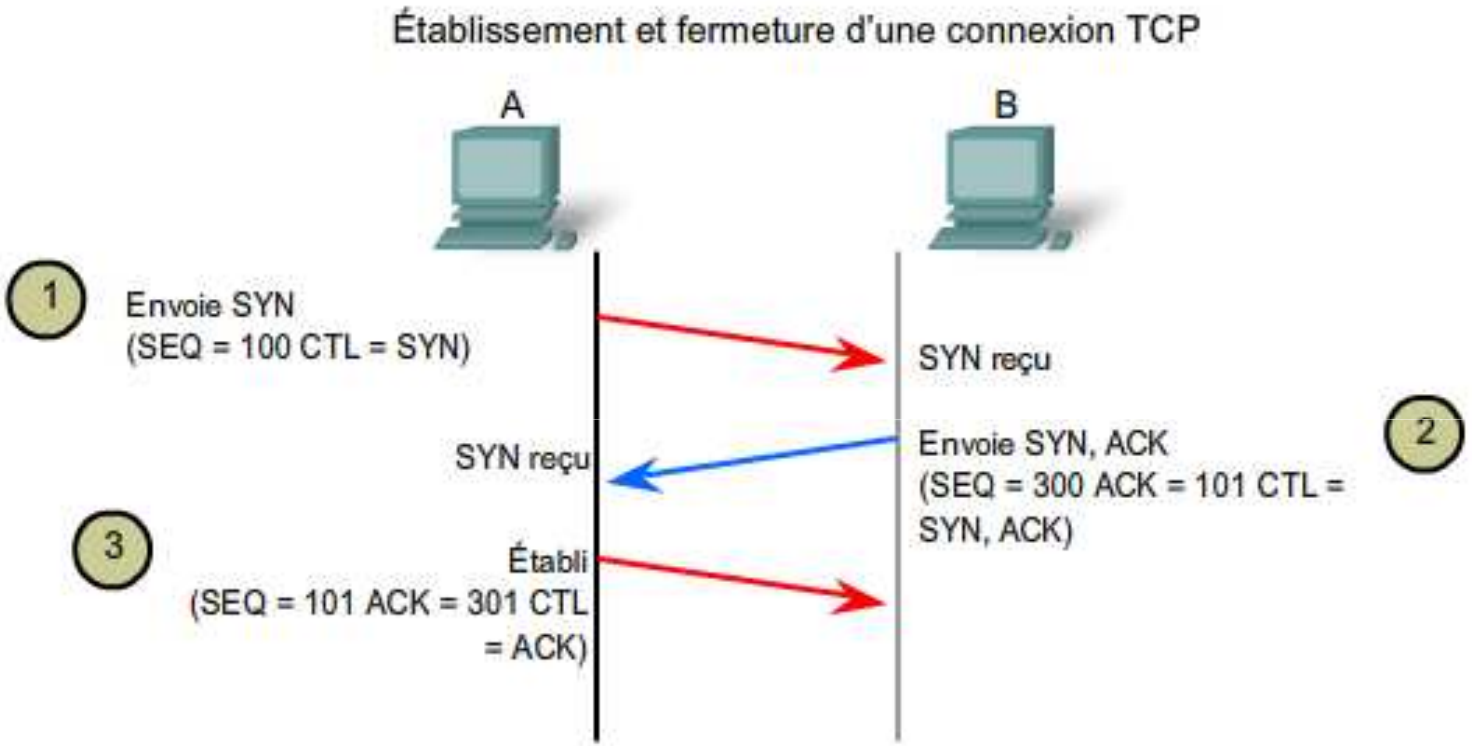
La couche Transport

Résultat Netstat

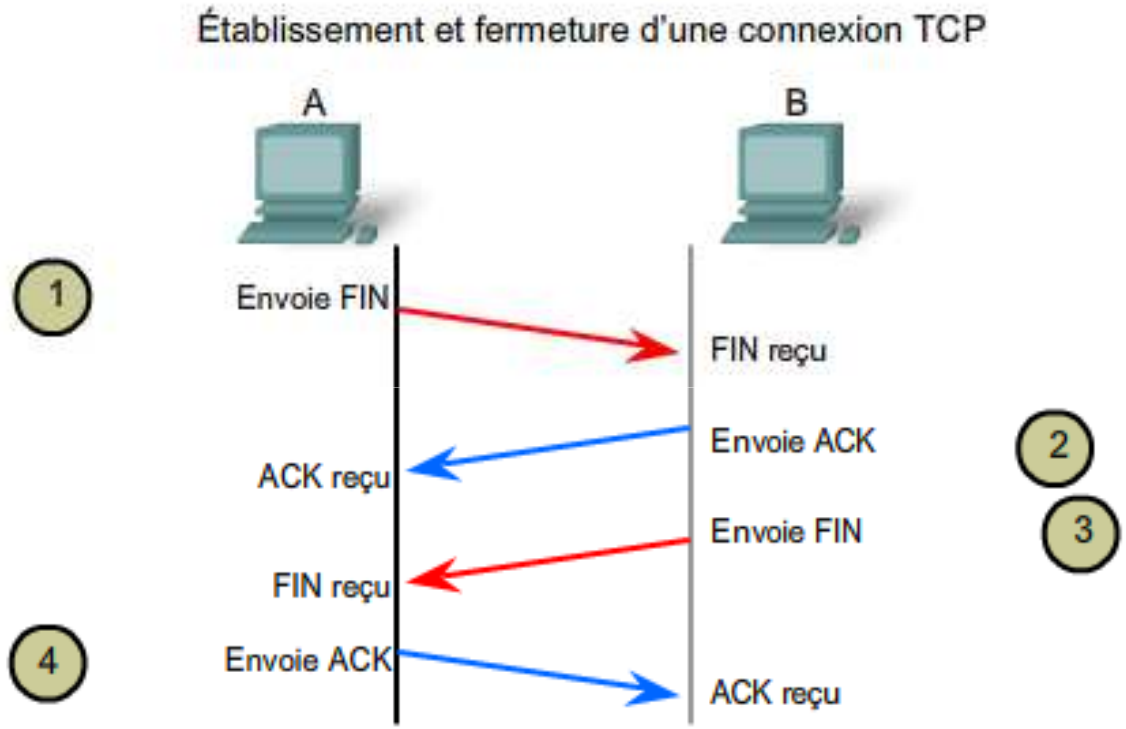
```
C:\>netstat

Active Connections

Proto    Local Address          Foreign Address        State
TCP      kenpc:3126             192.168.0.2:netbios-ssn    ESTABLISHED
TCP      kenpc:3158             207.138.126.152:http       ESTABLISHED
TCP      kenpc:3159             207.138.126.169:http       ESTABLISHED
TCP      kenpc:3160             207.138.126.169:http       ESTABLISHED
TCP      kenpc:3161             sc.msn.com:http            ESTABLISHED
TCP      kenpc:3166             www.cisco.com:http         ESTABLISHED

C:\>
```

État de la connexion

La couche Transport



La couche Transport



A envoie une réponse ACK à B.

La couche application

Serveur DNS (Domain Name System)

- Service qui fournit l'adresse IP d'un site Web ou d'un nom de domaine pour qu'un hôte puisse s'y connecter.

Serveur Telnet

- Service permettant aux administrateurs de se connecter à un hôte à partir d'un emplacement distant et de contrôler l'hôte comme s'ils étaient connectés localement.

Serveur de messagerie

- Utilise le protocole SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3) ou IMAP (Internet Message Access Protocol)
- Permet d'envoyer du courriel des clients vers les serveurs via Internet
- Les destinataires sont spécifiés via le format utilisateur@xyz.

Serveur DHCP (Dynamic Host Configuration Protocol)

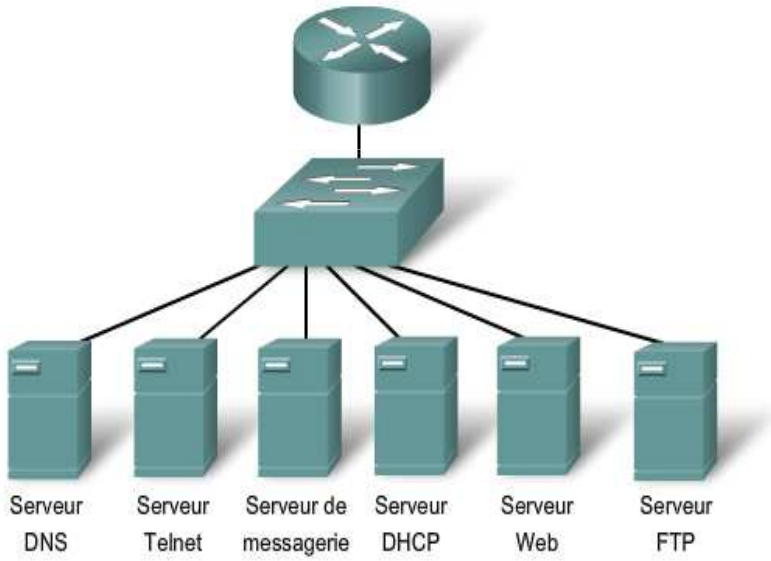
- Service qui assigne aux clients l'adresse IP, le masque de sous-réseau, la passerelle par défaut et autres informations.

Serveur FTP (File Transfer Protocol)

- Service qui permet de télécharger des fichiers entre un client et un serveur.

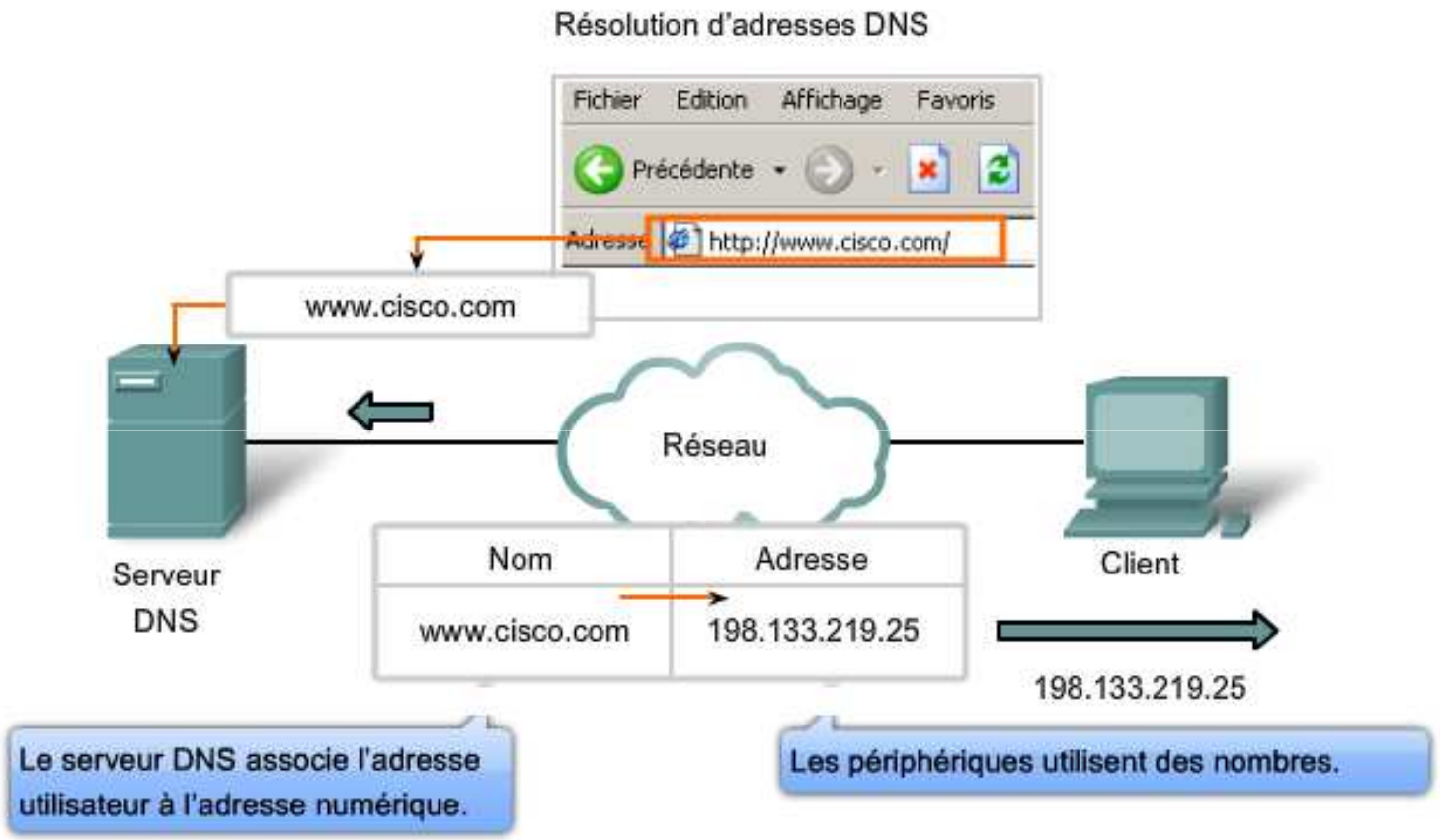
Serveur Web

- HTTP (Hypertext Transfer Protocol)
- Permet de transférer des informations entre des clients Web et des serveurs Web.
- La plupart des pages sont accessibles via HTTP.

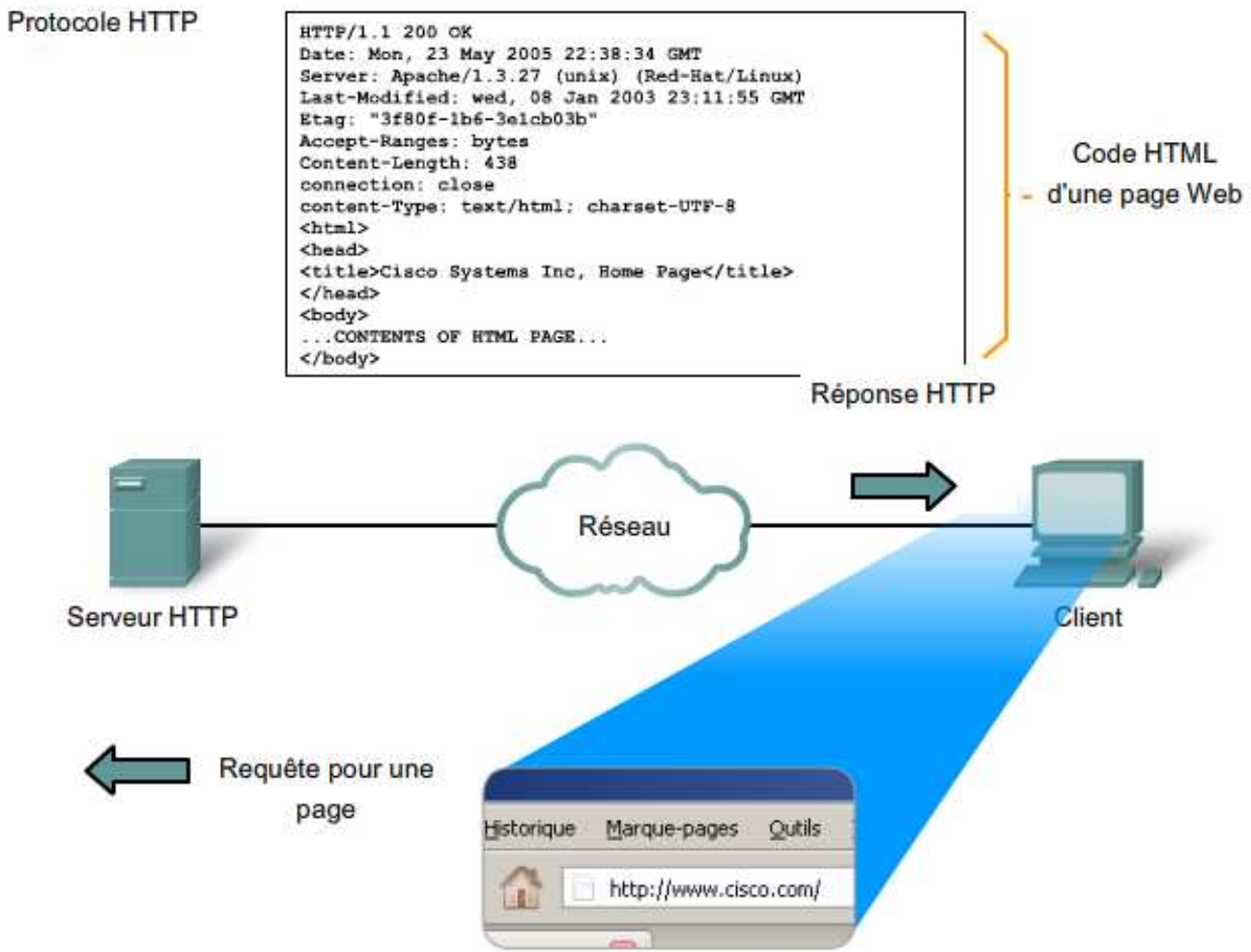


Batterie de serveurs

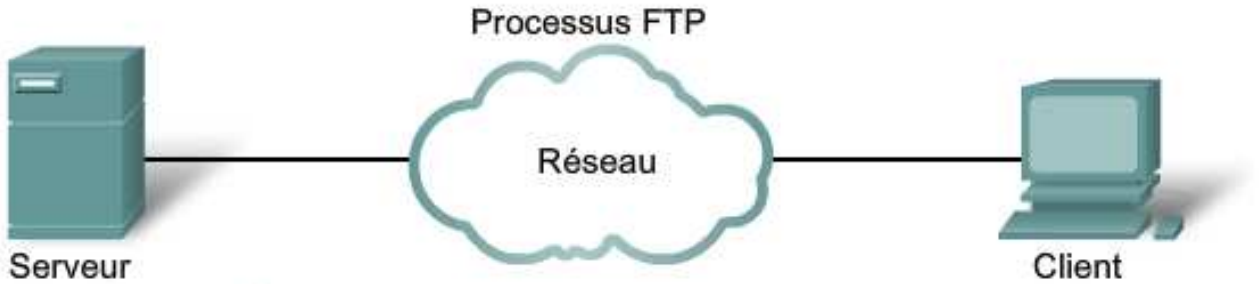
La couche application



La couche application



La couche application



Connexion de contrôle :
le client établit une première connexion au serveur pour contrôler le trafic.

Connexion de données :
le client établit une seconde connexion pour le trafic de données.

Obtention des données

En fonction de la commande envoyée via la connexion de contrôle, les données peuvent être téléchargées depuis le serveur ou depuis le client.