Réseau

Le LAN

LAN

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local représente un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'« égal à égal » (en anglais peer to peer, noté P2P), dans lequel la communication s'établit d'ordinateur à ordinateur sans ordinateur central et où chaque ordinateur possède un rôle similaire.

- dans un environnement « client/serveur », dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

Réseau

Le VLAN

VLAN

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

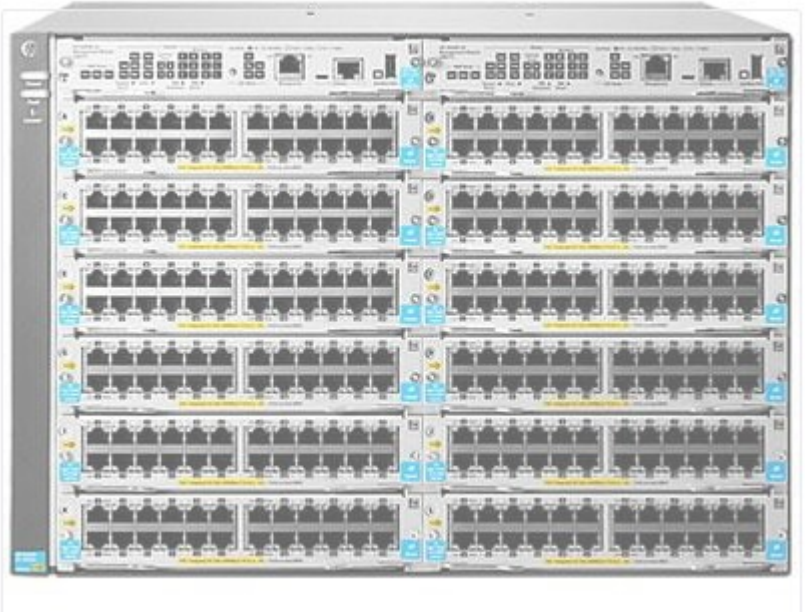
Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

L’avantage du VLAN est d’apporter plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs. De plus, les VLAN permettent un gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées ainsi qu’une réduction de la diffusion du traffic sur le réseau

VLAN : leur topologie

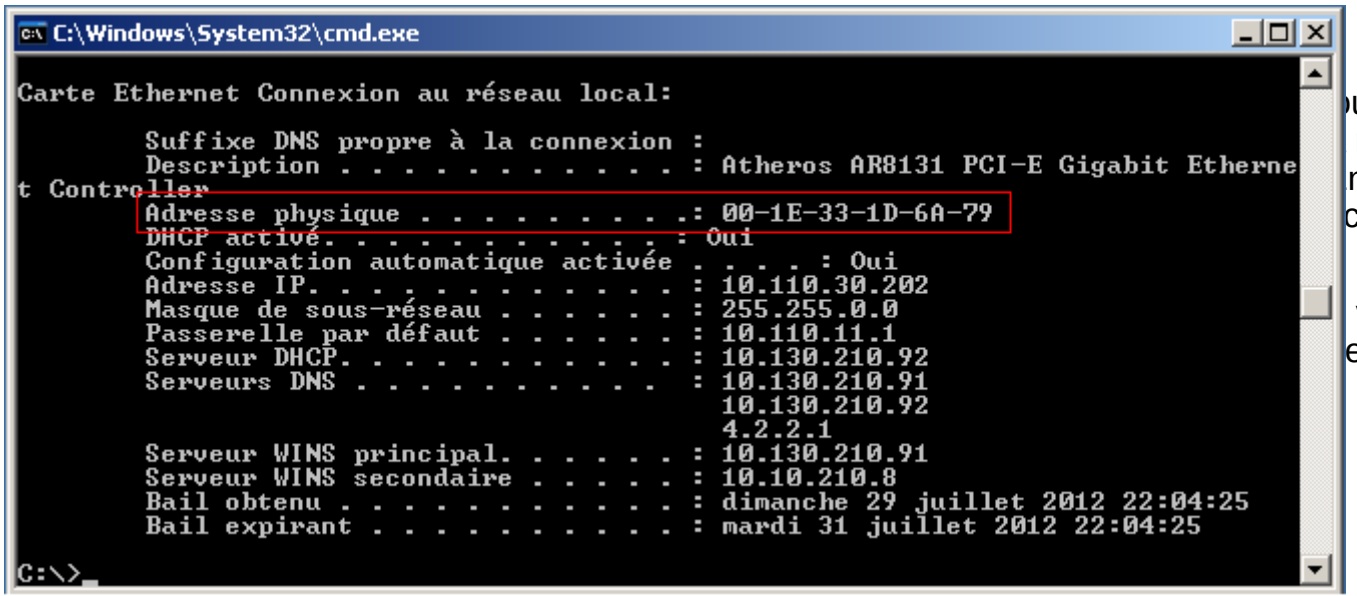
Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;
- Un VLAN de nive EEE ou en anglais MAC Address-Based VLAN) consiste à définir ions. Ce type de VLAN est beaucoup plus souple que le VL on de la station ;
- Un VLAN de nive :
  - Le VLAN pa associe des sous-réseaux selon l'adresse IP source des c uplesse dans la mesure où la configuration des commutateu d'une station. En contrepartie une légère dégradation s informations contenues dans les paquets doivent être
  - Le VLAN pa réer un réseau virtuel par type de protocole (par exemple TC hines utilisant le même protocole au sein d'un même résea



VLAN : leur topologie

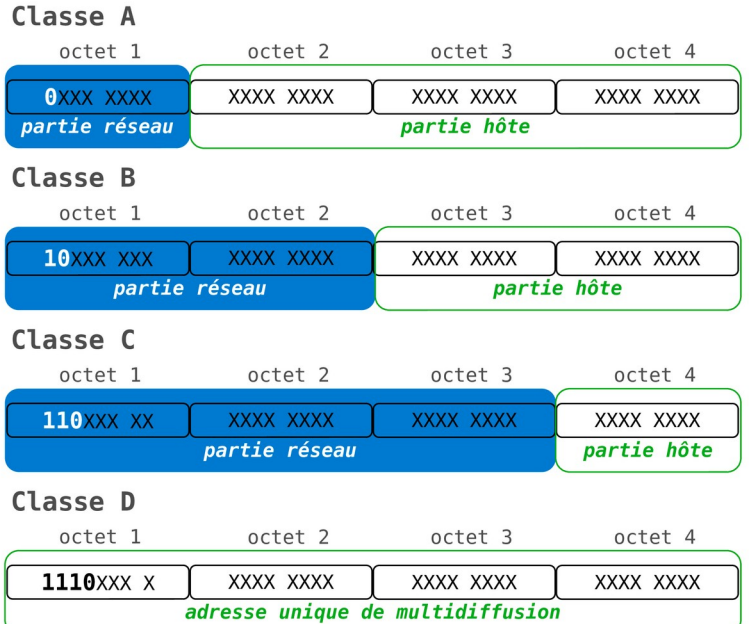
Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;
- Un VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;
- 

us-réseaux selon l'adresse IP
mesure où la configuration des
n contrepartie une légère
contenues dans les paquets

virtuel par type de protocole (par
e même protocole au sein d'un

VLAN : leur to



Plusieurs types de VLAN sont définis, selon le critère de commutation et l

- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-l ports de raccordement sur le commutateur ;
- Un VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adre consiste à définir un réseau virtuel en fonction des adresses MAC des souple que le VLAN par port car le réseau est indépendant de la loca
- Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de nive
  - Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

VLAN : leur topologie

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;
- Un VLAN de niveau 2 (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;
- Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :
  - Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

synthèse

- LAN, VLAN
- @Mac, commutateur = switch

Et maintenant

- Qui distribue les adresses IP ?
  → l'administrateur ou le serveur DHCP *(Dynamic Host Control Protocol)*

Le serveur DHCP

Le serveur DHCP

Le serveur DHCP

DHCP Discovery - Un client DHCP envoie un paquet de diffusion comprenant son nom et son adresse MAC pour trouver un serveur DHCP.

DHCP Offer - Un serveur DHCP répond au DHCP Discovery avec une offre pour une adresse IP disponible.

DHCP Request - Le client DHCP répond ensuite par une DHCP REQUEST pour demander au serveur DHCP l'adresse IP proposée.

DHCP Ack - Le serveur DHCP envoie un DHCP ACK pour informer le client qu'il est autorisé à utiliser l'adresse IP demandée qui lui est attribuée.

Le serveur DHCP

Baux statiques :
Imprimantes, serveurs,…
1@MAC = 1 @IP fixe

Baux DHCP statiques

nom	adresse IP	adresse MAC	
nouveau...			ajouter
[redacted]	IPv4 : [redacted]	00:22:[redacted]	supprimer
[redacted]	IPv4 : [redacted]	00:22:[redacted]	supprimer
[redacted]	IPv4 : [redacted]	00:e3:[redacted]	supprimer
[redacted]	IPv4 : [redacted]	00:19:[redacted]	supprimer
[redacted]	IPv4 : [redacted]	00:11:[redacted]	supprimer
[redacted]	IPv4 : [redacted]	b4:52:[redacted]	supprimer

Vous pouvez visualiser les adresses IP dynamiques attribuées par le serveur DHCP de la Livebox.

Baux dynamiques:
Les PC, les smartphones,…

Baux DHCP valides

nom	adresse IP	adresse MAC
[redacted]	IPv4 : [redacted]	00:11 [redacted]
[redacted]	IPv4 : [redacted]	D8:6C [redacted]
[redacted]	IPv4 :	38:EA [redacted]
[redacted]	IPv4 : [redacted]	00:22 [redacted]
[redacted]	IPv4 :	00:19 [redacted]

synthèse

- LAN, VLAN
- @Mac, commutateur = switch
- Le serveur DHCP

Et maintenant

- Sur le WEB, pourquoi les serveurs web ne sont pas en IP ?
  → les serveurs DNS

Le serveur DNS

Le serveur DNS

Chaque appareil et service sur le World Wide Web possède une adresse IP, par exemple 210.38.33.7. Elles ne sont pas facile à retenir pour les humains. Il n'est pas possible pour l'utilisateur de toujours utiliser l'adresse IP pour accéder à un site. DNS fournit une solution à ce problème en associant un nom de domaine à une adresse IP.

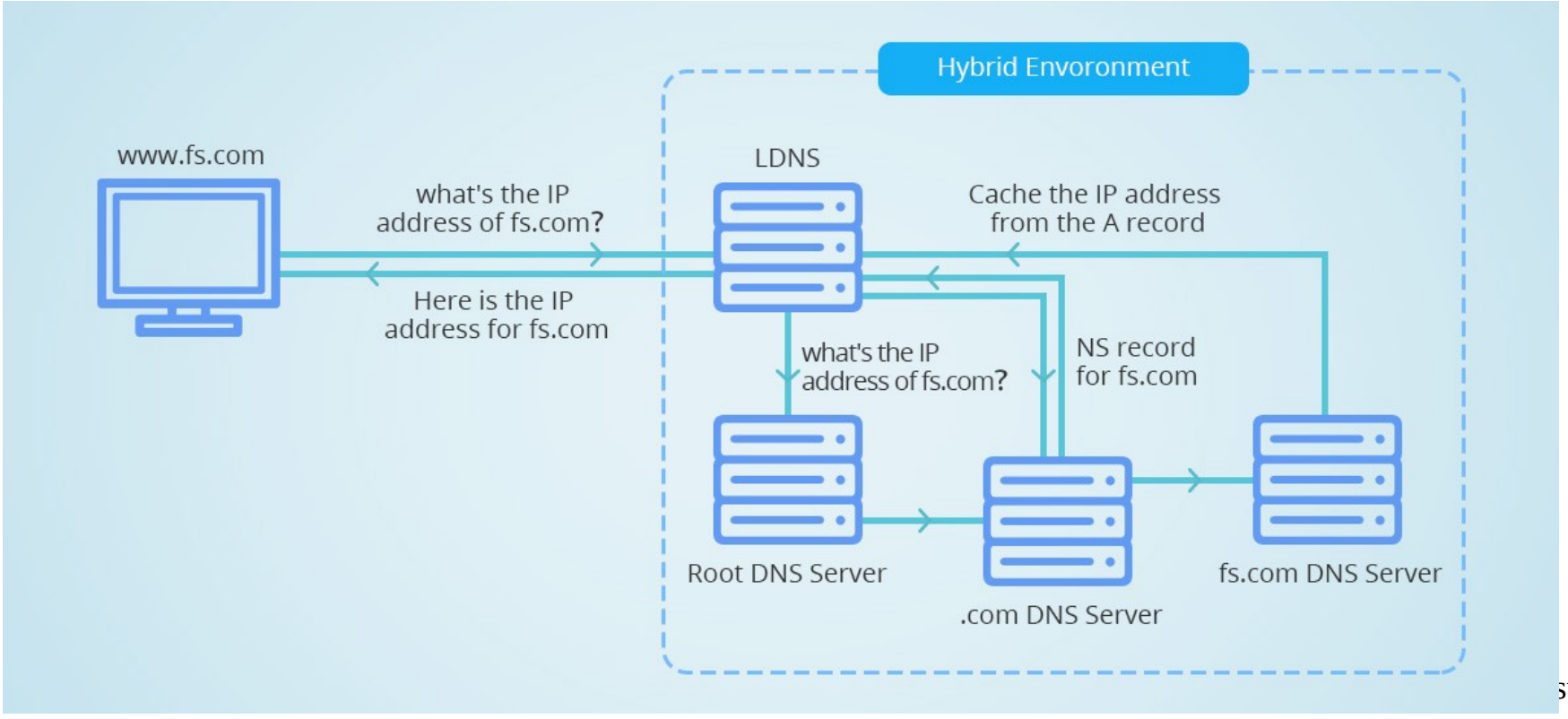
DNS est l'équivalent d'un annuaire téléphonique pour les serveurs connectés à l'internet. Lorsque l'utilisateur saisit un nom de domaine dans le navigateur Web, le serveur DNS mappe le nom de domaine sur l'adresse IP correspondante.

Le serveur DNS

Par exemple, lorsqu'un utilisateur saisit www.fs.com dans l'URL du navigateur Web, le navigateur n'a aucune idée de l'emplacement de www.fs.com, il va donc demander au serveur LDNS (Local DNS Server) l'adresse IP de www.fs.com. Ce dernier va lui répondre 151.101.113.2. Si le LDNS n'a pas d'enregistrement pour www.fs.com, il cherchera sur Internet le propriétaire de www.fs.com. Les procédures opérationnelles sont les suivantes :

- Tout d'abord, le LDNS s’adresse à l'un des serveurs racine qui le dirige vers le serveur DNS .com
- Le serveur DNS .com découvre ensuite le propriétaire de www.fs.com et notifie le LDNS avec un enregistrement de serveur de nom (NS) pour www.fs.com.
- Le LDNS répond en demandant un enregistrement d'Adresse (enregistrement A) qui inclut l'adresse IP pour www.fs.com.
- Après avoir reçu l'enregistrement A, le LDNS enverra l'adresse IP au navigateur et met en cache les informations d'adresse IP pour référence future.

Le serveur DNS



synthèse

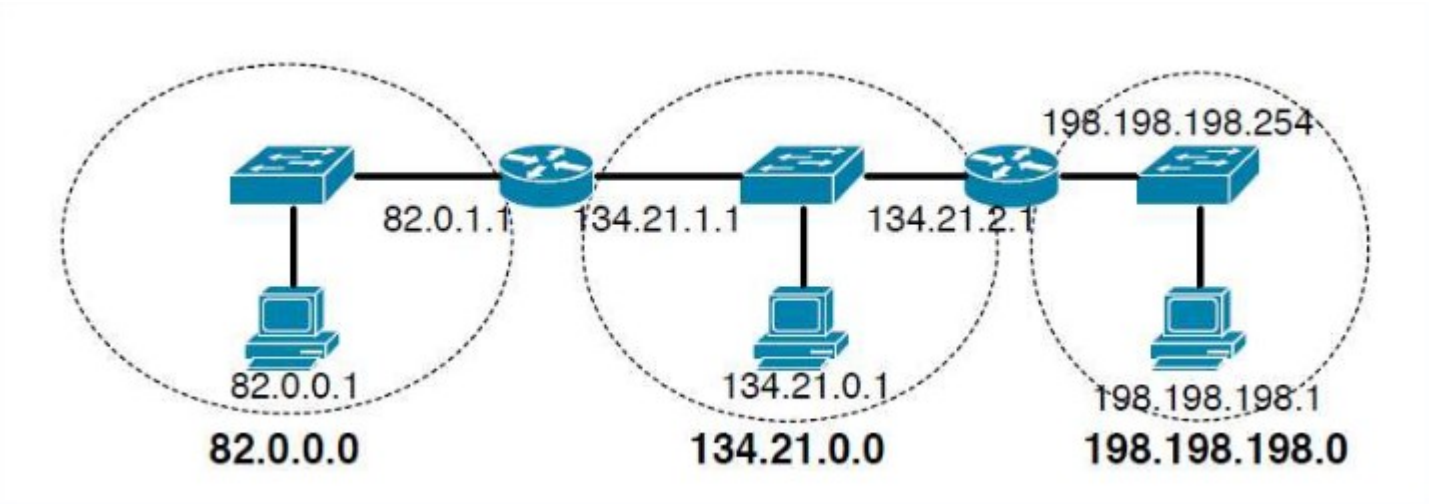
- LAN, VLAN
- @Mac, commutateur = switch
- Le serveur DHCP
- Le serveur DNS

Et maintenant

- Comment les machines (ordinateurs, imprimantes, smartphones,….) connaissent le chemin pour aller d'un PC à un autre à un site Internet ?
  → La table de routage (network address translation : NAT)

La table de routage
Couche 3 du modèle OSI

La table de routage



Il y a 3 switchs et 2 routeurs (routeur en anglais)

- *Un switch est un commutateur : il dirige l'information vers le destinataire : couches 1 & 2*
- *Un routeur fait le lien entres différents réseaux logiques non compatibles : couches 1,2 et 3*
  → Ils ont une table de routage

La table de routage

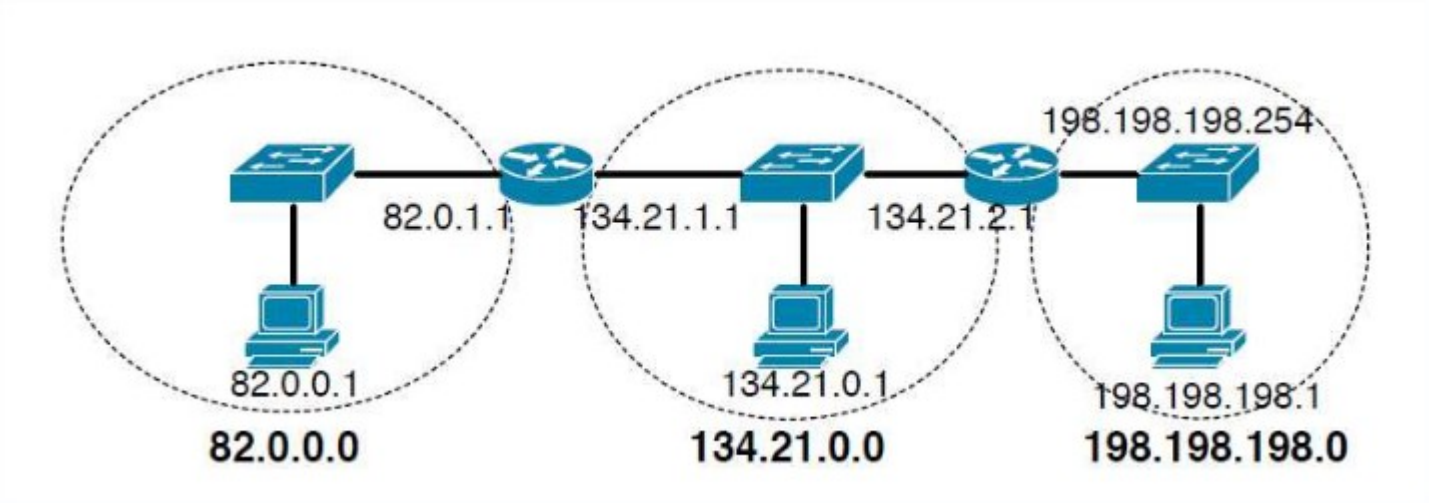


Table de routage du routeur de gauche :

destination	masque	passerelle	interface
82.0.0.0	*255.0.0.0*	*direct*	*82.0.1.1*
134.21.0.0	*255.255.0.0*	*direct*	*134.21.1.1*
198.198.198.0	*255.255.255.0*	*134.21.2.1*	*134.21.1.1*
default	*134.21.2.1*	*134.21.1.1*	

La table de routage

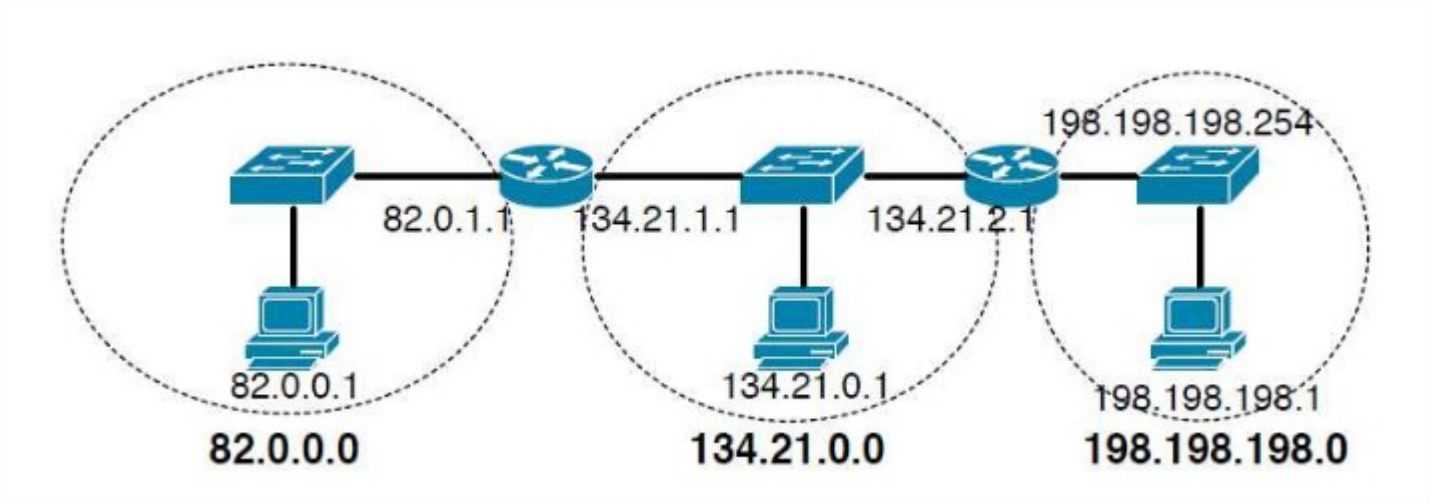


Table de routage du routeur de droite:

destination	masque	passerelle	interface
82.0.0.0	*255.0.0.0*	*134.21.1.1*	*134.21.2.1*
134.21.0.0	*255.255.0.0*	*direct*	*134.21.2.1*
198.198.198.0	*255.255.255.0*	*direct*	*198.198.198.254*
default	*134.21.1.1*	*134.21.2.1*	

La table de routage

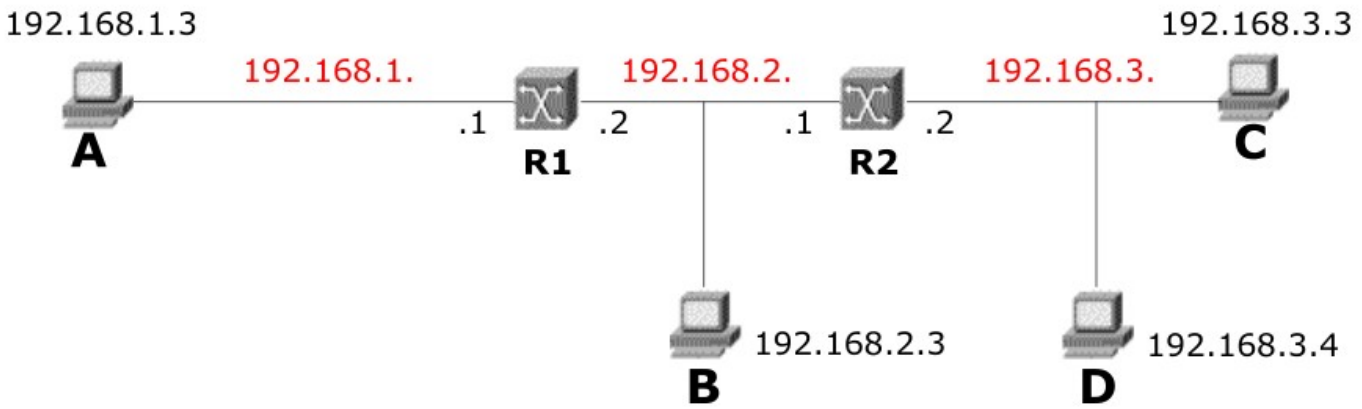


Table de routage de A

Destination	Netmask	Gateway	Interface	Cost
192.168.1.0	255.255.255.0	-	192.168.1.3	0
192.168.2.0	255.255.255.0	192.168.1.1	192.168.1.3	1
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.3	0

La table de routage

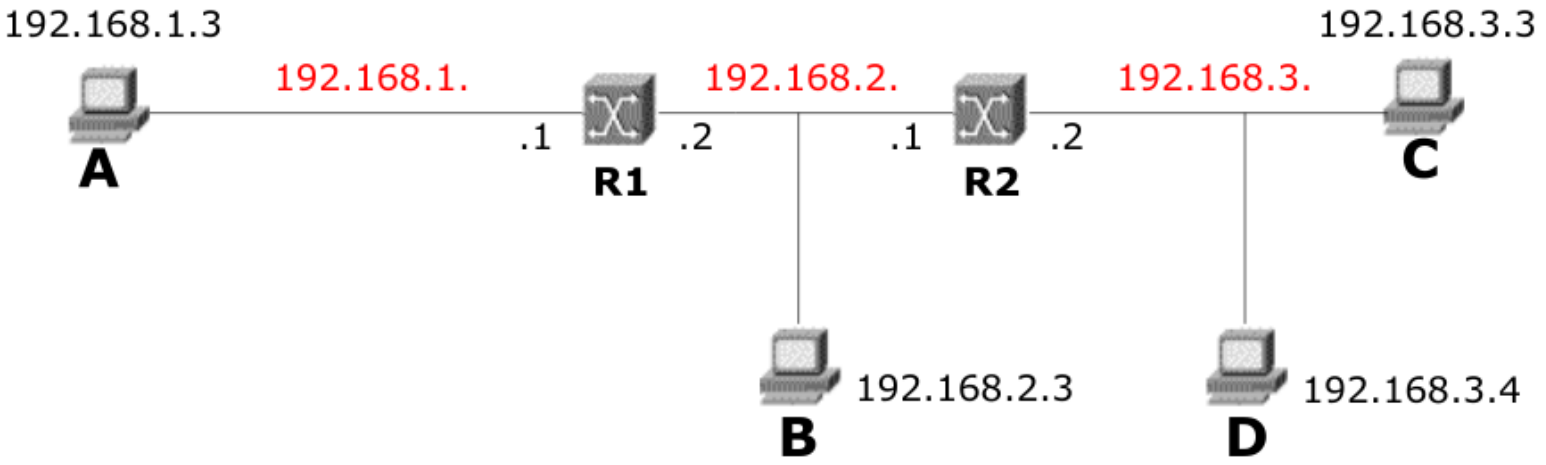


Table de routage de B

Destination	Netmask	Gateway	Interface	Cost
192.168.1.0	255.255.255.0	192.168.2.2	192.168.2.3	1
192.168.3.0	255.255.255.0	192.168.2.1	192.168.2.3	1
192.168.2.0	255.255.255.0	-	192.168.2.3	0

La table de routage

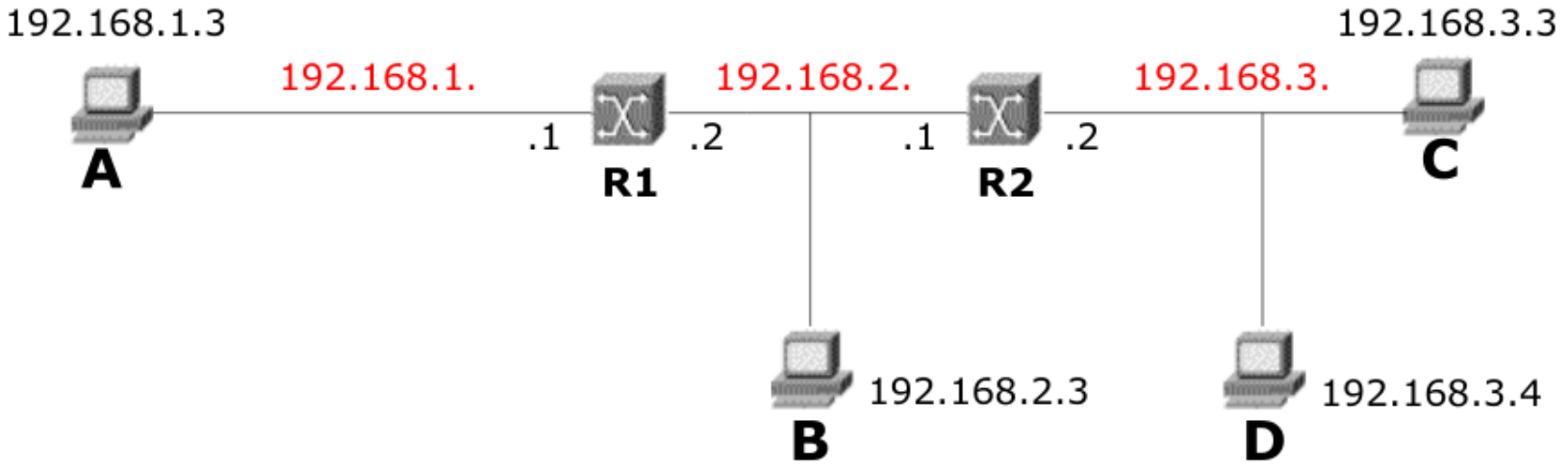
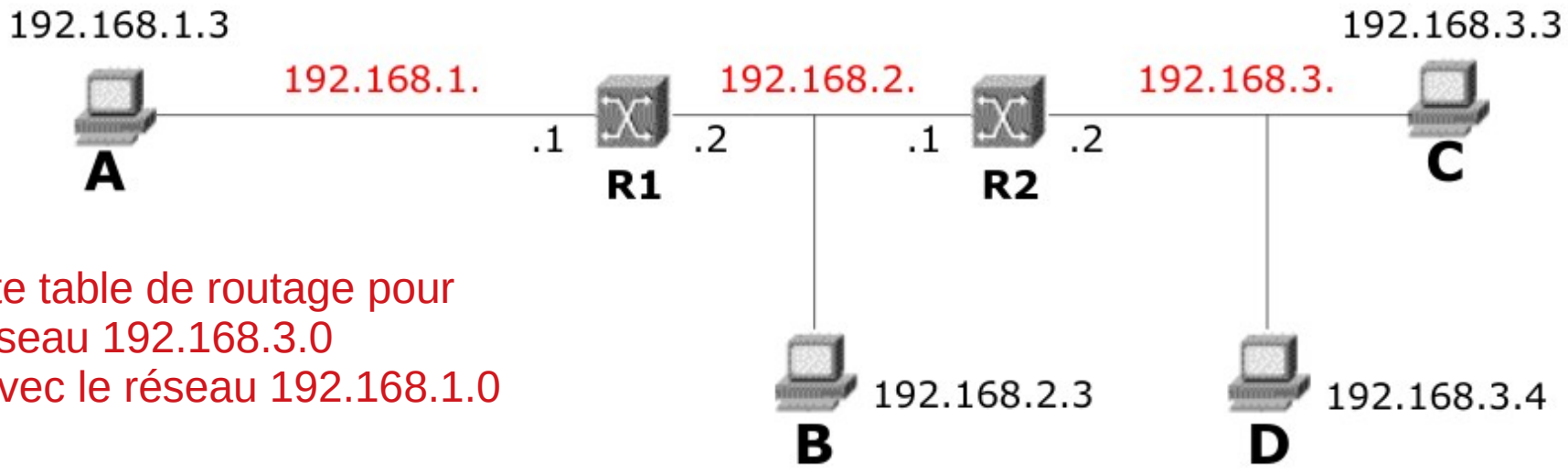


Table de routage de R1

Destination	Netmask	Gateway	Interface	Cost
192.168.1.0	255.255.255.0	-	192.168.1.1	0
192.168.2.0	255.255.255.0	-	192.168.2.2	0
192.168.3.0	255.255.255.0	192.168.2.1	192.168.2.2	1

La table de routage

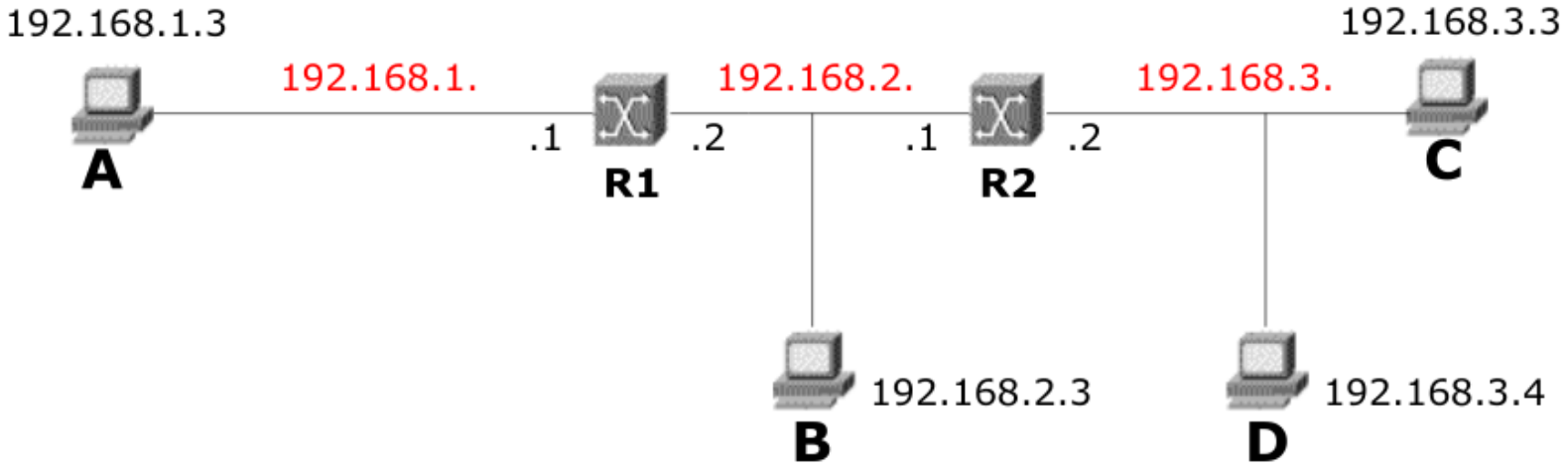


Complétez cette table de routage pour permettre le réseau 192.168.3.0 communique avec le réseau 192.168.1.0

Table de routage de R2

Destination	Netmask	Gateway	Interface	Cost
192.168.2.0	255.255.255.0	-	192.168.2.1	0
192.168.3.0	255.255.255.0	-	192.168.3.2	0

La table de routage



Solution

Table de routage de R2

Destination	Netmask	Gateway	Interface	Cost
192.168.2.0	255.255.255.0	-	192.168.2.1	0
192.168.3.0	255.255.255.0	-	192.168.3.2	0
192.168.1.0	255.255.255.0	192.168.2.2	192.168.2.1	1

La table de routage

Route vers une machine

route add 192.168.0.36 netmask 255.255.255.240 eth0 --------> ajouter

route del 192.168.0.36 netmask 255.255.255.240 eth0 --------> supprimer

Route vers un réseau

route add –net 192.168.0.0 netmask 255.255.255.240 eth0 --------> ajouter

route del –net 192.168.0.0 netmask 255.255.255.240 eth0 --------> supprimer

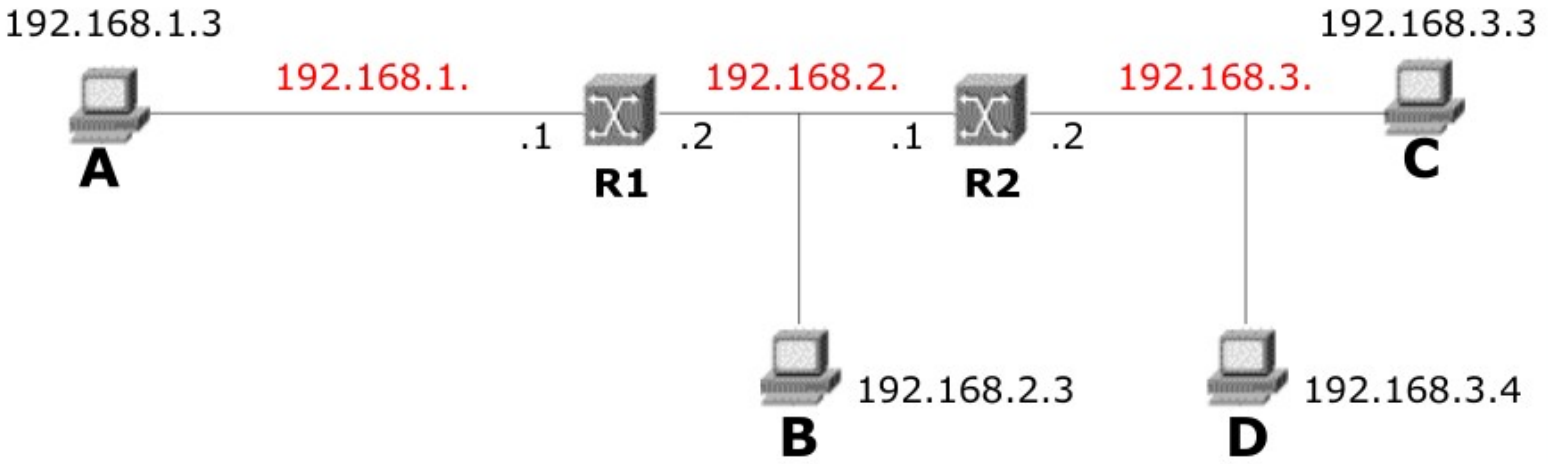
Route vers un réseau via une passerelle

route add –net 192.168.0.0 netmask 255.255.255.240 gw 192.168.0.7 eth0 ---> ajouter

route del –net 192.168.0.0 netmask 255.255.255.240 gw 192.168.0.7 eth0 --> supprimer

La configuration sous linux

La configuration sous Linux



Étape 1 : configuration des IP

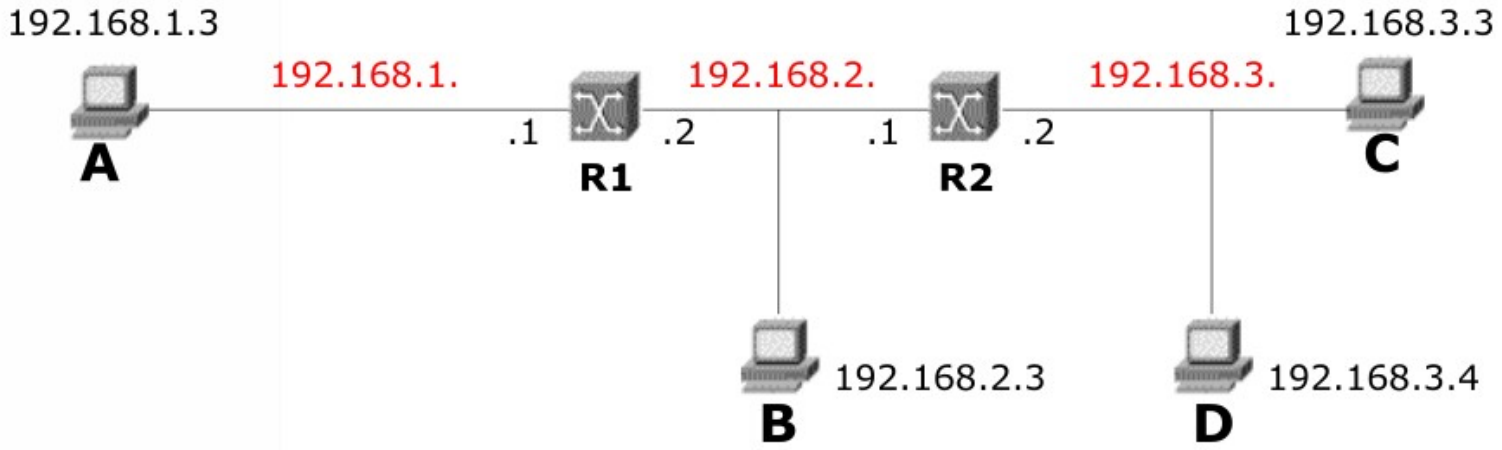
A : ifconfig eth0 192.168.1.3 netmask 255.255.255.0

B : ifconfig eth0 192.168.2.3 netmask 255.255.255.0

C : ifconfig eth0 192.168.3.3 netmask 255.255.255.0

D : ifconfig eth0 192.168.3.4 netmask 255.255.255.0

La configuration sous Linux



Étape 1 : configuration des IP

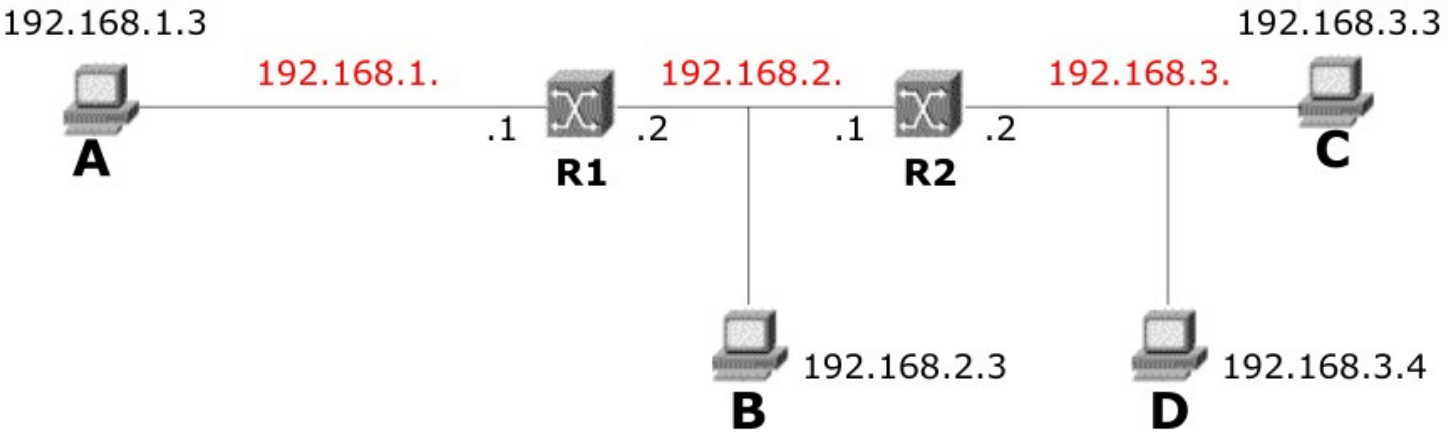
R1 : ifconfig eth0 192.168.1.1 netmask 255.255.255.0

ifconfig eth1 192.168.2.2 netmask 255.255.255.0

R2 : ifconfig eth0 192.168.2.1 netmask 255.255.255.0

ifconfig eth1 192.168.3.2 netmask 255.255.255.0

La configuration sous Linux



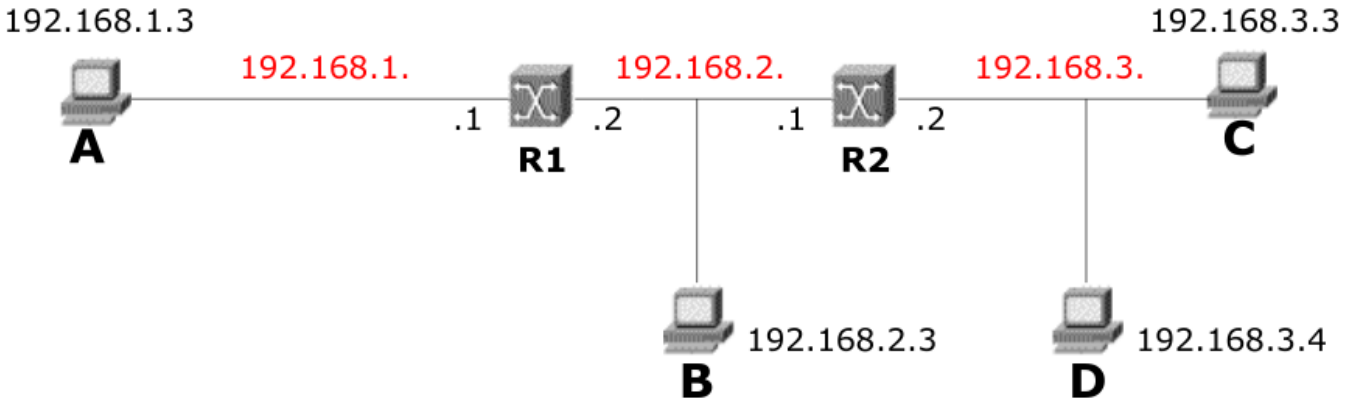
Étape 2 : configuration des tables de routage

A : route add default gw 192.168.1.1

B : route add -net 192.168.3.0 gw 192.168.2.1

route add -net 192.168.1.0 gw 192.168.2.2

La configuration sous Linux



Étape 2 : configuration des tables de routage

R1 : route add -net 192.168.1.0 netmask 255.255.255.0 eth0 eth0 : 192.168.1.1

route add -net 192.168.2.0 netmask 255.255.255.0 eth1 eth1 : 192.168.2.2

route add -net 192.168.3.0 gw 192.168.2.1

R2 : route add -net 192.168.2.0 netmask 255.255.255.0 eth0 eth0 : 192.168.2.1

route add -net 192.168.3.0 netmask 255.255.255.0 eth1 eth1 : 192.168.3.2

Sources :

Lien 1

Lien 2

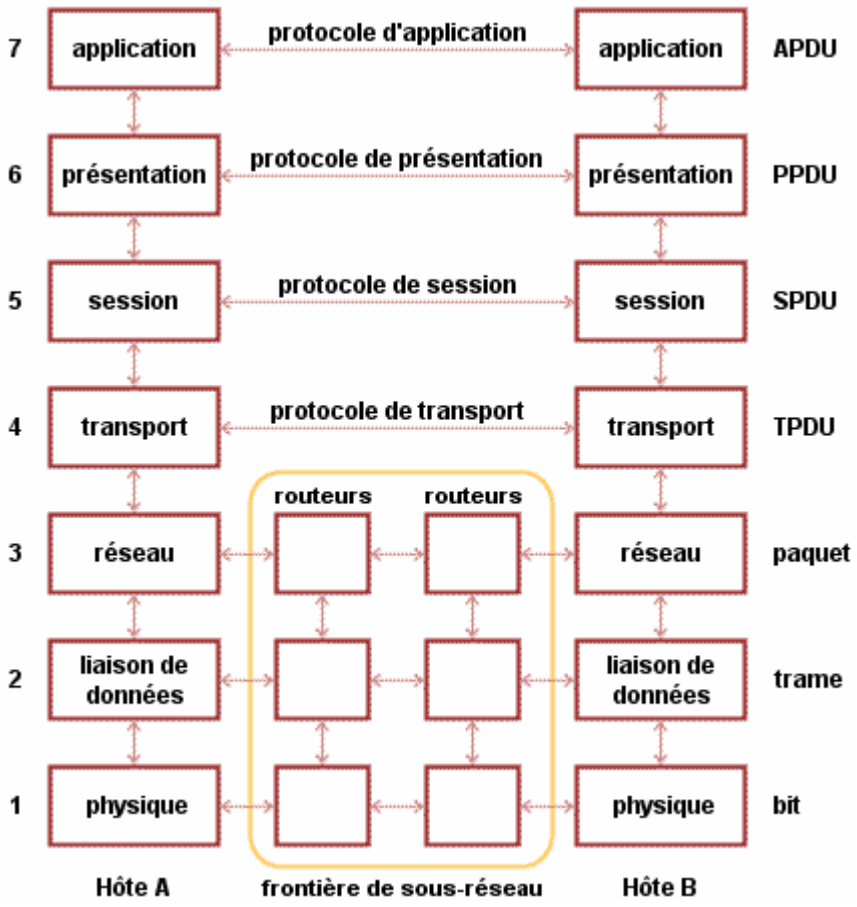
Merci à eux

Allez, on rentre dans le dur ?

Le réseau – niveau 2

Le modèle OSI

Le réseau – niveau 2

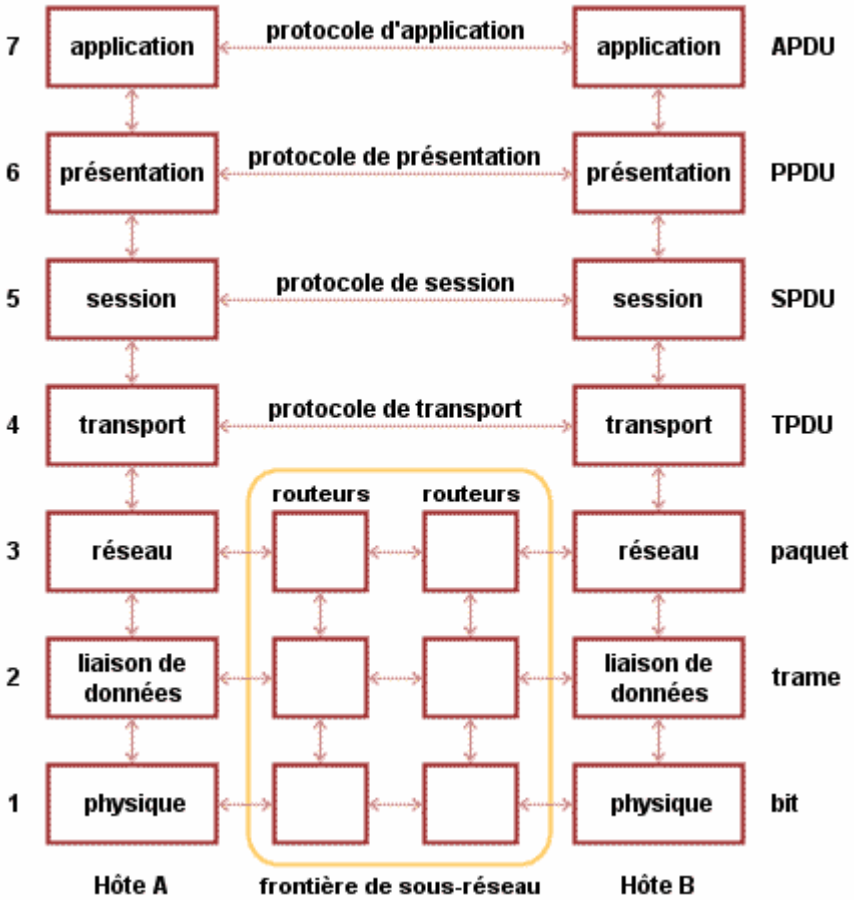


Les principes qui ont conduit à ces 7 couches sont les suivants :

- une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire,
- chaque couche a des fonctions bien définies,
- les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles,
- les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces,
- le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

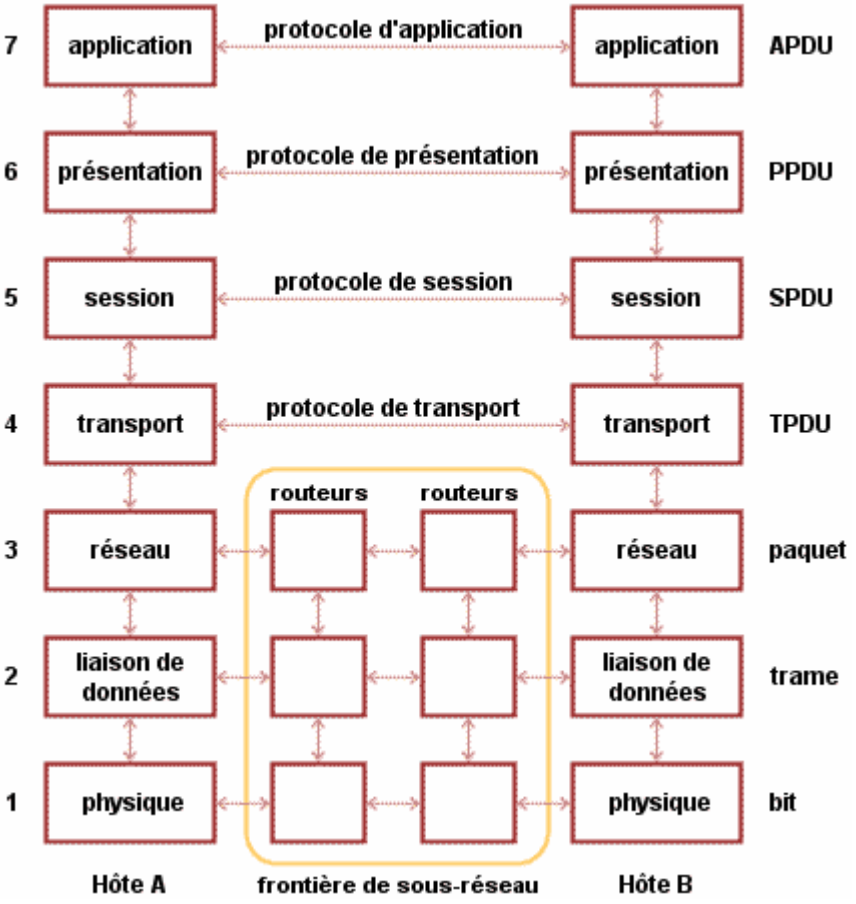
Le réseau – couche 1



La couche **physique** s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie…), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

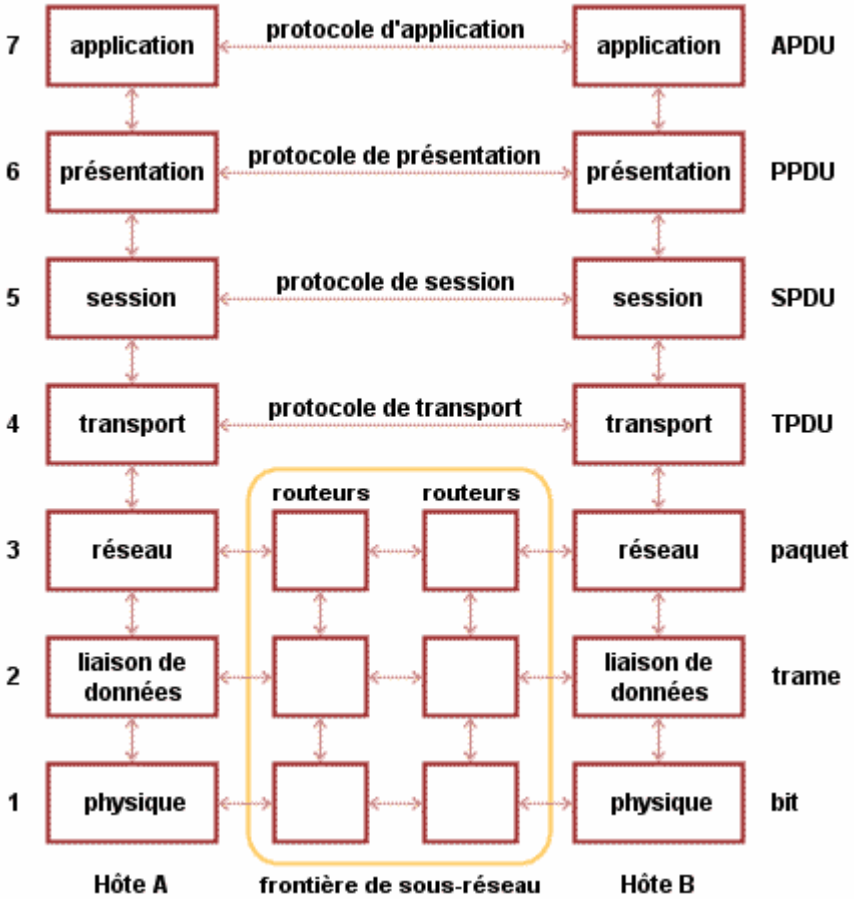
L'unité d'information typique de cette couche est le **bit**, représenté par une certaine différence de potentiel.

Le réseau – couche 1



La couche 1 concerne le support physique de transport des données : Cela peut aller du simple câble transportant un signal électrique, à la fibre optique, en passant par les ondes radio. Le rôle de la couche 1 est donc d'offrir un support de transmission permettant d'acheminer les données d'un point à un autre.

Le réseau – couche 2

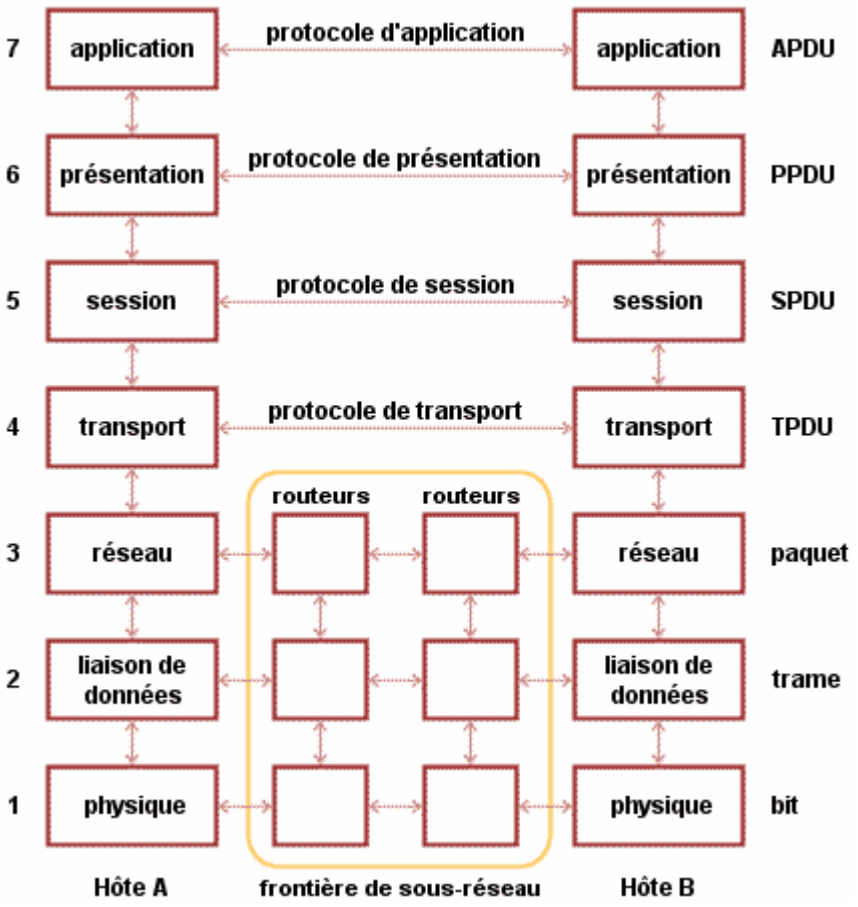


La couche **liaison de données** a un rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la **trame** qui est composées de quelques centaines à quelques milliers d'octets maximum.

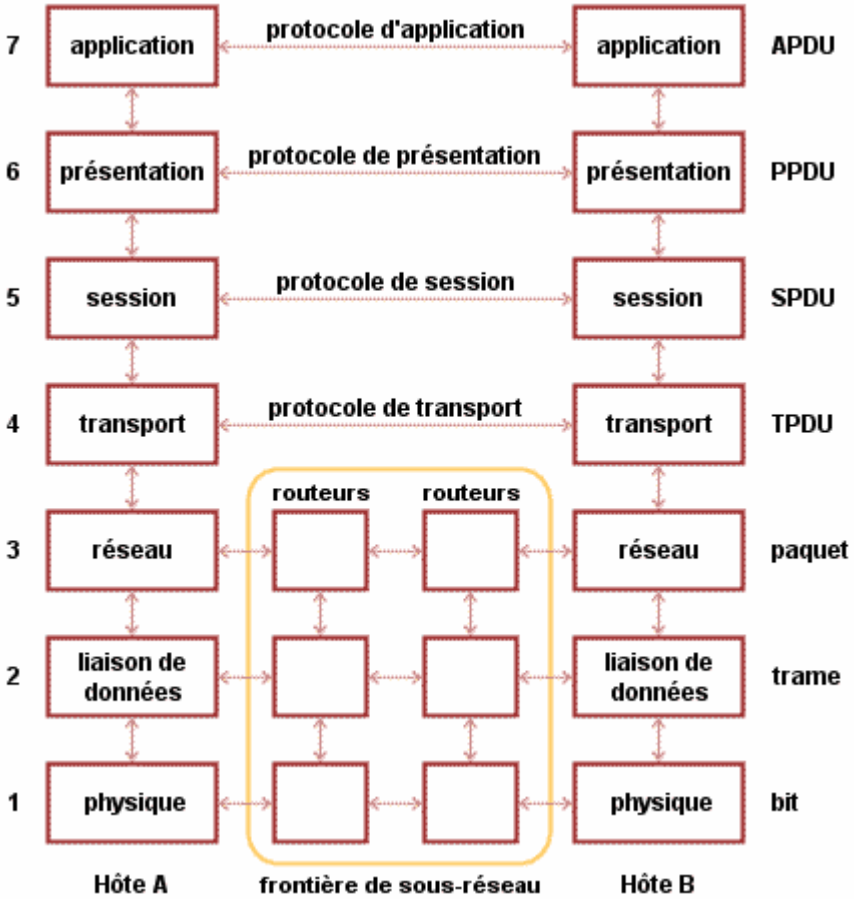
Le réseau – couche 2



Pour la couche 2, pour permettre aux machines de dialoguer, les adresses MAC sont utilisées.
Les adresses MAC sont codées sur 6 octets, soit 48 bits donc 2^{48} = … plusieurs milliers de milliards d'adresses possibles !
Elles sont la plupart du temps écrites par octet sous forme hexadécimale, séparés par le caractère « : » Ce qui donne par exemple 3C:AB:35:48:FF:D2 qui est une adresse MAC. Nous pouvons ainsi identifier chaque interface de machine individuellement. Il nous faut maintenant définir les règles qui permettront aux machines de dialoguer. Pour cela nous allons définir un protocole.
Le message sur la couche 2 est la trame Ethernet :

```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 | @MAC A| @MAC B | protocole supérieur | XXXXX | Bonjour |
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Le réseau – couche 3



La couche **réseau** permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques…).

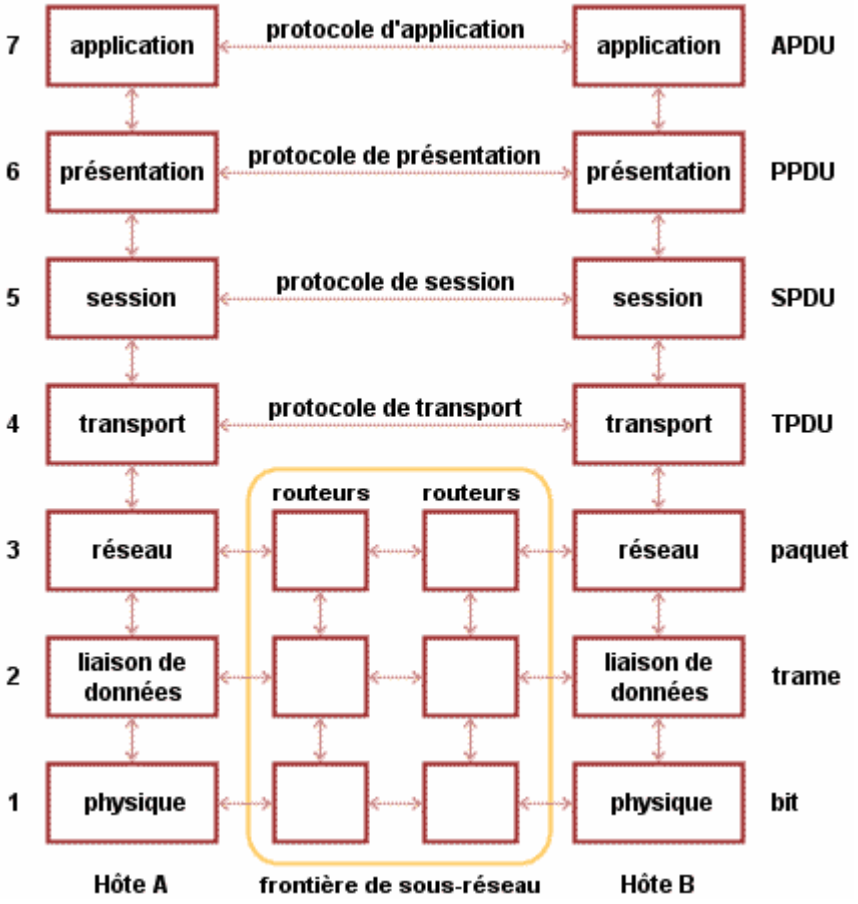
La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.

L'unité d'information de la couche réseau est le **paquet**.

```
Machine A                                                Machine B
     |                                                       |
 ---------- ---------- ---------- ---------- ----------
 |Réseau 1 | Routeur1 | Réseau 2 | Routeur2 | Réseau 3 |
 ---------- ---------- ---------- ---------- ----------
```

NB : ici, les adresses sont des adresses IP
NB' : Il existe des tables de routage…. ;-)

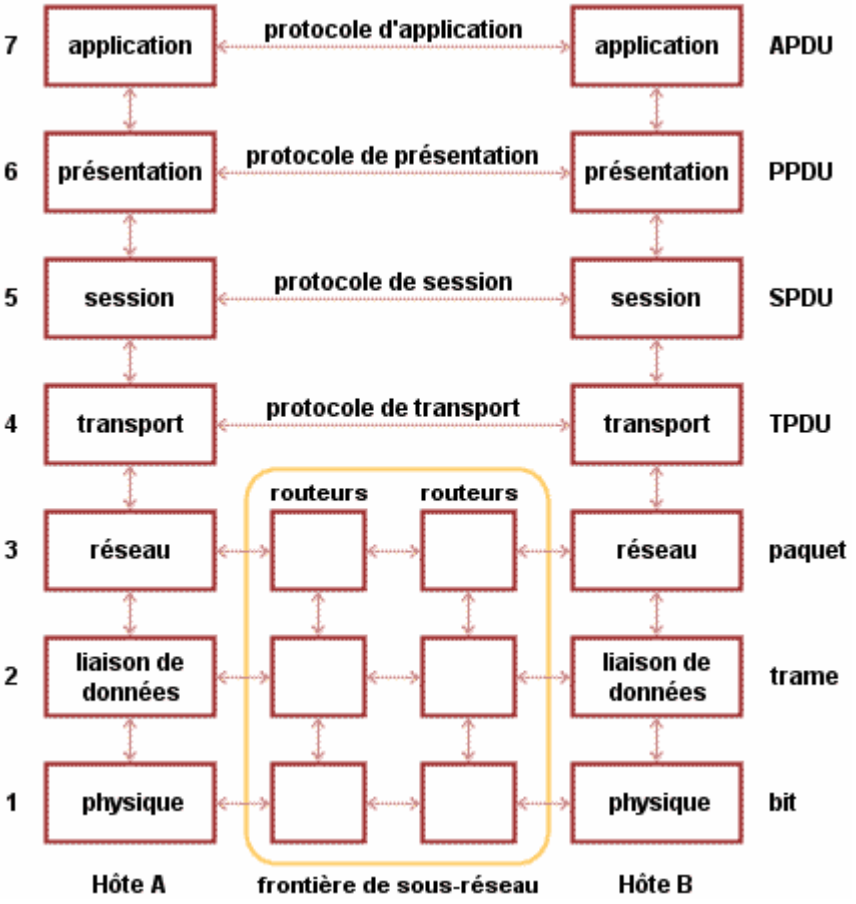
Le réseau – couche 4



La couche **transport** est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

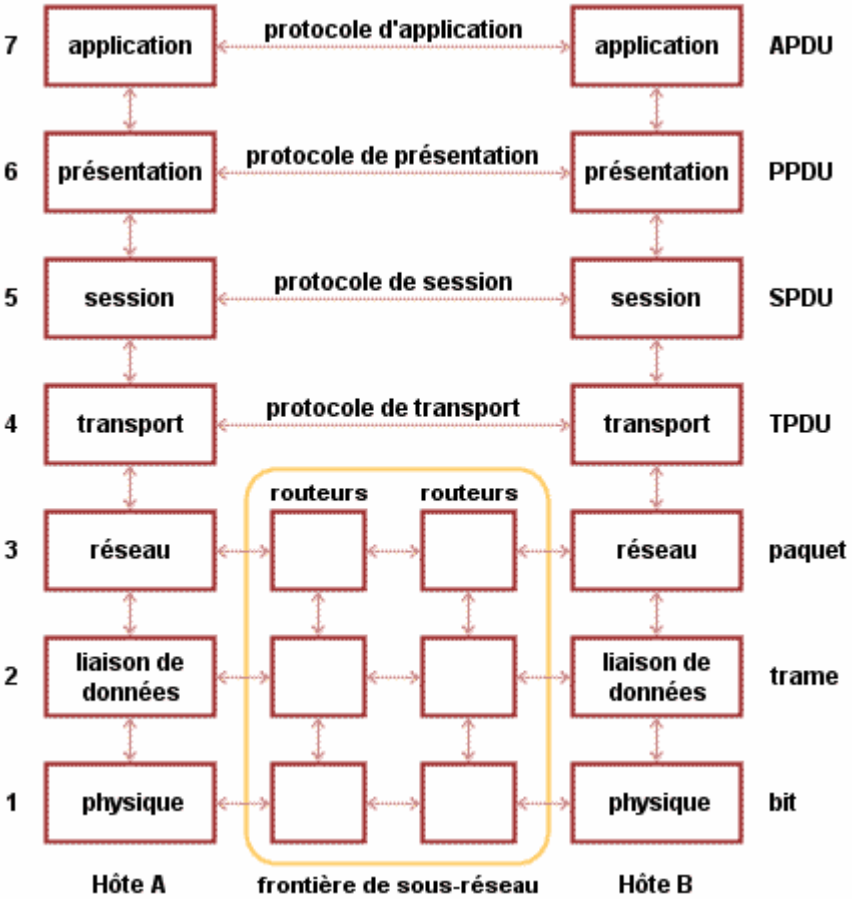
Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Le réseau – couche 4



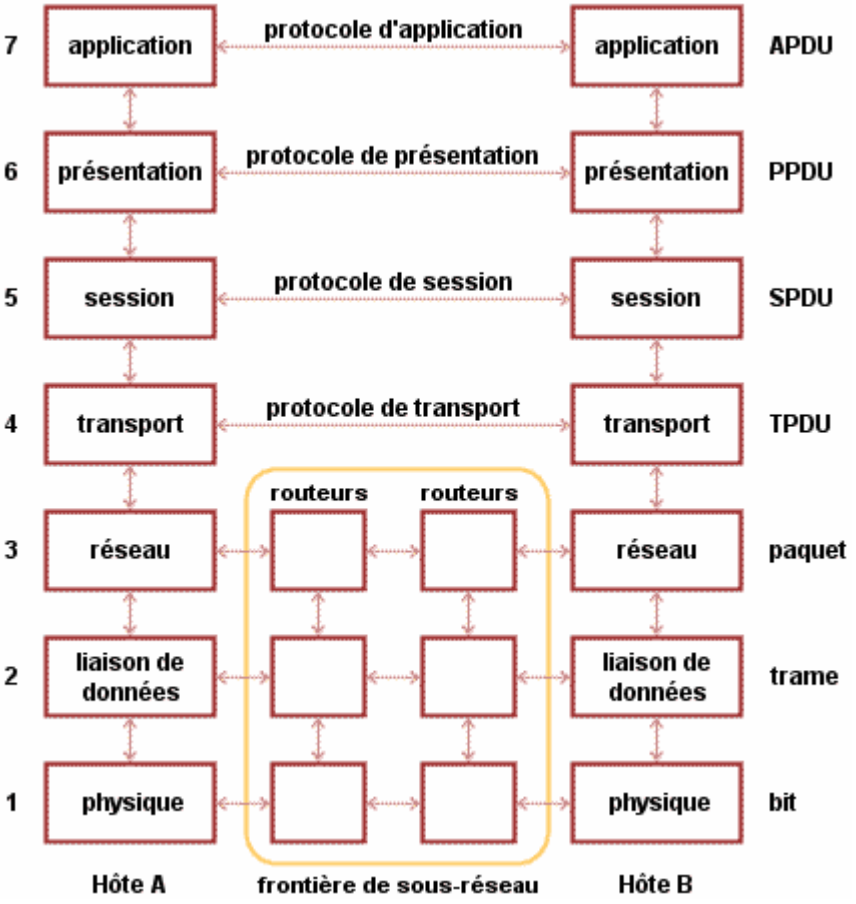
La couche transport est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois… Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau.
Un des tous derniers rôles à évoquer est le contrôle de flux. C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.
L'unité d'information de la couche transport est le **message**.

Le réseau – couche 5



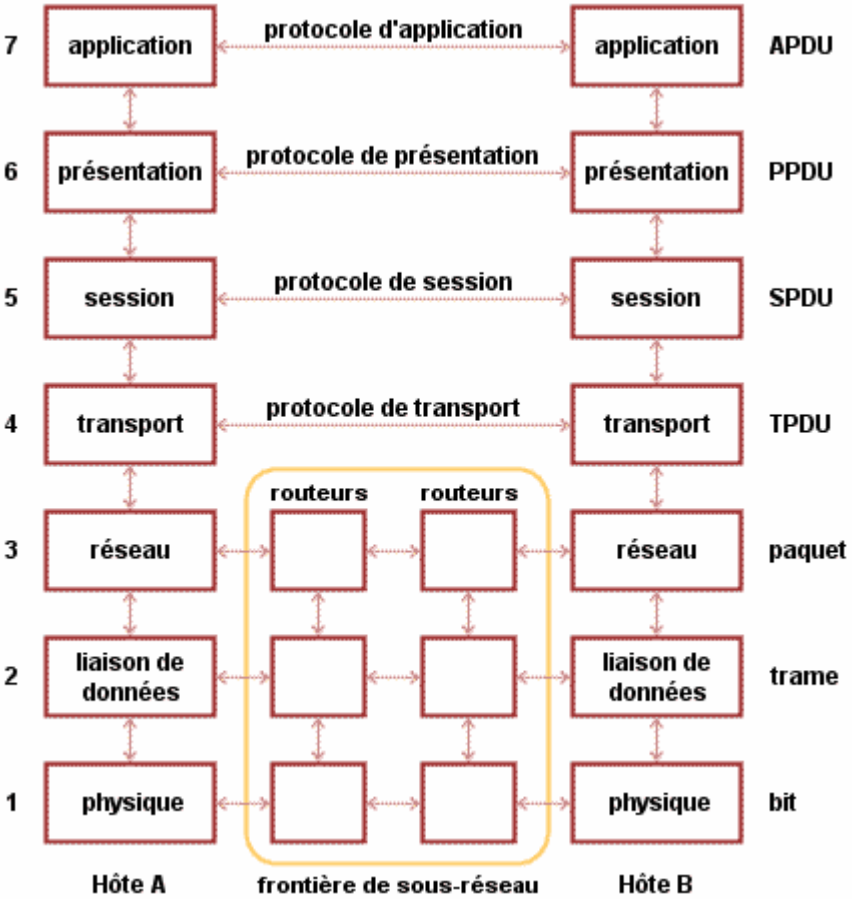
La couche **session** organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle…). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

Le réseau – couche 6



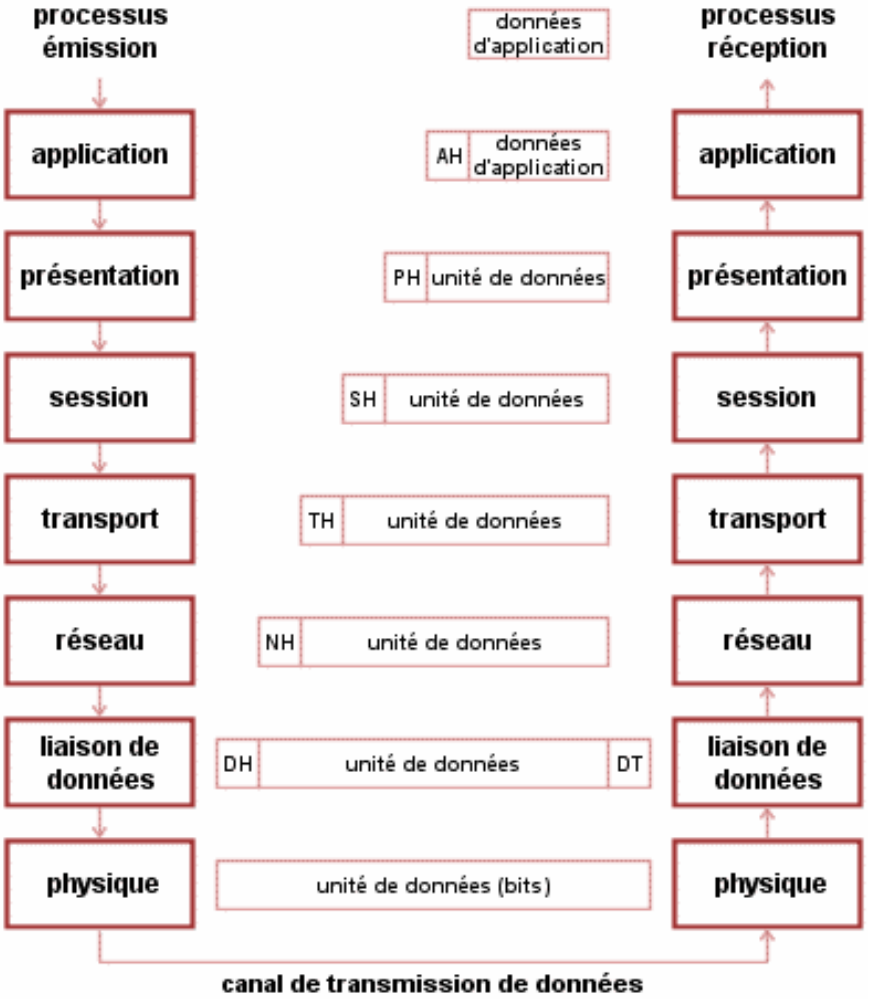
La couche **présentation** s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.
Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

Le réseau – couche 7



La couche **application** est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie

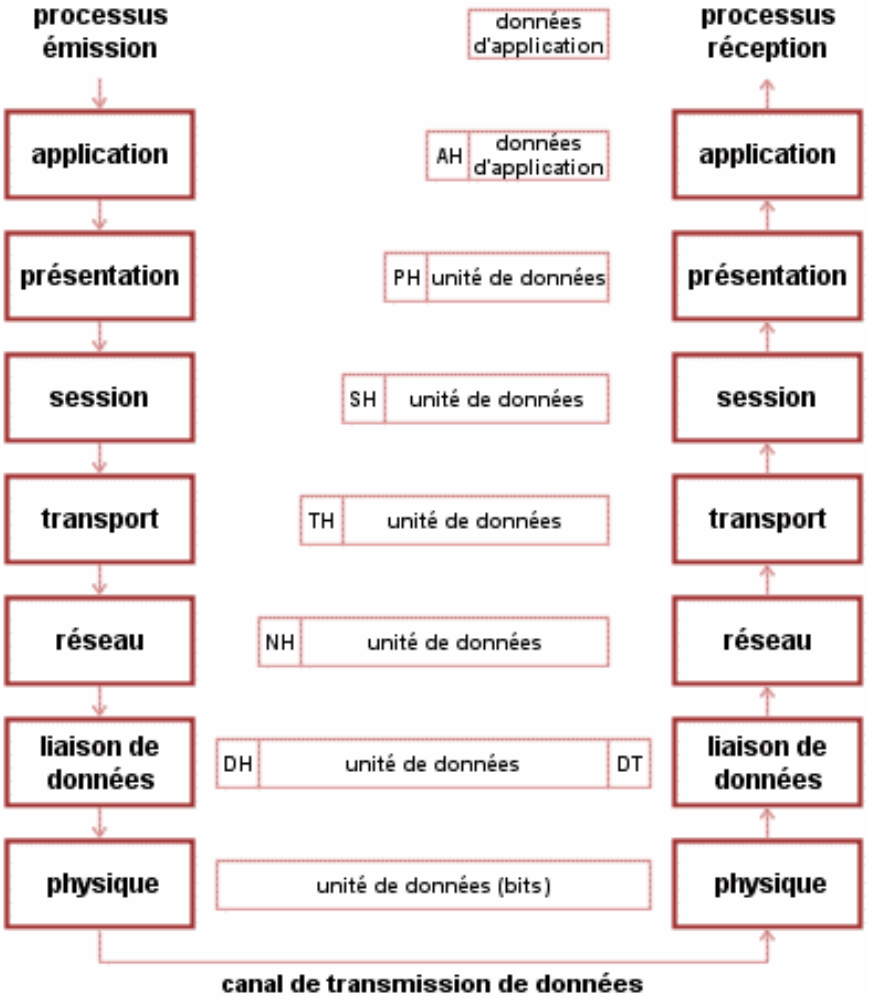
Transmission d’informations



Le processus émetteur remet les données à envoyer au processus récepteur à la couche application qui leur ajoute un entête application AH (éventuellement nul). Le résultat est alors transmis à la couche présentation.
La couche présentation transforme alors ce message et lui ajoute (ou non) un nouvel entête (éventuellement nul). La couche présentation ne connaît et ne doit pas connaître l’existence éventuelle de AH ; pour la couche présentation, AH fait en fait partie des données utilisateur. Une fois le traitement terminé, la couche présentation envoie le nouveau « message » à la couche session et le même processus recommence.

Les données atteignent alors la couche physique qui va effectivement transmettre les données au destinataire. A la réception, le message va remonter les couches et les entêtes sont progressivement retirés jusqu’à atteindre le processus récepteur

Transmission d'informations



Le concept important est le suivant : il faut considérer que chaque couche est programmée comme si elle était vraiment horizontale, c'est à dire qu'elle dialoguait directement avec sa couche paire réceptrice. Au moment de dialoguer avec sa couche paire, chaque couche rajoute un entête et l'envoie (virtuellement, grâce à la couche sous-jacente) à sa couche paire.

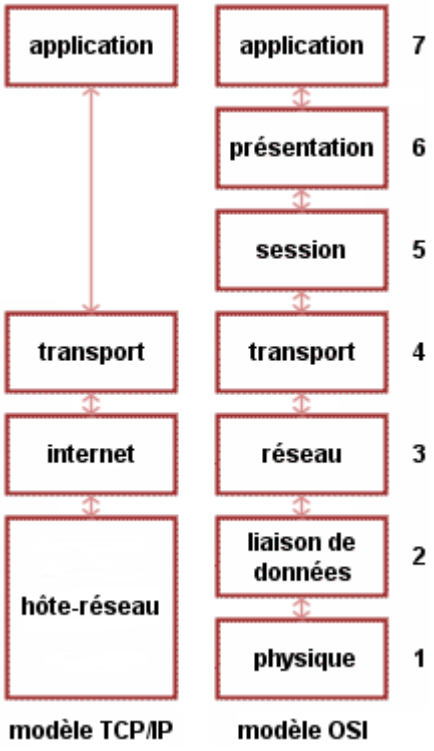
L’avenir du modèle OSI

Au niveau de son utilisation et implémentation, et ce malgré une mise à jour du modèle en 1994, OSI a clairement perdu la guerre face à TCP/IP. Seuls quelques grands constructeurs dominant conservent le modèle mais il est amené à disparaître d’autant plus vite qu’Internet (et donc TCP/IP) explose.

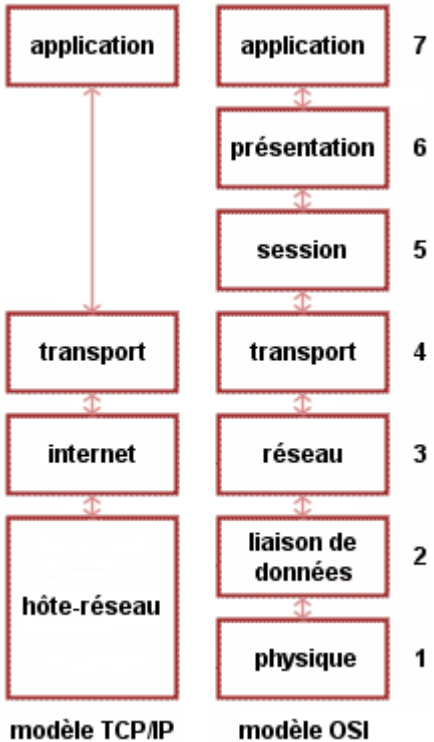
Le modèle OSI restera cependant encore longtemps dans les mémoires pour plusieurs raisons. C’est d’abord l’un des premiers grands efforts en matière de normalisation du monde des réseaux. Les constructeurs ont maintenant tendance à faire avec TCP/IP, mais aussi le WAP, l’UMTS etc. ce qu’il devait faire avec OSI, à savoir proposer des normalisations dès le départ. OSI marquera aussi les mémoires pour une autre raison : même si c’est TCP/IP qui est concrètement utilisé, les gens ont tendance et utilisent OSI comme le modèle réseau de référence actuel. En fait, TCP/IP et OSI ont des structures très proches, et c’est surtout l’effort de normalisation d’OSI qui a imposé cette « confusion » générale entre les 2 modèles. On a communément tendance à considérer TCP/IP comme l’implémentation réelle de OSI.

Le modèle TCP/IP

Le modèle TCP/IP



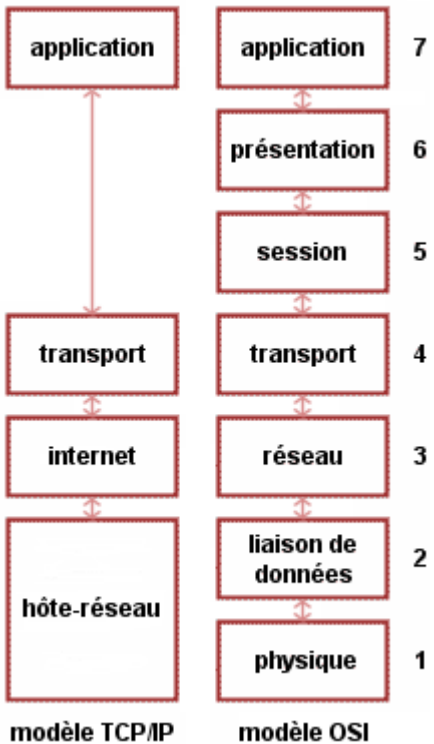
Le modèle TCP/IP



La couche hôte réseau

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

Le modèle TCP/IP

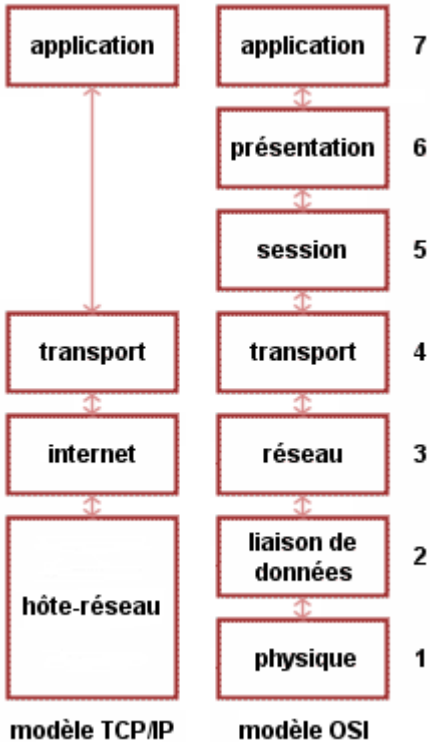


La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. 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.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.
La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

Le modèle TCP/IP

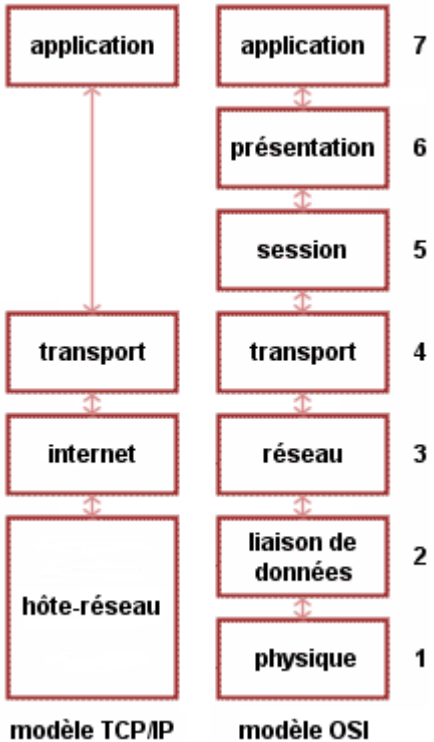


La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).

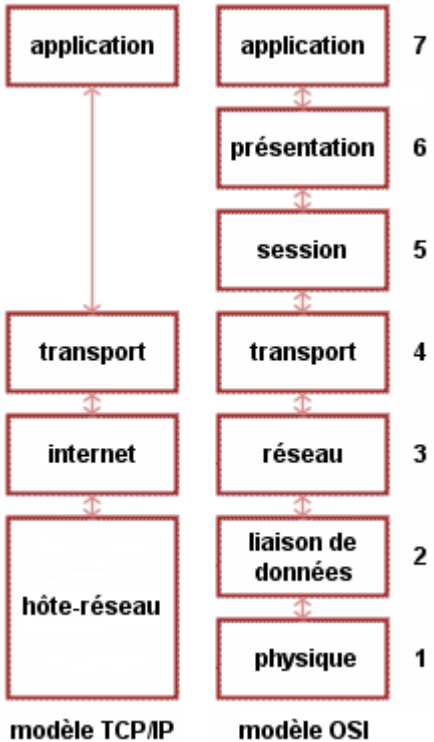
Le modèle TCP/IP



La couche transport

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.

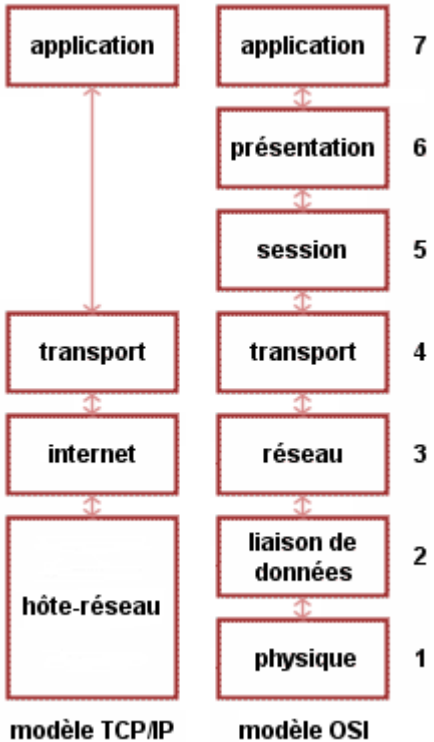
Le modèle TCP/IP



La couche transport

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là une avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

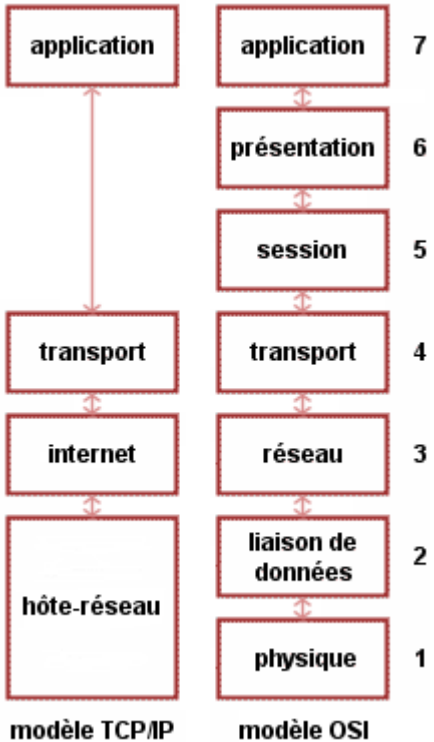
Le modèle TCP/IP



La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Le modèle TCP/IP



La couche application

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.