Architecture des réseaux

1 Réseaux et appareils connectés

Structure du réseau Internet

Un réseau informatique est composé d'appareils interconnectés. Sur le réseau mondial Internet, on distingue :

- , constitués d'appareils connectés à faible distance (exemples : le réseau du lycée, d'un hôpital, d'une entreprise, *etc.* mais aussi le réseau formé chez un particulier par les appareils connectés à une même box);
- , constitué de réseaux locaux distants (de l'ordre du km à plusieurs milliers de km) : le mot Internet désigne communément ce réseau.

Parmi les appareils connectés à un réseau figurent les : ordinateurs personnels (*PC*), consoles de jeu, smartphones, téléviseurs connectés, terminaux de paiement, imprimantes ou scanners (s'ils sont connectés au réseau), lave-vaisselles connectés, *etc.*

Pour assurer les liaisons entre les appareils terminaux, on distingue deux grandes familles d'appareils :

- les , qui assurent la communication entre les appareils connectés à un réseau local ;
- les , qui permettent l'échange de données entre des réseaux locaux distants.

D'autres appareils peuvent aussi intervenir dans la chaîne de transmission des données : satellites de télécommunication, antennes relais, *etc.*

> **Définition**
> Le **point d'accès** d'un appareil à un réseau est appelé
> Il s'agit d'un connecteur physique comme un port RJ45, une puce Wi-Fi, une puce Bluetooth, *etc.*

La communication dans un réseau local

Lors de sa fabrication, un appareil informatique se voit assignée une (*media access control*) qui l'identifie de manière unique parmi tous les autres appareils produits dans le monde.

Par ailleurs, chacune des interfaces d'un appareil connecté à un réseau (LAN ou WAN) se voit attribuée une , manuellement ou par un service telle que DHCP (*Dynamic Host Configuration Protocol*).

Dans un réseau local, afin d'assurer la liaison des données entre les appareils qui lui sont connectés, un commutateur tient à jour une table permettant d'effectuer la **traduction entre adresses IP et adresses MAC**.

Les mises à jour s'effectuent via le protocole ARP (*Address Resolution Protocol*).

Exercice 1 Une adresse MAC est formée de 6 octets, en général présentés sous la forme `XX:XX:XX:XX:XX:XX`, où `XX` désigne l'écriture hexadécimale de chacun des octets.

1. En théorie, quel est le plus grand nombre d'appareils qui pourraient être produits en respectant l'unicité des adresses MAC ?
2. Rapporté à la population mondiale, quel serait la limite moyenne du nombre d'appareils par habitant ?

2 L'adressage IPv4

Une adresse IPv4 (*Internet Protocol version 4*) est composée de 4 octets. et est présentée sous sa forme décimale pointée (les valeurs décimales de chaque octet séparées par des points). Exemple d'adresse IP : `192.168.1.35`.

La commande `ipconfig` (sous Windows) – `ifconfig` sous UNIX – affiche des informations sur les interfaces réseaux d'un ordinateur, dont son adresse IP.

Structure d'une adresse IP

Il est aussi utile de voir une adresse IP comme un nombre entier écrit en binaire sur 32 bits : on a par exemple

`192.168.1.35` $\longleftrightarrow$ `1100 0000 1010 1000 0000 0001 0010 0011`

En effet, un réseau local est identifié par

Par exemple, la notation `192.168.1.5/24` représente la plage d'adresses ci-dessous :

`192.168.1.0`	$\longleftrightarrow$	`1100 0000 1010 1000 0000 0001 0000 0000`
`192.168.1.1`	$\longleftrightarrow$	`1100 0000 1010 1000 0000 0001 0000 0001`
`192.168.1.2`	$\longleftrightarrow$	`1100 0000 1010 1000 0000 0001 0000 0010`
`192.168.1.xxx`	$\longleftrightarrow$	`1100 0000 1010 1000 0000 0001 .... ....`
`192.168.1.255`	$\longleftrightarrow$	`1100 0000 1010 1000 0000 0001 1111 1111`

On remarque que les 24 premiers bits sont fixes (c'est ce qu'indique le `/24` dans la notation de la plage) : ils permettent ainsi d'identifier le réseau, si bien que la première adresse (`192.168.1.0`) constitue **l'adresse du réseau.** Cette adresse est **réservée**, ce qui signifie qu'elle ne peut pas servir à identifier un appareil.

La dernière adresse de la plage (`192.168.1.255`), appelée **adresse de diffusion** (*brodcast*), est également réservée : elle est utilisée pour transmettre des données à tous les appareils connectés au réseau local.

Une adresse IP est donc constituée d'une **partie réseau**, commune à tous les appareils connectés au réseau local, et d'une **partie hôte**, qui permet d'identifier chacun de ces appareils.

`192.168.1.35` $\longleftrightarrow$ $\underbrace{1100\ 0000\ \ 1010\ 1000\ \ 0000\ 0001}_{\text{partie réseau}}\ \underbrace{0010\ 0011}_{\text{partie hôte}}$

Exercice 2

On considère le réseau local `132.20.40.80/28`.

1. Quelle est l'adresse de diffusion de ce réseau ?
2. Combien d'appareils au plus peuvent être simultanément connectés à ce réseau ?

Masque de sous-réseau

Le **masque d'un sous-réseau** (ou masque de réseau local) est un mot de 32 bits constitué d'autant de `1` que de bits fixes dans la partie hôte, suivi par autant de `0` que nécessaires. Par exemple, le masque de sous-réseau associé à la plage `192.168.1.0/24` est le mot

$$\underbrace{1111\ 1111\ \ 1111\ 1111\ \ 1111\ 1111}_{\text{24 bits}}\ \ 0000\ 0000.$$

Traduit en notation décimale pointée, ce masque a pour valeur `255.255.255.0`.

L'intérêt du masque de sous-réseau est qu'il permet de retrouver l'adresse du réseau local connaissant l'adresse IP d'un appareil qui lui est connecté : il suffit en effet pour cela de réaliser un ET logique entre l'adresse IP et le masque de sous-réseau.

adresse	`192.168.1.35`	`1100 0000`	`1010 1000`	`0000 0001`	`0010 0101`
masque	`255.255.255.0`	`1111 1111`	`1111 1111`	`1111 1111`	`0000 0000`
adresse ET masque	`192.168.1.0`	`1100 0000`	`1010 1000`	`0000 0001`	`0000 0000`

Exercice 3

1. Expliquer pourquoi le mot `255.255.255.160` n'est pas un masque de sous-réseau valide.
2. Un appareil a pour adresse IP `212.27.63.116` et pour masque de sous-réseau `255.255.224.0`.
   (a) En pratique, l'adresse IP d'un appareil et son masque de sous-réseau sont donnés conjointement en utilisant la **notation CIDR** : il s'agit de l'adresse IP de l'appareil suivi d'un slash `'/'` et du nombre de bits à `1` du masque de sous réseau. Donner la notation CIDR de l'adresse IP de cet appareil.
   (b) Quelle est l'adresse du réseau local auquel est connecté cet appareil ?
   (c) Quelle est l'adresse de diffusion de ce réseau ?
   (d) Combien d'appareils au plus peuvent être simultanément connectés à ce réseau ?

3 Le routage

Pour être échangées sur un réseau, les informations sont découpées et circulent sous la forme de **paquets** : ils contiennent en plus des données à transmettre (de l'ordre du kilo-octets par paquet) les adresse IP de l'appareil émetteur et de l'appareil destinataire, ainsi que d'autres informations.

Un **routeur** est un équipement connecté à plusieurs réseaux locaux : lorsqu'il reçoit un paquet d'un réseau, il examine sa destination et le transmet vers un autre réseau auquel il est connecté. De proche en proche, les routeurs permettent ainsi d'acheminer des paquets entre appareils distants, à condition toutefois qu'ils soient correctement configurés (manuellement ou en appliquant un protocole de routage) de sorte que le paquet suive une **route** depuis son émetteur jusqu'à son destinataire.

Pour cela, un routeur dispose en mémoire d'une table de routage indiquant pour chaque destination le prochain réseau à emprunter, c'est-à-dire l'adresse IP, appelée **passerelle**, du prochain routeur ou appareil vers lequel émettre les paquets. Une table de routage comporte donc pour chaque destination, les adresses IP de la passerelle et de l'interface associée.

Lorsqu'un routeur reçoit un paquet, il parcourt les lignes de sa table de routage et garantit la correspondance la plus précise entre l'adresse figurant dans la table et l'adresse de destination (*best match*).

Exercice 4

On présente ci-dessous une table de routage (fictive) d'un routeur.

Destination	Passerelle	Interface
`50.0.0.0/24`	`direct`	`50.0.0.3`
`60.0.0.0/24`	`direct`	`60.0.0.3`
`70.0.0.0/24`	`direct`	`70.0.0.3`
`100.0.1.0/24`	`50.0.0.2`	`50.0.0.3`
`100.0.2.0/24`	`60.0.0.2`	`60.0.0.3`
`100.0.10.0/24`	`50.0.0.2`	`50.0.0.3`
`100.0.0.0/16`	`70.0.0.2`	`70.0.0.3`
`110.1.0.0/16`	`50.0.0.2`	`50.0.0.3`
`0.0.0.0/0`	`60.0.0.7`	`60.0.0.3`

1. Quelle destination représente l'adresse IP `0.0.0.0/0` ?
2. À combien de sous-réseaux ce routeur est-il directement connecté ? À combien d'autres routeurs ?
3. Pour chacune des destinations ci-dessous, indiquer la passerelle sélectionnée par le routeur.
   - `100.0.1.39`
   - `100.0.3.39`
   - `110.0.1.39`
   - `50.0.0.39`
   - `100.0.10.39`
   - `110.0.0.39`
   - `110.1.0.39`
   - `50.0.1.39`
4. Représenter graphiquement la topologie du réseau au voisinage de ce routeur.

Exercice 5

En supposant (ce qui est faux) que chaque appareil connecté à Internet possède une adresse IP unique, quel est l'ordre de grandeur du plus grand nombre d'appareils qui pourraient simultanément être connectés à Internet ?

Les réseaux privés

Parmi toutes les adresses IP, certaines plages sont réservées à des usages spécifiques (RFC5735).

La plage `127.0.0.1/8` désigne par exemple la « boucle locale » (*localhost*), permettant à un appareil de se connecter à lui-même (c'est notamment utile pour faire fonctionner un serveur web local).

On trouve également des plages d'adresses privées, par opposition aux adresses publiques d'Internet :

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`

Ces adresse sont utilisées pour créer des réseaux privés, où il n'est pas utile qu'un appareil soit identifié de manière unique mondialement. Les adresses privées ne sont pas routées, ce qui signifie qu'elles sont tout simplement ignorées par les routeurs.

Exercice 6

Déterminer la première et la dernière adresse de chacune des plages d'adresses privées.

Exercice 7

Tout appareil connecté à Internet possède une table de routage. Chez un particulier, la table de routage d'un ordinateur connecté à une box ressemble typiquement à la suivante.

Destination	Passerelle	Interface
`192.168.1.5/32`	`127.0.0.1`	`127.0.0.1`
`127.0.0.0/8`	`127.0.0.1`	`127.0.0.1`
`0.0.0.0/0`	`192.168.1.254`	`192.168.1.5`

1. Quelle est l'adresse IP de cet ordinateur ?
2. Quelle est l'adresse IP de la box sur le réseau local ?
3. Combien d'appareils supplémentaires peuvent être simultanément connectés à la box ?
4. Une personne utilise cet ordinateur pour consulter la page nordvpn.com/fr/what-is-my-ip/ : expliquer pourquoi l'adresse IP affichée est différente.

4 L'architecture client/serveur

De nombreux services sur Internet sont construits selon le modèle client/serveur :

- un logiciel client effectue une demande de données (une **requête**) auprès d'un serveur *via* le réseau ;
- le logiciel serveur attend les requêtes des clients, et leur envoie les données demandées (une **réponse**).

Exemple

Pour le service web, le logiciel serveur s'appelle un serveur web (et par métonymie, ce terme désigne également l'ordinateur sur lequel il est installé).

Le logiciel client web est plus connu sous le nom de

Un même ordinateur peut faire fonctionner simultanément plusieurs logiciels serveurs, grâce aux numéros de ports.

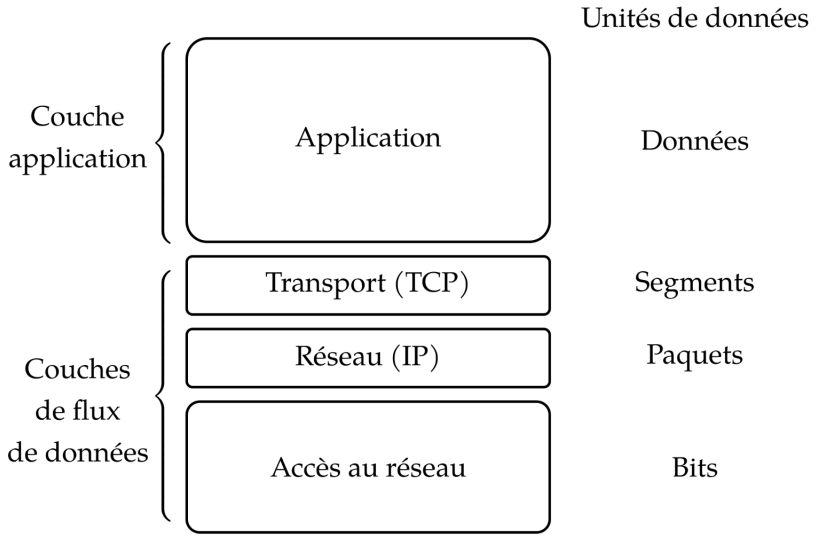
Un logiciel serveur peut également écouter et répondre à plusieurs clients (en gérant des *sockets*).

On peut enfin utiliser simultanément les logiciels serveur et client d'un même service sur un même ordinateur : c'est notamment le cas pour un serveur web local.

5 Le modèle TCP/IP et le modèle OSI

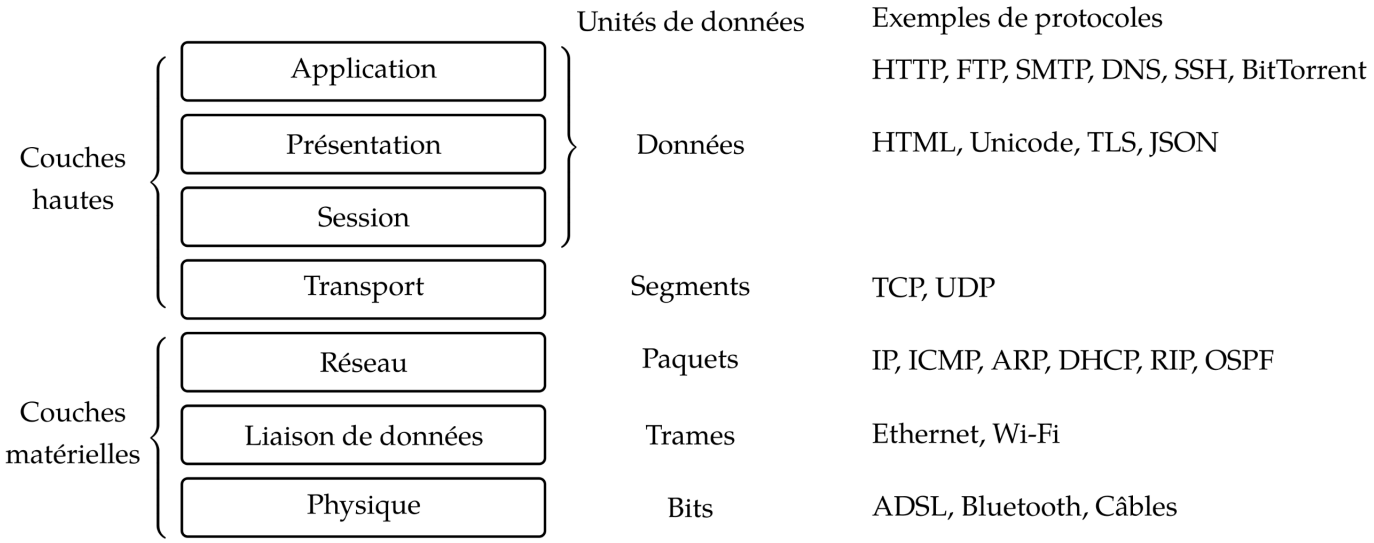
Ces modèles déterminent les règles d'échanges de données sur un réseau (local ou étendu). Il s'appuie sur une représentation verticale où chacune des couches communiquent avec celles directement accessibles.

Le modèle TCP/IP fait jouer un rôle central aux protocoles TCP (*Transmission Control Protocol*) et IP (*Internet Protocol*).



Lors d'un échange de données sur internet, une application (navigateur, serveur web, serveur de courriels, *etc.*) génère les données qui devront parvenir à destination via des protocoles adaptées (HTTP, FTP, SMTP, POP3, DNS, SSH, BitTorrent, *etc.*). La couche de transport, grâce au protocole TCP, a pour fonction de convertir ces données en segments qui seront utilisables par la couche inférieure. La couche de réseau transforme alors les segments en paquets comprenant les informations nécessaires (adresses IP notamment) pour acheminer et reconstituer le message. Enfin la couche d'accès au réseau comprend les protocoles (Ethernet, ADSL, Wi-Fi, *etc.*) permettant la circulation physique des informations (bits).

Le modèle OSI raffine le modèle TCP/IP pour offrir un cadre général permettant la création ultérieure de nouvelles normes et services. Il s'agit d'un modèle abstrait qui ne définit aucun service ou protocole particulier.



6 Exemples de protocoles

- TCP (*Transmission Control Protocol*) : permet de découper des données en segments, et réciproquement. TCP régit l'échange de données entre deux appareils (établissement de la connexion *via Three-way handshake* , transferts de données, fin de la connexion). Il assure une garantie du « meilleur effort » (*best-effort delivery*) : en cas d'erreurs de perte ou de corruption de paquets, TCP demande un nouvel envoi.
- IP (*Internet Protocol*) : permet de traduire des segments en paquets, et réciproquement.
  IP définit notamment l'identification des appareils connectés par le système d'adresses IP (v4 ou v6).
- UDP (*User Datagram Protocol*) : version « simplifiée » de TCP (pas de *handshaking*).
  Plus vulnérable que TCP à la fiabilité du réseau, car fournissant une garantie minimale (seul un contrôle d'erreur est effectué), il est utile pour échanger de petites quantités de données d'un serveur vers de nombreux clients (DHCP), ou pour des applications qui privilégient le temps réel sur les éventuelles pertes de paquets (jeux en ligne, *streaming*, voix sur IP, *etc.*).
- DHCP (*Dynamic Host Configuration Protocol*) : permet d'attribuer automatiquement une adresse IP à un appareil appartenant au réseau local.
- DNS (*Domain Name System*) : permet de traduire les noms de domaines Internet en adresses IP.
- SMTP (*Simple Mail Transfer Protocol*) : permet de transférer un courrier électronique vers un serveur de messagerie.
- POP3 (*Post Office Protocol*) : permet de récupérer les courriers électroniques situés sur un serveur de messagerie.
- IMAP (*Interactive Message Access Protocol*) : permet d'accéder en lecture/écriture directe aux courriers électroniques d'un serveur de messagerie.
- HTTP (*Hypertext Transfer Protocol*) : permet d'accéder à des pages web (sur un serveur web) par l'intermédiaire d'un client web (un navigateur).
- HTTPS (*Hypertext Transfer Protocol Secure*) : combinaison du protocole HTTP avec une couche de chiffrement comme SSL ou TLS. .
- FTP (*File Transfer Protocol*) : permet d'échanger des fichiers d'un appareil vers un autre.
  C'est notamment par ce protocole qu'il est possible de mettre en ligne un site web sur un serveur distant.
- ARP (*Address Resolution Protocol*) : permet de récupérer une adresse MAC à partir d'une adresse IP.
  Les commutateurs (*switch*) construisent automatiquement les tables de correspondance.
- ICMP (*Internet Control Message Protocol*) : permet le contrôle des erreurs de transmission.
  La commande `ping` utilise ce protocole pour tester la connexion avec un appareil distant.

Pour une liste plus complète : Protocoles dans le modèle OSI

7 Exemples de commandes réseau sous UNIX

- `ipconfig` : affiche les paramètres des interfaces réseaux (adresse IP, masque, *etc*).
- `ping` : teste la connexion avec un appareil distant.
- `host` : résout le nom d'un hôte en adresse IP.
- `traceroute` : analyse la route empruntée pour atteindre une destination.
- `route` : affiche la table de routage (utile sur un routeur).
- `arp` : affiche la table de correspondance entre adresse IP et adresse MAC (utile sur un switch).