NSI Première (2019-2020)
Communications 2

Pour communiquer entre elles, les machines utilisent différents protocoles dont fait partie le protocole IP (Internet Protocol). Ce protocole a été conçu en 1968.

Un machine a une adresse numérique codée sur 4 octets, l'adresse IP en version 4, ou codée sur 16 octets, l'adresse IP en version 6.

1 La norme TCP/IP

Elles est définie par les deux protocoles TCP et IP.

La norme TCP/IP permet à un appareil connecté de dialoguer sur tous les réseaux internet.

Le protocole TCP est chargé de la constitution des paquets à partir du contenu d'une requête en respectant une taille limite pour chaque paquet. TCP s'occupe de la partie transport qui doit être assurée entre l'expéditeur et le destinataire. À l'arrivée les paquets sont assemblés par TCP pour reconstituer l'ensemble de la requête.

Le rôle du protocole IP est d'ajouter l'adresse IP source et l'adresse IP destinataire aux données envoyées.

Le protocole Ethernet complète avec les adresses MAC du destinataire et de la source ainsi que le type d'IP (v4 ou v6), (14 octets de plus = 6+6+2).

Une adresse MAC est codée sur 6 octets et est inscrite dans chaque carte réseau équipant un appareil. C'est cette adresse MAC qui permet d'identifier physiquement l'appareil. Le protocole ARP est utilisé pour demander sur le réseau à qui appartient une adresse IP, c'est-à-dire quelle est son adresse MAC.

Le rôle du protocole IP est donc de faire arriver les paquets à la bonne destination en passant les différents supports rencontrés entre l'expéditeur et le destinataire. Grâce à l'adresse IP, à chaque carrefour sur le réseau, les routeurs savent où envoyer les paquets.

2 Adresse IP

L'adresse IP est une adresse numérique permettant d'identifier les appareils connectés à un réseau. Il en existe actuellement deux versions, IPv4 et IPv6.

Adresse IPv4 (version 4).

Elle est composée de 4 nombres entiers séparés par des points, chacun compris entre 0 et 255 inclus. Par exemple 90.8.220.20. Chaque nombre représente un octet (8 bits). Certaines adresses ou plages d'adresses sont réservées et ne peuvent être utilisées. Donc moins de $2^{32} = 4\,294\,967\,296$ adresses peuvent êtres attribuées aux interfaces des hôtes IPv4 (le matériel informatique connecté à un réseau utilisant l'Internet Protocol).

Chaque adresse IPv4 publique, utilisable sur Internet est unique dans le monde. Depuis plusieurs années, ce nombre d'adresses disponibles est devenu insuffisant pour connecter tous les appareils.

Les adresses privées sont ne sont utilisables que sur un réseau local. Ce sont par exemple les adresses commençant par les deux nombres 192.168. La question du nombre d'adresses permettant de satisfaire les besoins ne se pose donc pas dans les mêmes termes.

Afin d'augmenter le nombre d'adresses publiques disponibles, une nouvelle version a été mise en œuvre, avec les adresses IPv6 (version 6).

Adresse IPv6

Le principe est le même que pour les adresses IPv4, mais elles s'écrivent avec 8 nombres entiers séparés par des deux-points, chaque nombre représentant deux octets. L'adresse est donc codée sur un total de 16 octets.

Les deux versions d'adresses sont utilisées actuellement sur Internet.

Le plus souvent on demande une page Web à partir d'un raccourci ou d'un lien, parfois en écrivant le nom comme `python.org` ou `linuxfr.org`.

Voyons comment obtenir l'adresse IP d'un site ou le nom d'hôte à partir d'une adresse IP et quelques informations supplémentaires avec Python. Pour cela, nous utilisons le module `socket`. Le mot *socket* désigne dans ce contexte une interface de connexion qui se situe sous la couche TCP et inclut la couche réseau IP.

```
import socket

print(socket.gethostbyname("python.org"))
print(socket.getaddrinfo("python.org",80,proto=socket.IPPROTO_TCP))
print(socket.getaddrinfo("example.org",80,proto=socket.IPPROTO_TCP))
print(socket.gethostbyaddr("185.75.143.24"))
```

On obtient dans l'ordre l'adresse IPv4 de `python.org`, puis la famille d'adresses de `python.org`, `<AddressFamily.AF_INET: 2>`, avec le 2 pour le type IPv4, ensuite, c'est la famille d'adresses de `example.org` avec la famille IPv6 (type 23) puis IPv4 (type 2), enfin l'hôte ayant pour adresse `185.75.143.24`, il s'agit de `education.gouv.fr`, (on peut deviner le sens de MEN-WEBEDU).

```
45.55.99.72  # adresse IPv4 de python.org

[(<AddressFamily.AF_INET: 2>, 0, 6, '', ('45.55.99.72', 80))]

[(<AddressFamily.AF_INET6: 23>, 0, 6, '',
    ('2606:2800:220:1:248:1893:25c8:1946', 80, 0, 0)),
     (<AddressFamily.AF_INET: 2>, 0, 6, '', ('93.184.216.34', 80))]

('MEN-WEBEDU-PROXY01.dedie.ate.info', [], ['185.75.143.24'])
```

3 Constitution d'une adresse IPv4

Une adresse est constituée de deux parties permettant d'identifier le réseau et l'hôte. On utilise pour cela un masque. Si on donne une adresse 192.168.1.24 et le masque 255.255.255.0, le réseau est alors identifié par 192.168.1.0 et l'hôte par 0.0.0.24.

Il existe plusieurs classes de réseaux d'adresses IPv4. Les adresses des réseaux de classe A ont un premier nombre compris entre 1 et 126, (le premier bit du premier octet est un zéro). Un réseau x peut donc contenir toutes les adresses de x.0.0.0 à x.255.255.255, soit 16 777 216 adresses. On dit que le masque de réseau est 255.0.0.0. Les adresses des réseaux de classes B ont un premier nombre compris entre 128 et 191, (les deux premiers bits du premier octet sont 10), et le masque de réseau est 255.255.0.0. Un réseau x,y peut donc contenir toutes les adresses de x.y.0.0 à x.y.255.255, soit 65 536 adresses. Les adresses des réseaux de classes C ont un premier nombre compris entre 192 et 223, (les trois premiers bits du premier octet sont 110) et le masque de réseau est 255.255.255.0. Un réseau x,y,z peut donc contenir toutes les adresses de x.y.z.0 à x.y.z.255, soit 256 adresses.

Les adresses avec un premier nombre compris entre 224 et 255, (les trois premiers bits du premier octet sont 111), sont réservées à un autre usage (le multicast par exemple, qui n'utilise pas le protocole TCP, et consiste à diffuser vers un groupe de récepteurs).

Un particulier qui possède une connexion à Internet par l'intermédiaire d'une box est sur un réseau de classe C. Par exemple, la box a pour adresse 192.168.1.1, le masque de réseau est 255.255.255.0 et tous les appareils connectés à la box ont une adresse de la forme 192.168.1.a. Donc un ordinateur peut être connecté avec l'adresse 192.168.1.10, un smartphone avec l'adresse 192.168.1.14, une imprimante avec l'adresse 192.168.1.20, etc. Il s'agit ici d'un réseau privé. Si l'un des appareils se connecte à un réseau public comme Internet, il passe par la box, qui sert de passerelle. Celle-ci a une adresse IP assignée par le fournisseur d'accès et c'est cette seule adresse qui est visible depuis Internet et permet à tous les appareils connectés à la box d'y accéder en même temps.

Les classes sont de moins en moins utilisées. Actuellement les réseaux sont subdivisés en sous-réseaux et les notations utilisées permettent d'avoir un découpage plus fin.

Par exemple, la notation 192.168.1.18/27 indique l'adresse IP 192.168.1.18 et précise que les 27 premiers bits constituent l'adresse du sous-réseau, les 5 derniers l'adresse de l'hôte. Le masque s'écrit dont 11111111.11111111.11111111.11100000, soit 255.255.255.224 en notation décimale. L'adresse du sous-réseau est 192.168.1.0, l'adresse de broadcast est 192.168.1.31, c'est celle qui permet d'envoyer des informations à tous les postes du réseau. Il peut donc y avoir 30 machines hôtes d'adresses 192.168.1.1 à 192.168.1.30. L'adresse du sous réseau suivant est 192.168.1.32.

Le Domain Name System, ou DNS est le service informatique distribué utilisé pour traduire les noms de domaines Internet en adresse IP. Par exemple, le nom "example.org" est traduit en 93.184.216.34, l'adresse IP correspondante.

On peut savoir à qui est assignée une adresse IP sur le site `https://www.whois.com/whois/`. Il suffit d'entrer l'adresse 216.58.213.174 et on constate que cette adresse appartient à l'organisation Google qui possède la plage d'adresse de 216.58.192.0 à 216.58.223.255.

Avec le protocole IPv4, c'est en théorie au maximum $2^{32} = 4294967296$ adresses qui peuvent être attribuées simultanément. En pratique, certaines ne sont pas disponibles mais dans tous les cas ce nombre n'est plus suffisant. En 2018, on compte plus de quatre milliard d'internautes dont plus de trois milliards connectés sur des réseaux sociaux.

Les adresses IPv6, plus en plus souvent utilisées, utilisent 16 octets, ce qui permet 2^{128} adresses.

Pour la notation, les octets sont regroupés en 8 groupes de 2 octets séparés par le signe deux-points. Par exemple, l'adresse 2a00 : 1450 : 4007 : 80a : : 200e. Cette adresse est une abréviation de l'adresse 2a00 : 1450 : 4007 : 80a : 0000 : 0000 : 0000 : 200e

4 Architecture d'un réseau

Les machines connectées sur un réseau sont des ordinateurs, des tablettes, des smartphones et tout objet muni d'une carte réseau. Cette carte réseau peut être de type Ethernet avec une prise femelle RJ45, ou de type wifi.

Pour relier ces appareils, les connexions physiques peuvent être câblées ou bien réalisées par la technologie sans fil. Les connexions par câbles utilisent très souvent des câbles Ethernet munis de prises RJ45 mâles branchées sur les cartes réseaux des appareils.

Des appareils peuvent être connectés en pair-à-pair (ou peer-to-peer). Dans ce cas, un appareil traite d'égal à égal avec un autre appareil. Les deux sont à la fois demandeurs et distributeurs de données. Ils sont en même temps client et serveur. Une utilisation courante de ce type de réseaux est le partage de fichiers.

Un autre type de réseaux est le type client-serveur : des appareils uniquement clients envoient des requêtes ou demandes de ressources, des appareils uniquement serveurs répondent à ces requêtes et envoient les ressources demandées.

Du point de vue de la topologie, la mise en œuvre peut se faire par un réseau en bus (une ligne de communication unique est partagée par tous les appareils), en étoile (les appareils sont reliés à un élément central), en anneau, en arbre (réseau réparti sur plusieurs niveaux).

Dans le cas de réseaux wifi, un concentrateur wifi permet de connecter ensemble plusieurs appareils. Dans le cas de réseaux filaires, il est possible d'utiliser un hub, un switch ou un routeur. Suivant le nombre

d'ordinateurs, si par exemple un switch ne suffit pas, on peut en utiliser plusieurs reliés entre eux, chacun étant relié à plusieurs appareils.

Un switch, ou commutateur réseau, permet de connecter plusieurs appareils entre eux en différenciant chaque appareil. Il n'envoie à chacun que les données qui le concerne. Pour cela, tous les appareils qui se sont connectés au switch lui ont laissé leur adresse (adresse MAC et port).

Un routeur peut être connecté à différent réseaux et différencie chaque appareil connecté. Il permet de faire transiter un paquet entre deux interfaces réseaux. C'est par exemple une box internet chez un particulier où elle attribue une adresse locale à chaque appareil du réseau local connecté à la box par câble Ethernet ou wifi et assure la connexion au réseau internet.

Chez un particulier, un ordinateur est connecté à une box louée gracieusement par un FAI (fournisseur d'accès internet). D'autres appareils le sont également. Les appareils et la box forment un réseau local et chaque machine a une adresse IP. La box a par exemple l'adresse 192.168.1.1, et elle affecte des adresses à tous les appareils connectés, dans une certaine plage, avec un masque de sous-réseau 255.255.255.0. Les adresses dynamiques sont attribuées par un serveur DHCP à un ordinateur portable 192.168.1.12, un smartphone 192.168.1.19, une imprimante 192.168.1.14, un décodeur pour la télévision 192.168.1.13 connecté par câble Ethernet. Des adresses peuvent être aussi fixées manuellement. La box est relié physiquement au réseau internet par un câble DSL ou Fibre optique. Elle a enregistré des adresses de serveurs DNS qui sont proposées aux demandes des appareils.

Il est aussi possible de réaliser des simulations de réseaux à l'aide de logiciels. On trouve par exemple le logiciel Filius à cette adresse `http://www.lernsoftware-filius.de/Herunterladen`.

5 Ligne de commande

Quelques commandes réseaux sont utiles.

La commande `ipconfig` sous Windows nous donne le statut de notre connexion : notre adresse IP (v4 ou v6), le masque de sous-réseau, l'adresse de la passerelle (la box à laquelle nous sommes connectés). Dans un terminal Linux, la commande est `ifconfig` ou `ip a`. La commande `ip -4 a` fournit l'adresse IPv4 sous la forme 192.168.1.13/24 et l'adresse de broadcast 192.168.1.255. C'est la même forme pour les adresses IPv6 avec `ip -6 a`.

La commande `ping`, pour Packet INternet Groper, est disponible dans un terminal avec Linux ou dans l'invite de commande avec Windows.

Cette commande envoie des paquets à un destinataire et mesure le temps écoulé entre l'envoi et la réponse.

Exemple dans l'invite de commande avec Windows :

```
C:\Users\Toto>ping education.gouv.fr

Envoi d'un requêtre 'ping' sur education.gouv.fr [185.75.143.24]
avec 32 octets de données
Réponse de 185.75.143.24 : octets=32 temps=20 ms TTL=53
Réponse de 185.75.143.24 : octets=32 temps=20 ms TTL=53
Réponse de 185.75.143.24 : octets=32 temps=20 ms TTL=53
Réponse de 185.75.143.24 : octets=32 temps=20 ms TTL=53

Statistiques Ping pour 185.75.143.24:
    Paquets : envoyés 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 20ms, Maximum = 22ms, Moyenne = 20ms
```

Nous sommes renseignés sur l'adresse IPv4 ou IPv6, la durée de vie TTL, le pourcentage de paquets perdus, la durée moyenne du temps écoulé de l'envoi à la réponse.

La durée de vie est le nombre maximal de routeurs par lesquels la demande peut encore transiter. Par défaut elle est de 64 au début. Une valeur affichée de 53 nous permet donc de connaître le nombre de routeurs traversés par un paquet, soit 11.

La commande `tracert` permet de trouver l'itinéraire suivi entre l'émetteur et le récepteur, un peu comme l'itinéraire de voyageurs qui transitent par des escales avec même point de départ et même point d'arrivée. Elle précise les adresses IP et les noms de domaines des points de passage.

```
C:\Users\Toto>tracert education.gouv.fr

Détermination de l'itinéraire vers education.gouv.fr [185.75.143.24]
avec un maximum de 30 sauts :

1    1 ms    <1 ms    <1 ms lan.home [192.168.1.1]
2    3 ms    3 ms    5 ms 80.10.235.253
...
```

La première ligne de réponse montre la connexion à la box, la deuxième ligne est l'adresse IP du premier routeur après la box auquel la ligne est rattachée. Nous vérifions que cette adresse appartient à France Télécom, sur le site `https://www.whois.com/whois/`. Nous observons ensuite des passages par Marseille, Paris, Londres, etc.

Sur le site `https://www.ripe.net/`, (RIPE signifie Réseaux IP Européens), on entre l'adresse 80.10.235.253 et on obtient la réponse suivante :

Responsible organisation : Orange S.A. Abuse contact info : gestionip.ft@orange.com

inetnum : 80.10.232.0 - 80.10.239.255 netname : IP2000-ADSL-BAS descr : FBN country : FR admin-c : PG5119-RIPE tech-c : PG5119-RIPE status : ASSIGNED PA mnt-by : FT-BRX created : 2014-09-16T14 :12 :38Z last-modified : 2014-09-16T14 :12 :38Z source : RIPE

Sur le site `https://www.whois.com/whois/`, on obtient les informations suivantes :

domain : orange.fr status : ACTIVE hold : NO holder-c : O7771-FRNIC admin-c : BLF95-FRNIC tech-c : SNDD100-FRNIC zone-c : NFC1-FRNIC nsl-id : NSL52444-FRNIC registrar : ORANGE Expiry Date : 2019-10-14T15 :12 :55Z created : 2001-02-01T23 :00 :00Z last-update : 2018-10-14T15 :34 :22Z source : FRNIC

ns-list : NSL52444-FRNIC nserver : ns1.orange.fr [80.10.201.224 2a01 :cb04 :2040 :2 : :1] nserver : ns2.orange.fr [80.10.202.224 2a01 :cb14 :2040 : :1] source : FRNIC