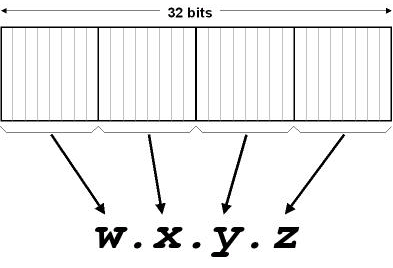
**Introduction à la réseautique IPv4**

|  |  |  |
| --- | --- | --- |
| **Internet** | **Intranet** | **Extranet** |
| réseau mondial | réseau corporatif privé | réseau corporatif accessible par les clients ou les fournisseurs |

TCP/IP (Transmission Control Protocol / Internet Protocol)

* un ordinateur peut avoir plusieurs cartes réseau
* une carte réseau peut avoir plusieurs adresses IP

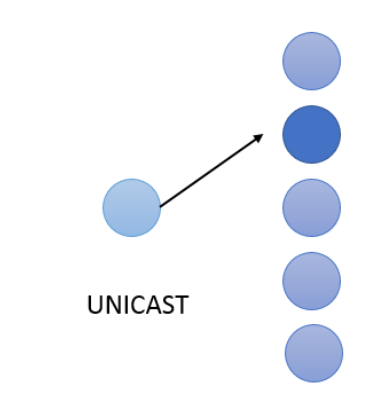
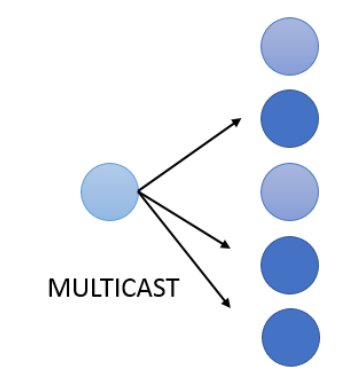
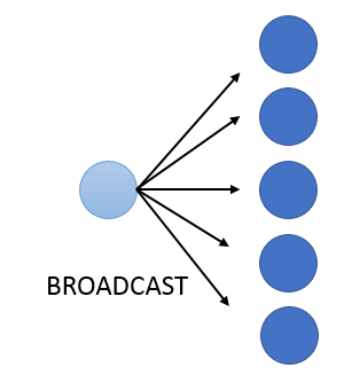
Une adresse IPv4 occupe 32 bits ou 4 octets.



4 294 967 296 est le maximum théorique d'adresses IPv4.

|  |  |  |
| --- | --- | --- |
| **nombre de bits** | **binaire** | **décimale** |
| 0 | 00000000 | 0 |
| 1 | 10000000 | 128 |
| 2 | 11000000 | 192 |
| 3 | 11100000 | 224 |
| 4 | 11110000 | 240 |
| 5 | 11111000 | 248 |
| 6 | 11111100 | 252 |
| 7 | 11111110 | 254 |
| 8 | 11111111 | 255 |

**Les différents types de communication entre les ordinateurs**

**un à un un vers plusieurs un vers tous**

**adresse IP de type monodiffusion "unicast"**

* permet d'envoyer des données à un seul ordinateur du réseau

**adresse IP de type multidiffusion "multicast"**

* permet d'envoyer des données à un groupe d'ordinateurs du réseau en une seule transmission
* exemples
* utilisation de WDS (Windows Deployment Services)
* VLC permet la diffusion vidéo en "multicast" sur plusieurs ordinateurs
* caméra de surveillance professionnelle

**adresse IP de type diffusion "broadcast"**

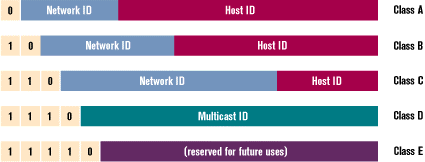
* permet d'envoyer des données à tous les ordinateurs du réseau
* exemples
* serveur DHCP
* WOL (Wake-On-LAN)

Pour démarrer un ordinateur à distance, on doit utiliser l'adresse IP de diffusion du réseau pour envoyer un "Magic Packet" qui contient 102 octets. Le "Magic Packet" est constitué de FF:FF:FF:FF:FF:FF suivi de 16 fois l'adresse MAC de la carte réseau de l'ordinateur.

**Les classes d'adresses**

À l'origine la communauté Internet a défini 5 classes d'adresses permettant de gérer des réseaux de taille différentes: classes: A, B, C, D, E.

Microsoft supporte les classes A, B, et C pour les hôtes.



**Adresses IP de classe A**

Adresses affectées aux réseaux avec de très nombreux hôtes.

* L'adresse commence toujours par le bit 31 égal à 0



* Un octet est utilisé pour l'identification du réseau
* Les adresses de classe A vont de 0.0.0.0 à 127.255.255.255

Les adresses de classe A de la forme 127.x.y.z sont réservées aux tests en boucle et aux communications entre processus sur l'ordinateur local.

* On peut avoir 126 réseaux (27 - 2)

une adresse IP de classe A ne peut pas débuter par 0 ou 127

* Trois octets sont utilisés pour l'identification des hôtes

Ce qui fait 16 777 214 hôtes possibles par réseau (224 - 2)

une adresse IP de classe A ne peut pas se terminer par 0.0.0

une adresse IP de classe A ne peut pas se terminer par 255.255.255

* Les adresses privées de classe A vont de 10.0.0.0 à 10.255.255.255

**Adresses IP de classe B**

Adresses affectées aux réseaux de taille moyenne à grande.

* L'adresse commence toujours par les bits 31 et 30 égaux à 10



* Deux octets sont utilisés pour l'identification du réseau
* Les adresses de classe B vont de 128.0.0.0 à 191.255.255.255
* Ce qui fait 16 384 réseaux (214)
* Deux octets sont utilisés pour l'identification des hôtes

Ce qui fait 65 534 hôtes possibles par réseau (216 - 2)

une adresse IP de classe B ne peut pas se terminer par 0.0

une adresse IP de classe B ne peut pas se terminer par 255.255

* Les adresses privées de classe B vont de 172.16.0.0 à 172.31.255.255

**Adresses IP de classe C**

Adresses affectées aux réseaux de petite taille.

* L'adresse commence toujours par les bits 31, 30, et 29 égaux à 110



* Trois octets sont utilisés pour l'identification du réseau
* Les adresses de classe C vont de 192.0.0.0 à 223.255.255.255
* Ce qui fait 2 097 152 réseaux (221)
* Un octet est utilisé pour l'identification des hôtes

Ce qui fait 254 hôtes possibles par réseau (28 - 2)

une adresse IP de classe C ne peut pas se terminer par 0

une adresse IP de classe C ne peut pas se terminer par 255

* Les adresses privées de classe C vont de 192.168.0.0 à 192.168.255.255

**Adresses IP de classe D**

Les adresses de classe D sont utilisées pour les communications multidiffusion (multicast).

* L'adresse commence toujours par les bits 31, 30, 29 et 28 égaux à 1110



* Les adresses de classe D vont de 224.0.0.0 à 239.255.255.255

**Les adresses privées**

Les adresses IP privées existent depuis février 1996.

Le document officiel "**RFC 1918 Address Allocation for Private Internets**" est disponible sur internet.

https://www.ietf.org/rfc/rfc1918.txt IETF signifie "Internet Engineering Task Force"

|  |  |  |
| --- | --- | --- |
| **Classe** | **Préfixe** | **Réseau privé** |
| **A** | 10.0.0.0/**8** | **10**.0.0.0 à **10**.255.255.255 |
| **B** | 172.16.0.0/**12** | **172.16**.0.0 à **172.31**.255.255 |
| **C** | 192.168.0.0/**16** | **192.168**.0.0 à **192.168**.255.255 |

**Le masque de sous-réseau**

Chaque classe d'adresse a un masque par défaut

* classe A 255.0.0.0
* classe B 255.255.0.0
* classe C 255.255.255.0

Le masque de sous-réseau permet aussi de savoir si l'hôte que l'on veut rejoindre est sur le même réseau que nous ou sur un autre réseau.

On effectue une opération ET logique sur les bits (ANDing).

* Si (Adresse Source ET Masque) = (Adresse Destination ET Masque) alors l'hôte destination est sur le même réseau que nous.
* Si (Adresse Source ET Masque) != (Adresse Destination ET Masque) alors l'hôte destination est sur un autre réseau. Dans ce cas pour le joindre il faudra avoir une adresse de passerelle par défaut (routeur) dans notre configuration.

**Exemple avec deux adresses IP dans le même réseau**

source 192.59.66.200

destination 192.59.66.17

masque de classe C 255.255.255.0

1. source ET masque

**11000000 00111011 01000010 11001000 source**

**11111111 11111111 11111111 00000000 masque**

**11000000 00111011 01000010 00000000 résultat**

1. destination ET masque

**11000000 00111011 01000010 00010001 destination**

**11111111 11111111 11111111 00000000 masque**

**11000000 00111011 01000010 00000000 résultat**

1. résultat (a) = résultat (b)

donc la source et la destination sont sur le même réseau

**Exemple avec deux adresses IP sur deux réseaux différents**

source 192.59.66.200

destination 192.13.130.12

masque de classe C 255.255.255.0

1. source ET masque

**11000000 00111011 01000010 11001000 source**

**11111111 11111111 11111111 00000000 masque**

**11000000 00111011 01000010 00000000 résultat**

1. destination ET masque

**11000000 00001101 10000010 00001100 destination**

**11111111 11111111 11111111 00000000 masque**

**11000000 00001101 10000010 00000000 résultat**

1. résultat (a) est différent du résultat (b)

donc la source et la destination sont sur deux réseaux différents

**Tests de validation**

* ping 127.0.0.1

vérifie si le protocole TCP/IP est installé et qu’il fonctionne correctement sur l'ordinateur local

* ping de l’adresse IP de l’hôte
* ping de la passerelle
* ping d’un hôte distant

**Adresse IP statique**

On doit configurer manuellement

* l'adresse IP
* le masque de sous-réseau
* la passerelle par défaut
* les serveurs DNS

Avec une adresse IP statique, il faut faire attention de ne pas configurer deux fois la même adresse IP.

**Adresse IP dynamique**

L'adresse IP est obtenue par un serveur DHCP.

**APIPA (Automatic Private IP Protocol Addressing)**

APIPA est une fonctionnalité qui permet à un appareil de s'**attribuer** une adresse IP lorsque le serveur DHCP n'est pas disponible.

* les adresses sont dans le réseau 169.254.0.0/16

169.254.0.1 à 169.254.255.254

* il n'y a pas de passerelle par défaut et pas de serveurs DNS
* permet de communiquer localement

**Les protocoles TCP et UDP**

Un réseau informatique est similaire à une route. Il existe des règles pour que tout le monde se comprenne pour éviter que les données circulent de manière anarchique.

Il existe deux protocoles pour le transport de données en IP

* TCP/IP Transmission Control Protocol / Internet Protocol
* UDP/IP User Datagram Protocol / Internet Protocol

TCP et UDP servent exactement à la même chose, soit le transport de paquets mais ils le font de façon assez différente.

TCP et UDP envoient des données par paquets d'une source vers une destination.

TCP et UDP utilisent des adresses IP pour identifier l'expéditeur et le destinataire et des numéros de ports (de 1 à 65535) pour identifier les applications.

**Le protocole TCP/IP**

* Avec le protocole TCP, les deux machines communiquent en permanence.

La machine source établit une connexion avec la machine destinataire pour se présenter et la prévenir qu'elle va lui envoyer des données.

Cette procédure s'appelle "handshaking" (poignée de mains).

* Une fois la connexion établie, la source envoie des paquets numérotés dans un certain ordre au destinataire qui accuse réception à chaque fois après avoir vérifié que les données sont intactes grâce à un mécanisme de contrôle.

Si ce n'est pas le cas, la source renvoie aussitôt le paquet manquant ou corrompu.

* Le protocole TCP est considéré comme un protocole axé sur la qualité de la transmission.

La transmission des données prend plus de temps parce les deux machines communiquent en permanence pour vérifier que les données sont intactes.

* Étant donné que le protocole TCP est qualifié de "robuste", il est utilisé dans des applications qui doivent recevoir des données intactes (navigateur Web, transfert de fichiers, messagerie, etc.).

**Le protocole UDP/IP**

* UDP est un protocole "sans connexion" ou "non connecté" dans lequel il n'y a pas d'échange permanent, pas même de "handshaking".
* En UDP, la machine source envoie des paquets non numérotés à la machine de destination.

Il n'y a pas de renvoi de données si un paquet est perdu ou corrompu pendant le transfert.

* Le protocole UDP est plus rapide et utilise moins de ressource que le protocole TCP.

Étant donné que le protocole UDP privilégie la vitesse à la fiabilité, il est surtout utilisé dans les applications nécessitant du temps réel, comme le jeu vidéo ou les conversations audio-vidéo.

**Numéro de port**

Les ports sont classés en trois catégories:

* les numéros de port de 0 à 1023 correspondent aux ports "bien-connus" (well-known ports)

ils sont utilisés pour les services réseaux les plus courants

* les numéros de ports de 1024 à 49151 correspondent aux ports enregistrés (registered ports)

ils sont assignés par l'IANA

* les numéros de ports de 49152 à 65535 correspondent aux ports dynamiques

ils sont utilisables pour tout type de requêtes TCP ou UDP autres que celle citées précédemment

|  |  |  |
| --- | --- | --- |
| **Port** | **Protocole** | **Description** |
| 21 | TCP | FTP (File Transfer Protocol) |
| 22 | TCP | SSH (Secure SHell) |
| 23 | TCP | TELNET |
| 25 | TCP | SMTP (Simple Mail Transfer Protocol) |
| 53 | TCP / UDP | DNS (Domain Name Server) |
| 69 | UDP | TFTP (Trivial File Transfer Protocol) |
| 80 | TCP | http (Hypertext Transfer Protocol) |
| 110 | TCP | POP3 (Post Office Protocol version 3) |
| 119 | TCP | NNTP (Network News Transfer Protocol) |
| 123 | UDP | NTP (Network Time Protocol) |
| 137  138  139  445 | UDP  UDP  TCP  TCP | Partage de fichiers et d'imprimantes |
| 161 | UDP | SNMP (Simple Network Management Protocol) |
| 443 | TCP | HTTPS (HTTP sécurisé) |
| 3389 | TCP | RDP (Remote Desktop Protocol) |

**La commande ping.exe**

La commande ping permet de mesurer le temps de réponse d'un ordinateur.

Exemples de la commande ping avec des adresses IPv4

* ping 127.0.0.1
* ping 192.168.1.10
* ping -a 192.168.1.10
* ping -t 192.168.1.10
* ping -n 2 192.168.1.10
* ping -4 serveur1
* ping -4 -a serveur1
* ping -4 -t serveur1
* ping -4 -n 2 serveur1

**ANNEXE 1**

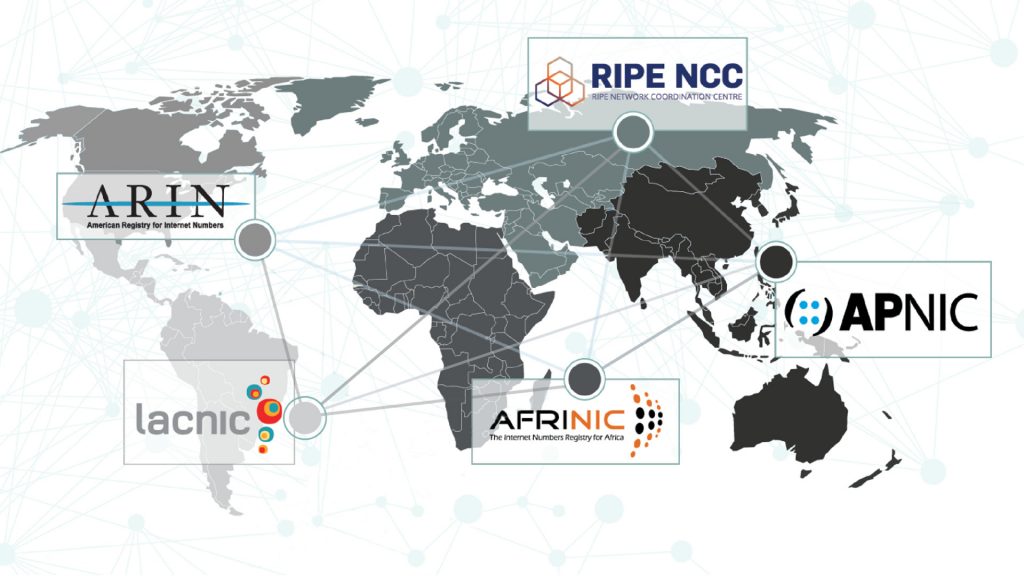
**La gestion des adresses IP dans le monde**

Il y a cinq **RIR "Regional Internet Registries**" dans le monde.

Chaque RIR gère, distribue et enregistre les adresses IPv4 et IPv6 dans leurs régions respectives.

**Regional Internet Registries**

https://www.nro.net/about/rirs



**AFRINIC** African Network Coordination Centre

Région de l'Afrique

**APNIC** Asia Pacific Network Information Center

Région de l’Asie et du Pacifique

**ARIN** American Registry for Internet Numbers

Région de l’Amérique du Nord et de l’Afrique subsaharienne

**LACNIC** Latin-American and Caribbean Network Information Center

Région pour l’Amérique latine et les Caraïbes

**RIPE NCC** Réseaux IP Européens Network Coordination Centre

Région pour l'Europe, le moyen orient et l'asie centrale

Le premier octet d'une adresse IPv4 permet de déterminer à quelle zone appartient l’adresse : http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

**ANNEXE 2**

**Adressage IPv6**

**Plusieurs avantages d'utiliser IPv6**

La structure d'adressage passe de 32 bits à 128 bits

2128  = 232 x 232 x 232 x 232

340 282 366 920 938 463 463 374 607 431 768 211 456 est le maximum théorique d'adresses IPv6.

Le nombre d'adresses IPv6 maximum correspond à plus de 667 millions de milliards d'appareils connectés à internet sur chaque millimètre carré de la surface terrestre (510 millions de km²).

Une adresse IPv6 occupe 128 bits.

* X:X:X:X:X:X:X:X

chaque X représente un nombre de 16 bits en format hexadécimal qui varie de 0000 à FFFF

Les premiers zéros de chaque champ sont optionnels

* 2001:0000:1234:0000:0000:0BC0:ABCD:5678

devient

2001:0:1234:0:0:BC0:ABCD:5678

La compression des zéros

Plusieurs champs successifs de 0 sont représentés par :: mais seulement une fois dans une adresse

* 2001:0:1234:0:0:BC0:ABCD:5678

devient

2001:0:1234::BC0:ABCD:5678

**Adresse IPv6 non assignée**

0:0:0:0:0:0:0:0 ::

* équivalent de l'adresse IPv4 0.0.0.0

**Adresse IPv6 de bouclage**

0:0:0:0:0:0:0:1 ::1

* équivalent de l'adresse IPv4 127.0.0.1

La structure d'une adresse IPv6 de type **liaison locale**

|  |  |
| --- | --- |
| **64 bits** | **64 bits** |
| **FE80:0:0:0** | **interface ID** |

* l'équivalent des adresses APIPA dans IPv4
* adresses utilisées seulement entre les périphériques d'un même réseau
* adresses non routées entre les sous-réseaux

L'adresse IPv6 de **www.facebook.com** est spéciale.

**nslookup.exe www.facebook.com 8.8.8.8**

**Serveur : dns.google**

**Address: 8.8.8.8**

**Réponse ne faisant pas autorité :**

**Nom : star-mini.c10r.facebook.com**

**Addresses: 2a03:2880:f10e:83:face:b00c:0:25de**

**31.13.80.36**

**Aliases: www.facebook.com**

Même si votre ordinateur n'a pas d'adresse IPv6, la commande nslookup permet de rechercher un nom de domaine à partir d'une adresse IPv6.

**nslookup 2001:503:ba3e::2:30**

**Serveur : cvmdc03.reseau.cvm**

**Address: 10.19.3.70**

**Nom : a.root-servers.net**

**Address: 2001:503:ba3e::2:30**

**Outils pour IPv6**

**https://www.kame.net**

la tortue danse à condition d'avoir une adresse IPv6 publique

**https://ip6.me**

retourne l'adresse IPv6 publique

**# Script PowerShell qui affiche l'adresse IPv6 visible sur internet**

**Clear-Host**

**$info = Invoke-RestMethod -Uri https://ip6only.me/api**

**$csv = ConvertFrom-CSV $info -Delimiter "," -Header "ipv6","adresse"**

**$csv.adresse**