

Eléments d'architecture réseau Internet



Internet : Réseau mondial d'inter-connexion de réseaux.

Toute machine connectée au réseau Internet peut "théoriquement" communiquer avec tout autre machine elle-même connectée. Dans la pratique, c'est loin d'être systématiquement le cas à cause de limitations techniques souhaitées ou non.

INTRODUCTION

INFRASTRUCTURE

MATERIELLE

Sous-réseau

Interconnexion

de sous-réseaux

Un message envoyé d'une machine à une autre machine est segmenté en un ensemble de morceaux appelés paquets. Chacun de ces paquets est marqué par la machine source avec son nom et le nom de la machine cible et est émis sur le réseau à destination de cette machine.

INFRASTRUCTURE

LOGICIELLE

NetBEUI

TCP/IP

Paramètres

généraux

Paramètres DNS

Paramètres WINS

Filtrage IP

DHCP

Rien n'interdit qu'un paquet se perde en cours de route. Suivant la technique de gestion de la communication, ces pertes peuvent être tolérées ou interdites. Dans le second cas, la perte est détectée et le paquet est envoyé de nouveau.

Le transfert de ces paquets requière la présence d'une infrastructure matérielle gérée au moyen d'une infrastructure logicielle.

COMMANDES

TCP/IP

ipconfig

ping

nslookup

tracert

Infrastructure matérielle

Sous-réseau

Un sous-réseau est un réseau caractérisé par le fait que chaque machine peut communiquer directement avec toute autre machine du même sous-réseau.

Dans le cas des réseaux ethernet sur double paires torsadées (technologie la plus courante actuellement), les machines sont interconnectées via des concentrateurs (hubs) ou des commutateurs (switchs).

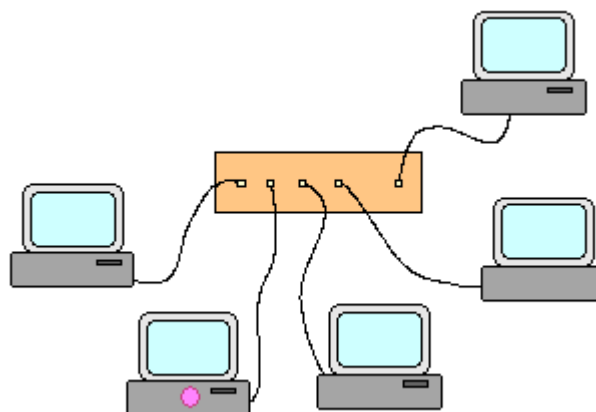


Concentrateur (hub)

Un concentrateur relie les machines en étoile. Il duplique et

transmet tout paquet à toutes les machines qui lui sont directement connectées. Une machine cible conservera et exploitera les paquets qui lui sont destinés et oubliera les autres. Du fait de la duplication des paquets, la somme des bandes passantes instantanées sur l'ensemble des machines connectée est limitée à la bande passante du concentrateur (généralement 10 ou 100 Mbits/s).

La capacité de transfert est donc partagée entre les machines connectées et est limitée à celle du concentrateur.



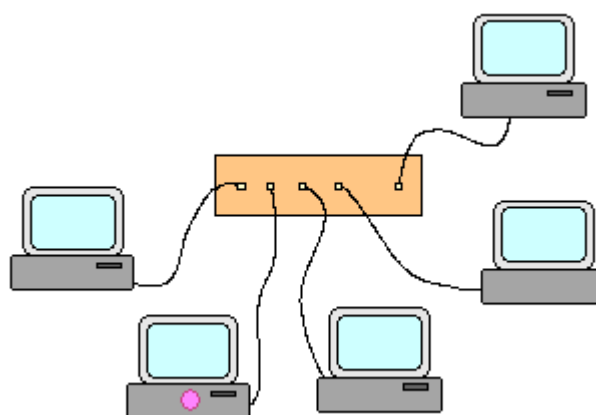
Commutateur (switch)

Un commutateur relie les machines en étoile et transmet un paquet à la seule machine à laquelle il est destiné.

-> Une machine reçoit les seuls paquets qui lui sont destinés.

Chaque machine possède une bande passante potentielle vers les autres machines qui lui sont connectées égale à celle de son interface réseau (10, 100 ou 1000 Mbits/s).

La bande passante globale du sous-réseau est toutefois limitée par la vitesse de commutation du fond de panier du commutateur (matrice de commutation).



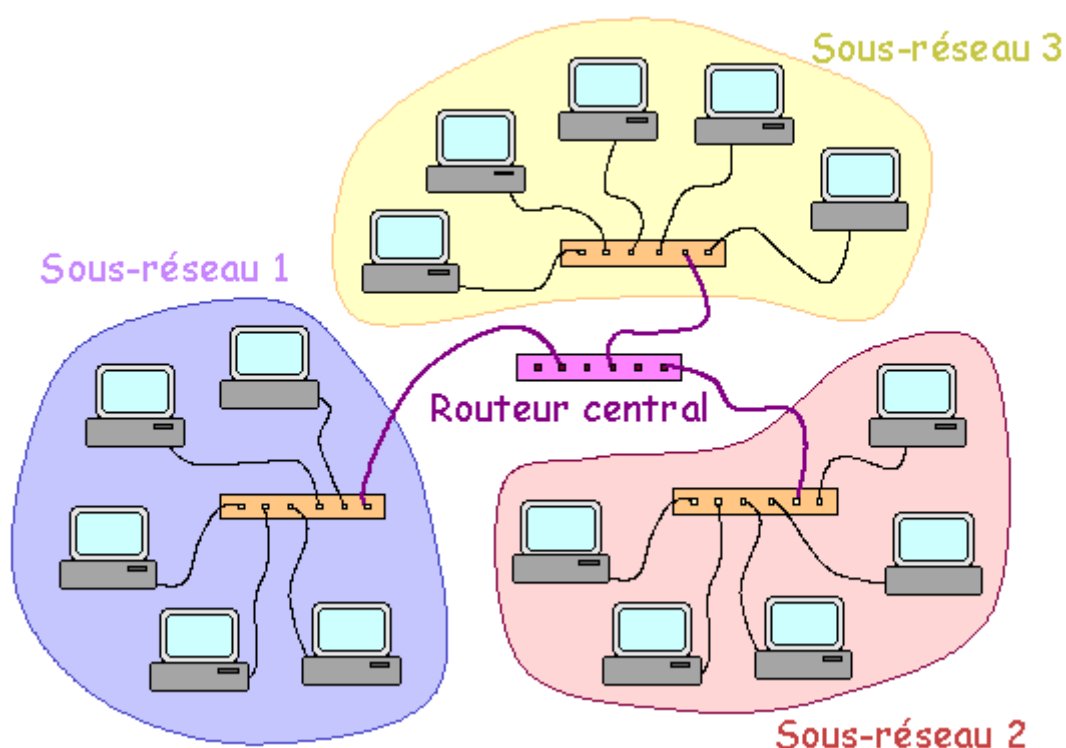
Un sous-réseau peut être constitué par une étoile (éventuellement

une étoile à plusieurs niveaux) de commutateurs ou concentrateurs sur lesquels viennent se connecter en étoile les machines. Quoiqu'il en soit, il ne doit exister qu'un seul chemin entre tout couple de machines.

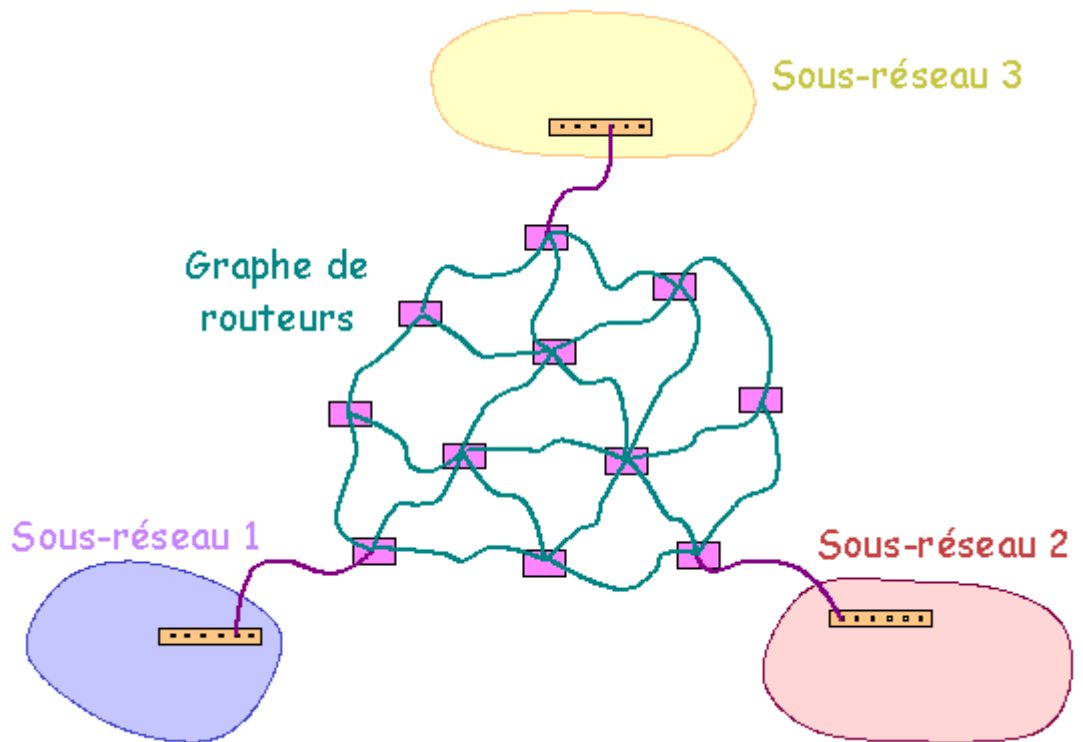
Inter-connexion des sous-réseaux

Toujours pour les réseaux ethernet, deux ou plusieurs sous-réseaux séparés peuvent être connectés entre eux via un routeur. Un tel matériel est capable de "router" les paquets entre les sous-réseaux qui contiennent respectivement les machines source et cible.

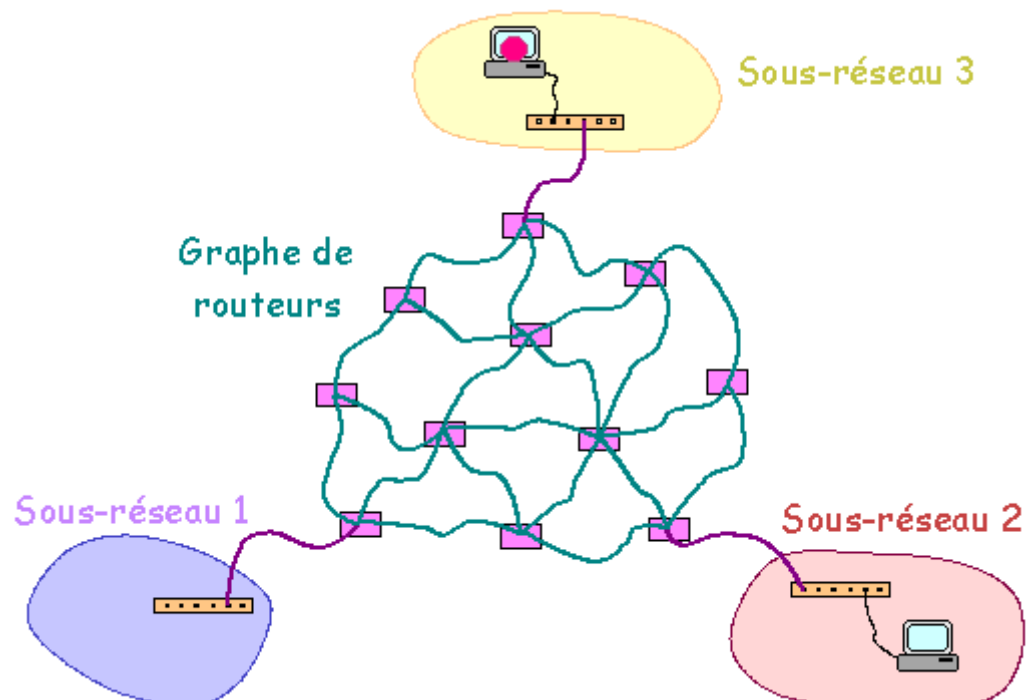
Dans les cas simples, les sous-réseaux sont directement connectés sur un routeur unique qui après configuration semble agir comme un commutateur.



Dans les cas plus complexes (réseaux d'entreprise, Internet), un seul routeur ne permet pas l'inter-connexion de l'ensemble des sous-réseaux. Plusieurs routeurs reliés entre eux consécutivement sont alors utilisés sur le chemin des paquets.



Pour des raisons de pérennité de fonctionnement et capacité de transfert d'information, le réseau de routeurs, au lieu d'être construit en étoile, pourra être construit en graphe (voir ci-dessus). Plusieurs chemins pourront exister pour relier un sous-réseau et un autre sous-réseau. Pour un même message, les paquets peuvent transiter par des chemins différents et même arriver dans un ordre différent de celui de départ. Le matériel actif du réseau se contente d'assurer le transfert de l'information. Ce sont les machines cibles qui reconstituent la cohérence des messages à l'arrivée.



Les routeurs ont une "connaissance" (statique ou dynamique) de la topographie globale du réseau fédérateur permettant ainsi de résoudre le problème du choix et de l'optimisation des liens de transit.

Remarque: Telle que présentée ci-dessus, l'ensemble des machines reliées en étoile par une suite de concentrateurs ou de commutateurs constitue un sous-réseau. Dans la pratique, l'infrastructure logicielle (voir ci-dessous) qui est greffée sur l'infrastructure matérielle permet de constituer "logiquement" des sous-réseaux moins étendus. Il est ainsi possible de gérer 2 (ou plusieurs) sous-réseaux indépendants en utilisant un seul concentrateur ou commutateur. S'il est souhaité d'interconnecter ces sous-réseaux, il faudra en plus faire appel à un appareil (routeur ou ordinateur assurant une fonction de routage) assurant le routage.

Infrastructure logicielle

L'infrastructure logicielle d'un réseau informatique est basée sur l'utilisation de un ou plusieurs protocoles de communication (i.e. langage de communication d'informations entre ordinateurs).

Les protocoles les plus courants sont TCP/IP, NetBEUI et IPX/SPX. TCP/IP est le protocole de l'Internet et tend à se généraliser.

Une des différences essentielle entre ces trois protocoles tient à la routabilité. En effet, TCP/IP est assez facilement "routable" (i.e. est géré par les routeurs) et permet donc d'interconnecter des sous-réseaux. NetBEUI ne l'est pas. IPX/SPX l'est moins facilement que TCP/IP. Cette caractéristique ainsi que sa relative simplicité explique son adoption pour le réseau Internet.

L'infrastructure logicielle comprend pour chaque protocole:

- Les logiciels de configuration, de gestion et d'audit du fonctionnement des matériels du réseau (concentrateurs, commutateurs, routeurs, ...) (non abordés ici).
- Les logiciels de configuration, de gestion et d'audit du

fonctionnement local des machines permettant en particulier de donner un nom à chaque machine pour autoriser les communications machine source <-> machine cible.

- Les services réseau implantés pour utiliser ou faciliter l'utilisation du protocole dans le cadre de fonctionnalités précises.

NetBEUI

NetBEUI possède le gros avantage d'être simple à installer et configurer. Cette simplicité est principalement une conséquence du fait qu'il n'a pas été conçu dans le but d'être routé et qu'il n'intègre donc pas les paramètres qui pourraient être nécessaires à la gestion du routage.

Les machines sont désignées par des noms alphanumériques sur 15 caractères.

Toutes les machines placées sur le même concentrateur, sur le même commutateur ou liées par une suite de concentrateurs ou commutateurs peuvent communiquer directement entre elles.

Un certain nombre de services réseau ont été développés pour NetBEUI. En particulier SMB (Server Message Block) et Lan Manager proposent les services:

- de gestion d'utilisateurs,
- de gestion de répertoires partagés,
- de gestion d'imprimantes partagées,
- ...

NetBEUI et les services qui lui sont associés sont disponibles sous les différentes versions de Windows, sous Linux, FreeBSD et Unix (Samba).

Outre sa non routabilité, NetBEUI, utilisé sous Windows, possède l'inconvénient de mettre en œuvre un processus d'exploration du réseau à la recherche des machines qui y sont présentes. Le but est d'en rendre accessible la liste.

Dans le cas le plus défavorable, chaque machine émet régulièrement un "broadcast" (i.e. un message destiné à toutes les machines de son sous-réseau) destiné à susciter une réponse

contenant le nom de la machine répondant. Si n machines génèrent un broadcast entraînant n réponses, on obtient de l'ordre de n^2 messages échangés régulièrement.

-> A partir d'un certain nombre de machines, une part importante du trafic du réseau (voire jusqu'à 100%) peut être consacrée à ce processus d'exploration.

Pour éviter ce problème, dans une version plus élaborée (en particulier depuis Windows NT), un "maître explorateur" est "élu" automatiquement sur chaque sous-réseau. Cette machine sera la seule à assurer l'exploration. Elle sera contactée par toute machine souhaitant connaître la liste des machines du réseau.

TCP/IP

Plus complexe que NetBEUI, TCP/IP intègre, outre des paramètres permettant de nommer les machines et de les placer dans des sous-réseaux, un ensemble de paramètres destinés au routage.

Paramètres généraux:

- **Adresse IP** : Une machine est nommée de manière unique sur son réseau par son "adresse IP" formée de 4 nombres compris entre 0 et 255. Exemple: 172.20.128.23
- **Masque de sous-réseau (Subnet Mask)** : Formé de 4 nombres compris entre 0 et 255, le masque de sous-réseau permet d'indiquer à une machine quelles sont les adresses IP des machines qui font partie de son sous-réseau (i.e. les machines avec lesquelles elle peut communiquer sans routage). Comme son nom l'indique, le masque de sous-réseau est un masque numérique. Il est géré en arithmétique binaire. Si les "et binaire" entre les adresses IP de deux machines et le masque sont égaux alors les deux machines appartiennent au même sous-réseau TCP/IP.

Exemple: Soient le masque $M = 255.255.255.128$ et les machines d'adresses IP $I1 = 172.20.128.164$ et $I2 = 172.20.128.213$.

En binaire, le masque est

$M = 11111111.11111111.11111111.10000000$

et les adresses

$I1 = 10101100.00010100.10000000.10100100$

et

$I2 = 10101100.00010100.10000000.11010101$

Si $(M \& I1) = (M \& I2)$ alors les machines font partie du même sous-réseau. Le signe $\&$ désigne le "et binaire".

$M \& I1 = 10101100.00010100.10000000.10000000$

$M \& I2 = 10101100.00010100.10000000.10000000$

$(M \& I1)$ est égal à $(M \& I2)$

-> Ces deux machines sont sur le même sous-réseau. Elles pourront communiquer directement si elles sont interconnectées par un concentrateur ou un commutateur.

Les masques de sous-réseau ne peuvent pas être considérés arbitrairement. Ils sont construits de gauche à droite au moyen d'une suite de bits à 1 suivie d'une suite de bits à 0.

Les masques de sous-réseau classiques sont :

255.255.255.0 -> 256 adresses dans le même sous-réseau (si les trois premiers entiers de deux adresses IP sont les mêmes, les deux adresses sont dans le même sous-réseau) (ce masque correspond à ce que l'on appelle usuellement une classe C),

255.255.255.128 -> 128 adresses (2 sous-réseaux sur une classe C : de 0 à 127 et de 128 à 255),

255.255.255.192 -> 64 adresses (4 sous-réseaux sur une classe C : de 0 à 63, de 64 à 127, de 128 à 191 et de 192 à 255),

255.255.255.224 -> 32 adresses (8 sous-réseaux sur une classe C),

255.255.255.240 -> 16 adresses (16 sous-réseaux sur une classe C),

255.255.255.248 -> 8 adresses (32 sous-réseaux sur une classe C),

255.255.255.252 -> 4 adresses (64 sous-réseaux sur une classe C).

Définition des différentes classes IP

- **Passerelle par défaut (Gateway)** : Il s'agit de l'adresse IP vers laquelle seront envoyés tous les paquets non destinés à une machine du même sous-réseau que la machine source. Un routeur ou un ordinateur assurant le routage sera installé à cette adresse pour les réceptionner et assurer la transmission (routage) vers le sous-réseau destination.

Paramètres de configuration DNS

La technique de dénomination par adresse IP (liste de 4 nombres) est pratique pour les ordinateurs car facilement manipulée par eux. En revanche, la mémorisation est difficile pour les individus.

Convention de dénomination supplémentaire:

Désignation de chaque machine par un ou plusieurs noms IP alphanumériques.

Une machine porte un nom et appartient à un domaine TCP/IP qui peut lui-même être le sous-domaine d'un autre domaine TCP/IP, ... Un domaine peut ainsi posséder plusieurs sous-domaines, qui eux-mêmes peuvent posséder des sous-domaines, ... créant ainsi une organisation arborescente.

Les parties alphanumériques du nom IP sont délimitées par des points avec, de gauche à droite, le nom de la machine, puis les différentes parties du nom de domaine du plus particulier au plus général.

Exemple: 172.20.128.99 \Leftrightarrow bunny.edu-info.univ-fcomte.fr (machine bunny du sous-domaine edu-info.univ-fcomte.fr du sous-domaine univ-fcomte.fr du domaine fr).

Les listes de couples (adresse TCP/IP, nom TCP/IP) peuvent être gérées de deux manières:

- localement sur chaque machine au moyen de fichiers "hosts" (sous \Windows\System32\drivers\etc sous Windows, sous /etc sous unix),
- globalement sur un ensemble de machines reliées en réseau au moyen d'un serveur DNS (Domain Name Server) qui gère la liste associée à un domaine et peut être interrogé via une connexion réseau normalisée.
La configuration TCP/IP de la machine cliente inclut alors une référence à ce serveur.

Les serveurs DNS sont généralement organisés sous une forme arborescente calquée sur l'arborescence des domaines TCP/IP qu'ils représentent. Chaque serveur gèrera tout ou partie des noms de machine associés au nom de domaine dont il est le nœud.

Il peut y avoir plusieurs serveurs DNS pour un même nom de domaine. On pourra alors distribuer entre eux les bases de données de machines enregistrées. On pourra aussi répliquer les bases de données de machines et ainsi garantir une redondance permettant une meilleure pérennité ou bien encore permettre un équilibrage de charge pour les domaines très consultés.

Un serveur DNS réalise les tâches suivantes:

- Gérer sa base de données de noms.
- Résoudre un nom pour les machines qui le lui demandent quand il connaît le nom (il appartient au domaine qu'il gère). Répondre que le nom n'existe pas, s'il est certain qu'il n'existe pas (i.e. il n'est pas défini dans le domaine qu'il gère).
- Propager la demande de résolution vers le ou les serveurs DNS du domaine concerné s'il s'agit d'un nom associé à l'un des domaines pour lesquels il connaît un serveur DNS (on parle de redirecteur).

Il connaît généralement les serveurs DNS de chacun de ses sous-domaines auxquels il transmet les seules requêtes qu'ils devraient savoir résoudre, ainsi que le serveur DNS de son domaine père auquel il transmet toutes les requêtes qu'il n'a pas transmises aux DNS de ses sous-domaines. Ils peut aussi connaître les adresses de serveurs DNS root.

- **Nom d'hôte** : Nom donné à la machine. Généralement identique au nom qui lui est donné sur le DNS dont elle dépend.
- **Suffixes DNS** : Nom du ou des domaines auxquels appartient la machine. Lorsque cette machine spécifie des noms IP sans indiquer explicitement de nom de domaine, les suffixes sont testés les uns après les autres comme domaines implicites.
- **DNS** : Un ou plusieurs serveurs DNS peuvent être désignés pour être joints lorsqu'une résolution de nom DNS doit être réalisée pour obtenir l'adresse IP correspondant au nom IP ou réciproque.

Paramètres de configuration WINS

Un problème spécifique aux machines Windows est qu'elles

peuvent devoir répondre à la convention de nommage NetBEUI (par exemple pour assurer la compatibilité avec d'anciennes applications).

Or, la non routabilité de ce protocole fait qu'il est impossible de l'utiliser pour des réseaux comportant un nombre important de machines.

Via une "Interface NetBIOS", il est possible de faire transiter des informations au moyen du protocole TCP/IP en utilisant les conventions de nom NetBEUI et donc d'autoriser le routage.

Le problème est de rendre compatibles les nommages par adresse IP et les noms NetBEUI. Windows Internet Name Service (WINS) est l'une des solutions possibles.

WINS est un service réseau pouvant être implanté sur un serveur pour lui permettre de gérer une base de données d'associations adresse IP \Leftrightarrow nom NetBEUI. Ce serveur sera à même d'effectuer des résolutions de nom via requêtes réseau normalisées. Il s'agit de l'équivalent résolution nom NetBEUI \leftrightarrow adresse IP de ce qu'est DNS pour les résolutions nom TCP/IP \leftrightarrow adresse IP.

Par rapport à DNS, WINS apporte quelques possibilités supplémentaires:

- L'apprentissage est dynamique (i.e. tous les clients d'un serveur WINS s'enregistrent automatiquement sur ce serveur).
- Les serveurs WINS peuvent enregistrer d'autres informations: des noms d'utilisateurs, des noms de machines, des noms de domaine, ...
- Des serveurs WINS peuvent être configurés pour s'échanger leurs bases de données et offrir ainsi des redondances et des possibilités d'administration plus élaborées.
- ...
- **WINS primaire** : Adresse IP du serveur WINS qui doit être joint lorsqu'une résolution WINS doit être réalisée. Le client WINS s'enregistre par la même occasion.
- **WINS secondaire** : Adresse IP du serveur WINS qui doit être joint lorsqu'une résolution WINS doit être réalisée et que le serveur primaire ne donne pas de réponse soit car il ne fonctionne pas, soit car il ne connaît pas l'association souhaitée.

Filtrage IP

Le protocole TCP/IP permet généralement l'implantation de fonctions de filtrage tant du point de vue des paquets sortants que du point de vue des paquets entrants.

Ces fonctions de filtrage pourront généralement être configurées soit en fonction de l'adresse IP du client, soit en fonction du port TCP/IP utilisé par l'ordinateur client.

DHCP

Tous les paramètres nécessaires à la configuration de l'infrastructure TCP/IP pourront être renseignés soit directement sur l'ordinateur hôte, soit sur un serveur DHCP (Dynamic Host Configuration Protocol) qui sera contacté par l'intermédiaire du réseau par l'hôte au moment de son démarrage.

L'intérêt de l'utilisation de DHCP réside dans les points suivants:

- La configuration des postes clients est centralisée et peut être réalisée clients éteints.
- L'affectation des paramètres pourra être réalisée dynamiquement ou statiquement.
Dans le cas de l'affectation dynamique, on pourra par exemple ne disposer que d'un pool restreint d'adresses IP permettant d'accéder à Internet et affecter ces adresses aux seules machines en fonctionnement.
- ...

De plus en plus, on constate une convergence entre DNS, DHCP et WINS permettant, via une base de données unique, d'assurer la cohérence des informations transmises. C'est le cas sous Windows 2000.

Commandes texte liées à TCP/IP

ipconfig

La commande ipconfig permet de visualiser la configuration TCP/IP des différentes cartes réseau présentes dans la machine. la syntaxe est

`ipconfig` pour obtenir un résumé et

`ipconfig -all` pour obtenir une description complète.

```

C:\>ipconfig

Configuration IP de Windows 2000

Ethernet carte Connexion au réseau local :

    Suffixe DNS spéc. à la connexion. :
    Adresse IP. . . . . : 194.57.88.125
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 194.57.88.254

C:\>_

```

ipconfig

```

C:\>ipconfig -all

Configuration IP de Windows 2000

    Nom de l'hôte . . . . . : raphaello
    Suffixe DNS principal . . . . . : univ-fcomte.fr
    Type de noud. . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche de suffixe DNS : univ-fcomte.fr

Ethernet carte Connexion au réseau local :

    Suffixe DNS spéc. à la connexion. :
    Description . . . . . : Intel(R) PRO/100 VE N
etwork Connection
    Adresse physique. . . . . : 00-0B-CD-05-4C-A1
    DHCP activé . . . . . : Non
    Adresse IP. . . . . : 194.57.88.125
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 194.57.88.254
    Serveurs DNS. . . . . : 194.57.91.200
                           194.57.91.201
    Serveur WINS principal. . . . . : 172.20.128.64
    Serveur WINS secondaire . . . . . : 172.20.128.100

C:\>

```

ipconfig -all

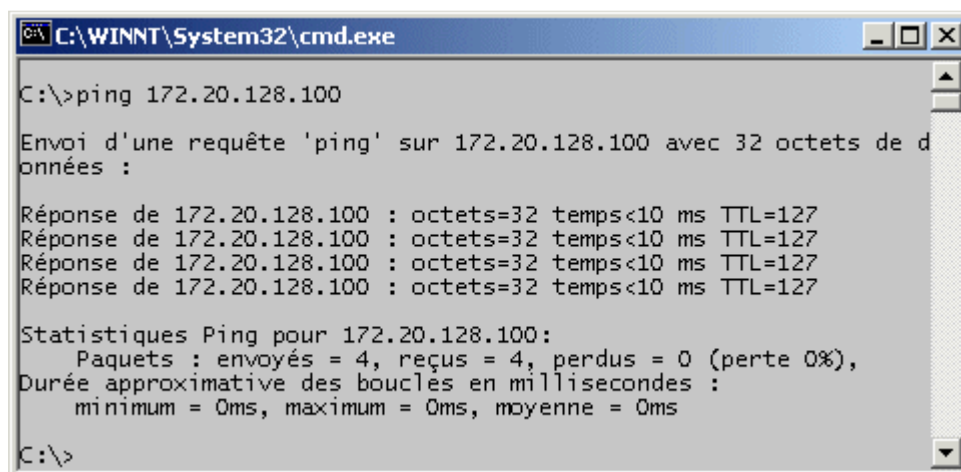
ping

La commande ping permet de tester la présence d'une machine sur le réseau. la syntaxe est

ping nom_IP

ou

ping adresse_IP



```
C:\WINNT\System32\cmd.exe
C:\>ping 172.20.128.100

Envoi d'une requête 'ping' sur 172.20.128.100 avec 32 octets de données :

Réponse de 172.20.128.100 : octets=32 temps<10 ms TTL=127
Réponse de 172.20.128.100 : octets=32 temps<10 ms TTL=127
Réponse de 172.20.128.100 : octets=32 temps<10 ms TTL=127
Réponse de 172.20.128.100 : octets=32 temps<10 ms TTL=127

Statistiques Ping pour 172.20.128.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        minimum = 0ms, maximum = 0ms, moyenne = 0ms

C:\>
```

ping

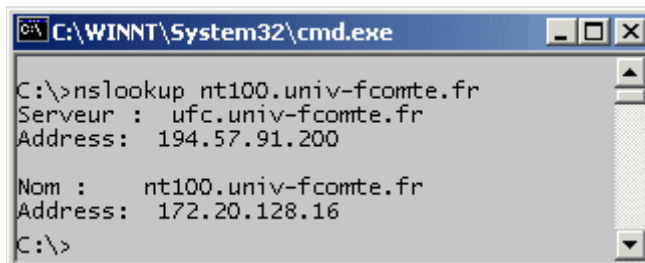
nslookup

La commande nslookup permet d'interroger son serveur DNS pour obtenir les adresses IP correspondant à un nom IP (résolution directe), ou les noms IP correspondant à une adresse IP (résolution inverse). La syntaxe est

`nslookup nom_IP`

ou

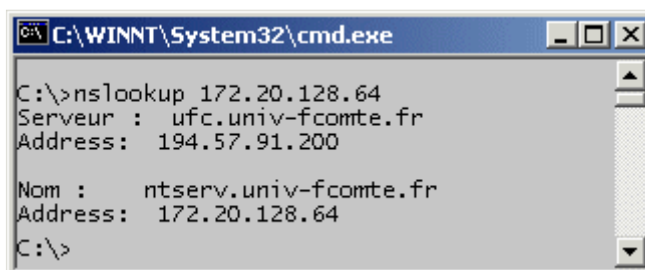
`nslookup adresse_IP`



```
C:\WINNT\System32\cmd.exe
C:\>nslookup nt100.univ-fcomte.fr
Serveur : ufc.univ-fcomte.fr
Address: 194.57.91.200

Nom :    nt100.univ-fcomte.fr
Address: 172.20.128.16

C:\>
```



```
C:\WINNT\System32\cmd.exe
C:\>nslookup 172.20.128.64
Serveur : ufc.univ-fcomte.fr
Address: 194.57.91.200

Nom :    ntserv.univ-fcomte.fr
Address: 172.20.128.64

C:\>
```

nslookup

tracert

La commande tracert permet d'obtenir la liste des matériels réseau (routeurs) traversés pour joindre une autre machine.

La syntaxe est

`tracert nom_IP`

ou

tracert adresse_IP

```
C:\WINNT\System32\cmd.exe
C:\>tracert www.inra.fr
Détermination de l'itinéraire vers granit.jouy.inra.fr [138.102.1.3]
avec un maximum de 30 sauts :

  1  <10 ms  <10 ms  <10 ms  gw-lib.univ-fcomte.fr [194.57.88.254]
  2  <10 ms  <10 ms  <10 ms  interco-7200-5500.univ-fcomte.fr [172.20.255.254]
  3  <10 ms  16 ms   <10 ms  10.1.12.2
  4  <10 ms  <10 ms  <10 ms  besancon-a0-1-4.cssi.renater.fr [193.51.181.54]
  5  31 ms   16 ms   15 ms   lyon-pos5-0.cssi.renater.fr [193.51.179.229]
  6  31 ms   15 ms   16 ms   nri-a-pos4-0.cssi.renater.fr [193.51.179.13]
  7  16 ms   31 ms   16 ms   rerif-nri-a.cssi.renater.fr [193.51.181.1]
  8  16 ms   16 ms   31 ms   stamand1.rerif.ft.net [193.48.53.106]
  9  15 ms   16 ms   31 ms   inra-jouy-josas.rerif.ft.net [193.48.53.110]
 10  15 ms   32 ms   15 ms   195.83.240.10
 11  31 ms   15 ms   32 ms   granit.jouy.inra.fr [138.102.1.3]

Itinéraire déterminé.
C:\>_
```

tracert

[RETOUR](#)