

Formation Protocole TCP-IP V4 & netbios et Systèmes Windows – sr41 - (sr43-sr22-sr24) - Cours

Michel Cabaré / www.cabare.net / michel@cabare.net

TCP-IP V4 & netbios et Systèmes Windows
- sr41- (sr43- sr 22- sr 24) - Cours V1-7 – Aout 2022



<https://WWW.CABARE.NET> ©



Microsoft
Partner

TABLE DES MATIÈRES

STRUCTURE DE TCP/IP	6
MODELE TCP/IP :	6
COUCHE 1 INTERFACE RESEAU :	6
COUCHE 2 INTERNET :	6
COUCHE 3 TRANSPORT :	7
COUCHE 4 APPLICATION :	7
LES PROTOCOLES DE TCP/IP	8
TCP (TRANSMISSION CONTROL PROTOCOL) :	8
<i>Port et Socket</i> :	8
<i>Communication en mode Connecté</i> :	8
<i>Fenêtres variables</i> :	9
UDP (USER DATAGRAM PROTOCOL) :	10
<i>Port et Socket</i> :	10
<i>Communication en mode non Connecté</i> :	10
<i>exemple SNMP</i>	10
<i>exemple Vidéo et Son en ligne</i>	10
IP (INTERNET PROTOCOL) :	10
<i>Adresse IP</i>	11
<i>Datagramme</i>	11
<i>Fragmentation MTU</i>	12
<i>Assemblage</i>	13
<i>Routage</i>	13
<i>Durée de Vie TTL</i>	13
ICMP (INTERNET CONTROL MESSAGE PROTOCOL) :	14
ARP (ADDRESS RESOLUTION PROTOCOL) :	14
<i>Exemple de fonctionnement de ARP en local</i>	14
<i>Exemple de fonctionnement de ARP et Routeur</i>	15
ADRESSE IP	16
ADRESSE IP :	16
ID RESEAU ET ID HOTE :	17
CLASSES D'ADRESSE :	17
ADRESSES IP PRIVEES :	18
MASQUE DE SOUS-RESEAU	20
SUBDIVISION DE RESEAU :	20
MASQUE DE SOUS-RESEAU :	20
MASQUE PAR DEFAUT :	20
MASQUE PERSONNALISE :	21
<i>Définir un masque de sous-réseau</i>	21
TABLES DE DEFINITION DES SOUS-RESEAUX :	24
<i>Exemple 6 sous réseaux de 30 postes</i> :	25
MASQUE DE SUR-RESEAU	26
OBJECTIF DU SUR-RESEAU :	26
PRINCIPE :	26
LE ROUTAGE TCP/IP	28
NOTION DE ROUTEUR :	28
ROUTAGE DE BASE :	29
ROUTAGE COMPLEXE :	30
TABLE DE ROUTAGE :	31
ROUTAGE STATIQUE :	31
ROUTAGE DYNAMIQUE :	31

RESEAU WINDOWS 10	32
GESTION CARTE RESEAU:	32
DESACTIVATION MEDIA SENSE:	34
ACCES AU CENTRE RESEAU ET PARTAGE :	35
DESACTIVATION CARTE EXCEDENTAIRE :	36
PROTOCOLES LLDP - MULTIPLEXAGE - TOPOLOGIE RESEAU WINDOWS:	37
PROTOCOLES IP-V4 IP-V6 QOS CLIENT ET PARTAGE RESEAUX	38
RE-INITIALISER TCP/IP SOUS WINDOWS 10 :	39
PROFIL – TYPE RESEAU WINDOWS 10 :	41
CHANGER DE TYPE DE PROFIL RESEAU – INTERFACE PARAMETRE :	42
CHANGER DE TYPE DE PROFIL RESEAU – POWERSHELL :	43
CHANGER DE TYPE DE PROFIL RESEAU WI FI – WINDOWS 1709	43
CHANGER DE TYPE DE PROFIL RESEAU – REGEDIT :	44
RESET - LISTES DES RESEAUX IDENTIFIES	45
RESEAU WINDOWS 7	46
PARAMETRAGE TCP/IP WINDOWS:.....	46
ACCES AU CENTRE RESEAU WINDOWS:	47
PROFIL – TYPE RESEAU SEVEN 7:.....	48
CHOISIR UN PROFIL RESEAU 7 :	48
PROFIL RESEAU AVANCE – VOISINAGE RESEAU	51
REGLAGE DISPONIBLES:.....	51
JEUX DE REGLAGES:.....	52
ACTIVER LA DECOUVERTE DU "VOISINAGE RESEAU":.....	53
MECANISME DU VOISINAGE RESEAU	55
PRINCIPE DE FONCTIONNEMENT :	55
RAFRAICHISSEMENT TESTS ET VERIFICATIONS :	56
PEUT ON EVITER L'ELECTION D'UN EXPLORATEUR ? :	56
PROTOCOLE DHCP	59
OBJECTIF DE DHCP :.....	59
FONCTIONNEMENT DE DHCP :	59
<i>DHCPDISCOVER</i> ou " <i>Demande de bail IP</i> " :	60
<i>DHCPOFFER</i> ou " <i>Offre de bail IP</i> " :	60
<i>DHCPREQUEST</i> ou " <i>Sélection de bail IP</i> " :	60
<i>DHCPACK / NACK</i> ou " <i>Accusé de réception de bail IP</i> " :	60
" <i>Renouvellement de bail IP</i> " :	61
<i>DHCPRELEASE</i> ou <i>libération des ressources</i> :	61
CLIENT DHCP	62
CLIENT DHCP WINDOWS 10 - SEVEN	62
IPCONFIG /RELEASE /RENEW :	63
ADRESSES IP AUTOMATIQUES (APIPA)	64
PRINCIPE APIPA ET DHCP:.....	64
APIPA ET WINDOWS:.....	64
DESACTIVATION ADRESSE APIPA:.....	64
ADRESSE IP ALTERNATIVE:	65
NOTION DE DNS	66
LE DNS:.....	66
<i>Noms DNS</i>	66
<i>Nom "Plat" Netbios</i>	66
<i>Nom "Hierarchique" DNS</i>	66
<i>Structure des domaines – délégation de zones</i>	67
ZONES DNS:	68
<i>Zone principale – secondaire</i>	69
<i>Requêtes itératives ou récursives</i>	69
<i>Résolution de Noms et Résolution inverse</i>	70
ORDRE DE RESOLUTION DNS PAR LE CLIENT WINDOWS :	70

NOM NETBIOS	72
PROCOLE NETBEUI :	72
RESOLUTION DE NOM NETBIOS	73
PARAMETRER LA RESOLUTION NETBIOS	74
NOM NETBIOS - NOM D'HOTE:	75
INTERPRETATION DES NOM NETBIOS :	76
HOSTS - LMHOSTS	79
FICHIER HOSTS ET LMHOSTS:.....	79
FICHIER LMHOSTS (NOM NETBIOS):.....	79
<i>Détails écriture lmhosts</i>	80
FICHIER HOSTS (NOM D'HOTE):	80
ANNEXE : TRAMES TCP/IP	81
BROADCAST :	81
UNICAST :	82
MULTICAST :	83
DOSSIER ..\SYSTEM32\DRIVER\ETC.....	84
FICHIERS EXEMPLES WINDOWS :	84
TP - WORKGROUP ENTRE RESEAUX	85
1 RESEAU IP ET X WORKGROUPS DIFFERENTS:	85
TEST ET VERIFICATION :	85
TP - MODIFIER LMHOSTS.....	86
INSCRIRE UNE MACHINE SIMPLE DANS LMHOSTS :	86
INSCRIRE UN CONTROLEUR DE DOMAINE DANS LMHOSTS :	86
TP - MODIFIER HOSTS	88
INSCRIRE UNE MACHINE DANS HOSTS :	88
INTERDIRE UNE MACHINE UN SITE DANS HOSTS :	89
TESTER TCP/IP.....	90
ICMP ET L'UTILITAIRE PING :	90
<i>Types de réponses à un ping</i>	90
<i>Méthodologie de test</i>	91
<i>Ping -a</i>	92
<i>Ping -t</i>	92
TEST TTL PING -I:	92
TRACERT :	94
PATHPING :	94
IPCONFIG.EXE /ALL:.....	95
ARP ET L'UTILITAIRE ARP -A :	96
<i>Arp -a</i>	96
USURPATION D'ADRESSE ARP :	97
TEST DE DNS.....	98
TEST DNS D'UN CLIENT D'UN DOMAINE :	98
<i>Nom d'hôte et FQDN</i>	98
<i>Nslookup en mode interactif</i>	98
NSLOOKUP ET NON-REPOSE DE SERVEUR WINDOWS :	102
NSLOOKUP ET PING :	103
SERVEUR DNS PUBLIC – CONNUS :	103
TESTER TCP-IP - NETSTAT.....	104
NETSTAT:	104
NETSTAT -A N PORT EN ECOUTE:.....	105
NETSTAT -A -P TCP PORT EN ECOUTE PAR PROTOCOLE:	105
TEST LIAISON FTP – AFFICHAGE DANS NETSTAT -AN :.....	106
NBTSTAT -N :	108

TELNET TEST DE SOCKET	109
INSTALLATION TELNET:	109
TELNET - TEST DE SOCKET = @IP+ PORT DISTANT:	110
<i>Port 3389 (RDP)</i>	110
<i>Port 22 (SFTP)</i>	111
<i>Port 21 (FTP)</i>	111
TESTER TCP/IP - COMPLEMENTS	112
TEST MTU PING -L -F:	112
<i>Constat de la valeur MTU 1500 en Wan</i>	112
<i>Jumbo Frames - MTU en Lan</i>	114
ROUTAGE ROUTE PRINT NETSTAT -R :	115
TEST ROUTAGE ROUTE ADD :	116

STRUCTURE DE TCP/IP

Modèle TCP/IP :

Par rapport au modèle OSI classique en 7 couches, le modèle présentant **TCP/IP** est composé de 4 couches uniquement :

OSI	TCP/IP
⑦ Application ⑥ Présentation ⑤ Session	④ Application : SNMP-FTP-SMTP...
④ Transport	③ Transport : TCP ou UDP
③ Réseau (routage)	② Internet : IP, ARP, ICMP routage : RIP, SPF
② Liaison ① Physique	① Interface Réseau

Couche 1 Interface Réseau :

Elle a en charge la communication physique avec le réseau. Par conséquent doit pouvoir accepter les normes **Ethernet, Token-Ring...**

Couche 2 Internet :

Elle s'occupe du routage et de la livraison des paquets au travers du protocole **IP (Internet protocol)**.

Tous les protocoles de la couche Transport passent par **IP** pour acheminer leurs données, mais IP est un protocole non connecté, il ne garantit pas donc que les paquets émis ne soient pas perdus, dupliqués ou inutilisables...

C'est aux couches supérieures (transport ou application) de vérifier le résultat!

La couche internet contient aussi un **protocole ICMP (Internet Control Messaging Protocol)** permettant de mettre en œuvre des contrôles sur le transport des paquets IP et de rapporter les erreurs...

La couche internet contient aussi un protocole **ARP (Adress resolution Protocol)** permettant de mettre en œuvre des mécanismes de résolution pour trouver une adresse physique avec une adresse IP...

Couche 3 Transport :

Elle a elle le rôle de fournir à la couche application une communication entre 2 machines...

2 protocoles existent selon que l'on souhaite utiliser une communication avec connexion ou sans...

le protocole **TCP (transmission Control Protocol)** est utilisé pour la communication connectée entre deux machines (fiable mais avec un débit relativement faible du fait des contrôles)

le protocole **UDP (user Datagram Protocol)** est utilisé pour la communication non connectée, sans garantie de distribution (moins fiable mais avec un débit plus élevé du fait de l'absence des vérifications)

Couche 4 Application :

Elle prend en charge toutes les activités supérieures du modèle OSI.

Plusieurs protocoles existent dans cette couche selon l'objectif visé :

SNMP (Simple Network management Protocol)	-> gestion de réseau
FTP (File transfer protocol)	-> transfert de fichier
SMTP (Simple Mail transfer Protocol)	-> courrier électronique
HTTP (Hyper Text Transfer Protocol)	-> serveurs web

LES PROTOCOLES DE TCP/IP

TCP (Transmission Control Protocol) :

TCP, on l'a dit, est un protocole utilisé pour la communication connectée entre deux machines (fiable mais avec un débit relativement faible du fait des contrôles)

Port et Socket :

Les **Ports** identifient les processus en cours d'exécution dans la couche application, et par conséquent un n° de port identifie un processus auquel on doit envoyer des données.

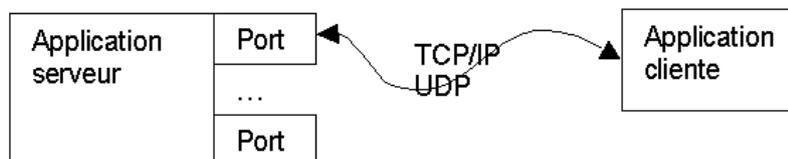
Les numéros de ports sont donnés de manière prédéterminée pour ceux allant de 1 à 1023, mais restent libres pour les autres

Il a été ainsi arbitrairement décidé d'un N° de Port pour chaque usage.

Port n° 21	: File Transfer Protocol
Port n° 22	: SSL connexion à distance sécurisée
Port n° 23	: Telnet
Port n° 25	: SMTP réception de courrier
Port n° 53	: DNS Domain Name Server
Port n° 80	: HTTP pages web
Port n° 88	: Kerberos authentification (NT 2000)
Port n° 110	: POP3 lecture de courrier
Port n° 137 à 139	: NetBios
Port n° 443	: HTTPS pages web sécurisées
Port n° 546	: DHCP

Les ports proposent 65535 point d'accès à un ordinateur à partir d'une seule adresse physique.

L'ensemble d'une adresse IP d'un ordinateur essayant de communiquer et du numéro de ports utilisé crée ce que l'on appelle un "**Socket**"



Communication en mode Connecté :

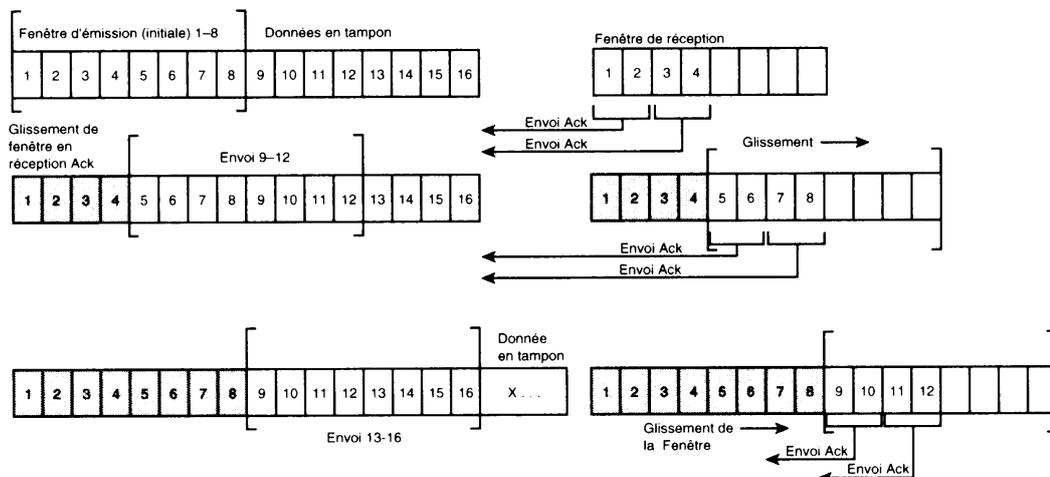
TCP demande qu'une session soit établie avant de transmettre les données entre les machines connectées.

En tant que protocole en mode connecté, TCP suit la transmission et la réception des paquets individuels durant la communication. TCP envoie les paquets en séquences et demande un accusé de réception de ces paquets avant d'en envoyer d'autres.

Etant donné le mécanisme de vérification effectué par TCP, le format d'un paquet TCP peut être assez complexe...

Fenêtres variables :

Chaque machine dispose d'une **fenêtre d'émission** et **d'une fenêtre de réception** qu'elle utilise comme tampon de donnée pour rendre la communication plus efficace.



Une **fenêtre de réception** permet à une machine de recevoir des paquets en désordre (en effet TCP utilise IP qui ne garantit pas l'ordre d'arrivée, ni même l'arrivée des paquets !) et de les classer pendant qu'elle attend les paquets suivants

Au fur et à mesure que la fenêtre de réception récupère des paquets, elle renvoi des accusés de réception (un accusé tous les 2 paquets reçus)

Si la fenêtre d'émission ne reçoit pas d'accusé de réception, elle attend puis retransmet les paquet non acquittés .

N.B : Dans la **fenêtre d'émission** un temporisateur est positionné pour chaque paquet envoyé, indiquant le temps à attendre avant d'estimer que le paquet n'est pas arrivé. En cas de non acquittement, le paquet est envoyé une nouvelle fois avec le temporisateur doublé, après cette nouvelle attente, s'il n'y a toujours pas d'acquittement, on recommence en doublant encore le temporisateur...avec un maximum de x tentatives...

N.B: Sous WINDOWS les fenêtres par défaut ont une taille de 8 kilo-octets, soit 8 trames Ethernet standard

N.B: Sous WINDOWS les fenêtres d'émission sont paramétrées par défaut pour tenter d'émettre 5 fois maximum

N.B: Lors d'une latence faible, la vitesse d'émission augmente progressivement, mais avec une latence forte, la vitesse d'émission va chuter !

UDP (User Datagram protocol) :

UDP, on l'a dit, est utilisé pour la communication non connectée, sans garantie de distribution (moins fiable mais avec un débit plus élevé du fait de l'absence des vérifications)

Port et Socket :

Les paquets **UDP** sont transmis comme pour TCP a des **Sockets**, c'est à dire à des couples adresses Ip + N° de Port, mais avec moins de fiabilité (puisque aucun contrôle n'est effectué...)

Port n° 67-68 : SNMP gestion - surveillance réseau
Port n° 520 : RIP routage IP dynamique

Communication en mode non Connecté :

On peut se demander où réside l'intérêt d'un tel protocole, fondamentalement dans sa faible surcharge (les données qu'il rajoute pour sa gestion sont très faibles par rapport aux données utiles transmises...)

Deux exemples suffiront à se convaincre de l'intérêt de ce protocole

exemple SNMP

SNMP utilise le protocole **UDP** pour véhiculer ses interrogations sur le réseau, et transmettre les messages d'erreurs d'une machine...

Il est normal que lorsque une machine soit défaillante, elle ne puisse réussir à mettre en place une session **TCP** pour transmettre son ... malaise !

une diffusion **UDP** est beaucoup plus raisonnable ne terme "espérance de vie" de la part de cette machine

exemple Vidéo et Son en ligne

Dans ce cas de figure il faut privilégier à tout prix le débit, ce que **UDP** fait, au détriment du paquet perdu, qu'il est bon d'ailleurs de ne pas tenter de réémettre...

En effet si on écoute un morceau de musique, et qu'un segment manque, notre oreille s'en rend à peine compte, et notre "cerveau" corrige ! Imaginons l'effet auditif du lecteur de CD qui bloque l'émission pour attendre la réception acquittée du fragment retardataire...

IP (Internet Protocol) :

Tous les protocoles de la couche Transport passent par **IP** pour acheminer leurs données, mais IP est un protocole non connecté, il ne garantit pas donc que les paquets émis ne soient pas perdus, dupliqués ou inutilisables...

C'est au couches supérieures (soit via TCP dans le transport ou application si on utilise UDP dans le transport) de vérifier le résultat!

Adresse IP

Ce protocole repose en partie sur la notion d'adresse IP (Internet Protocol) décernée de façon unique pour chaque élément matériel faisant partie d'un réseau

on verra cette notion en détail dans le chapitre "Adresse IP" (page 16)

Datagramme

IP reçoit des information des protocoles **TCP** ou **UDP** et les renvoi dans ce que l'on appelle un **Datagramme**, c'est à dire un bloc de donnée dans lequel IP à rajouté ses informations (type de protocole utilisé : udp ou tcp, adresse ip de la machine d'origine, adresse ip de la machine destinataire, durée de vie...) aux données utiles.

Les données qui circulent sur Internet sous forme de datagrammes (on parle aussi de paquets) sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination, ...).

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Voici ce à quoi ressemble un datagramme:

←----- 32 bits ----->

Version	Taille d'en-tête	type de service	Longueur totale	
Identification		Drapeau	Décalage fragment	
Durée de vie	Protocole	Somme de contrôle en-tête		
Adresse IP source				
Adresse IP destination				
Données				

Voici la signification des différents champs:

- **Version:** il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4 *IPv4*) afin de vérifier la validité du datagramme. Elle est codée sur 4 bits
- **Taille d'en-tête:** il s'agit du nombre de mots de 32 bits sur lesquels sont répartis l'en-tête
- **Type de service:** il indique la façon de laquelle le datagramme doit être traité
- **Longueur totale:** il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données
- **Identification, drapeaux (flags) et déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes, il sont expliqués plus loin dans l'assemblage.

- **Durée de vie: (appelée aussi TTL: Time To Live)** indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus
- **Protocole:** ce champ permet de savoir de quel protocole est issu le datagramme avec par exemple

ICMP:	1
IGMP:	2
TCP:	6
UDP:	17
- **Somme de contrôle de l'en-tête (header checksum):** ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.
- **Adresse IP Source:** Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre
- **Adresse IP destination:** Adresse IP du destinataire du message

Fragmentation MTU

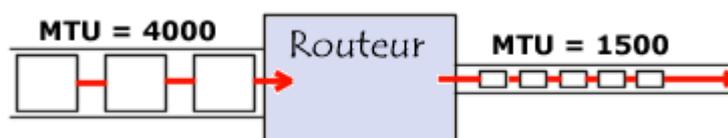
La taille d'un Datagramme dépendant du type de réseau utilisé, Ethernet, Token-Ring...IP doit alors éventuellement découper les données qu'il reçoit de TCP ou de UDP en morceau pour être émises dans plusieurs Datagrammes de taille adéquate. Ce découpage, avec repérage et étiquetage des morceaux s'appelle la Fragmentation.

la taille d'un datagramme maximale est de 65535 octets. Toutefois cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets. De plus, les réseaux sur Internet utilisent différentes technologies, si bien que la taille maximale d'un datagramme varie suivant le type de réseau.

La taille maximale d'une trame est appelée **MTU (Maximum Transfer Unit)**, elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont les MTU sont différents



Assemblage

Bien sûr à l'arrivée **IP** doit récupérer tous les morceaux et reconstruire les données d'origine, cela s'appelle l'**Assemblage**.

Le routeur va donc ensuite envoyer ces fragments de manière indépendante et ré-encapsulé (il ajoute un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment, et en ajoutant des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre (rien ne dit que les fragments vont arriver dans le bon ordre étant donné qu'ils sont acheminés indépendamment les uns des autres...).

Un datagramme possède plusieurs champs pour calculer l'assemblage:

Routage

Le protocole **IP** doit **router** les datagrammes d'un réseau à l'autre. Toutes les machines d'un réseau ne sont pas des routeurs, mais un **routeur** est une machine qui lorsqu'elle reçoit un datagramme qui ne lui est pas adressé, doit renvoyer ce paquet sur le réseau dans la bonne direction pour qu'il atteigne sa destination...Le principe du routage IP peut être résumé ainsi:

1. **Extraire** l'adresse IP de destination du datagramme.
2. Appliquer à cette adresse le masque de sous-réseau éventuel (ET logique entre l'adresse et le masque).
3. Extraire la partie "**Identificateur Réseau**" de l'adresse ainsi obtenue.
4. S'agit-il du réseau local ?
 - Si oui, procéder à l'encapsulation et au **routage direct**.
 - Si non, existe-t-il une entrée dans la **table de routage** pour ce réseau de destination ?
 - a. Si oui, envoyer le datagramme vers la passerelle spécifiée dans la table.
 - b. Si non, existe-t-il une **route par défaut** ?
 - Si oui, envoyer le datagramme à la passerelle spécifiée par la route par défaut.
 - Si non, déclarer une **erreur** de routage. (Protocole ICMP)

Durée de Vie TTL

La durée de vie ou **TTL (Time To Live)** correspond à l'idée suivante. Chaque fois qu'un **Datagramme** prend le départ d'une machine sur le réseau vers une destination connue, il a une espérance de vie exprimée en seconde.

A chaque passage dans un **routeur**, celui-ci décrémente de 1 seconde son compteur **TTL** de vie, de sorte que si le datagramme tarde trop à parvenir à la machine destinataire, un routeur le "détruit" en réduisant son **TTL** à 0

N.B: Sous Windows les Datagrammes ont une valeur de Vie par défaut de 128, Sous linux la valeur est à 64

ICMP (Internet Control Message Protocol) :

ICMP permet de mettre en œuvre des contrôles sur le transport des paquets IP et de rapporter les erreurs...

Les messages **ICMP** servent principalement à rapporter des erreurs et envoyer des requêtes.

Dans la pratique on utilise le protocole **ICMP** essentiellement pour envoyer des requêtes **d'Echo request** et pour attendre des réponses **d'Echo reply**, et encore ceci à travers un utilitaire **PING (Personnal Internet Groper)**

On verra cette notion en détail dans le chapitre "Tester IP" (page 90)

ARP (Address Resolution Protocol) :

A part dans le cas où on émet en diffusion, lorsque IP souhaite émettre, il doit connaître l'adresse physique, ou adresse mac, ou adresse Ethernet du poste destinataire

ARP permet de mettre en œuvre des mécanismes de résolution pour trouver l'adresse physique correspondant à une adresse IP locale...

Si **ARP** ne connaît pas l'adresse physique de l'adresse IP locale demandée, il fonctionne par diffusion locale et, une fois trouvée, stocke cette correspondance dans sa mémoire (pendant un certain temps)

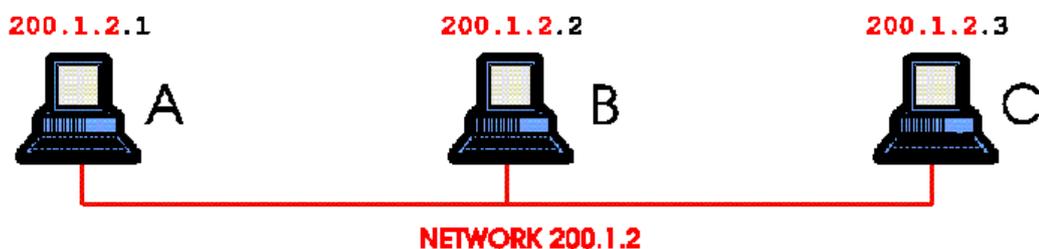
Si **ARP** connaît l'adresse physique dans son cache, il ne diffuse rien sur le réseau et cela fonctionne très bien

N.B : Mais **ARP** ne peut trouver que des adresses physiques locales, et il ne retourne jamais à IP une adresse physique qui se trouve sur un réseau distant ! Dans ce cas **IP** (qui peut via l'adresse ip se rendre compte que la machine demandée n'est pas une machine locale) ne demande pas à **ARP** de trouver l'adresse physique de la machine distante, mais il lui demande de trouver l'adresse physique du **routeur** !

On verra cette notion en détail dans le chapitre "Tester IP" (page 90)

Exemple de fonctionnement de ARP en local

Soit un réseau interne TCP/IP comprenant un segment Ethernet et trois machines. Le numéro de réseau IP de ce segment est 200.1.2. Les numéros d'hôte pour A, B et C sont 1, 2 et 3 respectivement. Ce sont des adresses de classe C, ce qui permet d'avoir 254 machines sur ce segment.



Supposons que A veuille envoyer un paquet à C pour la première fois, et qu'il connaît l'adresse IP de C. Pour envoyer ce paquet sur ce brin Ethernet, A aura besoin de connaître l'adresse MAC (ou adresse Ethernet) de C. Le

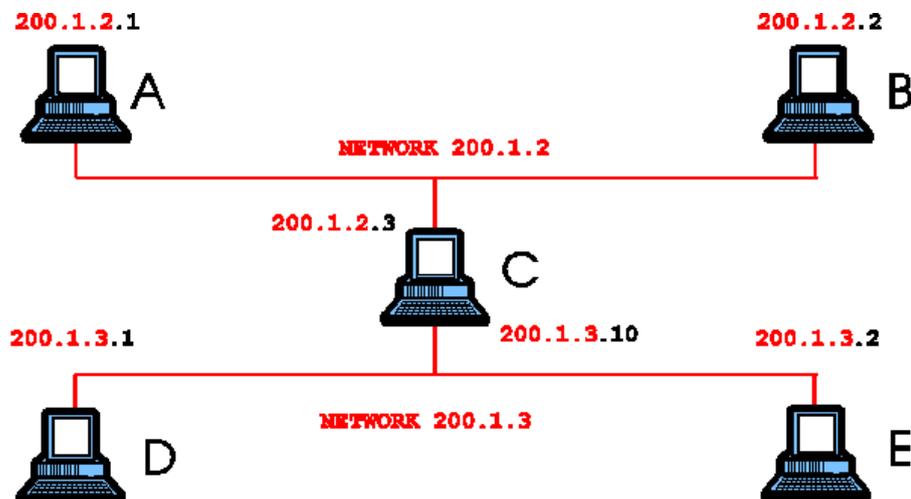
protocole **ARP (Address Resolution Protocol)** est utilisé pour trouver dynamiquement cette adresse.

ARP garde une table interne d'adresses IP et d'adresses MAC correspondantes. Quand A essaye d'envoyer un paquet IP à C, le module d'ARP consulte sa table d'adresses IP et ne découvrira aucune entrée pour C. ARP envoie alors un paquet spécial reçu par tous (broadcast), demandant l'adresse MAC correspondant à l'adresse IP qu'il connaît. S'il n'y a pas de "time-out", cela signifie que la machine C a répondu en incluant son adresse MAC dans sa réponse, et le tour est joué. A met à jour sa table d'adresse (ou table d'hôte) et peut envoyer son paquet.

Exemple de fonctionnement de ARP et Routeur

Considérons maintenant 2 réseaux Ethernet séparés et reliés par la machine C, fonctionnant comme un routeur.

La machine C agit comme un routeur entre ces deux réseaux. Un routeur est un élément qui choisit différentes directions pour les paquets en fonction de



l'adresse IP. Comme il y a deux segments Ethernet séparés, chaque réseau a son propre numéro de réseau de classe C. Ceci est indispensable car le routeur ne connaît que des interfaces sont associées à un réseau.

Si A veut envoyer un paquet à E, il doit d'abord l'envoyer à C qui peut faire suivre le paquet à E. Ceci est possible car A utilise l'adresse MAC de C et l'adresse IP de E. C va donc recevoir le paquet destiné à E et va le faire suivre en utilisant l'adresse MAC de E, soit parce qu'il la connaît, soit en faisant une requête ARP comme décrit précédemment.

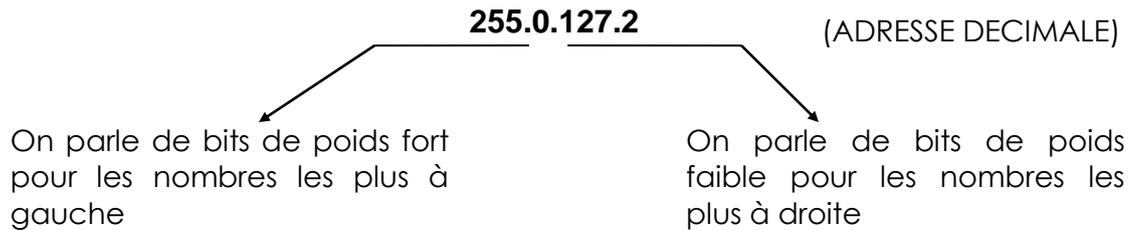
Si E reçoit le même numéro de réseau que A, soit "200.1.2", A essayera d'atteindre E de la même façon qui atteint C, par exemple, en envoyant une requête ARP et en attendant la réponse. Quoiqu'il en soit, comme E est physiquement sur un fil différent, il ne verra jamais la requête ARP et le paquet ne pourra pas être délivré. En spécifiant que E est sur un réseau différent, le module IP de A saura que E ne peut être atteint sans avoir été fait suivre par un nœud (élément reliant deux réseaux différents comme un routeur) de son réseau.

ADRESSE IP

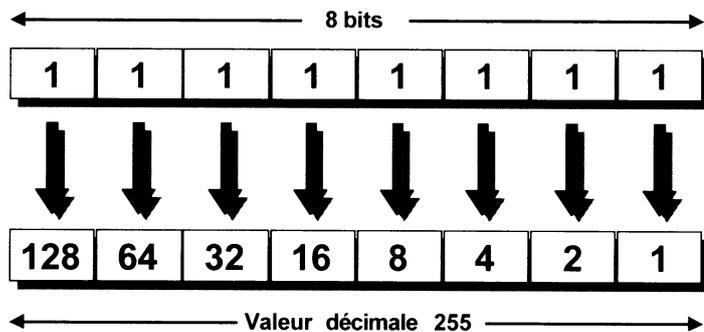
Adresse IP :

La version actuelle de ce protocole désormais quasi universel repose en partie sur la notion d'adresse **IP** (Internet Protocol) décernée de façon unique pour chaque élément matériel faisant partie d'un réseau

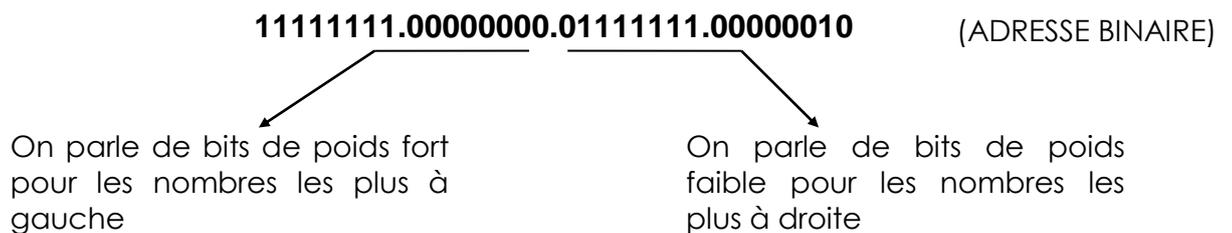
Ces adresses sont codées sur 32 bits, est sont représentées sous la forme de 4 nombre compris entre 0 et 255 (valeur d'un octet) et séparés par un point, soit (par exemple)



Chaque nombre décimal est la représentation d'un nombre binaire de 8 chiffres



On peut alors avoir aussi en notation binaire



On pourrait ainsi dire que les adresses IP varient de la plus petite 0.0.0.0 à la plus grande 255.255.255.255

N.B : En fait toutes les combinaisons ne sont pas disponibles, et elles reflètent une certaine logique

ID réseau et ID hôte :

Les bits de poids fort définissent l'adresse du réseau, on parle de **ID réseau** et Les bits de poids faible définissent l'adresse d'un équipement dans le réseau on parle de **ID hôte**.

L' **ID réseau** identifie toutes les machines qui se trouvent sur le même réseau physique , encore appelé domaine de collision. Il s'agit d'un identifiant pour un réseau local, toutes les machines se trouvant "du même côté d'un routeur...(sur la même « patte »...)

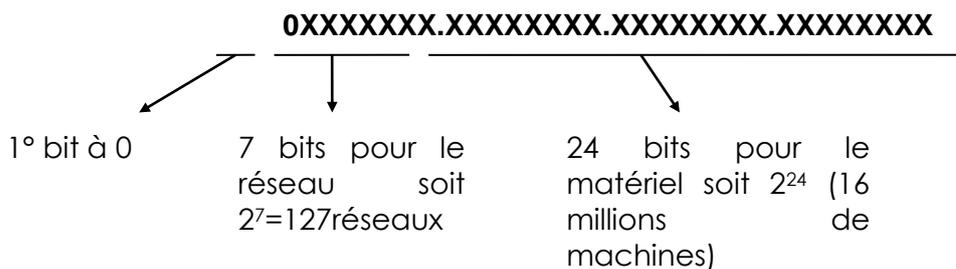
L' **ID hôte** identifie tout poste ou périphérique du réseau, il est unique à l'intérieur de tout **ID réseau**

Classes d'Adresse :

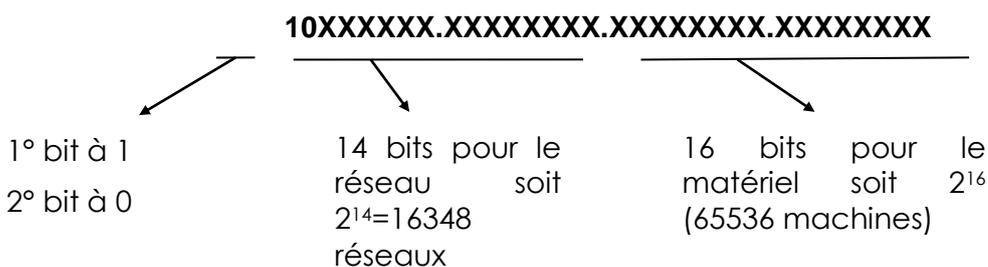
La limite entre poids fort et poids faible n'est pas toujours la même, c'est la notion de "**classe d'adresse**"

- plus les poids fort sont petits, et plus le nombre de machines dans un même réseau sera important, même si on aura peut de réseau
- plus les poids fort sont nombreux, on aura alors peut de machines connectable pour chacun de ces réseau, même s'il sont plus nombreux

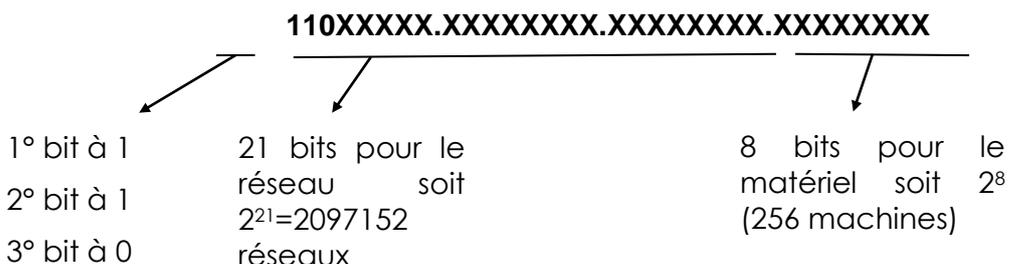
Réseau de **Classe A** : (commence par **1** à **127**)



Réseau de **Classe B** : (commence par **128** à **191**)



Réseau de **Classe C** : (commence par **192** à **223**)



Soit en résumant

	Premier octet	Deuxième octet	Troisième octet	Quatrième octet	Masque de sous-réseau
Classe A	Réseau	Hôte	Hôte	Hôte	255.0.0.0 ou /8
Classe B	Réseau	Réseau	Hôte	Hôte	255.255.0.0 ou /16
Classe C	Réseau	Réseau	Réseau	Hôte	255.255.255.0 ou /24

Classe de l'adresse	Première plage d'octets	Nombre de réseaux possibles	Nombre d'hôtes par réseau
Classe A	De 0 à 127	128 (2 sont réservés)	16,777,214
Classe B	De 128 à 191	16,348	65,534
Classe C	De 192 à 223	2,097,152	254

	Nombre de réseau	Nombre d'hôtes par réseau	Plage d'ID de réseau (premier octet)
Classe A	126	16 777 214	1 – 126
Classe B	16 384	65 534	128 – 191
Classe C	2 097 152	254	192 – 223

Avec quelques règles supplémentaires :

- l'**ID réseau 127**, est réservée pour les tests
- Un **ID réseau** composé exclusivement de 1 ou de 0 n'est jamais attribué
- Un **ID hôte** composé exclusivement de 1 ou de 0 n'est jamais attribué
- La valeur **255.255.255.255** correspond à une diffusion générale (**Broadcast**)

Adresses IP Privées :

Il est normal d'assigner des adresses globalement uniques à toutes les machines qui utilisent TCP/IP.

Les machines qui utilisent TCP/IP peuvent être divisées en 3 catégories:

- **Catégorie 1 :** les machines qui n'ont pas besoin d'accéder à des machines d'autres entreprises ou à l'Internet dans son ensemble. Les machines de cette catégorie peuvent utiliser des adresses IP qui sont uniques dans l'entreprise, mais qui peuvent être ambiguës entre différentes entreprises.

- **Catégorie 2 :** les machines qui ont besoin d'accéder à un nombre limité de services extérieurs (ex: E-Mail, WWW, FTP) qui peuvent être servis par des passerelles applicatives. Pour beaucoup de machines dans cette catégorie, un accès non restreint (fourni par la connectivité IP) n'est pas forcément nécessaire et même quelque fois non désiré pour des raisons de sécurité. Pour les mêmes raisons que pour les machines de la première catégorie, de telles machines peuvent utiliser des adresses IP uniques dans l'entreprise, mais qui peuvent être ambiguës entre différentes entreprises.
- **Catégorie 3 :** les machines qui ont besoin d'un accès réseau à l'extérieur de l'entreprise (fourni par la connectivité IP). Les machines de cette dernière catégorie ont besoin d'une adresse unique sur tout l'Internet.

On parle pour les machines des catégories 1 et 2 comme de machines "privées", et pour les machines de la 3ème catégorie comme des machines "publiques".

L'Autorité d'Affectation de Numéros sur Internet a réservé les 3 blocs suivants dans l'espace d'adressage pour des réseaux internes RFC 1918:

le premier bloc n'est rien d'autre qu'une classe A n° **10**.

10.0.0.0 - 10.255.255.255 (10/8 prefix)

le second, un ensemble de 16 classes B contiguës entre n° **172.16. et 172.31**.

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

N.B: pour **172.16.0**. le premier hôte disponible sera .0.1 (éviter N° à 0 totalement)

et le troisième, un ensemble de 256 classes C de n° **192.168.0. à 192.168.255**.

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

N.B: pour **192.168.0**. le premier hôte disponible sera .1 (éviter N° à 0 totalement)

Les **machines privées** peuvent communiquer avec toutes les autres machines de l'entreprise, à la fois publiques et privées. Néanmoins, elles ne peuvent avoir de connectivité IP avec une machine à l'extérieur de l'entreprise. Même si elles n'ont pas de connectivité IP vers l'extérieur, les machines privées peuvent toutefois avoir accès à des services extérieurs grâce à des passerelles (ex passerelles applicatives).

Pour connecter un réseau utilisant des adresses privées RFC 1918 sur Internet, il est nécessaire de prévoir un système de traduction d'adresse (Network Address Translator) ou un système de proxy

Les **machines publiques** peuvent communiquer avec d'autres machines privées ou publiques à l'intérieur de l'entreprise et possèdent une connectivité IP avec les machines publiques extérieures à l'entreprise. Les machines publiques n'ont pas de connectivité avec des machines privées d'autres entreprises.

MASQUE DE SOUS-RESEAU

Subdivision de réseau :

Très fréquemment on constitue un réseau à partir de segments ou brins interconnectés entre eux via des routeurs...

Les avantages à avoir un réseau bien segmenté sont nombreux :

- Différentes techniques de réseau peuvent être mélangées (Ethernet et Token-Ring par exemple...)
- Les collisions sont limitées car les diffusions générales sont limitées au segment local
- Extension à un nombre pratiquement infini d'hôtes

Masque de sous-réseau :

Le **masque de sous-réseau** permet de définir le découpage entre les bits de l'adresse qui servent à définir l'adresse de réseau, et ceux servant à définir l'adresse de la machine

En effet via un système de **ET bit à bit**, le **masque de sous-réseau** permet de distinguer l'**ID réseau** à partir de l'**Id hôte**, et par conséquent permet à **TCP/IP** de savoir si une **adresse IP** donnée se trouve sur le **réseau local** ou sur un **réseau distant**

Masque par défaut :

Ainsi dans des masques standards, tous les bits correspondants à l'**ID réseau** sont à 1, tous les bits correspondants à l'**ID hôte** sont à 0

Classe d'adresse	Bits utilisés pour le masque de sous-réseau				Notation décimale à points
Classe A	11111111	00000000	00000000	00000000	255.0.0.0
Classe B	11111111	11111111	00000000	00000000	255.255.0.0
Classe C	11111111	11111111	11111111	00000000	255.255.255.0

Masque personnalisé :

L'objectif est ici d'obtenir des adresses d'**ID réseau** et d'**Id hôte** groupées de manière un peu différente par rapport aux classes standardisées A-B-C qui servent de cadre

Pour définir des sous-réseaux personnalisés, il est nécessaire de définir :

- Combien de réseau veut on gérer à l'intérieur de la plage d'adresse attribuée
- Combien d'hôtes maximum veut on gérer à l'intérieur d'un sous-réseau

N.B: en prévoyant une évolution future raisonnable !

Puis travailler de la manière suivante :

- Définir le masque de sous-réseau qui donne le nombre de sous-réseau et d'hôte par sous-réseau voulu
- Déterminer les **ID réseaux** possibles à utiliser
N.B: (cf tables page 24 pour savoir combien il y en a)
- Déterminer les **ID hôtes** possibles à utiliser
N.B: (cf tables page 24 pour savoir combien il y en a)

Définir un masque de sous-réseau

On l'a dit, l'**ID réseau** se calcule en regardant le nombre de 1 du masque de sous-réseau.

Pour augmenter le nombre d'**ID réseau**, il faut ajouter des bits au masque de sous-réseau (Bien sûr si on augmente le nombre d'**ID réseau**, on diminue le nombre d'**ID hôte**...)

De combien de bit faut-il augmenter le masque de sous-réseau ?

Comme on travaille avec les puissances de 2, on augmente les combinaisons de $2^{\text{nb bits ajoutés}}$

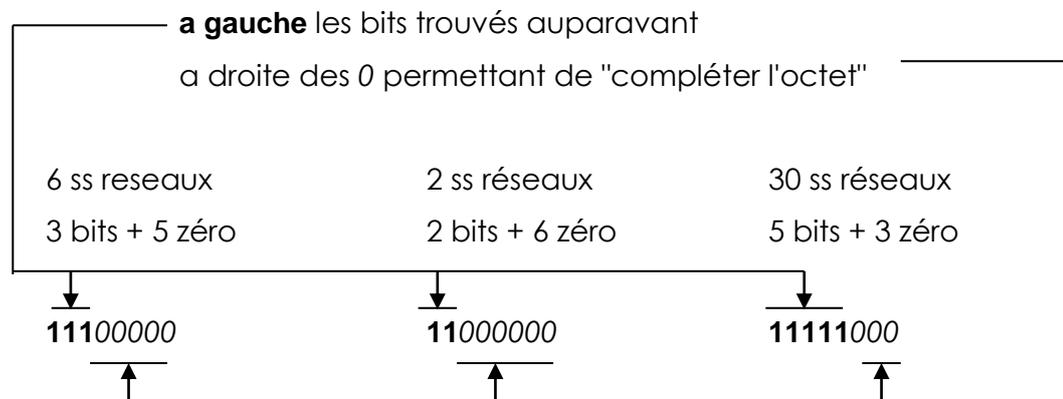
soit	1 bit	2 sous-réseaux
	2 bit	4 sous réseaux
	3 bits	8 sous réseaux
	4 bits	16 sous réseaux
	5 bits	32 sous réseaux
	x bits	2^x . sous-réseaux

mais rappelez vous, les adresse ne contenant que des 0 ou que des 1 ne sont pas autorisées, par conséquent il faut enlever les 2 adresses extrêmes possibles...ce qui nous donne

soit	1 bit	impossible	(2-2=0)
	2 bit	2 sous réseaux	(4-2)
	3 bits	6 sous réseaux	(8-2)
	4 bits	14 sous réseaux	(16-2)
	5 bits	30 sous réseaux	(32-2)
	x bits	$(2^x)-2$ sous-réseaux	

Comment calculer le nouveau masque de sous-réseau de mes réseaux?

1. Une fois trouvé le nombre de bits me permettant d'obtenir le nombre de sous-réseaux voulu, je dois créer un octet avec :



2. puis le convertir en décimal

11100000	11000000	11111000
=128+64+32	=128+64	=128+64+32+16+8
224	192	248

3. et remplacer dans la masque par défaut de ma classe d'adresse, le premier 0 par ce nombre...

6 ss reseaux	2 ss réseaux	30 ss réseaux
224	192	248

si l'adresse est de classe **A** cela donne par rapport au masque **255.0.0.0**

255.224.0.0	255.192.0.0	255.248.0.0
--------------------	--------------------	--------------------

si l'adresse est de classe **B** cela donne par rapport au masque **255.255.0.0**

255.255.224.0	255.255.192.0	255.255.248.0
----------------------	----------------------	----------------------

si l'adresse est de classe **C** cela donne rapport au masque **255.255.255.0**

255.255.255.224	255.255.255.192	255.255.255.248
------------------------	------------------------	------------------------

Comment calculer les ID réseau de mes réseaux?

1. Recenser toutes les combinaisons possibles (en excluant donc celles n'ayant que des 1 ou des 0) de bits ajoutées au masque de sous-réseau précédemment et les convertir en décimal:

6 ss réseaux	2 ss réseaux	30 ss réseaux
(111)00000	(11)000000	trop long !
11000000	10000000	
10100000	01000000	
01100000	(00)000000	
10000000		
01000000		
00100000		
(000)00000		

2. Les convertir en décimal:

6 ss réseaux	2 ss réseaux
192	64
160	32
128	
96	
64	
32	

3. Ajouter ces valeurs a l'**ID réseau** d'origine:

Comment calculer les ID hôtes disponibles dans mes réseaux?

Les **ID hôte** commencent par la valeur .001 dans le dernier octet et augmentent 1 par 1 jusqu'à atteindre la valeur ID de sous-réseau du réseau suivant, -1

Bien sûr le dernier octet lui aussi ne peut pas être égal à 0 ou 255.

Tables de définition des sous-réseaux :

Voilà le nombre de sous-réseau utilisables, avec le nombre d'hôte possible pour un masque de sous-réseau donné, et ce pour les

Adresses de classe A:

<i>Bits supplémentaires (n)</i>	<i>Nombre maximum de sous-réseaux (2ⁿ-2)</i>	<i>Nombre maximum d'hôtes par sous-réseau (2²⁴⁻ⁿ-2)</i>	<i>Masque de sous-réseau</i>
0	0	16 777 214	255.0.0.0
1	invalide	invalide	invalide
2	2	4 194 302	255.192.0.0
3	6	2 097 150	255.224.0.0
4	14	1 048 574	255.240.0.0
5	30	524 286	255.248.0.0
6	62	262 142	255.252.0.0
7	126	131 070	255.254.0.0
8	254	65 534	255.255.0.0

Adresses de classe B:

<i>Bits supplémentaires (n)</i>	<i>Nombre maximum de sous-réseaux (2ⁿ-2)</i>	<i>Nombre maximum d'hôtes par sous-réseau (2¹⁶⁻ⁿ-2)</i>	<i>Masque de sous-réseau</i>
0	0	65 534	255.255.0.0
1	invalide	invalide	invalide
2	2	16 382	255.255.192.0
3	6	8 190	255.255.224.0
4	14	4 094	255.255.240.0
5	30	2 046	255.255.248.0
6	62	1 022	255.255.252.0
7	126	510	255.255.254.0
8	254	254	255.255.255.0

Adresses de classe C:

<i>Bits supplémentaires (n)</i>	<i>Nombre maximum de sous-réseaux (2ⁿ-2)</i>	<i>Nombre maximum d'hôtes par sous-réseau (2⁸⁻ⁿ-2)</i>	<i>Masque de sous-réseau</i>
0	0	254	255.255.255.0
1	invalide	invalide	invalide
2	2	62	255.255.255.192
3	6	30	255.255.255.224
4	14	14	255.255.255.240
5	30	6	255.255.255.248
6	62	2	255.255.255.252
7	invalide	invalide	255.255.255.254
8	invalide	invalide	255.255.255.255

Exemple 6 sous réseaux de 30 postes :

Si on veut **6 sous réseaux** comportant chacun 30 machines maximum, on pourra prendre alors comme masque de sous réseau **255.255.255.224**

- **Id réseau**

pour trouver les Id réseau je dois trouver toutes les combinaisons de **3 bits** de 111 à 000 en laissant tomber les valeurs n'ayant que des 0 ou que des 1 (non autorisée).J'obtiens 110-101-011-100-010-001 soit en décimal 192-160-128-96-64-32.

que je rajoute à mon Id réseau d'origine 192.168.1.xx soit donc les Id réseau suivantes :

192.168.1.**192** 192.168.1.**160** 192.168.1.**128** 192.168.1.**96**
192.168.1.**64** 192.168.1.**32**

- Id hôte valide

un petit calcul nous donne :

sous-réseau	1° adresse IP	dernière adresse IP
192.168.1. 32	192.168.1.33	192.168.1.63
192.168.1. 64	192.168.1.65	192.168.1.95
192.168.1. 96	192.168.1.97	192.168.1.127
192.168.1. 128	192.168.1.129	192.168.1.159
192.168.1. 160	192.168.1.161	192.168.1.191
192.168.1. 192	192.168.1.193	192.168.1.223

MASQUE DE SUR-RESEAU

Objectif du sur-réseau :

La question ici n'est pas de délimiter des sous-réseaux (donc des sous-ensemble de moins de 255 machines pour une classe C par exemple), **mais plutôt de faire en sorte que l'on puisse adresser "ensemble" plus de 255 machines, mais en restant avec des adresses de classe C ! (par exemple)**

Ainsi imaginons un réseau constitué au départ d'une centaine de machines dont les adresses IP privées ont été définies en classe C, par exemple sur les adresses de base suivantes: 192.168.25.1 à 192.168.25.100. Ce réseau grandit, et voit le nombre des machines dépasser les 255 postes, que faire ?

classiquement on peut agir de différentes manières :

- Fractionner le réseau en plusieurs zones distinctes, et les relier par un (des) routeurs...
- Passer à des adresse de type Classe B, par exemple 172.16.0.1 à 172.16.1.xxx avec un masque par défaut de 255.255.0.0
- Augmenter la taille du masque par défaut, de 255.255.255 à c'est du sur-réseau !

Principe :

l'agrégation de plage d'adresse, ou "**super-netting**" s'effectue en modifiant le masque de sous-réseau. La modification, dépend du nombre (puissance de 2) de classe que l'on souhaite "agréger" :

Nombre Classes à agréger	Masque sous-réseau	nombre de Hosts maximum disponibles
1	255.255.255.0	256
2	255.255.254.0	512
4	255.255.252.0	1024
8	255.255.248.0	2048
16	255.255.240.0	4096
32	255.255.224.0	8192
64	255.255.192.0	16384
128	255.255.128.0	32768
256	255.255.0.0	65536

Dans notre cas pour adresser un maximum de 1024 machines, il faut agréger 4 classes par exemple, et comme masque prendre la valeur 255.255.252.0,

Ce qui permet d'avoir en fait 256/4 plages adressables de 1024 machines chacune, suivant le tableau ci-dessous :

N° plage	Adresse Début	Adresse Fin	Masque	nb Hosts maxi
1	192.168.0.0	192.168.3.255	255.255.252.0	1024
2	192.168.4.0	192.168.7.255	255.255.252.0	1024
3	192.168.8.0	192.168.11.255	255.255.252.0	1024
4	192.168.12.0	192.168.15.255	255.255.252.0	1024
5	192.168.16.0	192.168.19.255	255.255.252.0	1024
...x...	192.168. (x*4)-4 .0	192.168. (x*4)-1 .255	255.255.252.0	1024
64	192.168.252.0	192.168.255.255	255.255.252.0	1024

N.B: les adresses faisant partie du même N° plage sont vues comme faisant partie d'une même réseau, donc ne nécessitent pas de routage entre elles

N.B: les adresses ne faisant pas partie du même N° plage sont vues comme faisant partie de réseaux différents, donc nécessitent un routage entre elles

LE ROUTAGE TCP/IP

Notion de routeur :

De manière générale, une machine peut communiquer uniquement par défaut avec une autre machine de son réseau local, c'est à dire une autre machine faisant partie de son sous-réseau, encore appelé domaine de collision.

Que ce sous-réseau soit obtenu par l'application d'un masque de sous-réseau par défaut isolant des classes A, B ou C complète, ou qu'il soit obtenu par l'application d'un masque de sous-réseau personnalisé modifiant l'étendue par défaut des ID réseau et des ID hôtes, l'idée est la même :

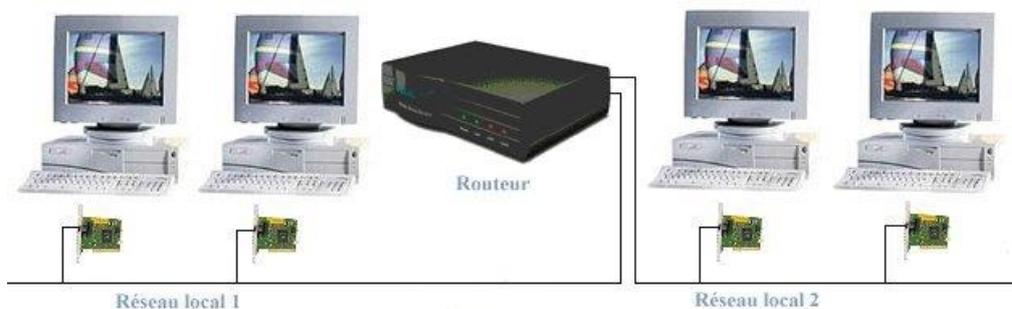
IP compare l'ID de sous-réseau de l'adresse IP que l'on cherche à joindre à l'ID de sous-réseau du réseau local dans lequel il se trouve :

- **Si les deux ID correspondent** : IP peut chercher localement la machine
- **Si les deux ID ne correspondent pas** : IP envoie la trame vers un équipement où il peut être routé

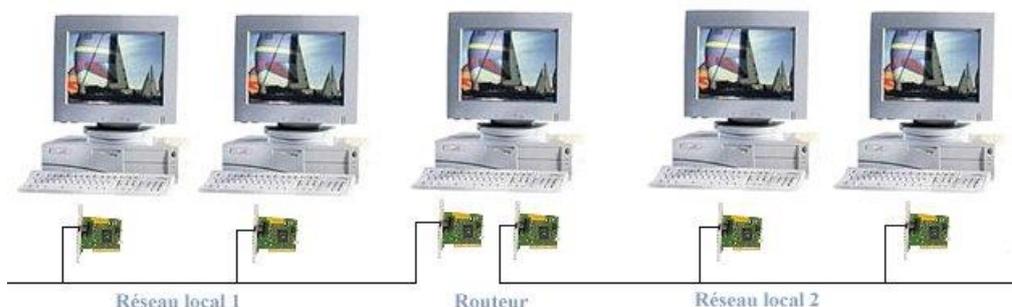
Lorsque des machines sont interconnectées en plusieurs sous-réseaux, elles doivent toutes avoir comme paramétrage l'adresse IP d'une passerelle - **routeur** par défaut

Une adresse IP différente est assignée à chaque carte sur chaque sous-réseau, permettant à ce **routeur** de faire partie de plusieurs réseaux différents. On parle alors aussi **d'hôte multi-résident**.

Un routeur peut être soit un matériel spécifique,



Soit une fonction assurée par une station de travail possédant au moins deux interfaces réseaux, et une application pour le routage.

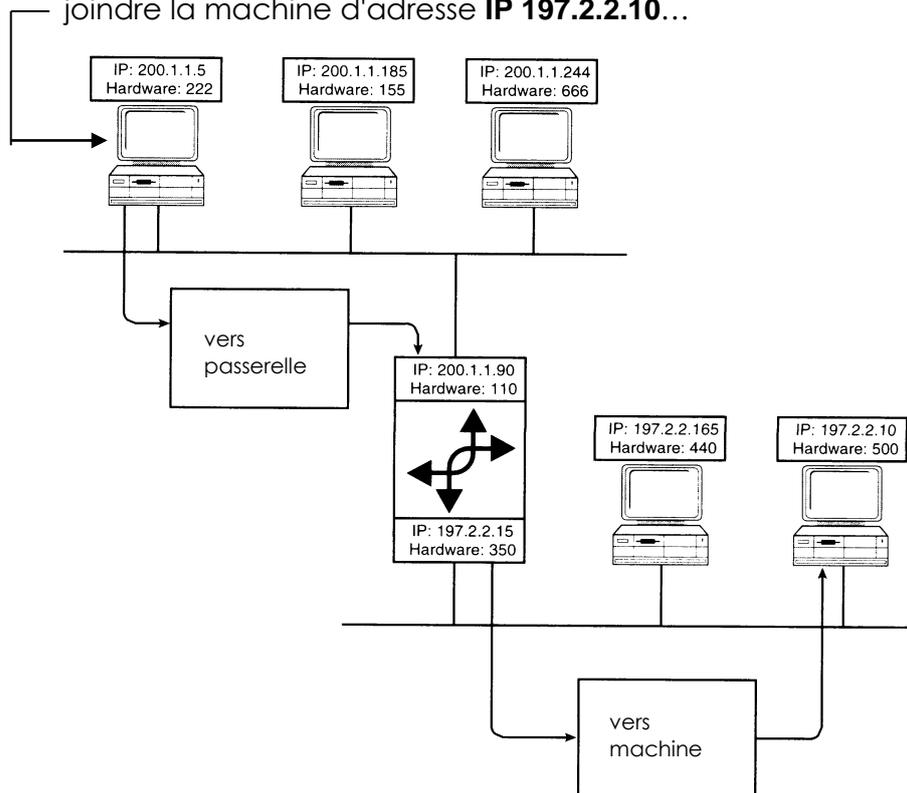


N.B: Toute machine windows Serveur peut faire office de routeur à partir du moment ou elle dispose d'autant de cartes réseaux que de sous-réseaux auxquels elle souhaite être rattachée.

Routing de base :

Dans la situation la plus simple, on relie **deux sous-réseaux** par **un routeur** ayant donc **deux cartes réseaux** et **deux adresses IP** dans chaque sous-réseau auxquels il appartient :

Dans l'exemple ci-dessous, la machine d'adresse **IP 200.1.1.5** essaye de joindre la machine d'adresse **IP 197.2.2.10...**



Le fonctionnement est le suivant :

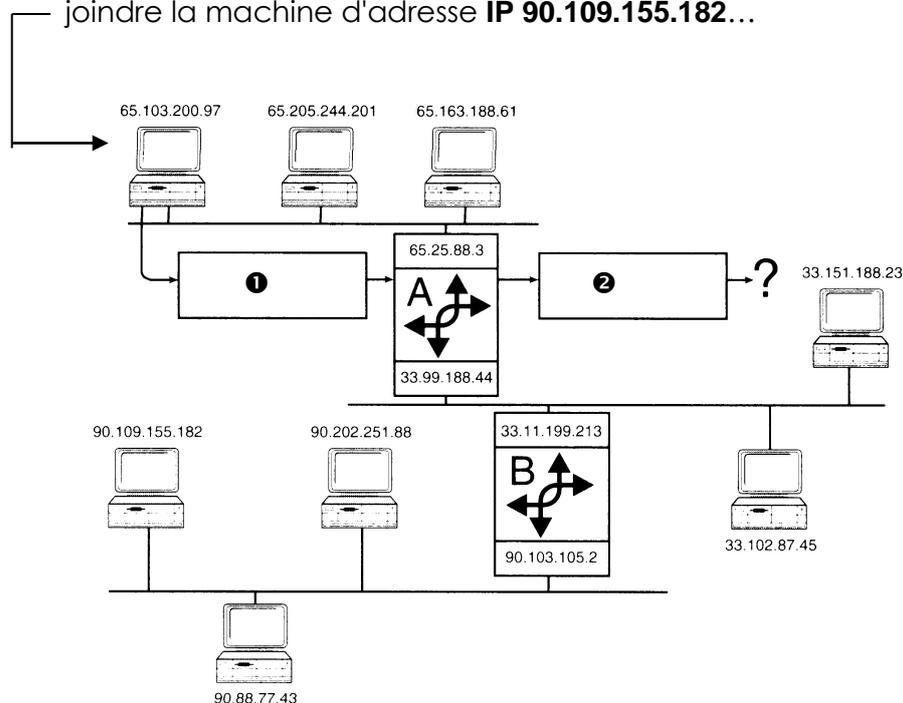
1. IP se rends compte que l'adresse de destination n'est pas une adresse locale (ID réseau cherchée **197.2.2.0** différente de ID réseau locale **200.1.1.0**)
2. IP transmet alors le paquet à la passerelle par défaut
3. IP sur le routeur détermine que l'ID cherchée est **197.2.2.0**, comme le routeur possède une carte paramétrée sur ce réseau il l'utilise pour envoyer ce paquet...
4. IP sur la machine de destination récupère le paquet qui lui est destiné...

N.B: Par défaut, les tables de routage sur Windows ne contiennent que des informations sur les sous-réseaux sur lesquels le routeur est directement connecté. Ce qui est sans doute un peu limitatif...

Routage complexe :

Dans une situation plus complexe, on relie **trois sous-réseaux par deux routeurs** ayant chacun **deux cartes réseaux** et **deux adresses IP** dans chaque sous-réseaux auxquels ils appartiennent :

Dans l'exemple ci-dessous, la machine d'adresse **IP 65.103.200.97** essaye de joindre la machine d'adresse **IP 90.109.155.182...**



Le fonctionnement est le suivant :

1. IP se rends compte que l'adresse de destination n'est pas une adresse locale (ID réseau cherchée **90.0.0.0** différente de ID réseau locale **65.0.0.0**), IP transmet alors le paquet à la passerelle par défaut
2. IP sur le routeur détermine que l'ID cherchée est **90.0.0.0**, mais comme le routeur **ne possède pas** une carte paramétrée sur ce réseau il ne sait pas où envoyer ce paquet...

N.B: Par défaut, les tables de routage sur Windows NT ne contiennent que des informations sur les sous-réseaux sur lesquels le routeur est directement connecté, ce qui fait que ici le paquet ne saurait être routé vers le réseau 90.0.0.0

Table de Routage :

Dans une situation plus complexe, il est nécessaire de configurer un routeur avec une table de routage qui contient des informations destinées à router des paquets vers d'autres routeurs lorsque l'on ne sait pas directement qui pourrait les prendre en charge.

Dans notre exemple il faudrait indiquer à notre premier routeur que lorsqu'il reçoit des paquets à destination d'un réseau 90 il doit les router vers le réseau 33.0.0.0

Dans notre exemple toujours, le cas n'étant que peu compliqué, on pourrait s'en sortir en paramétrant comme passerelle par défaut de ce routeur, l'adresse du deuxième routeur...

Cette méthode est limitée au cas où l'on a que 2 routeurs ...

D'une manière plus générale il va falloir configurer une table de routage...

Routage statique :

On appelle **routage statique** un routage qui est mis à jour manuellement sur chaque routeur par l'administrateur

La commande permettant de créer et maintenir une table de routage est la commande

route print

Routage dynamique :

On appelle **routage dynamique** un routage qui est mis à jour automatiquement sur chaque routeur par échange d'information entre les routeurs...

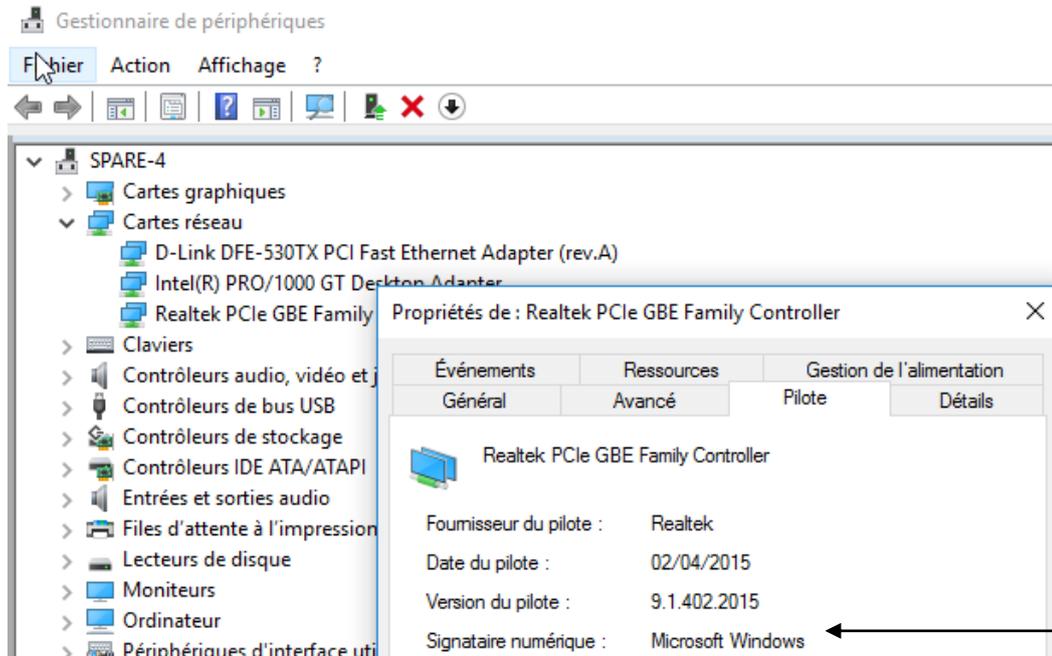
N.B: Windows ne dispose pas de cette capacité à travers le protocole RIP

RESEAU WINDOWS 10

Gestion Carte Réseau:

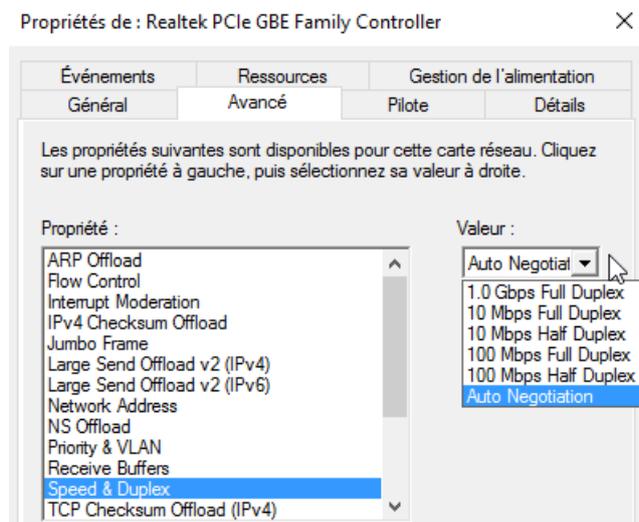
Depuis Windows 10, une myriade d'assistant se déclenchent à tous moments, les interfaces sont assez "fluctuantes" (selon les versions 1511, 1607, 1703, 1709) et "fournies"...

Si aucune carte réseau n'est détectée, il faut installer un driver certifié ...

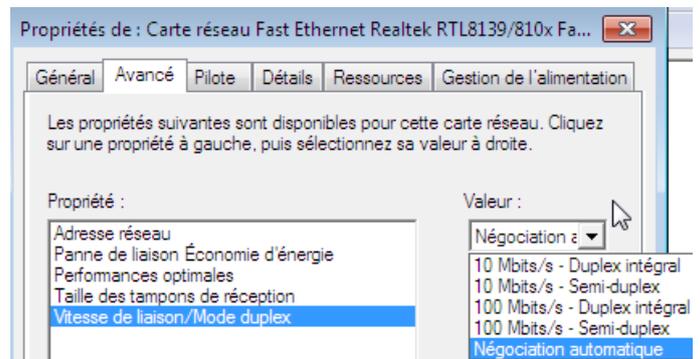


En cas de problème "physiques", on peut vérifier que le driver gère correctement nos flux Ethernet selon notre connectique (et passer en vitesse de remplis si besoin)

Carte Gb/s

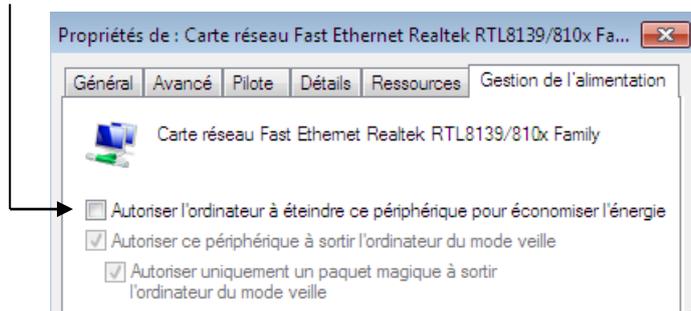


Carte 100Mb/s



N.B : ces réglages sont parfois difficiles à trouver, ils dépendent bien sur des drivers ...

On peut aussi éviter pour des raisons ACPI d'éteindre la carte réseau...



Toutes les cartes n'offrent pas tous les réglages, ni sous les mêmes libellés :
Ainsi pour **Adresse Mac**, **Vitesse + Mode**, **MTU**, on peut trouver par exemple

Locally Administered Address

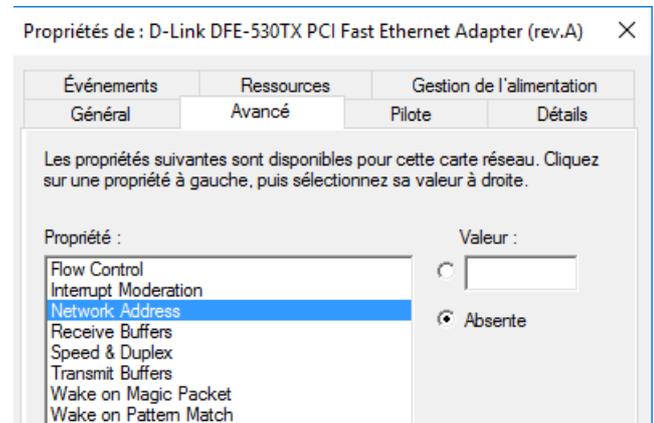
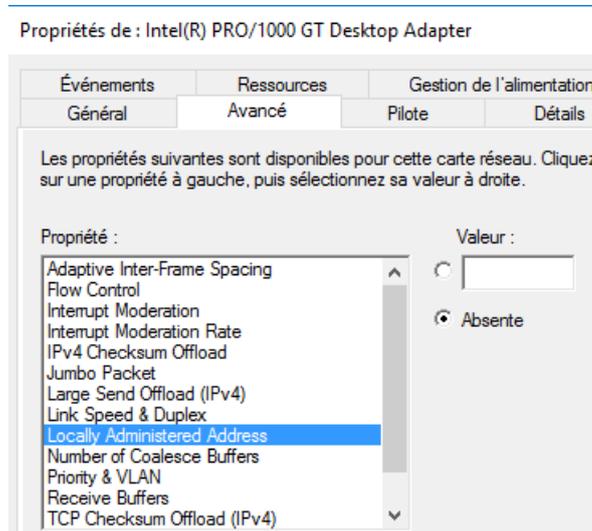
Link Speed & Duplex

Jumbo packet

Network Address

Speed & Duplex

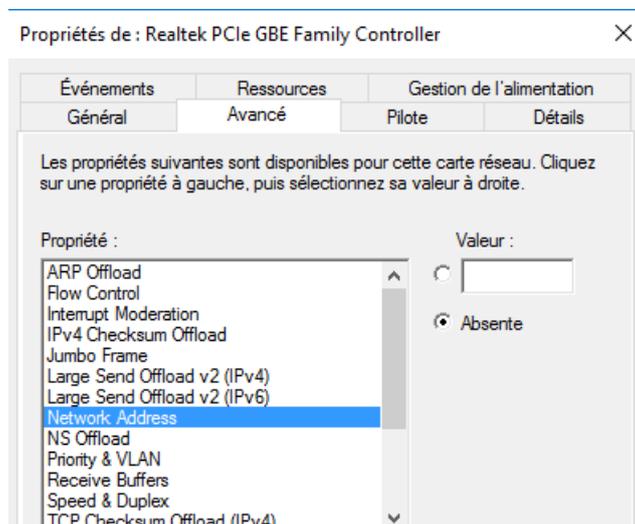
- non disponible



Network Address

Speed & Duplex

Jumbo Frame



Désactivation Media Sense:

Windows dispose de la fonction de « Détection de support ». **Media Sense**

Un « état de la liaison » est défini comme étant le support physique connecté ou inséré sur le réseau. Chaque fois que Windows détecte un état « inactif »

 sur le support, il supprime les protocoles liés de cette carte jusqu'à ce que l'état détecté soit de nouveau « actif ». Une telle carte, génère en réponse à un ping local (par exemple une application locale qui détecterait la présence d'un réseau) une défaillance générale

```
C:\Windows\system32>ping 192.168.1.170
Envoi d'une requête 'Ping' 192.168.1.170 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.
```

Pour que votre carte réseau ne désactive plus IP lors de cette situation, et **réponde sur un ping de l'adresse IP en local**

```
C:\Windows\system32>ping 192.168.1.170
Envoi d'une requête 'Ping' 192.168.1.170 avec 32 octets de données :
Réponse de 192.168.1.170 : octets=32 temps<1ms TTL=128
```

il faut utiliser en invite de commande la commande **netsh** . On peut voir l'état de la situation **Détection de médias DHCP**, dans la commande

Netsh interface ipv4 show global

```
C:\Windows\system32>netsh interface ipv4 show global
Recherche du statut actif...

Paramètres généraux globaux
-----
Limite de sauts par défaut           : 128 sauts
Limite de cache du voisin           : 256 entrées par interface
Limite de cache d'itinéraire        : 128 entrées par compartiment
Limite de réassemblage              : 125348608 octets
Redirections ICMP                   : enabled
Comportement du routage source      : dontforward
Déchargement de tâches              : enabled
→ Détection de médias DHCP          : enabled
Enregistrement de détection de supports : disabled
Niveau MLD                          : all
Version MLD                         : version3
Transmission en multidiffusion      : disabled
Fragments transmis en groupe        : disabled
Identificateurs aléatoires          : enabled
Réponse au masque d'adresses        : disabled
MTU minimum                         : 576
```

On désactive la fonctionnalité en IPV4 et IPV6 avec la commande

Netsh interface ipv4 set global dhcpmediasense = disabled

```
C:\Windows\system32>netsh interface ipv4 set global dhcpmediasense = disabled
Ok.
```

```
C:\Windows\system32>netsh interface ipv6 set global dhcpmediasense=disabled
Ok.
```

Puis reboot du poste !

Accès au Centre Réseau et partage :

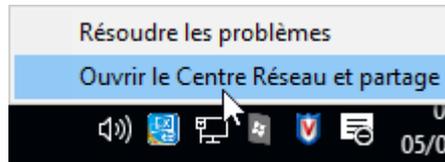
Si une carte réseau (minimum) est installée correctement, une icône "réseau" devrait apparaître en bas à droite...



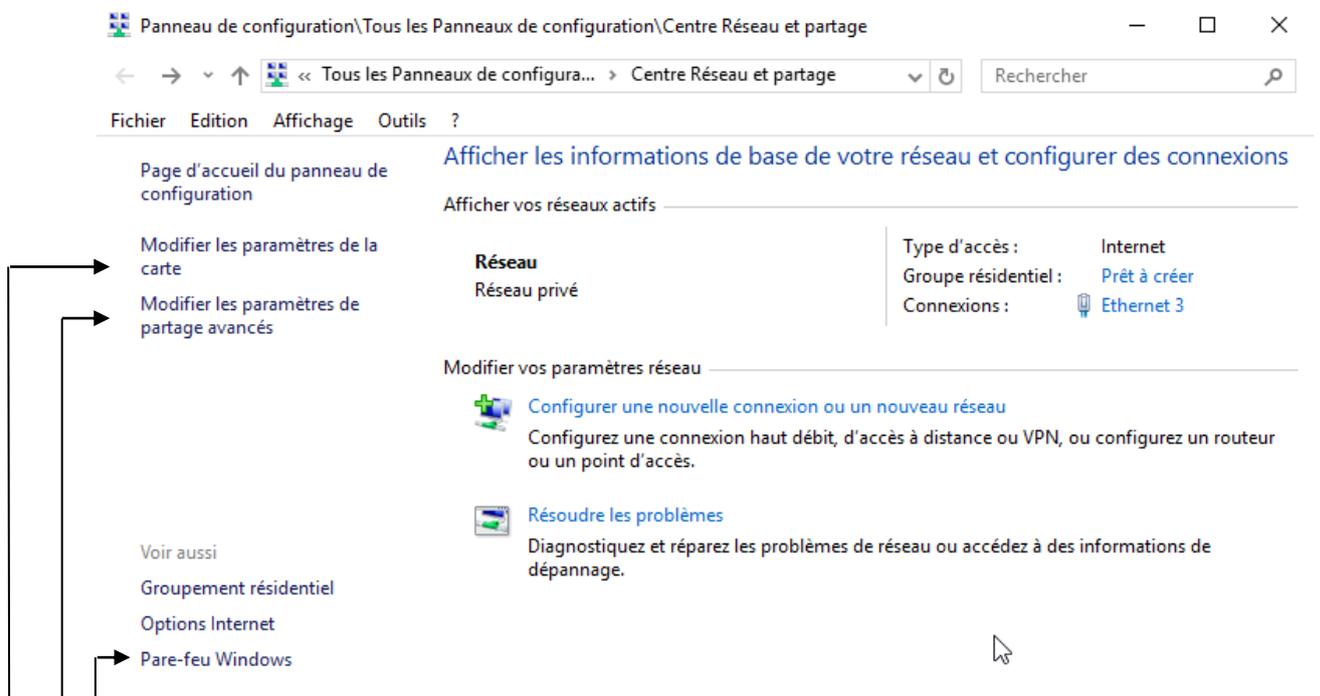
Quel que soit son aspect...



Un clic dessus puis "**Ouvrir le Centre Réseau et partage**"



Devrait amener



On peut aller aussi **Pare-feu Windows**

Modifier les paramètres de partage avancés

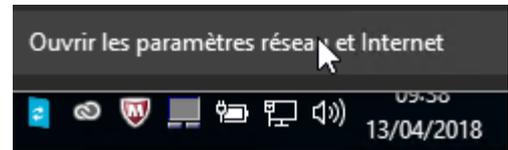
Permet de gérer les paramètres des "profils réseaux". On est depuis windows 10 toujours dans un profil réseau...

N.B: Il existe trois type de "profils" réseau au sens Windows, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause:

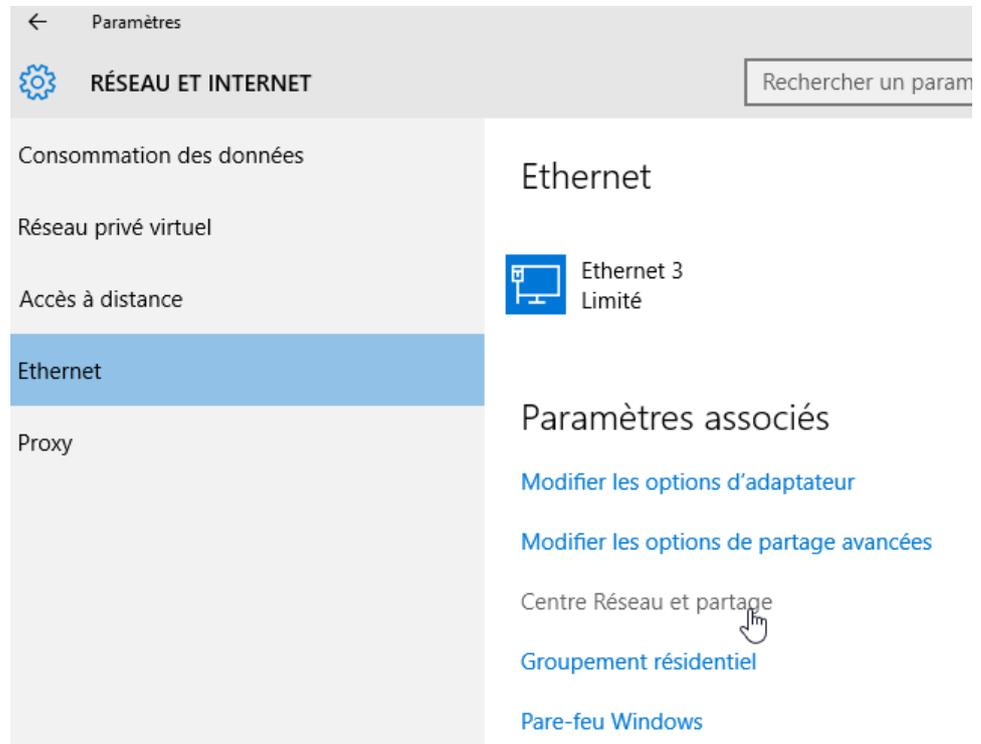
Modifier les paramètres de la carte

Permet pour chaque carte, de configurer les protocoles, dont TCP-IP...

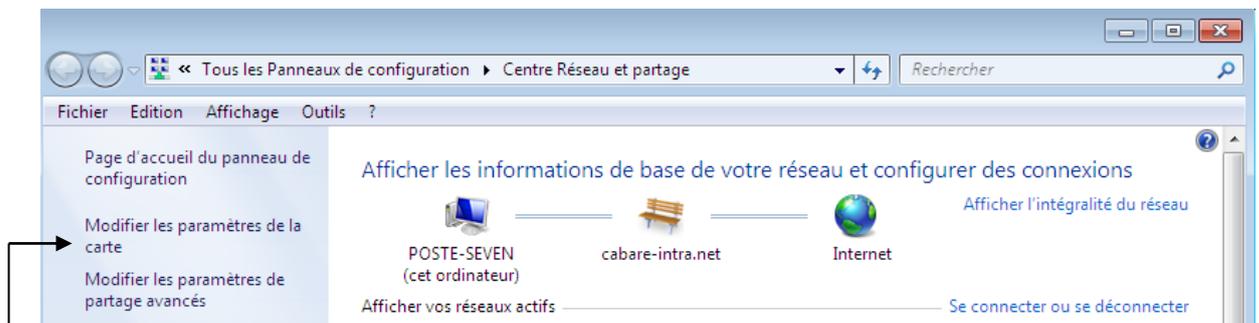
N.B : sous la version **Windows 10 - 1709** la boîte de dialogue change, et on n'accède au **Centre de réseau et partage** qu'après être passé d'abord via **Ouvrir les paramètres réseaux et internet** (équivalent du menu paramètre **Windows 10 / réseau et internet**)



Et on retrouve le **Centre de Réseau et partage** ensuite



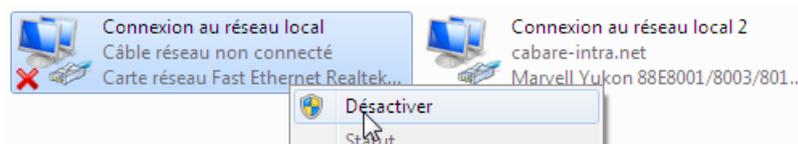
Désactivation Carte Excédentaire :



Modifier les paramètres de la carte donne accès en fait à toutes les cartes physiques... Si plusieurs cartes réseaux sont présentes, il est plus judicieux de désactiver celle que l'on n'utilise pas.



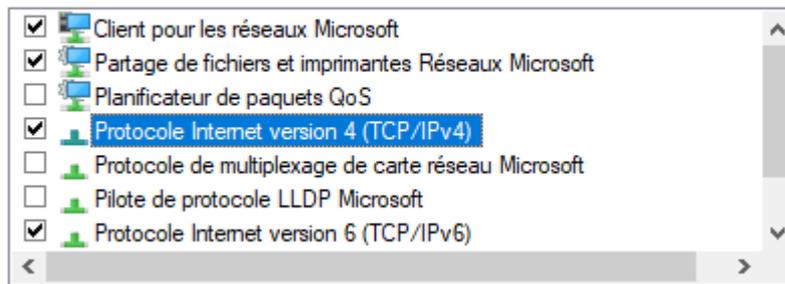
Clic droit **Désactiver**



Protocoles LLDP - multiplexage - Topologie réseau Windows:

Pour chaque Icône, les propriétés de la carte permettent de définir les services et les protocoles voulus, Lorsque l'on affiche les protocoles disponibles, il y en a beaucoup. Que 4 sont indispensables ! (voire 3)

Cette connexion utilise les éléments suivants :



Protocoles présents (à ne pas activer systématiquement)

 Pilote de protocole LLDP Microsoft

LLDP Link Layer Discovery Protocol (LLDP) est un protocole 802.1ab. C'est un protocole destiné à remplacer un bon nombre de protocoles propriétaires (Cisco CDP, Extreme EDP, etc.) utilisés dans la découverte des topologies réseau de proche en proche

 Protocole de multiplexage de carte réseau Microsoft

Protocole de multiplexage de carte réseau Microsoft utilisé pour deux scénarios d'utilisation typiques, chacun nécessitant au moins deux adaptateurs réseau fonctionnant (et connectés) sur un même PC. Le premier scénario s'appelle l'association d'adaptateurs, ce qui signifie l'utilisation simultanée de deux adaptateurs (trunk). Le second scénario est appelé basculement de l'adaptateur / haute disponibilité, où un adaptateur de secours prend en charge la connexion réseau en cas d'échec du serveur principal.

 Répondeur de découverte de la topologie de la couche de liaison
  Pilote E/S de mappage de découverte de topologie de la couche de li.

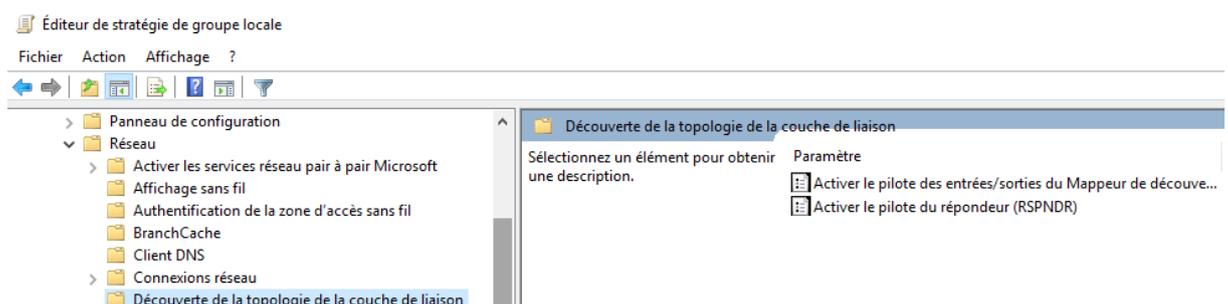
Si on veut du voisinage réseau. (cf chap spécifique)

Pilote E/S de mappage de découverte de topologie de la couche de liaison

Répondeur de découverte de la topologie de la couche liaison

Ces pilote permet de remonter sur une machine tous les partages et les accès sur un réseau local, comme on pouvait l'avoir sous Vista et les premiers Seven. (afficher l'intégralité du réseau). Associé à un répondeur (forcément)

Peut se gérer via **gpedit.msc / modèle d'administration / réseau/ Découverte de la topologie réseau**



Protocoles Ip-v4 Ip-v6 QoS Client et partage Réseaux

Les 3 protocoles absolument indispensables pour une connexion **ipv4** sont

- Client pour les réseaux Microsoft
- Partage de fichiers et imprimantes Réseaux Microsoft

Client pour les réseaux Microsoft

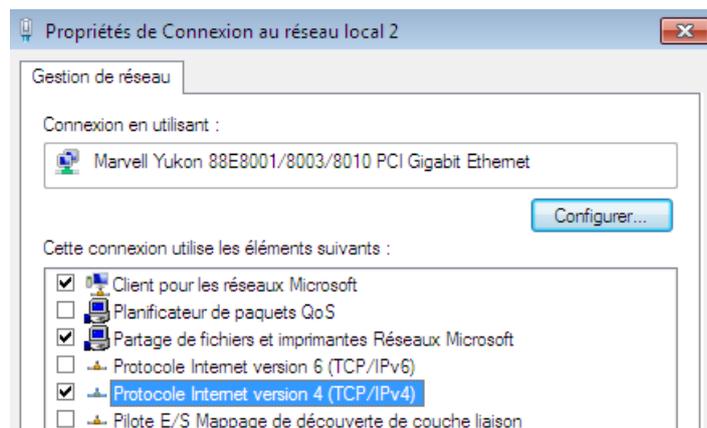
Partage de fichiers et imprimantes Réseaux Microsoft

Si on ne les active pas, on ne pourra rien "faire" avec notre machine.

- Protocole Internet version 4 (TCP/IPv4)

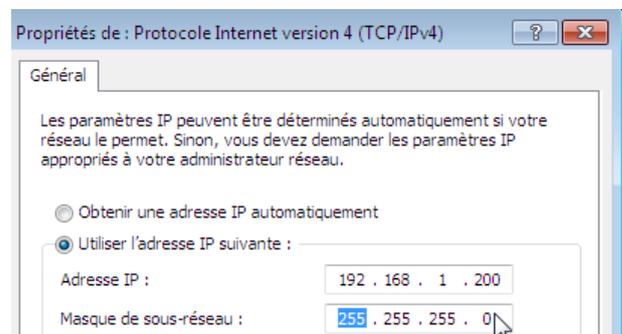
Protocole Internet version 4 (TCP/IPv4)

évidemment



L'adressage de base Minimum réside en une Adresse IP et un Masque.

N.B: Pour l'identification du profil réseau, une passerelle facilite les choses



- Planificateur de paquets QoS

Planificateur de paquets QoS

A ne pas activer, sauf si on utilise des applications le nécessitant

- Protocole Internet version 6 (TCP/IPv6)

Protocole Internet version 6 (TCP/IPv6)

Microsoft ne recommande pas la désactivation du protocole **IPv6**. Depuis Windows Vista et Windows Server 2008, IPv6 fait partie intégrante du système d'exploitation. Certains composants utilisent nativement IPv6 : **Remote Assistance** – **DirectAccess** – **Client Side Caching** (offline files) et **BranchCache**

Il ne faut plus prioriser les flux comme on pouvait tenter de le faire sous Windows Seven ou 2008R2 ! Il faut laisser le protocole IPVv6 en client DHCP v6 et ce depuis la version Windows 10 1607.

Ré-initialiser TCP/IP Sous Windows 10 :

Dans des cas extrêmes, pour réinitialiser la « Pile Ip » on ne peut plus désinstaller le protocole TCP-IP dans l'interface, mais on peut passer une commande en invite de commande.

Il faudra impérativement

- redémarrer le poste et
- reprendre toutes les configurations réseaux existantes

Donc en Invite de commande

netsh int ip reset

devrait donner

```
C:\Windows\system32>netsh int ip reset
Réinitialisation de Interface réussie.
Réinitialisation de Adresse unicast réussie.
Réinitialisation de Chemin d'accès réussie.
Réinitialisation de réussie.
Redémarrez l'ordinateur pour terminer cette action.
```

N.B : Il se peut que l'on ait un petit souci sur la composante DHCP, en Workgroup

```
C:\Windows\system32>netsh int ip reset
Réinitialisation de Général réussie.
Réinitialisation de Interface réussie.
Réinitialisation de Adresse unicast réussie.
Réinitialisation de Voisin réussie.
Réinitialisation de Chemin d'accès réussie.
Réinitialisation de Routage réussie.
Échec de la réinitialisation de .
Accès refusé.

Réinitialisation de réussie.
Redémarrez l'ordinateur pour terminer cette action.
```

Cela peut se résoudre via la Base de Registre où il faut donner les droits en **Contrôle total à tout le monde** sur la ruche **26** de la ruche **{eb004a00-xxxxx}** située en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nsi**

The image shows the Windows Registry Editor with the following tree structure:

- NetProvision
- NetTrace
- Network
- NetworkProvider
- NetworkSetup2
- NetworkUxManager
- Nls
- NodeInterfaces
- Notifications
- Nsi
 - {eb004a00-9b1a-11d4-9123-0050047759bc}
 - 10
 - 12
 - 26
 - 4
 - 7
 - {eb004a01-9b1a-11d4-9123-0050047759bc}
 - {eb004a02-9b1a-11d4-9123-0050047759bc}
 - {eb004a03-9b1a-11d4-9123-0050047759bc}
 - {eb004a11-9b1a-11d4-9123-0050047759bc}

The permissions window for the subkey 26 is shown with the following settings:

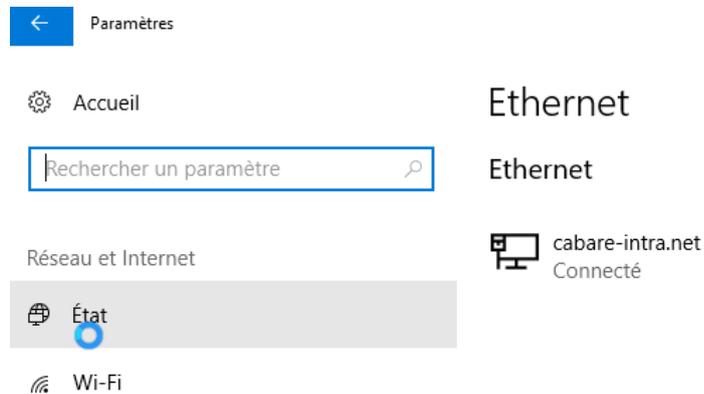
Autorisations pour Tout le monde		Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Autorisations spéciales	<input type="checkbox"/>	<input type="checkbox"/>	

Depuis la version **1607** de windows on peut directement demander depuis l'interface graphique, via les paramètres, une ré-initialisation de TCP-IP. Il faudra impérativement

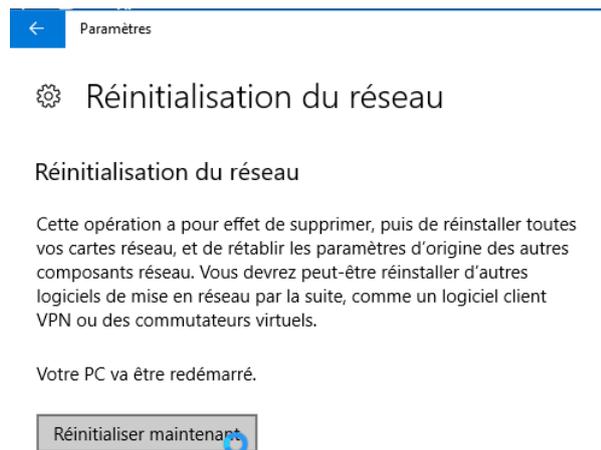
- redémarrer le poste et
- reprendre toutes les configurations réseaux existantes

1. Sélectionnez le bouton **Démarrer** , puis sélectionnez **Paramètres**  > **Réseau et Internet**  > **État** > **Réinitialisation réseau**.

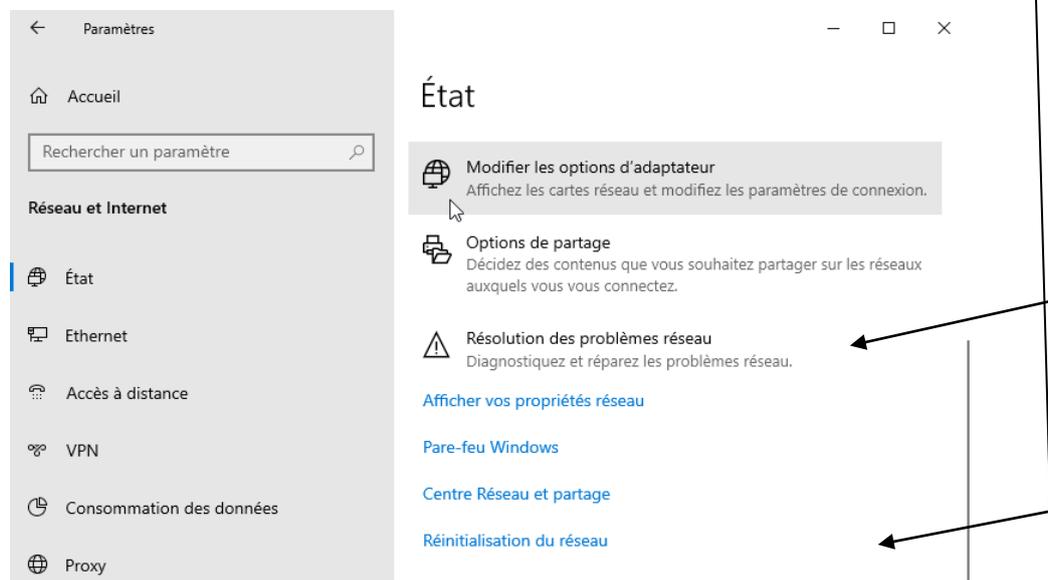
Dans **État** on va chercher (tout en bas) **Réinitialisation du réseau**



Et on demande de **Réinitialiser maintenant**



A chaque nouvelle version / builds, des diagnostics sont ajoutés... en plus



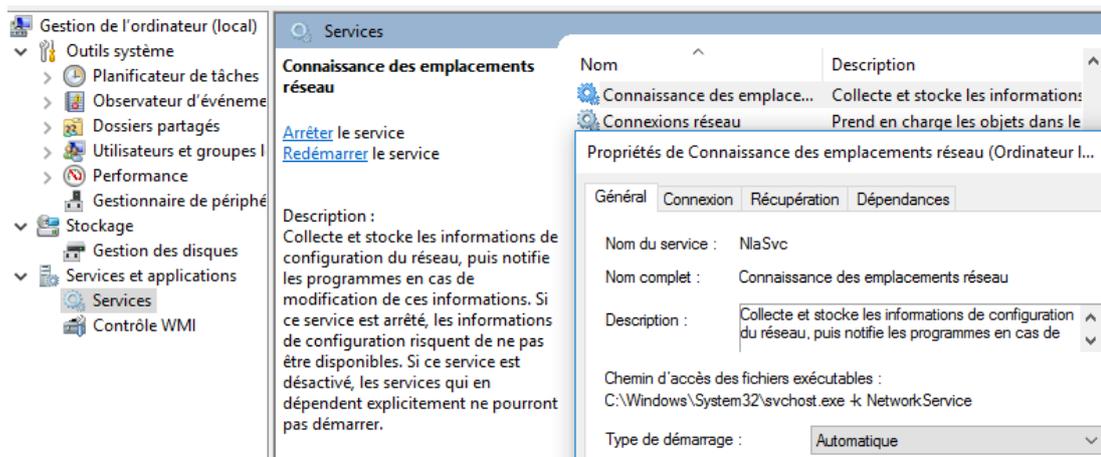
Profil – Type Réseau Windows 10 :

On est avec Windows 10 toujours dans un profil réseau... Dès qu'un réseau est détecté. Il existe trois type de réseau, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause.

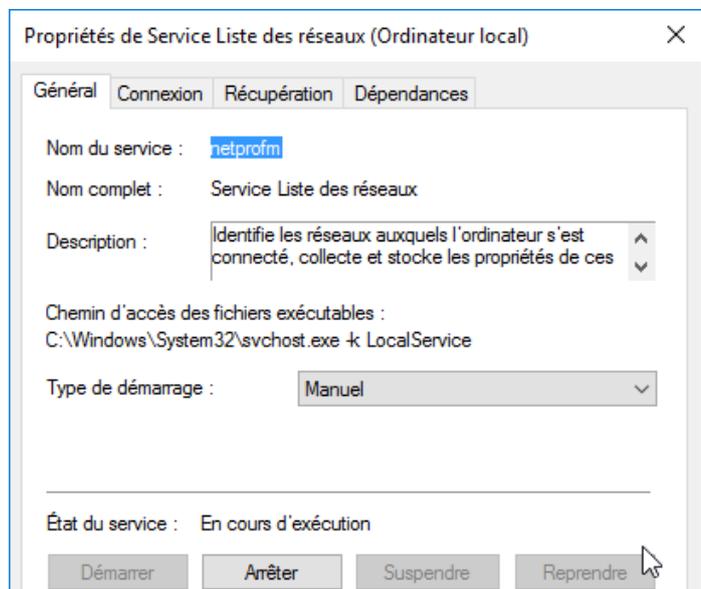
- Domaine
- Privé
- Public

La différence entre **Public / Privé** est une différence des paramétrages par défaut, disponible dans les "partages avancés" et dans le pare-feu.

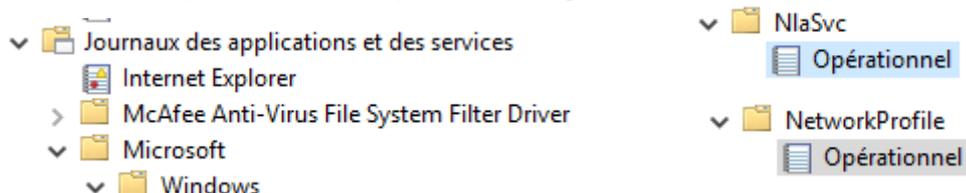
C'est le service "**Connaissance des emplacements réseau**" (**NlaSvc**) qui gère cela. Vérifier qu'il soit bien démarré sur les clients



Il y a un service dépendant également qui intervient c'est "**Service Liste des réseaux**" (**Netprofm**)



Dans l'observatoire d'évènement les sources: **Microsoft-Windows** avec **NlaSvc** et **NetworkProfile** peuvent aider pour un diagnostic

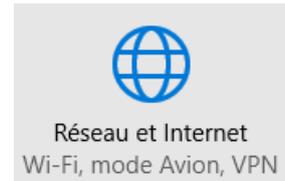


Changer de type de Profil réseau – interface Paramètre :

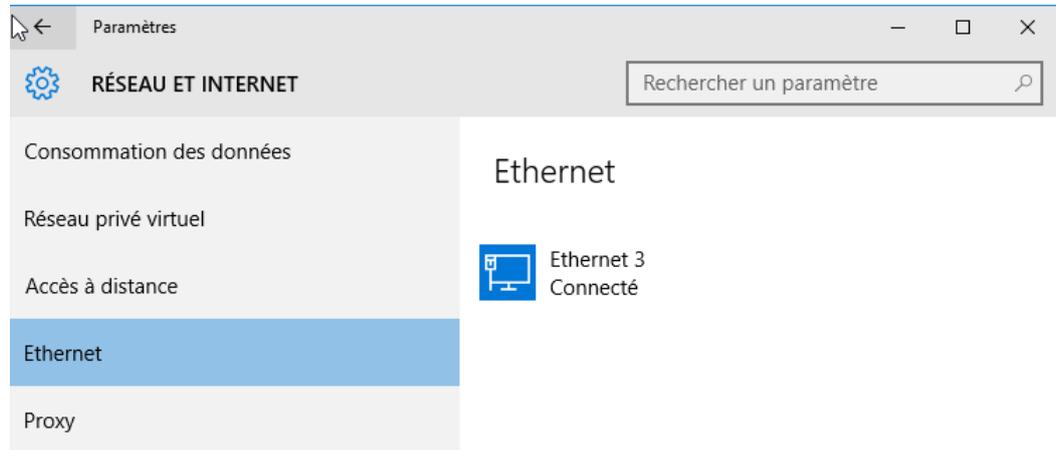
Dans l'interface Windows 10 on demande **Paramètres** et ensuite **réseau et internet**



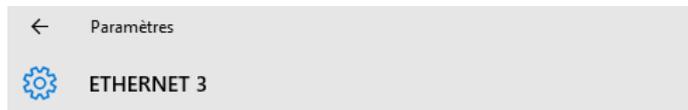
On se place ensuite sur **Ethernet**, et on sélectionne la carte réseau pour laquelle on veut modifier le type de Profil



Dans l'exemple **Ethernet 3**



Dans la boîte de dialogue qui s'ouvre, on ne choisit pas public ou privé, mais simplement le fait de dire **Rendre ce pc détectable**, fera le réseau de type **Réseau privé**



Afficher vos réseaux actifs —

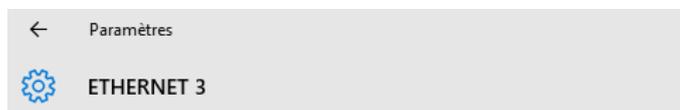
Réseau
Réseau privé

Rendre ce PC détectable

Autorisez les autres PC et appareils de ce réseau à détecter votre PC. Nous vous recommandons d'activer cette option sur les réseaux privés à domicile ou au travail, mais de la désactiver sur les réseaux publics pour maintenir la protection de vos données.

Activé

Et si on indique ne pas vouloir, alors cela fera le réseau de type **Réseau public**



Afficher vos réseaux actifs —

Réseau
Réseau public

Rendre ce PC détectable

Autorisez les autres PC et appareils de ce réseau à détecter votre PC. Nous vous recommandons d'activer cette option sur les réseaux privés à domicile ou au travail, mais de la désactiver sur les réseaux publics pour maintenir la protection de vos données.

Désactivé

N.B : sous la version **Windows 10 - 1709** la boîte de dialogue change, et on a de nouveau la mention **profil réseau public / privé** qui apparaît (à la place de détectable...)

⚙️ cabare-intra.net

Profil réseau

Public

Votre PC est masqué des autres appareils sur le réseau et ne peut pas être utilisé pour l'imprimante et le partage de fichiers.

Privé

Pour un réseau de confiance, par exemple à votre domicile ou au travail. Votre PC est détectable et vous pouvez l'utiliser pour l'imprimante ou le partage de fichiers si vous le configurez.

[Configurer le pare-feu et les paramètres de sécurité](#)

Changer de type de Profil réseau – Powershell :

Il faut d'abord récupérer le nom du profil réseau en cours par la commande • **Get-NetConnectionProfile**

```
PS C:\Users\Administrateur> Get-NetConnectionProfile

Name                : Réseau non identifié
InterfaceAlias      : Ethernet 3
InterfaceIndex      : 6
NetworkCategory     : Public
IPv4Connectivity    : NoTraffic
IPv6Connectivity    : NoTraffic
```

Puis passer une commande du genre **Set-NetConnectionProfile**

Avec 2 paramètres - **name (et entre guillemets le nom du profil)**

et **- NetworkCategory (avec mot clé Private ou Public)**

```
Set-NetConnectionProfile -name "Réseau non identifié" -NetworkCategory Private
```

Changer de type de Profil réseau WI FI – windows 1709

Cela n'est possible que si la connexion est uniquement en WiFi

Si une connexion en RJ45 est active en parallèle, on ne peut choisir le type de réseau pour la connexion WiFi

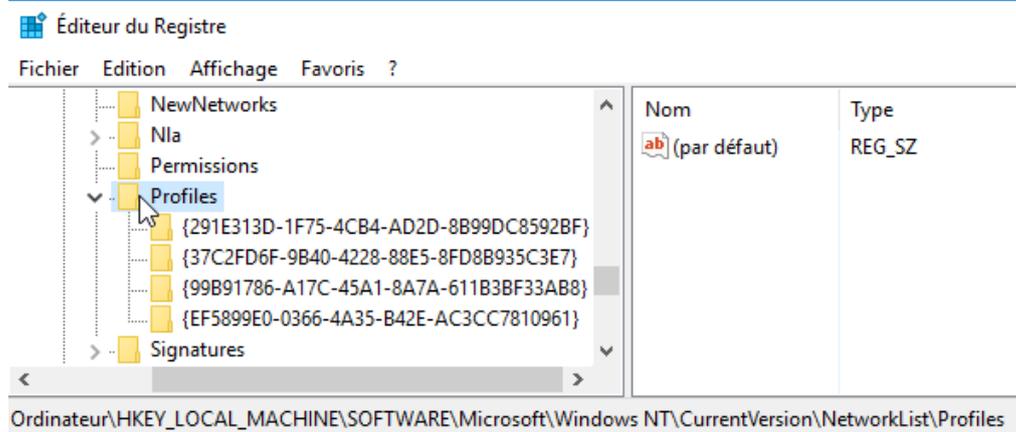
^ Pour modifier le statut d'un réseau Wi-Fi en public ou privé

1. Sélectionnez **Démarrer** , puis **Paramètres**  > **Réseau et Internet**  > **Wi-Fi** .
2. Sélectionnez **Gérer les réseaux connus**, sélectionnez le réseau dont vous souhaitez modifier les paramètres, puis sélectionnez **Propriétés**.
3. Sous **Profil réseau**, sélectionnez **Public** ou **Privé**.

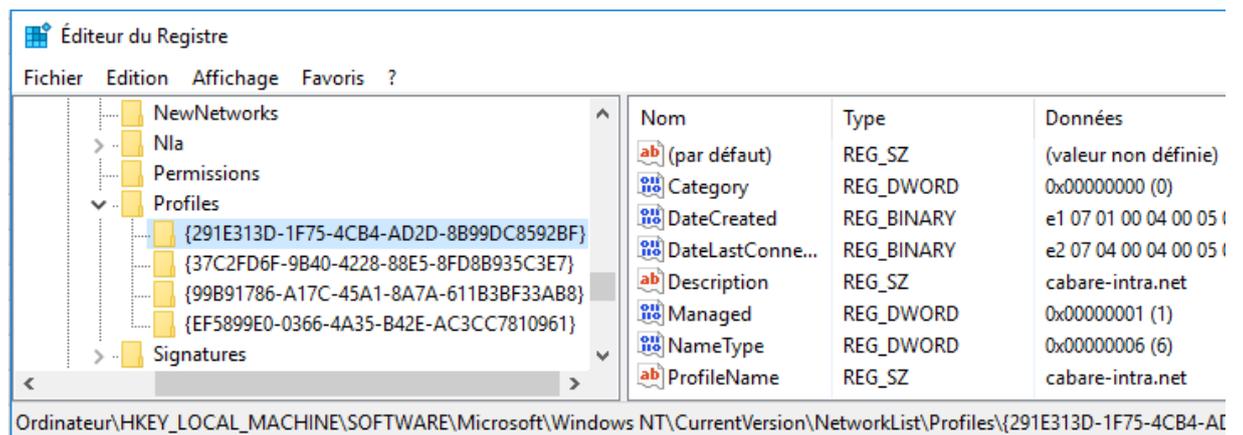
Changer de type de Profil réseau – Regedit :

Se placer dans la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

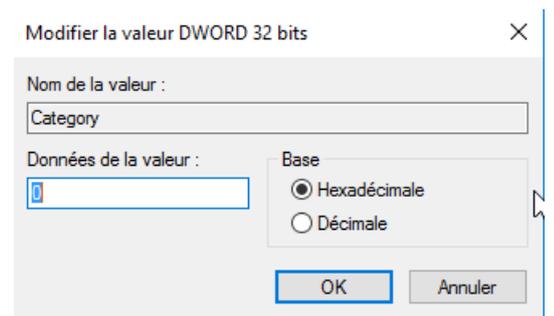


Rechercher dans les sous-clé, (ici dans l'exemple il y en a **4**) celle correspondant à votre réseau (la valeur **ProfileName** doit porter le nom de votre connexion réseau, ici dans l'exemple **cabare-intra.net**)



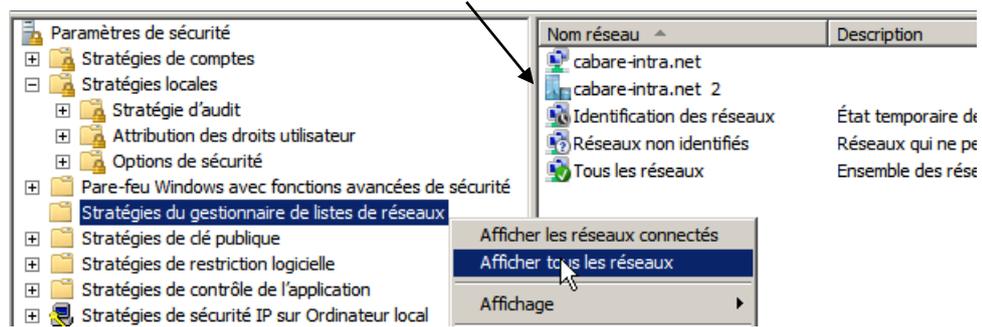
La valeur **DWORD Category** correspond au type de profil (Public/Privé/Domaine) avec les conventions suivantes

Public 0 Privé 1 Domaine 2



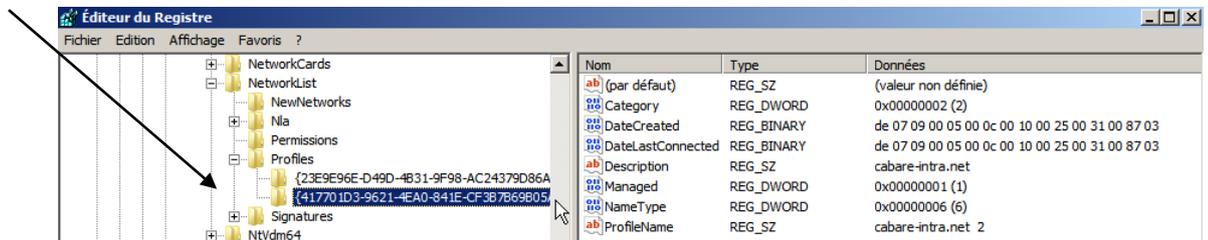
Reset - Listes des réseaux identifiés

N.B : la liste de tous les réseaux détectés par Windows se trouve en demandant dans les **stratégies de sécurité locales**, dans les **stratégie du gestionnaire de liste de réseaux / Afficher tous les réseaux**



N.B : la liste des réseaux détectés par Windows est stockée en dans la base de Registre en

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

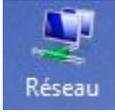


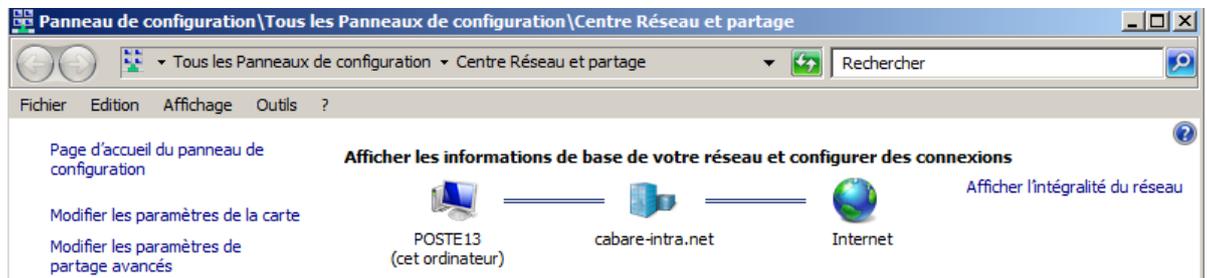
Pour faire un **Reset** de la situation il peut être nécessaire de

- Désactiver la carte réseau
- Modifier l'adressage IP
- Purger les **NetworkList\Profiles** de la base de registre
- Re-demarrer le service **Service Liste des réseaux (netprofm)**
- Réactiver la carte réseau

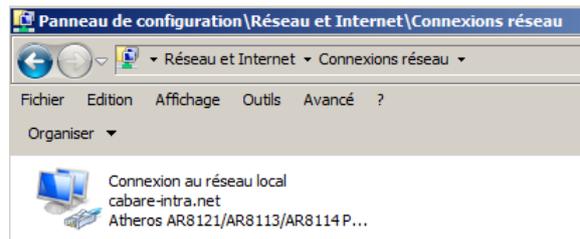
RESEAU WINDOWS 7

Paramétrage TCP/IP Windows:

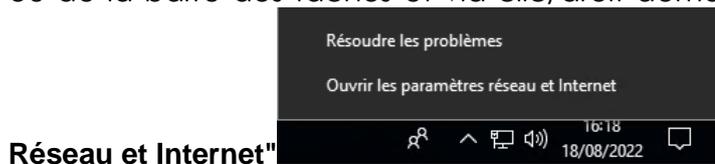
selon les versions , Clic / droit sur l'icône **Réseau** du bureau ,



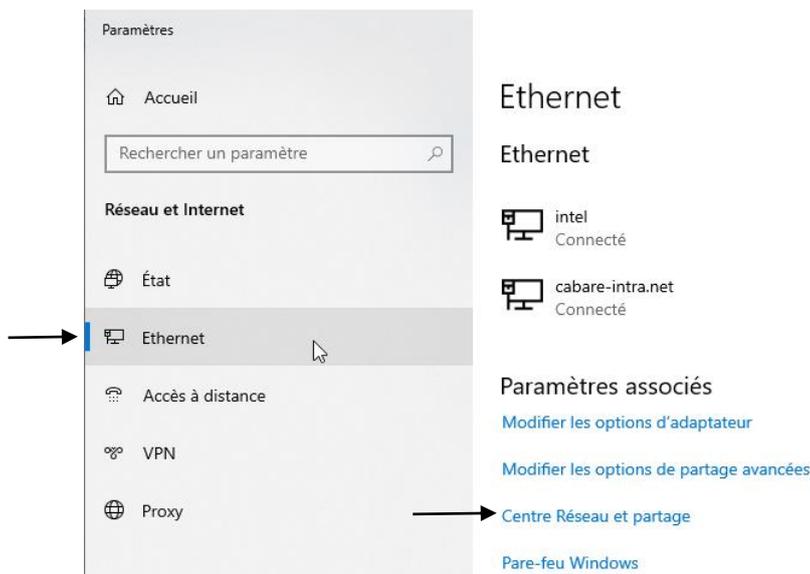
On demande **Modifier les paramètres de la carte**, et on choisit notre carte réseau...



ou de la barre des tâches et via clic/droit demander **Ouvrir les paramètres**

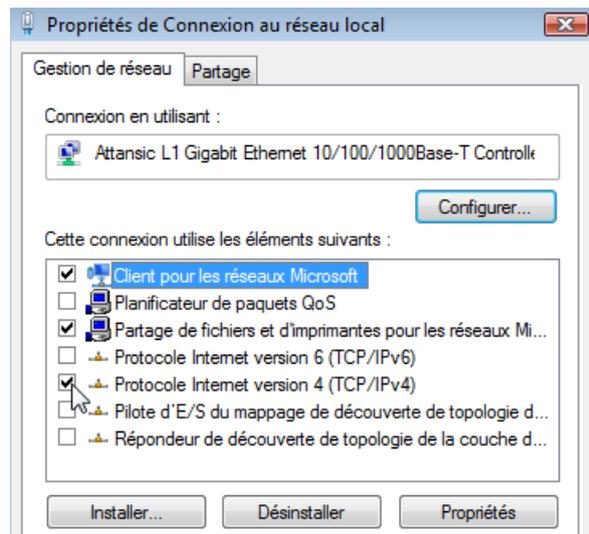


Sur des postes Windows 10, cela amène une autre boîte de dialogue, où, dans **Ethernet**, on demande ensuite **Centre Réseau et Partage**



N.B: accès possible également via les paramètres de Windows 10 / **Réseaux et internet** / puis on retrouve **Ethernet / Centre Réseau et partage**

pour retrouver enfin les propriétés



Il est important dans un premier temps de :

- Désactiver IPv6
- les nouveaux protocoles de découverte Windows...

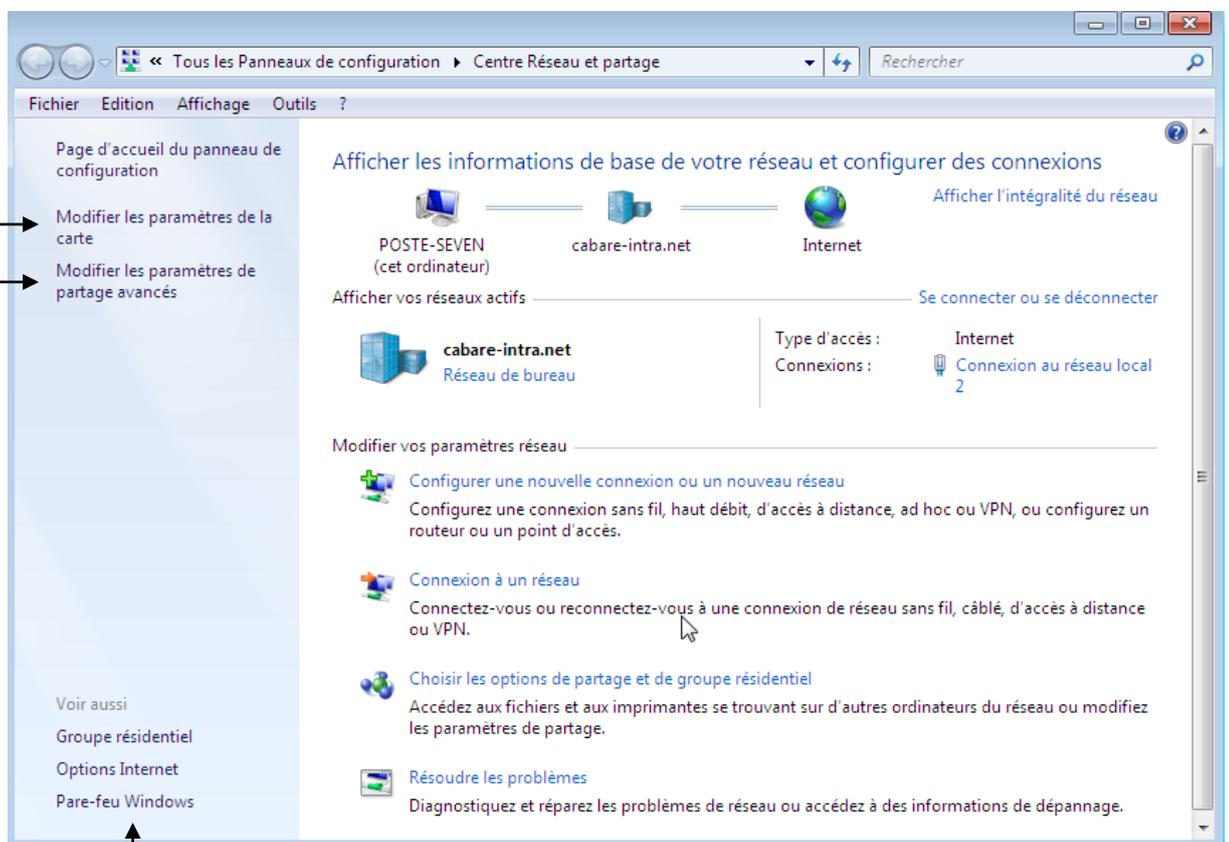
Accès au Centre Réseau Windows:

Si une carte réseau (minimum) est installée correctement, une icône "réseau" devrait apparaître en bas à droite...



Quel que soit son aspect...

Devrait amener



On peut aller aussi aux réglages du pare-feu

Modifier les paramètres de partage avancés

Permet de gérer les paramètres des "profils réseaux". On est depuis windows SEVEN, et donc avec 10 toujours dans un profil réseau...

N.B: Il existe trois type de "profils" réseau au sens Windows, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause:

Modifier les paramètres de la carte

Permet pour chaque carte, de configurer les protocoles, dont TCP-IP...

Profil – Type Réseau seven 7:

On est avec SEVEN toujours dans un profil réseau... Des que un réseau est détecté (pour ce faire il faut un adressage IP minimum, Adresse/Masque + Passerelle) alors il faut décider de son "type" parmi ceux proposés



Réseau domestique

Si tous les ordinateurs de ce réseau sont à votre domicile et que vous les reconnaissez, il s'agit d'un réseau domestique approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.



Réseau de bureau

Si tous les ordinateurs de ce réseau sont sur votre lieu de travail et que vous les reconnaissez, il s'agit d'un réseau de bureau approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.



Réseau public

Si vous ne reconnaissez pas tous les ordinateurs du réseau (par exemple si vous êtes dans un cybercafé ou un aéroport, ou si vous disposez d'un haut débit mobile), il s'agit d'un réseau public et il n'est pas approuvé.

De l'appartenance à tel ou tel type de réseau, découleront

Les paramètres des partages avancés

Les réglages du Pare-Feu

Il existe trois type de réseau au sens SEVEN, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause:

- Domaine
- Privé
- Public

La différence entre **Public / Privé** est une différence des paramétrages par défaut des "partages avancés" et du pare-feu.

Choisir un profil Réseau 7 :

Si on n'est pas dans un domaine, alors on peut en cliquant sur le type de réseau en cours... choisir le nouveau profil réseau.

Page d'accueil du panneau de configuration

- Modifier les paramètres de la carte
- Modifier les paramètres de partage avancés

Afficher les informations de base de votre réseau et configurer des connexions

POSTE-SEVEN (cet ordinateur) — cabare-intra.net — Internet

Afficher l'intégralité du réseau

Afficher vos réseaux actifs — Se connecter ou se déconnecter

cabare-intra.net
Réseau public

Type d'accès : Internet
Connexions : Connexion au réseau local 2

N.B: Si **Réseau non identifié** s'affiche, une passerelle sera la bienvenue...!

Car dans ce cas on ne peut pas changer de profil...

Des que l'on donne une adresse IP en passerelle, cela débloque la détection, et windows nous demande de choisir un profil

Sélectionner l'emplacement du réseau « Réseau »

Cet ordinateur est connecté à un réseau. Windows appliquera automatiquement les paramètres réseau appropriés pour cet emplacement.



Réseau domestique

Si tous les ordinateurs de ce réseau sont à votre domicile et que vous les reconnaissez, il s'agit d'un réseau domestique approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.



Réseau de bureau

Si tous les ordinateurs de ce réseau sont sur votre lieu de travail et que vous les reconnaissez, il s'agit d'un réseau de bureau approuvé. Ne choisissez pas cette option pour des endroits publics tels que des cybercafés ou des aéroports.



Réseau public

Si vous ne reconnaissez pas tous les ordinateurs du réseau (par exemple si vous êtes dans un cybercafé ou un aéroport, ou si vous disposez d'un haut débit mobile), il s'agit d'un réseau public et il n'est pas approuvé.

Traiter tous les réseaux auxquels je me connecterai à l'avenir comme des réseaux publics, et ne plus me poser la question.

[Comment choisir ?](#)

Cet état de fait est réglable dans les **stratégies locales de sécurité**, dans les **Stratégies du gestionnaire de liste de réseaux / Réseaux non identifiés**

Stratégie de sécurité locale

Fichier Action Affichage ?

Paramètres de sécurité

- Stratégies de comptes
- Stratégies locales
 - Stratégie d'audit
 - Attribution des droits utilisateur
 - Options de sécurité
- Pare-feu Windows avec fonctions avancées de :
- Stratégies du gestionnaire de listes de réseaux
- Stratégies de clé publique
 - Système de fichiers EFS (Encrypting File Syst
 - Chiffrement de lecteur BitLocker
- Stratégies de restriction logicielle
- Stratégies de contrôle de l'application
 - AppLocker
- Stratégies de sécurité IP sur Ordinateur local
- Configuration avancée de la stratégie d'audit

Nom réseau	Description
Réseaux non identifiés	Réseaux qui ne peuvent pas être identifiés en raison d'un problème rése..
Identification des réseaux	État temporaire des réseaux en cours d'identification.
Tous les réseaux	Ensemble des réseaux auxquels un utilisateur se connecte.
Réseau	

Propriétés de : Réseaux non identifiés

Emplacement réseau

L'emplacement réseau identifie le type de réseau auquel se connecte un ordinateur et définit automatiquement les paramètres de pare-feu appropriés.

Type d'emplacement

- Non configuré
- Privé
- Public

Autorisations des utilisateurs

- Non configuré
- L'utilisateur peut changer l'emplacement
- L'utilisateur ne peut pas changer l'emplacement

PROFIL RESEAU AVANCE – VOISINAGE RESEAU

Réglage Disponibles:

Les réglages suivants existent selon les profils réseaux... Surtout

Recherche du réseau

Quand la découverte de réseau est activée, l'ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau. [Qu'est-ce que la découverte de réseau ?](#)

- Activer la découverte de réseau
- Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- Activer le partage de fichiers et d'imprimantes
- Désactiver le partage de fichiers et d'imprimantes

Pour voir les postes dans les favoris réseaux...

Mais pour que cela soit possible, il faut absolument que les 4 services suivants soient démarrés sur le poste (ce qui n'est pas toujours le cas):

Client DNS

 Client DNS

Publication des ressources...

 Publication des ressources de découverte de fonctions

Découverte SSDP

 Découverte SSDP

Hôte de périphérique

 Hôte de périphérique UPnP

Dossiers publics et **groupe résidentiels** ne devraient pas être activés sur des machines professionnelles...

Partage de dossiers publics

Lorsque le partage des dossiers Public est activé, les utilisateurs du réseau, y compris les membres du groupe résidentiel, peuvent accéder aux fichiers des dossiers Public. [Que sont les dossiers Public ?](#)

- Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public
- Désactiver le partage des dossiers Public (les personnes connectées à cet ordinateur peuvent continuer d'accéder à ces dossiers)

Partage protégé par mot de passe

Lorsque le partage protégé par mot de passe est activé, seules les personnes disposant d'un compte d'utilisateur et d'un mot de passe sur cet ordinateur peuvent accéder aux fichiers partagés, aux imprimantes connectées à l'ordinateur et aux dossiers publics. Pour donner accès à d'autres personnes, vous devez désactiver le partage protégé par mot de passe.

- Activer le partage protégé par mot de passe
- Désactiver le partage protégé par mot de passe

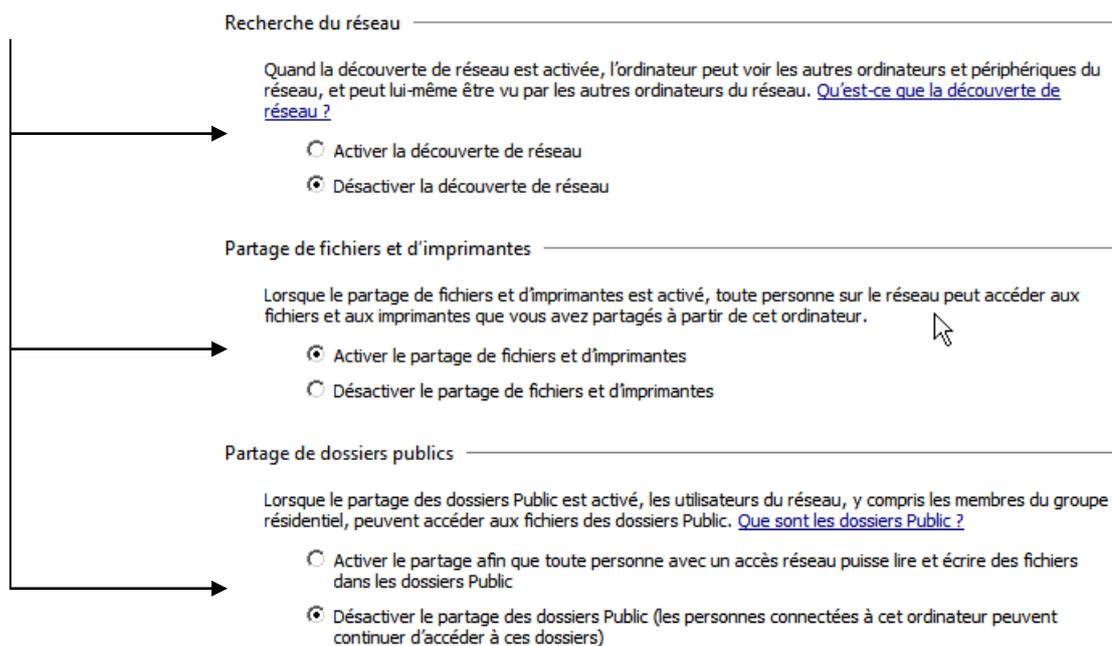
Connexions de groupe résidentiel

En général, Windows gère les connexions aux autres ordinateurs du groupe résidentiel. Mais si vous avez le même compte d'utilisateur et le même mot de passe sur tous vos ordinateurs, vous pouvez configurer le groupe résidentiel pour utiliser votre compte. [Comment choisir ?](#)

- Autoriser Windows à gérer les connexions des groupes résidentiels (recommandé)
- Utiliser les comptes d'utilisateurs et les mots de passe pour se connecter à d'autres ordinateurs

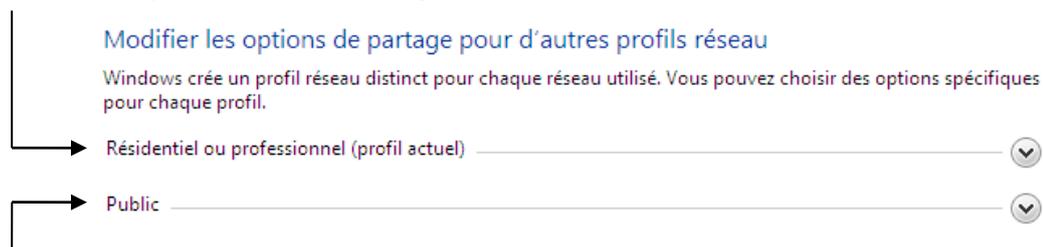
Jeux de Réglages:

Le jeu des réglages est quasiment le même dans tous les profils...
à chaque emplacement correspond un "jeu de réglage" pré-réglé



Sur une machine en workgroup deux profils type existent

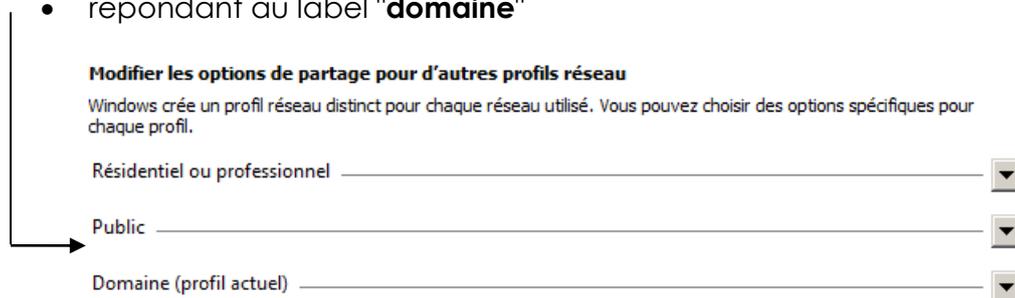
- un répondant au label "**privé**"



- un répondant au label "**public**"

Sur une machine appartenant à un domaine un troisième profil apparaît (et on ne peut pas en choisir un autre)

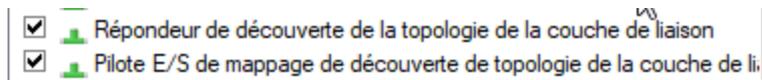
- répondant au label "**domaine**"



Activer la découverte du "voisinage réseau":

On a indiqué que 4 services devaient être démarrés sur le poste pour que notre ordinateur puisse être vu, Pour le voisinage réseau il en faut ajouter 2

- Hôte du fournisseur de découverte de fonctions (fdPHost)
- Mappage de découverte de topologie de la couche de liaison (lltdsvc)



Donc au total 6 services

- Client DNS
- Publication des ressources de découverte de fonctions
- Découverte SSDP
- Hôte de périphérique UPnP
- + Hôte du fournisseur de découverte de fonctions
- + Mappage de découverte de topologie de la couche de liaison

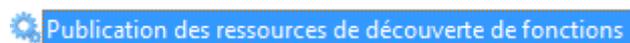
Client DNS

Service **Dnscache**



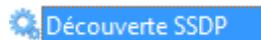
Publication des ressources...

Service **Fdrespub**



Découverte SSDP

Service **SSDPSRV**



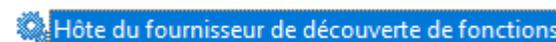
Hôte de périphérique

Service **upnphost**



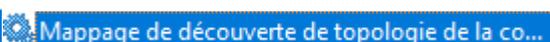
Hôte fournisseur découverte...

Service **fdpHost**



Mappage de découverte de topologie...

Service **lltdsvc**



Pourquoi pas un script du genre en Powershell pour les démarrer...

```
$list = "Dnscache","FDResPub","SSDPSRV","upnphost","fdPHost","lltdsvc",
foreach ( $service in $list) {
    $TheService = get-service | ?{$_ -like "$service*"}
    $TheService
    if ( $TheService.Status -eq "Stopped" ){
        set-service $service -StartupType Manual -Status Running
    }
}
```

Gestion de l'ordinateur (local) > Services

Client DNS

Description : Le service client DNS (dnscache) met en cache les noms DNS (Domain Name System) et inscrit le nom complet de cet ordinateur. Si le service est arrêté, les noms DNS continuent d'être résolus. Toutefois, les résultats des requêtes de noms DNS ne sont pas mis en cache et le nom de l'ordinateur n'est pas inscrit. Si le service est désactivé, les services qui en dépendent explicitement ne peuvent pas démarrer.

Nom	Description	État	Type de démarrage
BranchCache	Ce service met en...		Manuel
CaptureService_18bd1e	Active la fonction...		Manuel
CaptureService_20d45	Active la fonction...		Manuel
Carte à puce	Gère l'accès aux c...		Manuel (Déclencher le démarra...
Carte de performance WMI	Fournit des infor...		Manuel
Centre de sécurité	Le service WSCSV...	En cours d'e...	Automatique (début différé)
Cliché instantané des volu...	Gère et impléme...	En cours d'e...	Manuel
Client de stratégie de groupe	Le service est res...	En cours d'e...	Automatique (déclencher le dé...
Client de suivi de lien distri...	Conserve les liens...	En cours d'e...	Automatique
Client DHCP	Inscrit et met à jo...	En cours d'e...	Automatique
Client DNS	Le service client ...	En cours d'e...	Automatique (déclencher le dé...

Gestion de l'ordinateur (local) > Services

Publication des ressources de découverte de fonctions

Arrêter le service
Redémarrer le service

Description : Publie cet ordinateur et les ressources qui y sont attachées, de façon à ce que leur découverte soit possible sur le réseau. Si ce service est arrêté, les

Nom	Description	État	Type de démarrage	Ouvrir u...
Protocole EAP (Extensible A...	Le service EAP (E...		Manuel	Système
Protocole PNRP	Permet la résoluti...		Manuel	Service I...
Publication des ressources de...	Publie cet ordinat...	En cours d'e...	Manuel (Déclencher le démarra...	Service I...
Redirecteur de port de mod...	Permet la redirect...	En cours d'e...	Manuel	Système
Registre à distance	Permet aux utilis...		Désactivé	Service I...
Requête du service VSS Mic...	Coordonne les co...	En cours d'e...	Manuel (Déclencher le démarra...	Système
Routage et accès distant	Offre aux entrepri...		Désactivé	Système
Sauvegarde Windows	Sauvegarde Wind...		Manuel	Système
Serveur	Prend en charae l...	En cours d'e...	Automatique (déclencher le dé...	Système

Gestion de l'ordinateur (local) > Services

Découverte SSDP

Arrêter le service
Redémarrer le service

Description : Découvre les périphériques et services en réseau qui utilisent le protocole de découverte SSDP, tels que les périphériques UPnP. Annonce également les périphériques et services SSDP exécutés sur l'ordinateur local. Si ce service est arrêté, les périphériques SSDP ne

Nom	Description	État	Type de démarrage	Ouvrir u...
Consommation des données	Consommation d...	En cours d'e...	Automatique	Service I...
Conteneur Microsoft Passp...	Gère les clés d'ide...		Manuel (Déclencher le démarra...	Service I...
Contrôle parental	Applique le contr...		Manuel	Système
Coordinateur de transactio...	Coordonne les tr...		Manuel	Service r...
CoreMessaging	Manages commu...	En cours d'e...	Automatique	Service I...
CredentialEnrollmentMana...	Gestionnaire d'in...		Manuel	Système
CredentialEnrollmentMana...	Gestionnaire d'in...		Manuel	Système
Découverte SSDP	Découvre les péri...	En cours d'e...	Manuel	Service I...
Détection matériel noyau	Fournit des notifi...	En cours d'e...	Automatique	Système
DeviceAssociationBroker_18...	Enables apps to p...		Manuel	Système
DeviceAssociationBroker_20...	Enables apps to p...		Manuel	Système

Gestion de l'ordinateur (local) > Services

Hôte de périphérique UPnP

Démarrer le service

Description : Autorise l'hébergement des périphériques UPnP sur cet ordinateur. Si ce service est arrêté, tous les périphériques UPnP hébergés cesseront de fonctionner et aucun autre périphérique hébergé ne pourra être ajouté. Si ce service est désactivé,

Nom	Description	État	Type de démarrage	Ouvrir u...
Gestionnaire des utilisateurs	Le Gestionnaire d...	En cours d'e...	Automatique (déclencher le dé...	Système
Gestionnaires des paiement...	Gère les paiemen...		Manuel (Déclencher le démarra...	Service I...
GraphicsPerfSvc	Graphics perform...		Manuel (Déclencher le démarra...	Système
Groupe de mise en rés...	Permet la comm...		Manuel	Service I...
Heure cellulaire	Ce service définit ...		Manuel (Déclencher le démarra...	Service I...
Hôte de DLL de compteur d...	Permet aux utilis...		Manuel	Service I...
Hôte de périphérique UPnP	Autorise l'héberg...		Manuel	Service I...
Hôte de synchronisation_18...	Ce service synchr...	En cours d'e...	Automatique (début différé)	Système
Hôte de synchronisation_20...	Ce service synchr...	En cours d'e...	Automatique (début différé)	Système
Hôte du fournisseur de dé...	Le service FDPHO...	En cours d'e...	Manuel	Service I...

Gestion de l'ordinateur (local) > Services

Hôte du fournisseur de découverte de fonctions

Arrêter le service
Redémarrer le service

Description : Le service FDPHOST héberge les fournisseurs de découverte de réseau de découverte de fonction (FD). Ces fournisseurs de découverte de fonction fournissent des services de découverte de réseau pour les protocoles SSDP (Simple Services Discovery Protocol) et WS-D (Web Services - Discovery). L'arrêt ou la désactivation du service FDPHOST

Nom	Description	État	Type de démarrage	Ouv...
Gestionnaire des utilisateurs	Le Gestionnaire d...	En cours d'e...	Automatique (déclencher le dé...	Syst
Gestionnaires des paiements et ...	Gère les paiemen...		Manuel (Déclencher le démarra...	Serv
GraphicsPerfSvc	Graphics perform...		Manuel (Déclencher le démarra...	Syst
Groupe de mise en réseau ...	Permet la comm...		Manuel	Serv
Heure cellulaire	Ce service définit ...		Manuel (Déclencher le démarra...	Serv
Hôte de DLL de compteur de pe...	Permet aux utilis...		Manuel	Serv
Hôte de périphérique UPnP	Autorise l'héberg...		Manuel	Serv
Hôte de synchronisation_18bd1e	Ce service synchr...	En cours d'e...	Automatique (début différé)	Syst
Hôte de synchronisation_20d45	Ce service synchr...	En cours d'e...	Automatique (début différé)	Syst
Hôte du fournisseur de découve...	Le service FDPHO...	En cours d'e...	Manuel	Serv
Hôte système de diagnostics	Le service Hôte s...	En cours d'e...	Manuel	Syst
Identité de l'application	Détermine et véri...		Manuel (Déclencher le démarra...	Serv
Informations d'application	Permet d'exécute...	En cours d'e...	Manuel (Déclencher le démarra...	Syst

Gestion de l'ordinateur (local) > Services

Mappage de découverte de topologie de la couche de liaison

Arrêter le service
Redémarrer le service

Description : Crée un mappage réseau, consistant en informations sur la topologie des ordinateurs et des périphériques (connectivité) et en métadonnées décrivant chaque ordinateur et chaque périphérique. Si ce service est désactivé, le mappage réseau ne

Nom	Description	État	Type de démarrage
Isolation de clé CNG	Le service d'isolat...	En cours d'e...	Manuel (Déclencher le dé...
Jeu sauvegardé sur Xbox Live	Ce service synchr...		Manuel (Déclencher le dé...
Journal d'événements Windows	Ce service gère le...	En cours d'e...	Automatique
Journaux & alertes de performance	Le service des jou...		Manuel
Lanceur de processus serveur DCOM	Le service DCOM...	En cours d'e...	Automatique
Localisateur d'appels de procédure distante (R...	Dans Windows 20...		Manuel
Mappage de découverte de topologie de la co...	Crée un mappag...	En cours d'e...	Manuel
Mappeur de point de terminaison RPC	Résout les identifi...	En cours d'e...	Automatique
MessagingService_18bd1e	Service prenant e...		Manuel (Déclencher le dé...
MessagingService_20d45	Service prenant e...		Manuel (Déclencher le dé...
Mettre à jour le service Orchestrator	Gère les mises à j...	En cours d'e...	Automatique (début diffé...

MECANISME DU VOISINAGE RESEAU

Principe de fonctionnement :

Lorsque l'on clique sur voisinage réseau, on a souvent une réponse lors du démarrage de la machine comme quoi le "parcours du réseau est impossible", or **il suffit d'attendre et tout rentre dans l'ordre...**

Mais la signification du message est la suivante : actuellement un **Explorateur Principal** n'est pas encore identifié...

Environ toutes les 12 minutes, les serveurs annoncent leur présence avec des trames spéciales au format NetBios. Une élection d' Explorateur Principal peut arriver lorsque

- un ordinateur n'arrive pas à trouver un Explorateur Principal
- Lorsque un Explorateur Principal arrive sur le réseau, ou s'arrête.
- Lorsque un Contrôleur de Domaine démarre:

Lorsque une élection est lancée, un algorithme compliqué basé sur plusieurs variables se déroule (type de OS, version d'OS, configuration, adressage IP, nombre de machines présentes etc) et un seul Explorateur Principal sera déclaré !

A chaque fois qu'un PC démarre, il est configuré par défaut pour tenter de savoir s'il doit devenir Explorateur...

Il peut exister jusqu'à 5 types de machines dans un réseau Windows

Non-Browser / Non Explorateur

Un **non-browser** ou **non Explorateur** est un ordinateur qui a été configuré pour ne pas maintenir une liste des ordinateurs devant apparaître dans le voisinage réseau

Potential Browser / Explorateur Potentiel

Un **Potential-Browser** ou **Explorateur Potentiel** est un ordinateur capable de maintenir une liste des ordinateurs devant apparaître dans le voisinage réseau , et pouvant être promu comme Explorateur principal. Un **Explorateur Potentiel** est aussi capable de jouer le rôle d'un **Explorateur de Secours**, s'il est piloté par un **Explorateur Principal**

Backup Browser / Explorateur de Secours

Un **Backup-Browser** ou **Explorateur de Secours** reçoit une copie des ordinateurs devant apparaître dans le voisinage réseau depuis un **Explorateur Principal** et fournis cette liste à la demande des autres ordinateurs du domaine ou du groupe de travail

N.B: Lorsqu'un poste démarre, c'est l' **Explorateur Principal** qui lui indique s'il doit devenir un **Explorateur de Secours** ou non

Master Browser / Explorateur Principal

Un **Master-Browser** ou **Explorateur Principal** est responsable de la collecte des informations nécessaires à la création et à mise à jour de la liste des ordinateurs figurant dans le voisinage réseau. Cette liste inclut tous les serveurs du domaine de l' **Explorateur Principal** et la liste de tous les domaines sur le réseau. Les machines windows annoncent leur présence à l' **Explorateur Principal** par un datagramme appelé "server announcement", et celui-ci les ajoute

- Si un Domaine s'étend sur plus d'un sous-réseau, l' **Explorateur Principal** travaille de la manière suivante :
 - ✓ Il gère la liste pour le sous-réseau dont il fait partie
 - ✓ fournit cette liste à chaque Explorateur de Secours de chaque sous-réseau
- Si un sous-réseau comprends plusieurs Domaines, chaque Domaine à son **Explorateur Principal** et éventuellement ses **Explorateurs de Secours**

Domain Master Browser / Explorateur Principal de Domaine

Un **Domain Master-Browser** ou **Explorateur Principal de Domaine** est responsable de la collecte des informations pour la création et la mise à jour de la liste pour tout le domaine, collecte les informations des **Explorateur Principaux** des autres sous-réseaux et fournit les informations aux **Explorateur Principaux** des autres sous-réseaux.

Un **Explorateur Principal de Domaine** est toujours le Contrôleur Principal de Domaine

N.B: Un poste peut jouer plusieurs rôles, par exemple l' **Explorateur Principal** peut aussi être un **Explorateur Principal de Domaine**

Rafraîchissement Tests et vérifications :

Quelles sont les vitesses de rafraîchissement ?

de quelques secondes, à plusieurs minutes, jusqu'à 12 minute pour la prise en compte d'un serveur dans un Domaine, ce qui par rebonds peut aller à 24 minutes entre 2 Domaines...

Pour la suppression d'une machine c'est pire, Microsoft annonçant jusqu'à 36 minutes pour la mise à jour d'une liste "rayant" une machine qui ne se serait pas correctement déconnectée du réseau (arrêt système brutal...)

Peut on éviter l'élection d'un Explorateur ? :

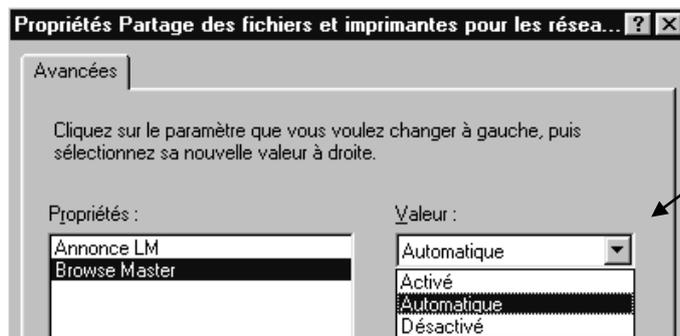
la réponse est non; il doit y en avoir toujours un, mais on peut à la limite accélérer un peu les choses

En implémentant un serveur WINS qui diminuera le trafic réseau pour les résolutions de nom Netbios,

En implémentant un serveur DNS qui diminuera le trafic réseau pour les résolutions de nom

En modifiant le status d'une machine : si on modifie dans propriété de partage des fichiers et imprimantes le fait qu'une machine soit éligible ou non (on peut éviter les élections et diminuer les trâmes émises...)

Sous Windows 95-98

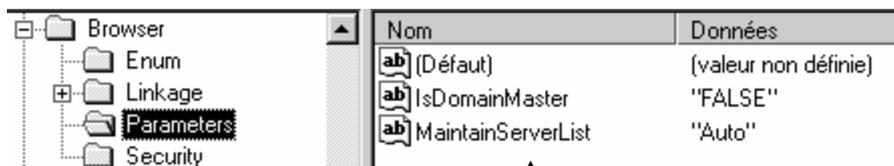


définir qui peut être Browse Master

N.B: Il doit y en avoir toujours 1 seul !

Sous Windows NT ou 2000

Il faut modifier la base de registre NT "ce qui reste délicat"

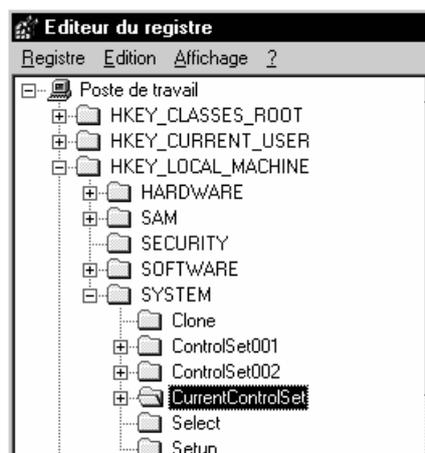


Il faut se positionner sur la clé

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters

et y modifier la clé de type DWORD-value nommée **MaintainServer List** les valeurs possibles sont **"Auto" "No" et "Yes"**

En accélérant la vitesse de rafraîchissement... Il faut modifier la base de registre NT "ce qui reste délicat"



Il faut se positionner sur la clé **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**

et y créer une clé de type DWORD-value

en allant dans le menu

Edition / nouveau / valeur Dword

et y entrer la clé **Announce**

Nom	Données
[ab] (Défaut)	(valeur non définie)
[00] Lmanannounce	0x00000000 (0)
[00] NullSessionPipes	43 4f 4d 4e 41 50 00 43 4f 4d 4e 4f 44 45 00 53
[00] NullSessionShares	43 4f 4d 43 46 47 00 44 46 53 24 00 00
[00] Size	0x00000001 (1)
[00] Announce	0x00000000 (0)

cette valeur Announce il faut ensuite la modifier via le menu

Edition / modifier



une valeur de 60 secondes (3c hexa) semble un bon compromis entre vitesse et nombre de trames...

PROTOCOLE DHCP

Objectif de DHCP :

Le protocole **DHCP (Dynamic Host Configuration Protocol)** centralise et gère l'attribution des informations de configuration **TCP-IP** en affectant automatiquement des adresses **IP** à des ordinateurs configurés pour utiliser DHCP. La mise en œuvre de **DHCP** élimine certains problèmes de configuration liés à la configuration manuelle de **TCP-IP**.

A chaque démarrage d'un client **DHCP**, ce dernier demande des informations d'adressage IP à un serveur **DHCP**. Un client ne choisit pas un serveur DHCP, il interroge le réseau avec un **broadcast DHCP** pour repérer les serveurs **DHCP** potentiel en vue de récupérer a terme notamment :

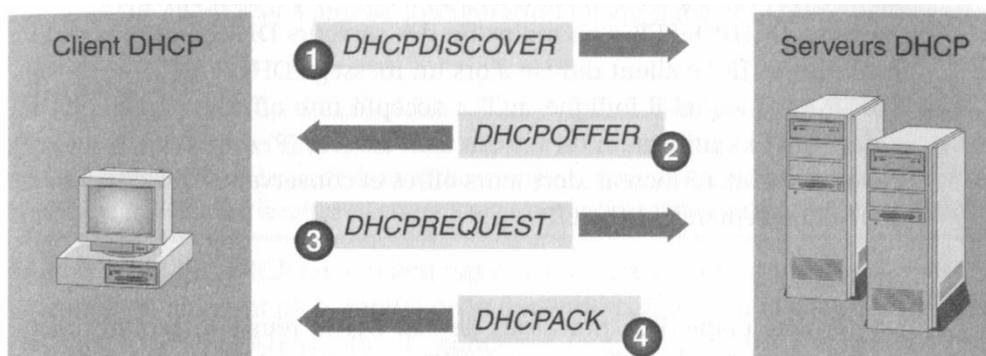
- Une adresse IP
- Un masque de sous-réseau.
- Des valeurs facultatives, comme une adresse de **passerelle** par défaut, une adresse **DNS** ou l'adresse du serveur WINS.

Lorsqu'un serveur **DHCP** reçoit une requête, il sélectionne des informations d'adressage IP dans une réserve d'adresses définie dans une base de données et les propose au client **DHCP**. Si le client les accepte, les informations d'adressage **IP** lui sont cédées sous la forme d'un bail d'une durée spécifique. Si aucune information d'adressage IP n'est disponible dans la réserve pour location au client, ce dernier ne peut pas initialiser **TCP/IP**. Il peut selon les cas se doter d'une adresse **APIPA**.(cf chap spécifique).

Remarque : Le protocole **DHCP** est défini dans les RFC 1533, 1534, 1541 et 1542. et est dérivé du protocole **BootP**.

Fonctionnement de DHCP :

Pour configurer un client DHCP, le protocole DHCP travaille en 4 phases :



DHCPDISCOVER ou "Demande de bail IP" :

Le client ne disposant pas d'adresse IP et ne connaissant l'adresse IP d'aucun serveur, il utilise 0.0.0.0 comme adresse de source et 255.255.255.255 comme adresse de destination.

La demande de bail est envoyé au sein d'un message **DHCPDISCOVER**. Ce message contient également l'adresse matérielle et le nom d'ordinateur du client, afin que les serveurs DHCP puissent identifier l'émetteur de la requête. Tous les serveurs répondent s'ils le peuvent.

Le processus de bail IP est utilisé dans l'une des situations suivantes:

- TCP/IP est initialisé pour la première fois en tant que client DHCP.
- Le client demande une adresse IP spécifique qui lui est refusée. Il est possible que le serveur DHCP ait supprimé le bail.
- Le client disposait auparavant d'un bail d'adresse IP mais y a mis fin et en demande un nouveau.

DHCPOFFER ou "Offre de bail IP" :

Tous les serveurs DHCP qui ont reçu la demande et qui disposent d'une configuration valide vis-à-vis du client diffusent une proposition.

Le client ne disposant pas encore d'une adresse IP, l'envoi de la proposition s'effectue par diffusion sous forme de message **DHCPOFFER**.

Remarque : Lorsque aucun serveur DHCP n'est en ligne, le client DHCP attend une proposition pendant 1 seconde. S'il n'en reçoit aucune, il diffuse à nouveau la requête à trois reprises (selon des intervalles successifs de 9, 13 et 16 secondes). Si aucune proposition n'est reçue après quatre tentatives, le client essaie à nouveau toutes les 5 minutes.

DHCPREQUEST ou "Selection de bail IP" :

Après avoir reçu une proposition d'au moins un serveur DHCP, le client informe par diffusion tous les autres serveur DHCP de sa sélection, en acceptant la première proposition reçue.

La diffusion est envoyé dans un message **DHCPREQUEST** et comprend l'identificateur du serveur (AI) dont la proposition a été acceptée. Tous les autres serveurs DHCP retirent leur proposition afin que les adresses IP dont ils disposent restent disponibles pour la requête de bail IP suivante.

DHCPACK / NACK ou "Accusé de réception de bail IP" :

Le serveur DHCP dont la proposition est acceptée diffuse au client un accusé de réception stipulant la conclusion du bail, sous la forme d'un message **DHCPACK**. Ce message contient un bail valide pour une adresse IP et éventuellement d'autres informations de configurations.

Si un accusé de réception stipulant la non conclusion du bail (**DHCPNACK**) est diffusé (le client tente de souscrire le bail d'une adresse IP dont il disposait précédemment alors que cette adresse n'est plus disponible par exemple) le client retourne au processus de demande de bail IP.

"Renouvellement de bail IP" :

Tous les clients DHCP tentent de renouveler leur bail lorsqu'il atteint **50 %** de sa durée. Pour renouveler, un client DHCP envoie un message **DHCPREQUEST** directement au serveur DHCP avec qui il a conclu le bail en vigueur.

Si le serveur DHCP est disponible, il renouvelle le bail et envoie au client un accusé de réception stipulant la conclusion du renouvellement (**DHCPACK**) et la nouvelle durée, ainsi que les éventuelles mises à jour des paramètres de configuration.

Lorsque le client reçoit l'accusé de réception, il met à jour sa configuration. Si un client tente de renouveler son bail mais est dans l'impossibilité de contacter le serveur DHCP à l'origine de ce dernier, le client peut encore utiliser l'adresse, puisqu'il lui reste 50 % de la durée du bail.

Lorsqu'un client DHCP redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine. Pour ce faire, il diffuse un message **DHCPREQUEST** spécifiant la dernière adresse IP dont il avait le bail. Si la tentative se solde par un échec et qu'il lui reste encore du temps avant l'expiration du bail, le client DHCP continue à utiliser la même adresse IP.

Si un bail, lorsqu'il atteint **50 %** de sa durée, n'a pas pu être renouvelé par le serveur DHCP d'origine, le client tente de contacter les autres serveurs DHCP disponibles lorsque **87,5% du temps s'est écoulé**. Le client diffuse alors un message **DHCPREQUEST**. Tous les serveurs DHCP peuvent répondre par un message **DHCPACK(renouvellement du bail)** ou **DHCPNACK (obligeant le client DHCP à se réinitialiser)** et à obtenir le bail d'une adresse IP différente).

Lorsque le bail expire ou qu'un message DHCPNACK est reçu, le client DHCP doit immédiatement cesser d'utiliser l'adresse IP. Il retourne alors au processus de souscription d'un nouveau bail d'adresse IP.

DHCPRELEASE ou libération des ressources:

Le client peut envoyer un message DHCPRELEASE lorsqu'il s'arrête. Ainsi le serveur DHCP peut de nouveau utiliser ces adresses pour un autre client...

N.B: Microsoft n'utilise pas cette commande. Lorsqu'une machine s'arrête, son bail court encore sur le serveur DHCP. Si le client se reconnecte au réseau avant la fin du bail, son bail sera réattribué par une demande DHCPREQUEST...

CLIENT DHCP

Client DHCP Windows 10 - Seven

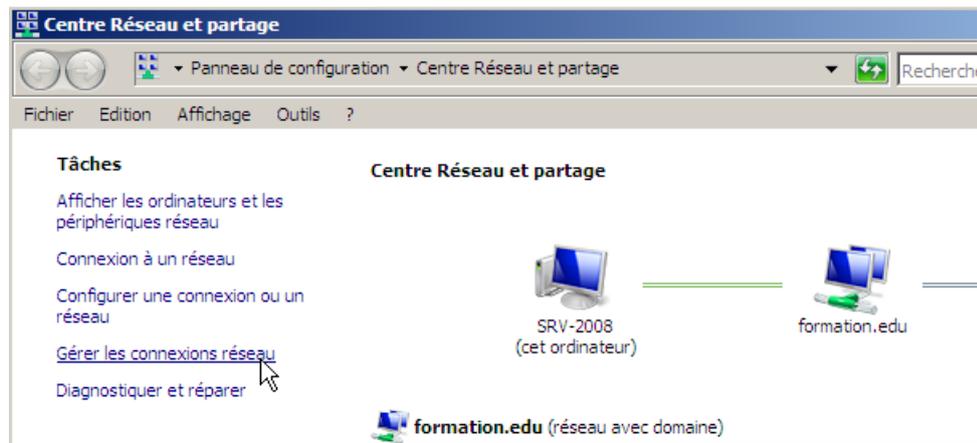
Un poste devient client DHCP simplement en demandant dans le paramétrage de TCP/IP « **Obtenir automatiquement une adresse IP** »

soit par **propriétés de réseau**, (sur le bureau)

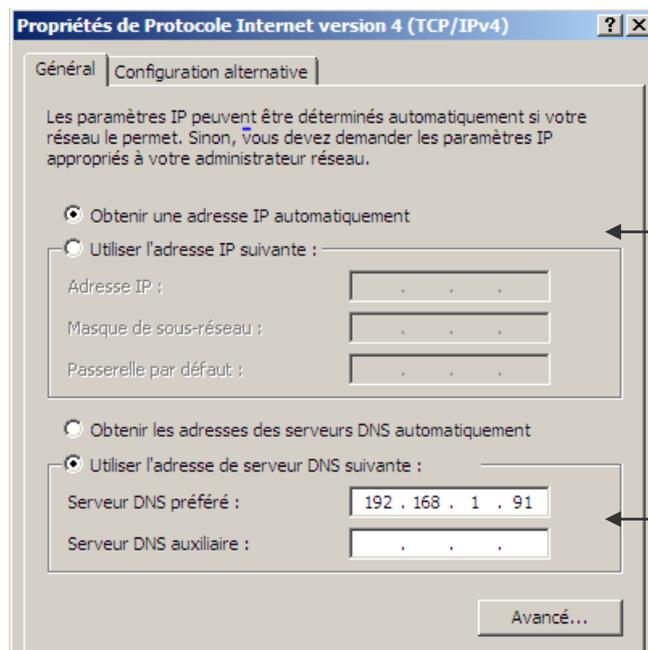
Gérer les connexions réseau



soit par **démarrer / paramètres / panneau de configuration / centre réseau et partage / Gérer les connexions réseau**



puis **propriétés de Protocole Internet Version4 (TCP/IPv4)**



Attention, on ne gère pas forcément l'adresse Ip est le paramétrage DNS de la même manière...

N.B: Lorsque l'on demande une **adresse automatique**, tout le reste du paramétrage IP devient "inactif"

Ipconfig /release /renew :

Depuis **Seven** (et à partir de NT) , à travers l'utilitaire **ipconfig** on peut demander de libérer – renouveler une adresse reçue dynamiquement...par les options

Ipconfig /release et

Ipconfig /renew ...

```
C:\Users\Administrateur>ipconfig /release
Configuration IP de Windows
```

Depuis **Seven** si plusieurs cartes existent, (et plusieurs protocole) on peut cibler le périphérique de destination de la commande **ipconfig**...

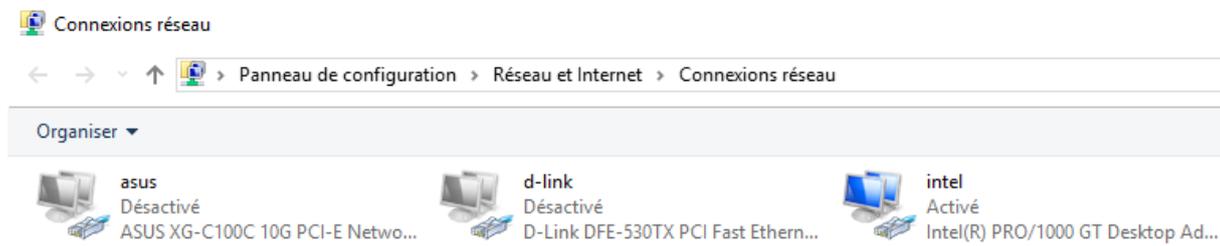
On parle du nom logique de la carte et nom du nom technique. Si la carte est nommée par défaut, cela sera "**Connexion au Réseau local**"

```
C:\Users\Administrateur>ipconfig /release "Connexion au Réseau Local"
Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . :
    Passerelle par défaut. . . . . :

Carte Tunnel Connexion au réseau local* :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
```

Mais si les cartes ont été nommées...



```
C:\Users\Administrateur>ipconfig /release "Connexion au Réseau local"
Configuration IP de Windows

L'opération a échoué car aucune carte n'a le statut autorisé pour cette
opération.
```

N.B: si aucun serveur DHCP n'est présent, un mécanisme dit "adresses APIPA" se met en œuvre, (voir "adresses automatiques APIPA") uniquement pour des postes **Windows 10, Seven, (Windows)**

N.B: attention à la possibilité d'une **Configuration alternative....**(voir chapitre adresse **APIPA**)

ADRESSES IP AUTOMATIQUES (APIPA)

Principe APIPA et DHCP:

L'origine du mécanisme vise à pallier une défaillance du Serveur DHCP.

Le fonctionnement est le suivant :

1. Une machine installée avec un protocole TCP/IP tente de contacter un serveur DHCP pour recevoir une adresse IP de manière dynamique (elle doit être configurée pour...)
2. Si aucun serveur DHCP ne répond, la fonction APIPA génère une adresse IP au format 169.254.xxx.xxx avec un masque de sous-réseau 255.255.0.0. Si cette adresse est déjà utilisée la fonction APIPA en sélectionne une autre pour un maximum de 10 coups.
3. Une fois une adresse prise, l'ordinateur la diffuse et l'utilise jusqu'à ce qu'un serveur DHCP n'apparaisse opérationnel sur le réseau !

Quelques remarques :

- l'IANA (Internet Assigned Number Authority) a réservé les adresses de **169.254.0.0** à **169.254.255.255** à la fonction APIPA, ces adresses n'étant pas routables !
- Les machines utilisant des adresses APIPA ne peuvent communiquer qu'avec des machines faisant partie du même sous-réseau de classe B, et dotée d'une adresse au format 169.254.xxx.xxx

APIPA et Windows:

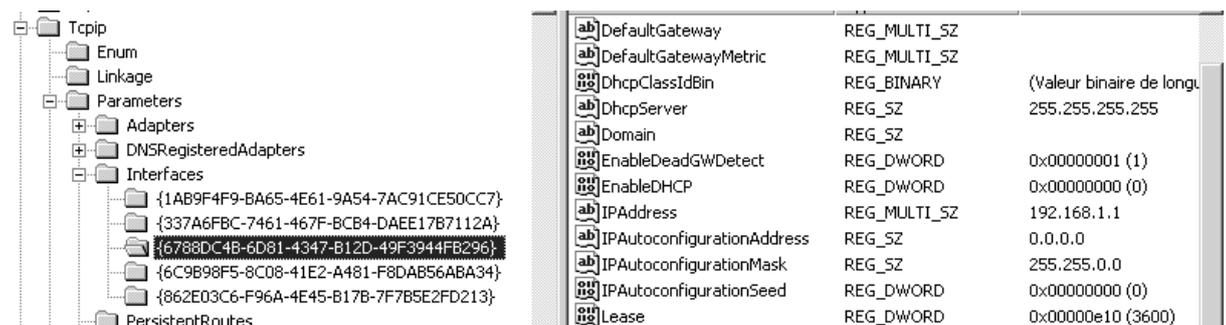
Pour que Windows puisse gérer les adresses APIPA, il est nécessaire d'utiliser TCP/IP comme protocole et de demander le bouton Option "Obtenir une adresse IP automatiquement" dans Propriétés de Protocole Internet (TCP/IP). Il s'agit en fait de configurer le client DHCP.

Désactivation adresse APIPA:

Par défaut les adresses APIPA sont actives, il est possible de les inhiber en allant dans la base de registre et en demandant

Pour chaque carte réseau sélectivement :

HKEY_LOCALMACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameter s\Interfaces\GUID_carte_reseau et en lui ajoutant l'entrée



The screenshot shows the Windows Registry Editor. On the left, the tree view is expanded to 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces'. A specific network interface GUID is selected. On the right, the list of registry values for this interface is displayed:

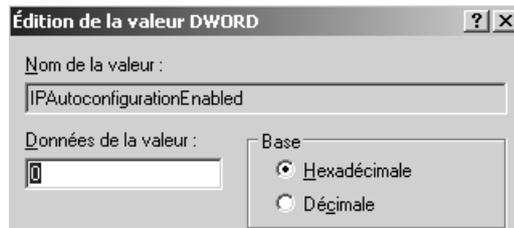
ab]DefaultGateway	REG_MULTI_SZ	
ab]DefaultGatewayMetric	REG_MULTI_SZ	
00]DhcpClassIdBin	REG_BINARY	(Valeur binaire de longu...
ab]DhcpServer	REG_SZ	255.255.255.255
ab]Domain	REG_SZ	
00]EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
00]EnableDHCP	REG_DWORD	0x00000000 (0)
ab]IPAddress	REG_MULTI_SZ	192.168.1.1
ab]IPAutoconfigurationAddress	REG_SZ	0.0.0.0
ab]IPAutoconfigurationMask	REG_SZ	255.255.0.0
00]IPAutoconfigurationSeed	REG_DWORD	0x00000000 (0)
00]Lease	REG_DWORD	0x00000e10 (3600)

IPAutoconfigurationEnabled avec une valeur de 0

(si cette entrée n'existe pas ou que sa valeur est fixée à 1 APIPA est activée)

On peut aussi invalider les adresses **APIPA** globalement pour toutes les cartes en ajoutant la même clé

IPAutoconfigurationEnabled avec une valeur de 0



Directement au niveau de l'entrée

...**CurrentControlSet\Services\Tcpip\Parameters**

Adresse IP alternative:

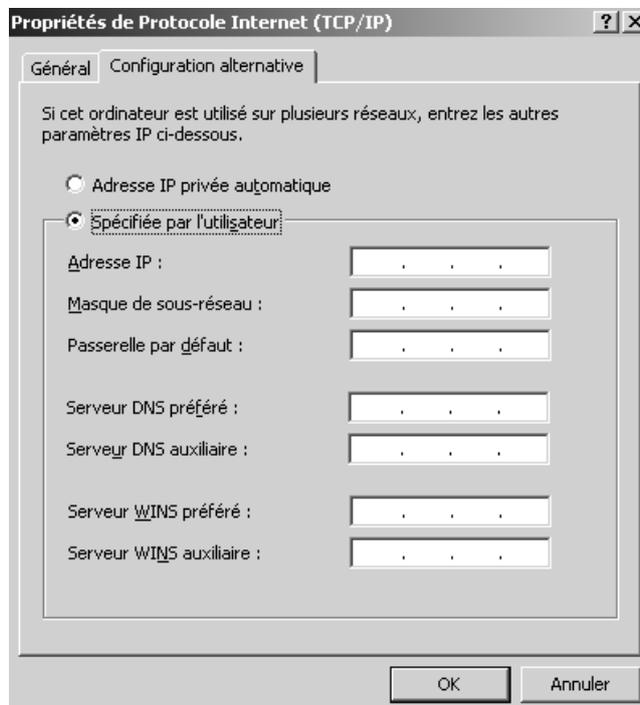
Si un client DHCP ne trouve pas de serveur DHCP, il peut donc prendre une adresse APIPA.

Mais il est possible de lui spécifier une adresse alternative, qui lui sera attribuée dans le cas où un serveur DHCP est manquant. Et donc prenant la place du mécanisme APIPA.

Cela peut permettre ainsi de pouvoir avoir sur un portable, une configuration « Bureau » en tant que client DHCP, et une configuration « maison » avec une adresse privées classique.

N.B : seuls les **Admins** ou **Opérateurs de configuration Réseau** peuvent modifier ce paramétrage.

Lorsque sur une carte on est en client DHCP, alors un onglet supplémentaire est activé : l'onglet **Configuration alternative**



Il est possible ici d'indiquer une configuration complète...

N.B : si on utilise ce mécanisme de **Configuration Alternative**, il ne faut pas alors dévalider les adresses APIPA avec la modification de la base de registre du chapitre précédent.

Toute présence de clé **IPAutoconfigurationEnabled** annulera ce mécanisme

NOTION DE DNS

Le DNS:

DNS est au centre de la gestion des domaines dans Windows. Il faut en comprendre certaines notions fondamentales

Noms DNS

Selon la définition de la RFC 952 le nom DNS d'un ordinateur est constitué de plusieurs parties séparées par des virgules, par exemple, **www.fnac.presse.fr**.

	NetBIOS	Full computer name
Type	Flat	Hierarchical
Character Restrictions	A-Z, a-z, 0-9, "espace", symbols: ! @ # \$ % ^ & ') (. - _ { } ~ Unicode chars,	A-Z, a-z, 0-9, symbols: -, Unicode chars. Le point '.' est le séparateur
Maximum Length	16 (dont 1 réservé) dont 15 en pratique	63 pour un nom de domaine 255 pour un FQDN
Name Service	NBNS (WINS and broadcast)	DNS

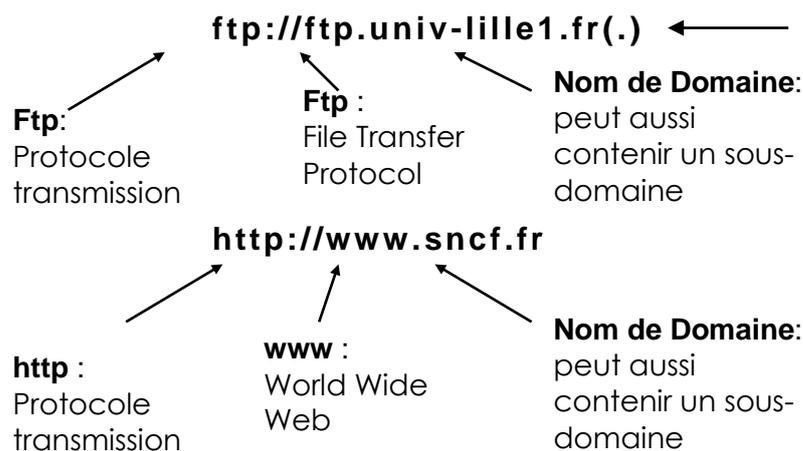
Windows utilise les noms DNS comportant des caractères soulignés, une fonction qui affectera le choix de serveur DNS

Nom "Plat" Netbios

Les nom netbios sont créés-enregistrés lors du démarrage de chaque poste, et doivent être uniques sur tous le réseau. Ce simple constat pose les limites d'envergure des noms Netbios gérés par broadcast, d'ou l'apparition de serveur WINS sur les réseaux de taille moyenne-grande. Mais même ainsi, il paraît impossible d'assurer l'unicité sur des réseau de grandes envergure...

Nom "Hierarchique" DNS

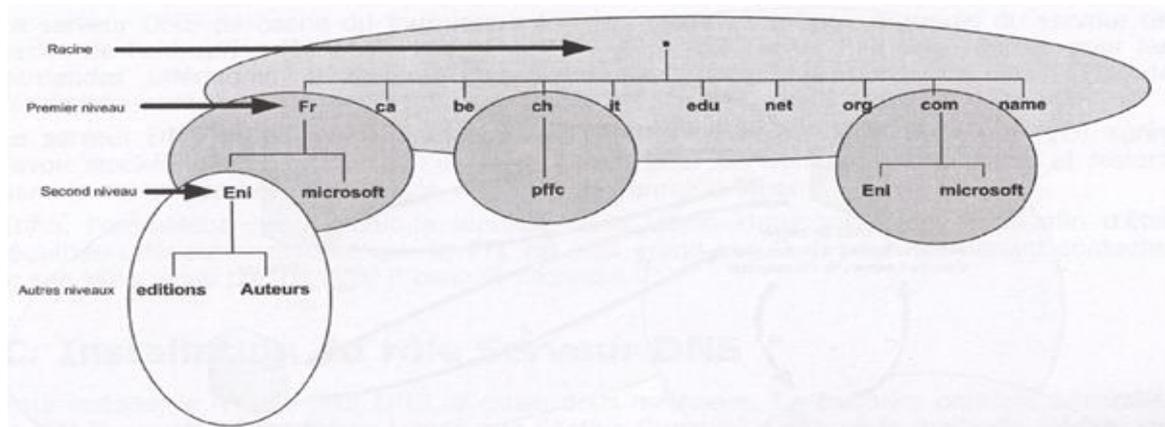
une URL se lit de droite à gauche



Un nom de domaine (**sncf.fr**) se décompose en

- ⇒ Un Top Level Domain (exemple : **fr**)
- ⇒ Un nom d'organisation (appelé aussi nom de domaine) (ex : **sncf**)

Structure des domaines – délégation de zones



Sur un espace de nom, une délégation de zone, signifie que l'on a autorité pour ce domaine.

- L'IANA a autorité pour les domaines de Premier niveau, les organismes du 1^o niveau, ont autorité jusqu'au second niveau...
- Les entreprises / particuliers n'ont autorité qu'à partir des autres niveaux.

Les Top Level Domain les plus courants sont:

Clé	Contenu
.com	Entreprise commerciale
.edu	éducation
.gov	organismes gouvernementaux
.mil	organisations militaires
.net	intervenant d'internet
.org	instance gouvernementale ou institution administrative

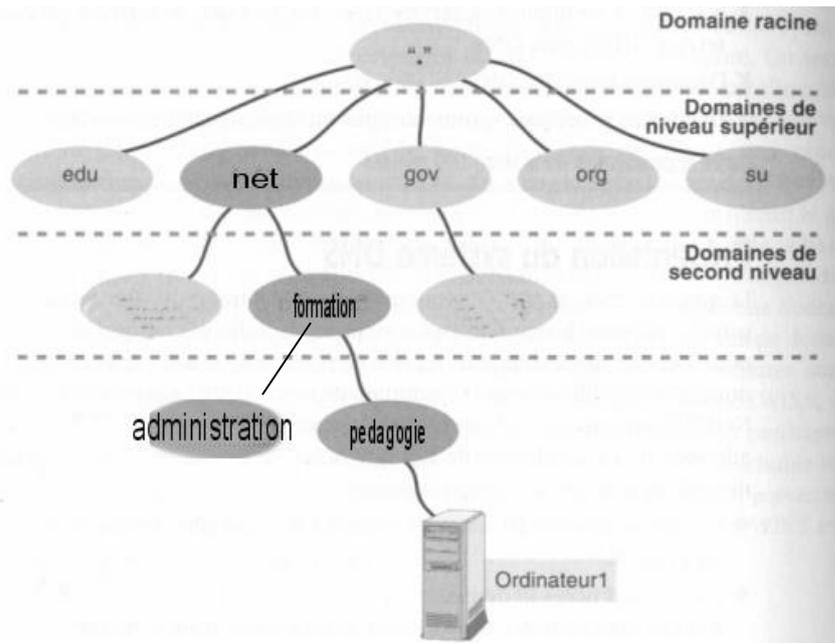
Cependant si ces domaines sont a priori internationaux, ils sont à forte dominante américaine. De plus chaque pays possède son nom de domaine (à l'exception des USA qui utilisent les 6 domaines précédents).

Clé	Contenu
.au	Australie
.ca	Canada
.fr	France
.uk	United Kingdom

L'internic se chargeant de l'attribution des adresses dans les domaines internationaux, c'est l'AFNIC France qui se charge des attributions des noms de domaine en .fr <http://www.afnic.fr>

Zones DNS:

Une **Zone** représente une partie de l'espace de nom de Domaine, à des fins de gestion.



Supposons que vous ayez deux régions, **administration** et **pedagogie**. Chaque région souhaite exploiter un serveur **DNS local**.

Pour répondre aux besoins des deux régions, vous pouvez ajouter un niveau comme par exemple :

administration.formation.net et

pedagogie.formation.net.

Chaque serveur DNS a une sous-section de domaine (une **zone** en jargon DNS).

Le serveur DNS central **formation.net** ne gère alors plus qu'un très petit nombre de noms de hosts. Il stocke en outre les noms et adresses IP des serveurs DNS de ces zones, à savoir **pedagogie.formation.net** et **administration.formation.net**.

Ainsi, si une machine **ordinateur1** se trouve dans la région **pedagogie**, elle se nommera **ordinateur1.pedagogie.formation.net**

- Si cette machine **ordinateur1** essaye d'atteindre un autre poste du domaine pédagogie, sa requête sera traitée par le serveur DNS de **pedagogie.formation.net**
- Si cette machine **ordinateur1** essaye d'atteindre un poste du domaine administration, sa requête sera traitée par le serveur DNS de **pedagogie.formation.net**, et **redirigée** vers le serveur racine de niveau supérieur, à savoir **formation.net**. celui-ci connaît le serveur qui gère la zone administration, c'est **administration.formation.net** il renvoie l'adresse de ce serveur DNS au serveur DNS **pedagogie.formation.net** qui peut alors refaire sa demande...

Zone principale – secondaire

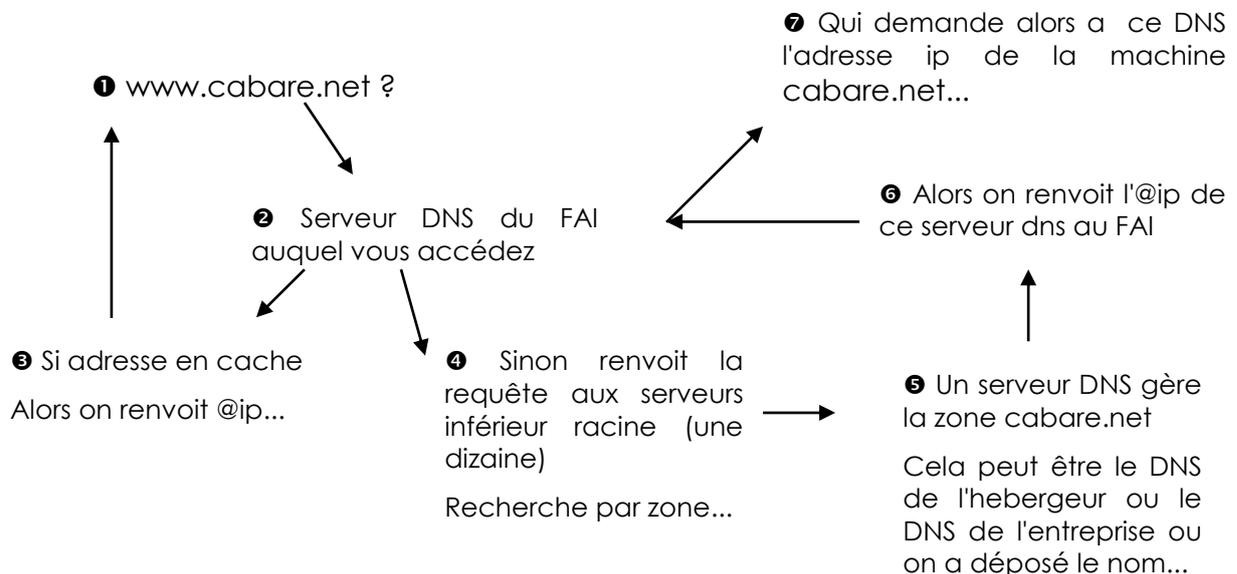
Le serveur DNS peut remplir plusieurs fonctions par rapport à une zone, le serveur chargé de la gestion initiale de la zone est appelé **serveur principal** ou **primary**. mais les informations d'une zone peuvent être répliquées sur d'autres serveurs soit dans un objectif de fiabilité, soit pour un objectif de répartition de charge. Dans ce cas le serveur DNS qui recopie les informations depuis le serveur DNS principal s'appelle un **serveur secondaire** ou **backup**. L'édition du fichier de la zone est faite sur le serveur principal qui envoie la version la plus récente du fichier au serveur DNS secondaire. Lorsqu'une machine envoie une requête au serveur secondaire, ce dernier y répond avec sa copie du fichier. Le fichier de zone du serveur secondaire a généralement une durée de vie (généralement de 24 heures). Si le serveur DNS primaire ne met pas à jour le fichier avant la période d'expiration, le serveur secondaire considère l'information comme dépassée. Si votre serveur DNS principal tombe en panne pendant quelques heures, vous n'aurez donc pas de problème. Les serveurs DNS secondaires peuvent être aussi nombreux que l'on le souhaite.

Requêtes itératives ou récursives

Avec un raisonnement identique à celui précédant pour la formation-administration décomposons la requête envoyée à un DNS pour un accès à un site sur Internet.

Vous êtes sur un poste et vous essayez d'atteindre l'URL **www.cabare.net**.

Vous pouvez vous permettre de demander en fait **www.cabare.net**, et cette demande est transmise au serveur DNS de votre FAI.



- Le processus ➊ ➋ puis ➌ est appelé requête récursive
- Le processus ➊ ➋ puis ➌ ➍ ➎ ➏ est appelé requête itérative

Résolution de Noms et Résolution inverse

Chaque composant informatique d'Internet a une adresse IP unique sur 32 bit (par exemple **154.23.17.8**). Il est possible de nommer un élément en se référant à son adresse IP. Mais la plupart des utilisateurs préfèrent les noms plus faciles à retenir comme **http://toto.com**. Pour pouvoir utiliser ce type de noms, il faut une base de données capable de convertir les adresses IP en adresses mémorisables. On appelle cela la **résolution de noms**.

la **résolution de nom (forward lookup)** permet de trouver une adresse IP à partir d'un nom

la **résolution inverse (reverse lookup)** permet de trouver un nom à partir d'une adresse IP

Du fait du faible nombre de systèmes présents sur Internet à ses origines, les machines connectées à Internet prenaient en charge la résolution de noms via une simple table ASCII (**fichier HOSTS**) qui listait les adresses IP et les noms de machines correspondants. (Le code de TCP/IP permet toujours de placer un fichier HOSTS sur un système). Depuis 1984, les systèmes ont recours principalement à **DNS** pour la résolution de noms. Sinon il faudrait maintenir un fichier HOSTS qui contiendrait non seulement des centaines de millions d'ordinateurs, mais qui changerait quotidiennement !

Ordre de Résolution DNS par le client Windows :

RECHERCHE HOTE DNS

1. d'abord le cache DNS local en RAM est utilisé
2. Ensuite un fichier Host peut être utilisé
3. le serveur DNS est interrogé (rappel de l'ordre de résolution sur un serveur DNS :)
 - a. cache serveur
 - b. zone faisant autorité (ou zone déléguée ou zone de stub)
 - c. re-directeurs conditionnels
 - d. re-directeurs par défaut
 - e. indications de racine
4. on enchaîne sur une résolution NetBIOS si le nom est NON FQDN, c'est-à-dire du genre « poste1 » (si le nom est du genre « poste1.domaine.com » alors on n'enchaîne pas sur une recherche NetBios...)
 - a. cache local Netbios
 - b. serveur WINS
 - c. Diffusion Broadcast
 - d. Consultation fichier LMHost

N.B : il est facile d'effacer le contenu du cache DNS local, par la commande **ipconfig /flushdns**

Caractéristiques des Serveurs DNS

L'implémentation la plus populaire de DNS est **BIND** (Berkeley Internet Name Domain) sous UNIX

DDNS

La méthode utilisée pour ajouter un nouvel enregistrement correspondant à un nouvel ordinateur - un nouveau host en terminologie DNS, dépend de votre logiciel serveur DNS. La plupart utilisent des fichiers ASCII.

Les solutions de serveur DNS les plus récentes n'exigent plus de mises à jour grâce au standard **DDNS (Dynamic DNS)** que décrit en détail la RFC 2136. Dans un réseau compatible DDNS, les ordinateurs font d'eux-mêmes les présentations sans qu'un administrateur ne doive intervenir sur le DNS

Enregistrements SRV

Les solutions de serveur DNS les plus récentes gèrent une autre sorte d'enregistrement DNS : les **enregistrements SRV** que décrit en détail la RFC 2052. Ces enregistrements permettent de demander à un serveur DNS si il connaît des machines jouant le rôle de serveur d'un type spécifique

Serveur principal - secondaire

Le serveur DNS peut remplir plusieurs fonctions par rapport à une zone, le serveur chargé de la gestion initiale de la zone est appelé **serveur principal** ou **primary**. mais les informations d'une zone peuvent être répliquées sur d'autres serveurs soit dans un objectif de fiabilité, soit pour un objectif de répartition de charge. Dans ce cas le serveur DNS qui recopie les information depuis le serveur DNS principal s'appelle un **serveur secondaire** ou **backup**. L'édition du fichier de la zone est faite sur le serveur principal qui envoie la version la plus récente du fichier au serveur DNS secondaire. Lorsqu'une machine envoie une requête au serveur secondaire, ce dernier y répond avec sa copie du fichier. Le fichier de zone du serveur secondaire a généralement une durée de vie (généralement de 24 heures). Si le serveur DNS primaire ne met pas à jour le fichier avant la période d'expiration, le serveur secondaire considère l'information comme dépassée. Si votre serveur DNS principal tombe en panne pendant quelques heures, vous n'aurez donc pas de problème. Les serveurs DNS secondaires peuvent être aussi nombreux que l'on le souhaite.

NOM NETBIOS

Protocole NetBeui :

Windows 9x et NT pouvaient utiliser le protocole propriétaire Netbeui pour communiquer avec d'autre machine Windows.

Pour les réseaux de petite taille, une vingtaine de postes, cette solution permettait un partage simple des ressources. Les **applications NETBIOS** accédaient au réseau en s'appuyant sur le **protocole NETBEUI**.

Quelques définitions :

NetBIOS :

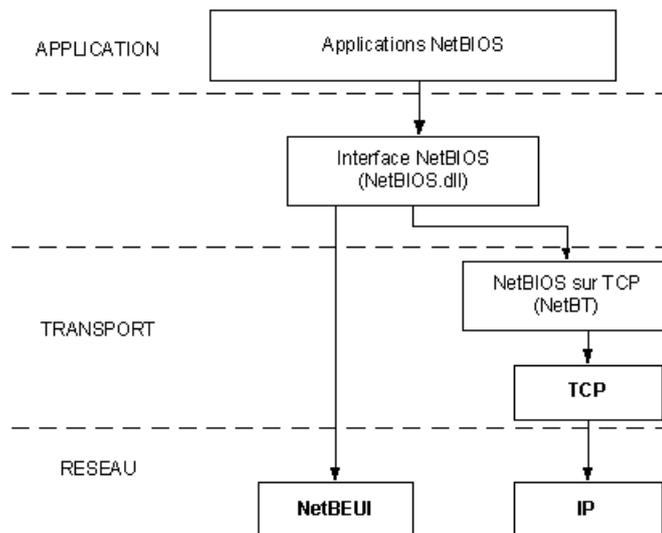
(Network Basic Input/output System) Interface de programmation qui permet aux applications d'accéder au réseau local. NetBIOS utilise un service de noms pour contrôler les échanges de point à point.

NetBEUI :

(NetBIOS Extended User Interface) est le protocole de transport des réseaux Windows. Il ne peut pas être routé et repose principalement sur les diffusions.

NetBT

(NetBIOS sur TCP/IP) est le service de résolution de noms NetBIOS pour les réseaux Windows sous TCP/IP.



Résolution de nom NetBIOS

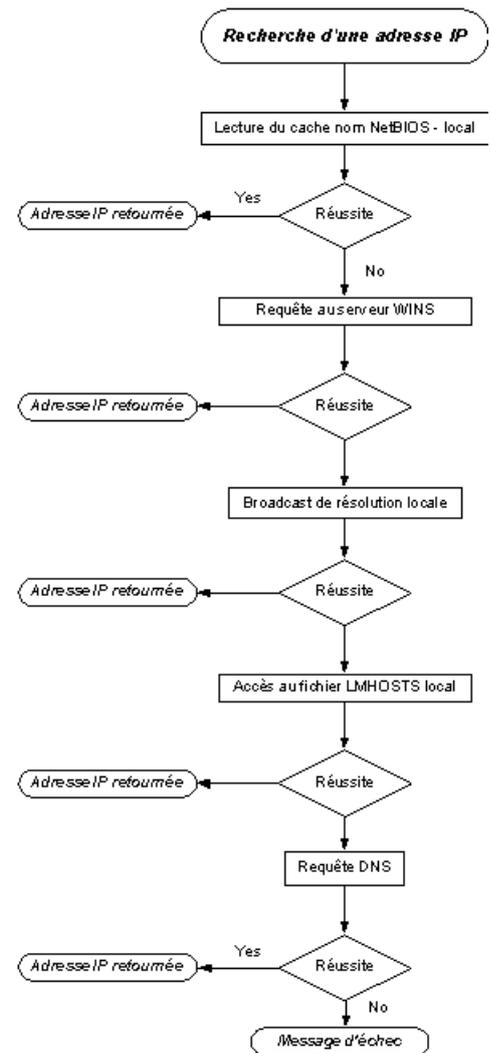
Windows peut utiliser différentes méthode pour effectuer la résolution de nom **netbios** :

- NetBIOS name cache (vérifiable via nbtstat -n)
- NetBIOS name server (WINS Il existe sous NT un serveur de nom NetBIOS connu sous l'appellation serveur WINS.)
- IP subnet broadcasts (limité au sous-réseau)
- Static Lmhosts file. (pour résoudre un nom netbios sur un autre réseau)
- Static Hosts file (**optionnel** pour un nom d'hôte)
- DNS servers (optionnel)

La manière dont Windows va résoudre les nom Netbios, dépends du paramétrage du poste, et de la configuration du réseau existant. Les différents modes de résolution suivants sont possibles, on parle de type de noeud:

- **B-node (diffusion)** : utilise des broadcast pour l'enregistrement et la résolution des noms Netbios.
- **P-node** : utilise un serveur de nom NetBios (Wins) pour l'enregistrement et la résolution des noms Netbios.
- **M-node** : utilise des broadcast pour l'enregistrement. Pour la résolution, utilise d'abords des Broadcast, puis en l'absence de réponse passe ne mode P-node (donc utilise un serveur WINS)
- **H-node (hybride)** : utilise un serveur de nom NetBios (Wins) pour l'enregistrement et la résolution des noms Netbios . Si un serveur ne peut pas être trouvé, il passe en b-node. (donc utilise des boradcast) . Il continue à chercher une serveur WINS et repasse en p-node des qu'il en trouve un disponible
- **Microsoft-enhanced** : utilise les fichiers Lmhosts en plus des mode standard.

Par défaut, la plupart des clients sont paramétrés en B-nodes, c'est à dire émettent des broadcast...



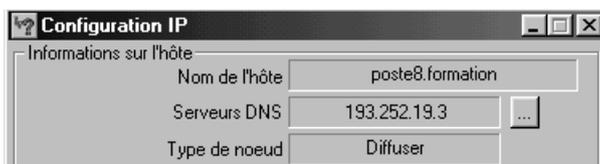
Paramétrer la résolution NetBIOS

il est bien sûr possible de voir le mode de résolution actuellement en cours sur une machine avec **IPCONFIG /ALL** dans la rubrique "**type de noeud**"

- on peut facilement demander de passer de **B-nodes** à **h-nodes**, et vice-versa.

Il suffit de renseigner ou non l'adresse d'un serveur Wins sur le client...

serveur Wins **non** renseigné



serveur Wins renseigné



L'accès aux autres modes de résolution n'est possible que sur des machines NT ou 2000 (et ultérieurs):

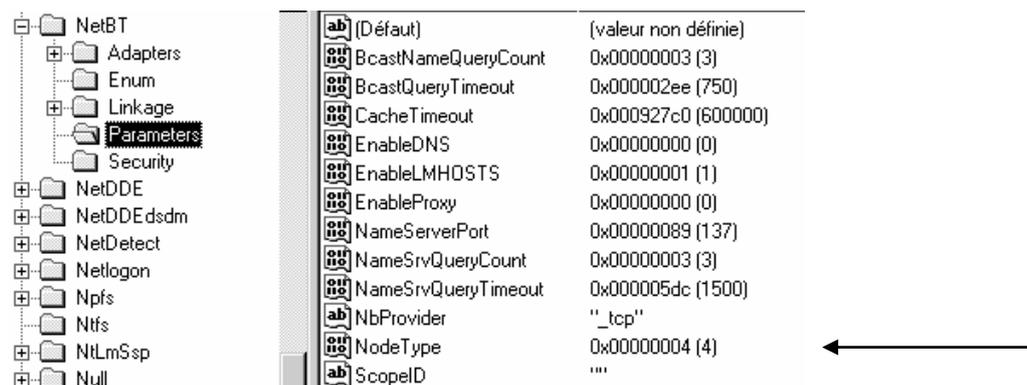
- Par exemple, l'activation des **LmHosts** se fait dans les propriétés avancées de TCP-IP, onglets Wins.
- Par exemple le passage en Type de noeud M-Nodes,

```

Configuration IP de Windows NT
Nom d'hôte . . . . . : wksnt4
Serveurs DNS . . . . . :
Type de noeud . . . . . : Mixte
Id d'étendue NetBIOS . . . . . :
Routage IP activé . . . . . : Non
WINS Proxy activé . . . . . : Non
Résolution NetBIOS utilisant DNS . . . . . : Non
    
```

ne peut se faire via modification de la base de registre par ajout d'une clé de type Dword dans l'entrée

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBt\Parameters



"type noeud"

Les valeurs possibles étant :	1	b-node	diffuser
	2	p-node	homologues
	4	m-node	mélangé - mixte
	8	h-node	hybride

Nom Netbios - Nom d'hôte:

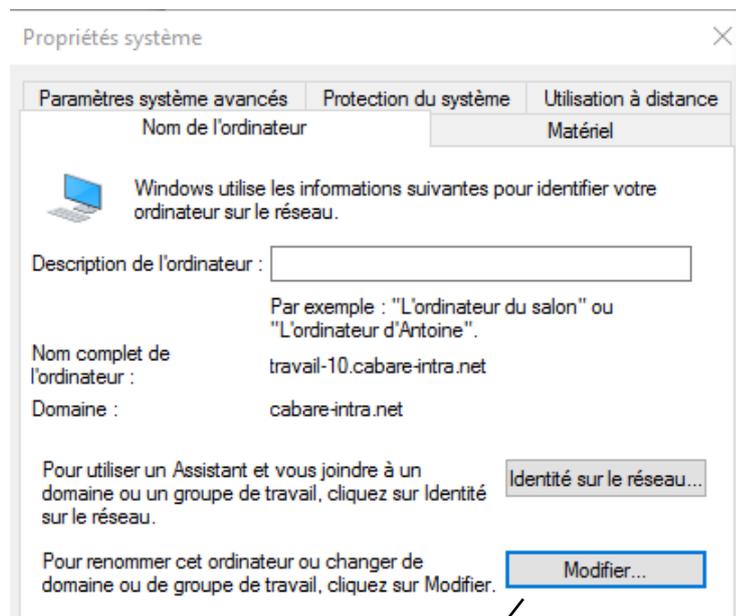
A noter qu'un nom d'hôte et un nom d'ordinateur (nom netbios 15 caractères maxi, lettre chiffre tiret pas de différence à la casse) sont deux choses différentes, même si par défaut, dans un réseau microsoft, ce sont les mêmes. Depuis **Seven: Nom netbios = Nom d'hôte** Par défaut, il y a une traduction automatique !

Sous **windows 10** on demande **Modifier les paramètres**

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur :	win10-1511	
Nom complet :	win10-1511	
Description de l'ordinateur :		
Groupe de travail :	WORKGROUP	

Puis via **Modifier**



Propriétés système

Paramètres système avancés | Protection du système | Utilisation à distance

Nom de l'ordinateur | Matériel

Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.

Description de l'ordinateur :

Par exemple : "L'ordinateur du salon" ou "L'ordinateur d'Antoine".

Nom complet de l'ordinateur : travail-10.cabare-intra.net

Domaine : cabare-intra.net

Pour utiliser un Assistant et vous joindre à un domaine ou un groupe de travail, cliquez sur Identité sur le réseau.

Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier.

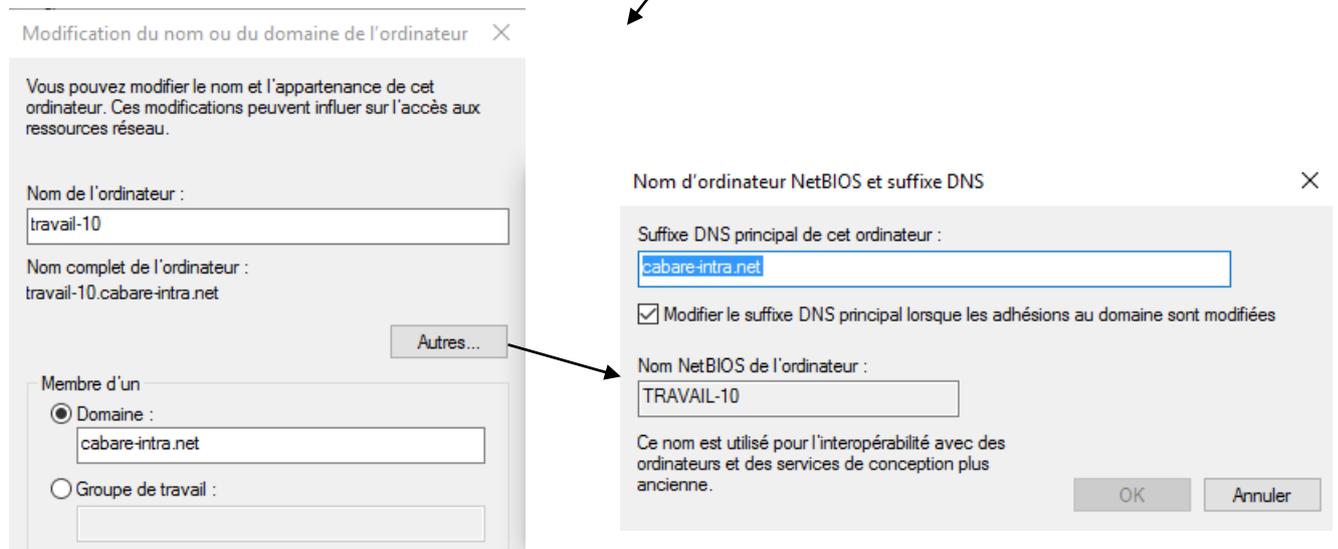
Identité sur le réseau... | Modifier...

Apparition d'une zone **"Description de l'ordinateur"**

A ne pas confondre avec le nom de l'ordinateur

Accessible par **Modifier...**

Puis **Autres**



Modification du nom ou du domaine de l'ordinateur

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur : travail-10

Nom complet de l'ordinateur : travail-10.cabare-intra.net

Autres...

Membre d'un

Domaine : cabare-intra.net

Groupe de travail :

Nom d'ordinateur NetBIOS et suffixe DNS

Suffixe DNS principal de cet ordinateur : cabare-intra.net

Modifier le suffixe DNS principal lorsque les adhésions au domaine sont modifiées

Nom NetBIOS de l'ordinateur : TRAVAIL-10

Ce nom est utilisé pour l'interopérabilité avec des ordinateurs et des services de conception plus ancienne.

OK | Annuler

N.B: ne jamais rentrer une **Description de l'ordinateur** différente du **Nom de l'ordinateur** (ne jamais suivre l'exemple, mais utiliser les règles classiques (- de 15 caractères... etc...))

Intérpretation des Nom NetBios :

N.B: On peut utiliser l'utilitaire **nbtstat** pour voir les noms NetBIOS avec la syntaxe suivante :

nbtstat -n

ou

nbtstat -a nommachine

ou nbtstat -R permet de purger les noms et force les réinscription depuis le fichier LMHOST

ou nbtstat -c permet de visualiser les noms présent dans le cache

ou nbtstat -RR permet de purger les noms et force les réinscription sans avoir a redémarrer le poste (win XP)

Les **15 premiers caractères** d'un nom peuvent être spécifiés par un utilisateur. En revanche, le **16e caractère** du nom (hexadécimal 00-FF) indique toujours un type de ressource:

Name	Nb (hexa)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
-- MSBrowse --	01	G	Domain Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Microsoft Exchange Connector
<computername>	23	U	Microsoft Exchange Store
<computername>	24	U	Microsoft Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Clients Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Clients Remote Chat
<computername>	46	U	SMS Clients Remote Transfer
<computername>	4C	U	DEC TCPIP service on NT

<computername>	42	U	mccaffee anti-virus
<computername>	52	U	DEC TCPIP service on NT
<computername>	87	U	Microsoft Exchange MTA
<computername>	6A	U	Microsoft Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service
<domain>	0	G	Domain Name
<domain>	1B	U	Domain
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
<IS~computer name>	00	U	IIS
<computername>	[2B]	U	Lotus Notes Server Service

Il existe essentiellement 2 groupes

Unique (U): Utilisé pour associer l'ordinateur par son nom à une adresse IP unique. Avec ce type de nom, trois types d'enregistrements sont ajoutés statiquement à la base de données WINS pour le nom d'ordinateur spécifié. Les types [00h] **WorkStation**, [03h] **Messenger** et [20h] **Serveur de fichiers**.

Noms uniques NetBIOS

Format	Description
nom_ordinateur [00h]	Inscrit par le service Station de travail sur le client WINS. En général, ce nom est appelé <i>nom d'ordinateur NetBIOS</i> .
nom_ordinateur [03h]	Inscrit par le service Affichage des messages sur le client WINS. Ce service est utilisé par le client pour envoyer et recevoir des messages. Ce nom est généralement ajouté au nom d'ordinateur NetBIOS du client WINS et au nom de l'utilisateur actuellement connecté à ce client pour envoyer des messages sur le réseau.
nom_ordinateur [06h]	Inscrit sur le client WINS par le service de routage et d'accès distant (lorsque ce service est démarré).
nom_domaine [1Bh]	Inscrit par chaque contrôleur de domaine Windows NT Server qui s'exécute en tant qu'explorateur principal de domaine. Cet enregistrement de nom est utilisé pour permettre l'exploration à distance des domaines. Lorsque ce nom est demandé à un serveur WINS, ce dernier renvoie l'adresse IP de l'ordinateur qui a inscrit ce nom.
nom_ordinateur [1Fh]	Inscrit par les services NetDDE (Network Dynamic Data Exchange). Ne s'affiche que si les services NetDDE sont démarrés sur l'ordinateur.
nom_ordinateur [20h]	Inscrit par le service Serveur sur le client WINS. Ce service est utilisé pour fournir des points de service au client WINS, qui lui permettent de partager ses fichiers sur le réseau.
nom_ordinateur [21h]	Inscrit sur le client WINS par le service Client RAS (lorsque ce service est démarré).
nom_ordinateur [BEh]	Inscrit par l'Agent de surveillance du réseau et n'apparaissant que si ce service est démarré sur le client WINS. Si le nom d'ordinateur compte moins de 15 caractères, les espaces restants sont remplis par des signes plus (+).
nom_ordinateur [BFh]	Inscrit par l'utilitaire de surveillance du réseau (livré avec Microsoft Systems Management Server). Si le nom d'ordinateur compte moins de 15 caractères, les espaces restants sont remplis par des signes plus (+).
nom_utilisateur [03h]	Les noms des utilisateurs actuellement connectés sont inscrits dans la base de données WINS. Chaque nom d'utilisateur est inscrit par le service Serveur de sorte que les utilisateurs peuvent recevoir toutes les commandes net send envoyées au nom d'utilisateur. Si plusieurs utilisateurs se connectent sous le même nom, seul le premier ordinateur connecté avec ce nom enregistre le nom.

Group (G): Appelé aussi groupe ordinaire. Avec ce type, l'adresse IP de l'ordinateur n'est pas stockée dans WINS, mais résolue par le biais des diffusions du sous-réseau local.

Noms de groupes NetBIOS

Format	Description
<i>nom_domaine</i> [00h]	Inscrit par le service Station de travail de sorte qu'il puisse recevoir les diffusions d'exploration provenant d'ordinateurs LAN Manager.
<i>nom_domaine</i> [1Ch]	Inscrit à l'usage du contrôleur de domaine dans le cadre du domaine. Peut contenir jusqu'à 25 adresses IP.
<i>nom_domaine</i> [1Dh]	Inscrit à l'usage des explorateurs principaux (un seul explorateur principal par sous-réseau). Les explorateurs de sauvegarde utilisent ce nom pour communiquer avec l'explorateur principal, en extrayant la liste des serveurs disponibles de l'explorateur principal. Les serveurs WINS renvoient toujours une réponse positive d'inscription pour <i>nom_domaine</i> [1D], même si le serveur WINS n'inscrit pas ce nom dans sa base de données. En conséquence, lorsque le <i>domain_name</i> [1D] est demandé à un serveur WINS, ce dernier renvoie une réponse négative, ce qui force le client à lancer une diffusion de résolution de noms.
<i>nom_groupe</i> [1Eh]	Un nom de groupe ordinaire. Tout ordinateur configuré en tant qu'explorateur de réseau peut diffuser vers ce nom, et écouter les diffusions vers ce nom, pour choisir un explorateur principal. Un nom de groupe mappé statiquement utilise ce nom pour s'inscrire sur le réseau. Lorsqu'un serveur WINS reçoit une demande de nom se terminant par [1E], il renvoie toujours l'adresse de diffusion du réseau local du client qui a émis la demande. Le client peut ensuite utiliser cette adresse pour diffuser aux membres du groupe. Ces diffusions sont destinées au sous-réseau local et ne doivent pas traverser de routeurs.
<i>nom_groupe</i> [20h]	Un nom de groupe spécial appelé <i>groupe Internet</i> est inscrit sur les serveurs WINS pour identifier des groupes d'ordinateurs pour des besoins administratifs. Par exemple, "printersg" peut être un nom de groupe inscrit utilisé pour identifier un groupe administratif de serveurs d'impression.
-- __MSBROWSE__ [01h]	Inscrit par l'explorateur principal pour chaque sous-réseau. Lorsqu'un serveur WINS reçoit une demande concernant ce nom, il renvoie toujours l'adresse de diffusion du réseau local du client qui a émis la demande.

enfin, moins important

Multihomed (M): Utilisé pour inscrire un nom unique pour un ordinateur ayant plusieurs adresses IP (plusieurs cartes utilisant chacune une adresse unique ou une seule carte réseau configurée avec plusieurs adresses IP).

Domain Name (D): Indique une entrée mappée de *nom de domaine* [1C] pour la localisation des contrôleurs de domaine Windows NT

HOSTS - LMHOSTS

Fichier Hosts et LMHosts:

Un fichier **HOSTS** permet d'établir un mappage entre une adresse IP et un nom de machine (nom d'hôte), c'est un fichier issu du monde unix. L'alternative au fichier hosts est un serveur DNS.

A utiliser lorsque : on souhaite effectuer des transactions IP (ping, ftp...) lorsque la machine à atteindre n'a pas eut son nom résolu par DNS. Permet donc d'être sûr de trouver un poste, indépendamment du fonctionnel d'un serveur DNS.

Un fichier **LMHOSTS** permet également d'établir un mappage entre une adresse IP et un nom de machine (nom d'ordinateur ou nom netbios). L'alternative au fichier LMHOSTS est le service WINS. Le fichier LMHOSTS (Lan Manager HOSTS) concerne essentiellement les réseaux Microsoft.

A utiliser lorsque : on souhaite effectuer des transactions réseau microsoft, (Lan Manager commande net..., mécanisme de voisinage réseau...) lorsque la machine à atteindre ne fait pas partie du même sous-réseau, et qu'il n'y a pas de serveurs WINS opérationnel. Permet donc d'être sûr de trouver un poste, indépendamment du fonctionnel d'un serveur WINS.

Fichier lmHosts (nom netbios):

Situé pour les postes NT – 2000 en **WINNT\SYSTEM32\DRIVERS\ETC**

Un exemple est fournit avec le fichier **lmhosts.sam** avec une extension .sam pour sample qu'il faut évidemment enlever pour rendre actif le fichier **lmhosts**. Il permet de solutionner un nom netbios sur un autre sous-réseau.

```
# Ce fichier est compatible avec les fichiers lmhosts de
Microsoft LAN
# Manager 2.x TCP/IP et les extensions offertes sont les
suivantes:
#      #PRE
#      #DOM:<domaine>
#      #INCLUDE <nom_de_fichier>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (caractère non imprimable)
```

Donc un fichier lmhost peut contenir une ligne du genre

192.168.1.1 NOMPOSTE #PRE

avec 192.168.1.1 l'adresse ip du POSTE

avec NOMPOSTE le nom NETBIOS du POSTE

Après modification du fichier **lmhosts** il faut impérativement redémarrer le poste, ou faire une commande en ligne

Nbtstat -R (avec le R majuscule...)

Pui vérifier la prise ne compte avec un

Nbtstat -c (avec le c minuscule...)

Détails écriture lmhosts

1. 10.0.0.1 PDCName #PRE #DOM:Domain-name

2. 10.0.0.1 "Domain-name \0x1b" #PRE

N.B.: L'espacement de ces entrées est obligatoire. Remplacez 10.0.0.1 par l'adresse IP de votre contrôleur principal de domaine, PDCName par le nom NetBIOS de votre contrôleur principal de domaine, et Domaine par le nom de domaine de Windows. Au total il doit y avoir 20 caractères à l'intérieur des guillemets (le nom de domaine, + le nombre d'espaces appropriés pour obtenir 15 caractères, + la barre oblique inverse, + la représentation hexadécimale NetBIOS du type de service).

N.B.: Pour déterminer l'emplacement du 16e caractère, copiez la ligne suivante dans votre fichier LMHOSTS :

Adresse IP "123456789012345*7890"

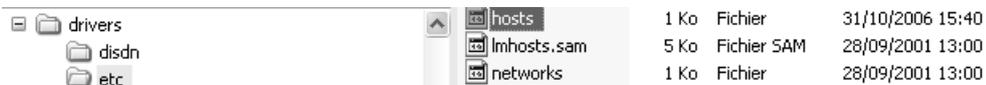
Alignez les guillemets doubles (") en ajoutant ou supprimant des espaces dans la ligne de commentaire, et placez la barre oblique inverse sur la 16e colonne (marquée d'une astérisque). N'utilisez de tabulation mais des ESPACES après le nom et avant la barre oblique inverse (\).

NB: Attention, le fichier contient toujours une ligne blanche vide à la fin !

Fichier hosts (nom d'hôte):

Un exemple est fourni sur les machines avec le fichier **hosts**

Il permet de solutionner un nom d'hôte.



drivers	hosts	1 Ko	Fichier	31/10/2006 15:40
disdn	lmhosts.sam	5 Ko	Fichier SAM	28/09/2001 13:00
etc	networks	1 Ko	Fichier	28/09/2001 13:00

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

NB: Attention, le fichier contient toujours une ligne blanche vide à la fin !

ANNEXE : TRAMES TCP/IP

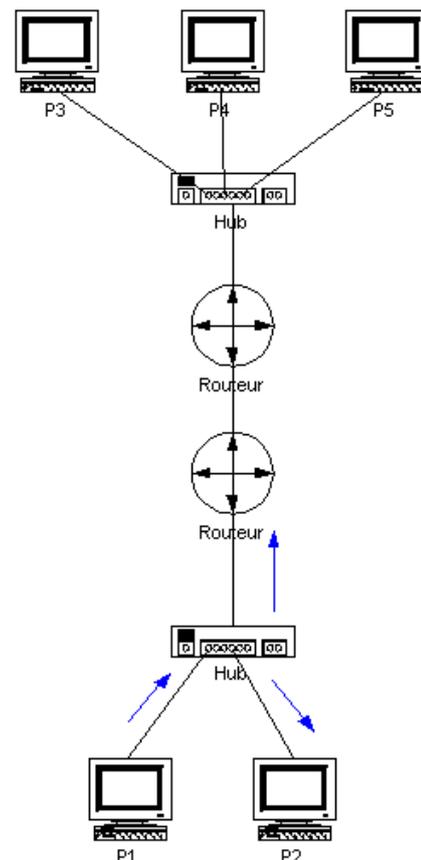
Broadcast :

Le principe du **broadcast** est d'envoyer une information à tous les ordinateurs du réseau où l'on est. Au lieu d'envoyer en unicast vers l'adresse IP de la chaque machine (ex. 193.169.1.37 avec un masque 255.255.255.0),

L'adresse de **broadcast** est une adresse IP qui termine en .255 dans des réseaux de classe A, B ou C, cette adresse est celle qui permet de faire de la diffusion à toutes les machines du réseau

On envoie la trame à tous les ordinateurs du sous-réseau en utilisant l'adresse de **broadcast** (ici, 193.169.1.255). Cette adresse est réservée à cet usage. Chacun des ordinateurs du sous-réseau regarde et traite la trame comme si elle leur était personnellement adressée.

Les trames de **broadcast** ont une caractéristique particulière : c'est de ne pas pouvoir passer les routeurs puisqu'il s'adresse uniquement à tous les ordinateurs d'un même sous-réseau.



Broadcast

P1 envoie des informations à tous les éléments de son sous-réseau

Unicast :

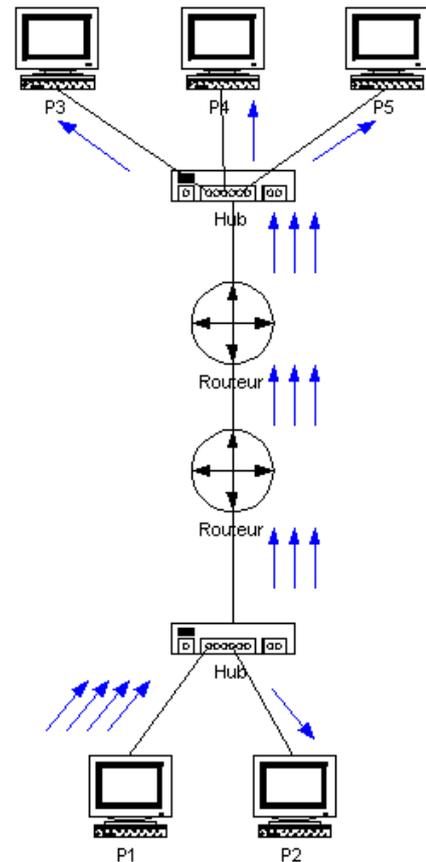
C'est le principe le plus utilisé et le plus simple. Les ordinateurs possédant chacun une adresse IP, on peut envoyer les trames en spécifiant l'adresse IP de l'ordinateur à qui on veut envoyer les informations. Les éléments actifs et passifs du réseau (commutateurs, répéteurs, routeurs, ...) dirigent l'information dans la bonne direction pour que les trames arrivent au bon endroit. Seule la machine ayant l'adresse contenue dans la trame regarde et traite l'information.

Il existe 3 classes d'adresses unicast :

La classe A : Adresses comprises entre 1.0.0.x et 127.255.255.x

La classe B : Adresses comprises entre 128.0.0.x et 191.255.255.x

La classe C : Adresses comprises entre 192.0.0.x et 223.255.255.x



Unicast

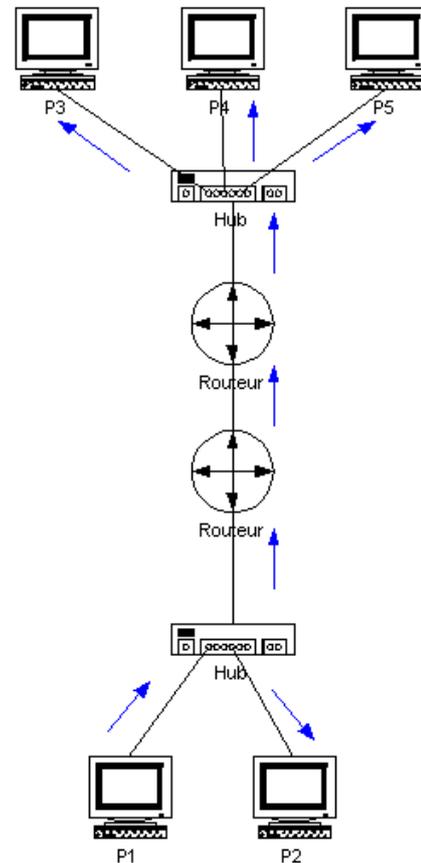
P1 envoie des informations à P2, P3, P4 et P5

Multicast :

Plutôt que d'envoyer les fichiers du serveur vers chacune des machines clientes (unicast) on peut n'envoyer l'information qu'une seule fois et chaque ordinateur client la récupère. En effet, dans un réseau Ethernet par exemple, toutes les trames qui circulent passent par tous les ordinateurs. C'est le principe du multicast : on envoie l'information à une adresse et tous les clients écoutent cette adresse.

Chaque client multicast s'enregistre avec une adresse IP multicast de classe D (entre 224.0.0.0 et 239.255.255.255 sauf 224.0.0.0 non utilisée et 224.0.0.1 qui correspond au "broadcast du multicast"). C'est sur cette adresse que les informations vont être envoyées.

Les clients écoutent ce qui arrive sur cette adresse et suivent la procédure décrite par le protocole multicast implémenté.



Multicast

P1 envoie des informations à P2, P3, P4 et P5

DOSSIER ..\SYSTEM32\DRIVER\ETC

Fichiers exemples Windows :

Depuis Windows Seven, on peut trouver dans les machines Windows un "mémo" stocké dans le dossier d'installation de l'OS
%system%\system32\driver\etc

Sur les N° de port : fichier **service**

```
services - Bloc-notes
Fichier Edition Format Affichage ?
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
echo                7/tcp
echo                7/udp
discard            9/tcp    sink null
discard            9/udp    sink null
systat             11/tcp    users          #Active users
systat             11/udp    users          #Active users
daytime            13/tcp
daytime            13/udp
qotd               17/tcp    quote         #Quote of the day
qotd               17/udp    quote         #Quote of the day
chargen            19/tcp    ttytst source #Character generator
chargen            19/udp    ttytst source #Character generator
ftp-data           20/tcp
ftp                21/tcp
ssh                22/tcp
telnet             23/tcp
smtp              25/tcp    mail          #Simple Mail Transfer Protocol
time              37/tcp    timserver
time              37/udp    timserver
rpl               39/udp    resource
nameserver        42/tcp    name          #Host Name Server
nameserver        42/udp    name          #Host Name Server
nicname           43/tcp    whois
domain            53/tcp
domain            53/udp
bootps            67/udp    dhcps        #Bootstrap Protocol Server
bootpc            68/udp    dhcps        #Bootstrap Protocol Client
```

sur les N° de protocole fichier **protocol**

```
protocol - Bloc-notes
Fichier Edition Format Affichage ?
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This file contains the Internet protocols as defined by various
# RFCs. See http://www.iana.org/assignments/protocol-numbers
#
# Format:
# <protocol name> <assigned number> [aliases...] [#<comment>]
#
ip                 0        IP           # Internet protocol
icmp              1        ICMP        # Internet control message protocol
ggp               3        GGP         # Gateway-gateway protocol
tcp               6        TCP         # Transmission control protocol
ead               8        EGP         # Exterior gateway protocol
```

Ainsi que des exemples de fichier host et lmhost...

TP - WORKGROUP ENTRE RESEAUX

1 réseau IP et x Workgroups différents:

on donne à des machines faisant partie de différents réseaux des adresses en classe C privée dans un seul réseau :

id réseau **192.168.1** donc

adresse **192.168.1.1** pour la 1^o,

adresse **192.168.1.2** pour la 2^o,

adresse **192.168.1.X** pour la X^o,

masque 255.255.255.0

Pour certaines machines, on donne un workgroup d'appartenance « grpdroit »,

à d'autres on donne un workgroup d'appartenance « grpgauche »,

test et vérification :

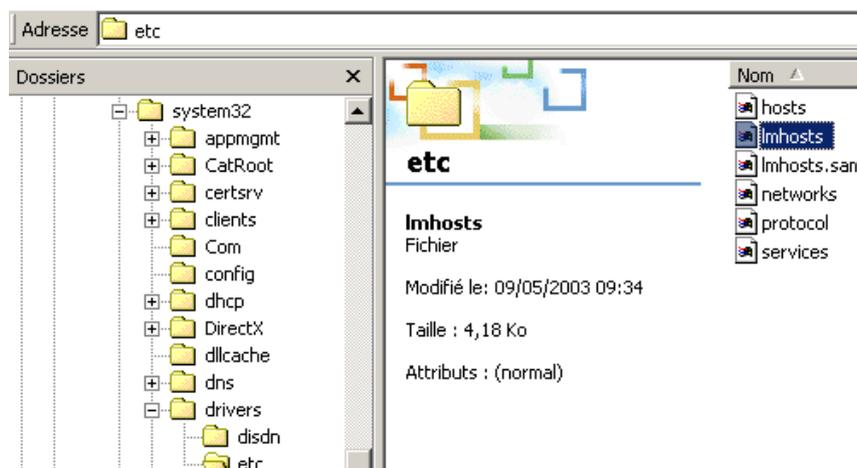
Vérifier la communication entre les machines ?, les workgroups ?

Que se passe-t-il et pourquoi ?

TP - MODIFIER LMHOSTS

Inscrire une machine simple dans lmhosts :

Inscrivons le poste nommé **pdistant** d'adresse **192.168.2.2** dans la table préchargée de résolution de nom netbios d'une machine:



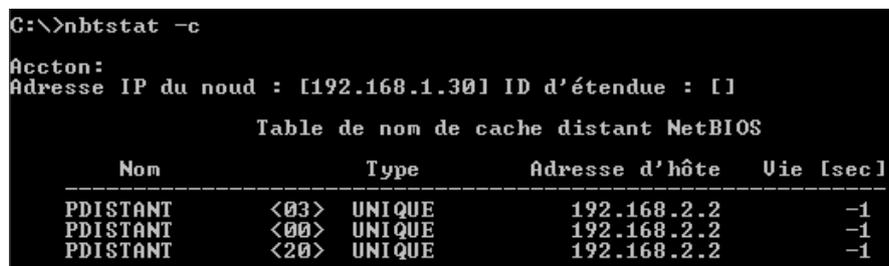
Il suffit d'éditer le fichier texte et d'y inscrire la ligne suivante



On recharge par la commande **nbtstat -R**



et on visualise par la commande **nbtstat -c**:



Inscrire un Contrôleur de Domaine dans lmhosts :

En général, on n'a pas besoin d'inscrire des postes génériques, mais plutôt un contrôleur de domaine... Dans ce cas la ligne se complique un petit peu puisqu'il est nécessaire d'indiquer le nom de domaine en plus.... Il faut effectuer donc 2 entrées, une pour le PDC et l'autre pour le nom de domaine.

10.0.0.1 PDCName #PRE #DOM:Domain-name
10.0.0.1 "Domain-name \0x1b" #PRE

N.B : Le nom de domaine dans cette entrée respecte la casse.

N.B: L'espacement de ces entrées est obligatoire. Remplacez **10.0.0.1** par l'adresse IP de votre contrôleur principal de domaine, **PDCName** par le nom NetBIOS de votre contrôleur principal de domaine, **Domain** par le nom de domaine de Windows

Inscrivons le contrôleur de domaine **TEST** nommé **S1** d'adresse **192.168.1.1** dans la table préchargée de résolution de nom netbios d'une machine:

```

Imhosts - WordPad
Fichier Edition Affichage Insertion Format ?
192.168.1.1 S1 #PRE #DOM:TEST
192.168.1.1 "TEST \0x1b" #PRE
    
```

avec pour vérification

```

C:\>nbtstat -R
Purge et préchargement de la table nom de cache distant NBT terminés.
C:\>nbtstat -c
Accton:
Adresse IP du noud : [192.168.1.2] ID d'étendue : []

Table de nom de cache distant NetBIOS
-----
Nom                Type                Adresse d'hôte      Vie [sec]
-----
S1                  <03> UNIQUE            192.168.1.1        -1
S1                  <00> UNIQUE            192.168.1.1        -1
S1                  <20> UNIQUE            192.168.1.1        -1
TEST                <1C> GROUP           192.168.1.1        -1
TEST                <1B> UNIQUE            192.168.1.1        -1
    
```

NB: Au total il doit y avoir 20 caractères à l'intérieur des guillemets (le nom de domaine, + le nombre d'espaces appropriés pour obtenir 15 caractères, + la barre oblique inverse, + la représentation hexadécimale NetBIOS du type de service).

NB: Attention, le fichier contient toujours une ligne blanche vide à la fin !

Ainsi une simple erreur de nombre de caractère (différent de 20 ici)

```

192.168.1.1 S1 #PRE #DOM:TEST
192.168.1.1 "TEST \0x1b" #PRE
    
```

ne génère aucun message d'erreur, mais simplement une mauvaise inscription :

```

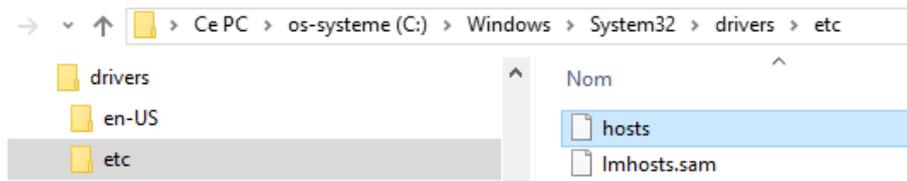
C:\>nbtstat -c
Accton:
Adresse IP du noud : [192.168.1.2] ID d'étendue : []

Table de nom de cache distant NetBIOS
-----
Nom                Type                Adresse d'hôte      Vie [sec]
-----
S1                  <03> UNIQUE            192.168.1.1        -1
S1                  <00> UNIQUE            192.168.1.1        -1
S1                  <20> UNIQUE            192.168.1.1        -1
TEST                <1C> GROUP           192.168.1.1        -1
TEST                <03> UNIQUE            192.168.1.1        -1
TEST                <00> UNIQUE            192.168.1.1        -1
TEST                <20> UNIQUE            192.168.1.1        -1
    
```

TP - MODIFIER HOSTS

Inscrire une machine dans hosts :

Le fichier est fourni directement dans les postes Windows, en `%system%\system32\driver\etc`



On peut noter que les boucles locales IPV4 et IPV6 ne sont plus gérées dans le Hosts

```
hosts - Bloc-notes
Fichier Edition Format Affichage ?
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

N.B : pour éditer le fichier **host**, il faut penser à plusieurs choses

- Vérifier s'il est noté avec l'attribut lecture seule
- Il faut vérifier que l'on a bien les droits en accès
- Il faut d'abords lancer le bloc note en tant qu'administrateur et ouvrir le fichier. (si on demande depuis le fichier de l'ouvrir avec le bloc note, si l'UAC est configuré, on ne pourra pas l'enregistrer..)
- Redémarrer le poste

Faisons un **ping** sur une machine inexistante **test**, on obtient

```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.19042.685]
(c) 2020 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping test
La requête Ping n'a pas pu trouver l'hôte test. Vérifiez le nom et essayez à nouveau.
```

Inscrivons le poste nommé **test** d'adresse **192.168.1.175** (une adresse fictive) dans la table de résolution locale, puis reboot du poste

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
|       192.168.1.175 test
```

Du coup si avant on n'avait aucune possibilité de faire un **ping test** désormais, on peut désormais au moins envoyer la trame... (Évidemment le retour est plus... délicat !)

```
C:\Users\Administrateur>ping test

Envoi d'une requête 'ping' sur test [192.168.1.175] avec 32 octets de données :
Réponse de 192.168.1.171 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.171 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.171 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.171 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.1.175:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

N.B: Si une réponse est émise, cela ne veut pas dire que cette machine **test** existe, cela veut dire qu'une machine 192.168.1.175 a répondu !

Interdire une machine un site dans hosts :

N.B: Un moyen simple d'invalider un nom consiste à le renvoyer sur l'adresse de bouclage **127.0.0.1**, **idem pour une URL d'un site à proscrire**

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
|       127.0.0.1 test
|       127.0.0.1 fnac.com
```

donnera

```
C:\Users\Administrateur>ping test

Envoi d'une requête 'ping' sur test [127.0.0.1] avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
```

Et une tentative d'accès sur le site de la **Fnac** donnera



TESTER TCP/IP

ICMP et l'Utilitaire PING :

Permet d'envoyer une trame IP de test vers une machine,

Types de réponses à un ping

```
C:\Users\Administrateur>ping 192.168.0.1
Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=63
```

"**Réponse de ... octets=32 temps= TTL**" indique que 4 trames de 32 octets ont été acquittées par l'adresse IP de destination, avec un temps et le TTL:

```
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

"**Délai d'attente de la demande dépassé**" signifie généralement qu'aucune réponse ICMP n'a été reçue par la machine qui lance le ping. Plusieurs causes possibles :

- la cible est configurée pour ne pas envoyer d'ICMP Reply,
- il y a au moins un firewall qui bloque ces ICMP entre la cible et la station qui lance le ping,
- effectivement la cible répond avec un ICMP qui possède un TTL trop petit et donc le paquet est droppé quelque part.

```
C:\Users\Administrateur>ping 192.168.1.101
Envoi d'une requête 'Ping' 192.168.1.101 avec 32 octets de données :
Réponse de 192.168.1.170 : Impossible de joindre l'hôte de destination
Réponse de 192.168.1.170 : Impossible de joindre l'hôte de destination
```

"**Impossible de joindre l'hôte de destination**" devrait normalement être le cas où le réseau IP destination existe mais l'adresse IP cible ne répond pas. Plusieurs causes possibles:

- La pile IP de la cible n'est pas active
- la cible est configurée pour ne pas envoyer d'ICMP, etc.

La différence entre "délai d'attente dépassé" et "impossible de joindre l'hôte", c'est que dans le 1er cas, la station qui lance le ping ne reçoit rien, tandis que dans le 2ème cas de figure, il reçoit quelque chose...

```
C:\Users\Administrateur>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
```

"**échec de la transmission. Défaillance générale**" devrait normalement être le cas où la trame IP ne peut partir. Plusieurs causes possibles:

- Paramétrage IP erroné
- Filtrage IP par un élément externe sur le réseau

Méthodologie de test

En tapant **Ping 127.0.0.1** si on ne reçoit pas les 4 lignes suivantes, cela veut dire que la pile TCP/IP n'est pas installée correctement

```
Invite de commandes
E:\>ping 127.0.0.1
Pinging 127.0.0.1 avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<10ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<10ms TTL=128
```

En tapant **Ping XX.XX.XX.XX** avec l'adresse de notre propre station depuis laquelle on « pingue », si on ne reçoit pas les 4 lignes suivantes, cela veut dire que l'adresse de la station est erronée

```
Invite de commandes
E:\>ping 200.200.200.200
Pinging 200.200.200.200 avec 32 octets de données :
Réponse de 200.200.200.200 : octets=32 temps<10ms TTL=128
```

Jusqu'à présent on n'a rien envoyé sur le réseau, maintenant considérer que notre poste est correctement configuré sous TCP/IP, on va utiliser le réseau

En tapant **Ping XX.XX.XX.XX** avec l'adresse de la station que l'on souhaite atteindre, si on ne reçoit pas les 4 lignes suivantes, cela veut dire soit que l'adresse de la station est erronée soit que la connectique est mauvaise

```
Invite de commandes
E:\>ping 200.200.200.202
Pinging 200.200.200.202 avec 32 octets de données :
Réponse de 200.200.200.202 : octets=32 temps<10ms TTL=128
```

En tapant **Ping NOMSTATION (peu conseillé)** avec le nom d'hôte à atteindre, si on ne reçoit pas les 4 lignes suivantes, cela veut dire que le nom est erroné, ou qu'il n'est pas dans le même réseau IP s'il n'y a pas de **DNS**. (Les **broadcasts** ne sont pas routable)

S'il n'y a pas de **DNS**, la résolution de nom se fera par des mécanismes de **broadcass netbios**

```
Invite de commandes
E:\>ping station_nt_p2
Pinging station_nt_p2 [200.200.200.202] avec 32 octets de données :
Réponse de 200.200.200.202 : octets=32 temps<10ms TTL=128
```

Ping -a

On peut aussi taper **Ping -a XX.XX.XX.XX**.

Le nom de la station que l'on souhaite atteindre sera résolu en même temps que le retour de frame, ce qui permet de connaître en cas de problème le nom renvoyé par la machine...

```
C:\Windows\system32>ping 192.168.1.171

Envoi d'une requête 'Ping' 192.168.1.171 avec 32 octets de données :
Réponse de 192.168.1.171 : octets=32 temps<1ms TTL=128
```

L'option **-a** force la résolution de nom ici **WIN10-1703**

```
C:\Windows\system32>ping -a 192.168.1.171

Envoi d'une requête 'ping' sur WIN10-1703 [192.168.1.171] avec 32 octets de données :
Réponse de 192.168.1.171 : octets=32 temps<1ms TTL=128
```

Ping -t

Une option intéressante est présente est **-t** dans **Ping XX.XX.XX.XX -t**

```
C:\Documents and Settings\Administrateur>ping 192.168.1.1 -t

Envoi d'une requête 'ping' sur 192.168.1.1 avec 32 octets de données :

Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=254
Réponse de 192.168.1.1 : octets=32 temps=2 ms TTL=254
```

avec la combinaison de touche **CTRL + Attn** pour afficher les statistiques

```
Statistiques Ping pour 192.168.1.1:
  Paquets : envoyés = 34, reçus = 34, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

avec la combinaison de touche **CTRL + C** pour arrêter la commande

Test TTL ping -i:

L'option **-i x** permet de spécifier la valeur **Time to Live**

Si un TTL très court à 3 permet d'atteindre la machine d'a coté

```
C:\Users\Administrateur>ping -i 3 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=64
```

```
C:\Users\Administrateur>ping -i 3 192.168.1.116

Envoi d'une requête 'Ping' 192.168.1.116 avec 32 octets de données :
Réponse de 192.168.1.116 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.116:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Le même TTL à 3 ne permet pas d'atteindre une machine distante, telle que un serveur DNS de Google en 8.8.8.8

```
C:\Users\Administrateur>ping -i 3 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 80.10.232.237 : Durée de vie TTL expirée lors du transit.
Réponse de 80.10.232.237 : Durée de vie TTL expirée lors du transit.
Réponse de 80.10.232.237 : Durée de vie TTL expirée lors du transit.
Réponse de 80.10.232.237 : Durée de vie TTL expirée lors du transit.
```

Ce message en provenance du 3^e routeur indique la mise à mort de la requête ! Car en effet ici il lui faudrait 11 sauts...

```
C:\Users\Administrateur>tracert 8.8.8.8

Détermination de l'itinéraire vers dns.google [8.8.8.8]
avec un maximum de 30 sauts :

 1  <1 ms  <1 ms  <1 ms  192.168.1.1
 2   1 ms   1 ms   <1 ms  192.168.0.1
 3   5 ms   3 ms   3 ms   80.10.232.237
 4  10 ms  10 ms  10 ms  ae115-0.ncgre102.rbc1.orange.net [193.253.85.110]
 5  12 ms  11 ms  11 ms  ae43-0.nilyo202.rbc1.orange.net [193.252.101.134]
 6  14 ms  14 ms  17 ms  ae40-0.nilyo201.rbc1.orange.net [193.252.101.65]
 7  14 ms  14 ms  13 ms  81.253.184.86
 8  14 ms  13 ms  13 ms  72.14.222.118
 9  15 ms  15 ms  15 ms  108.170.227.165
10  13 ms  13 ms  13 ms  142.251.78.91
11  13 ms  13 ms  13 ms  dns.google [8.8.8.8]

Itinéraire déterminé.
```

Le TTL d'une machine Windows est par défaut à 128

Le TTL d'une machine Linux est par défaut à 64

D'autres OS ont d'autres valeurs par défaut

Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
MacOS/MacTCP	2.0.x	TCP and UDP	60
MacOS/MacTCP	X (10.5.6)	ICMP/TCP/UDP	64
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255

Tracert :

En tapant **tracert xx.xx.xx.xx** on demande de tracer la route pour atteindre une adresse ip

```
C:\Windows\system32>tracert 216.58.204.131

Détermination de l'itinéraire vers 216.58.204.131 avec un maximum de 30 sauts.

  1    1 ms    1 ms    <1 ms  192.168.1.1
  2    2 ms    1 ms    1 ms   SAGEMCOM [192.168.0.1]
  3   11 ms   10 ms   10 ms   80.10.115.230
  4   11 ms   12 ms   11 ms   10.123.204.86
  5   12 ms   11 ms   12 ms   193.252.159.153
  6   17 ms   16 ms   12 ms   193.252.137.78
  7   12 ms   11 ms   11 ms   209.85.148.16
```

On peut aussi si une résolution DNS est présente, (possible) utiliser un nom

```
C:\Windows\system32>tracert www.google.fr

Détermination de l'itinéraire vers www.google.fr [216.58.206.227]
avec un maximum de 30 sauts :

  1    1 ms    <1 ms    <1 ms  192.168.1.1
  2    2 ms    1 ms    1 ms   SAGEMCOM [192.168.0.1]
  3   11 ms   10 ms   12 ms   80.10.115.230
  4   11 ms   12 ms   10 ms   10.123.204.82
  5   11 ms   11 ms   11 ms   ae42-0.niidf301.Paris15eArrondissement.francetelecom.net [193.252.159.149]
  6   11 ms   19 ms   11 ms   ae40-0.niidf302.Paris13eArrondissement.francetelecom.net [193.252.103.38]
  7   14 ms   14 ms   14 ms   193.252.137.78
```

N.B : comme de nos jours les routeurs ne donnent souvent plus leur nom, on peut accélérer le temps de réponse (ne pas attendre une résolution de nom qui, ne viendra pas dans 99% des cas), en tapant l'option **-d**

```
C:\Windows\system32>tracert -d www.google.fr

Détermination de l'itinéraire vers www.google.fr [216.58.206.227]
avec un maximum de 30 sauts :

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    2 ms    1 ms    1 ms   192.168.0.1
  3   11 ms   10 ms   10 ms   80.10.115.230
  4   11 ms   10 ms   12 ms   10.123.204.82
  5   11 ms   23 ms   33 ms   193.252.159.149
  6   11 ms   11 ms   13 ms   193.252.103.38
  7   19 ms   14 ms   14 ms   193.252.137.78
  8   12 ms   11 ms   11 ms   72.14.219.248 *
```

Pathping :

Depuis windows 2000 une commande combinée existe **PATHPING**

Elle commence à faire le même travail qu'un **tracert**, mais ensuite elle donnera un certain nombre de statistiques (un peu comme **ping /t**)

```
C:\Windows\system32>pathping www.google.fr

Détermination de l'itinéraire vers www.google.fr [216.58.215.35]
avec un maximum de 30 sauts :
  0  win10-1511 [192.168.1.170]
  1  192.168.1.1
  2  SAGEMCOM [192.168.0.1]
  3  80.10.115.230
  4  10.123.204.86
  5  ae42-0.niidf302.Paris13eArrondissement.francetelecom.net [193.252.159.153]
  6  193.252.137.78
  7  google-11.gw.opentransit.net [193.251.255.82]
```

avec dans un 2° temps (25secondes par nœud)

```
Traitement des statistiques pendant 175 secondes...
Source vers ici Ce nœud/liens
Saut RTT Perdu/Envoyé = % Perdu/Envoyé = % Adresse
0 | win10-1511 [192.168.1.170]
1 0ms 0/ 100 = 0% 0/ 100 = 0% 192.168.1.1
2 2ms 0/ 100 = 0% 0/ 100 = 0% SAGEMCOM [192.168.0.1]
3 --- 100/ 100 =100% 100/ 100 =100% |
4 --- 100/ 100 =100% 0/ 100 = 0% 80.10.115.230
5 --- 100/ 100 =100% 0/ 100 = 0% 10.123.204.86
6 --- 100/ 100 =100% 0/ 100 = 0% ae42-0.niidf302.Paris13eArrondissement.francetelecom.net
7 --- 100/ 100 =100% 0/ 100 = 0% 193.252.137.78
8 --- 100/ 100 =100% 0/ 100 = 0% google-11.gw.opentransit.net [193.251.255.82]
```

- Le nom de la première machine de départ est donné
- Une perte de paquet régulière supérieure ou égale à 1 % sur un routeur indique un défaut

Ipconfig.exe /all:

Sous Windows **Ipconfig.exe** depuis une boîte dos ou une invite système

```
UTILISATION :
ipconfig [/allcompartments] [/? ! /all !
/renew [adapter] ! /release [adapter] !
/renew6 [adapter] ! /release6 [adapter] !
/flushdns ! /displaydns ! /registerdns !
/showclassid adapter !
/setclassid adapter [classid] !
/showclassid6 adapter !
/setclassid6 adapter [classid] !
```

L'affichage complet **ipconfig /all** donne le nom d'hôte, le type de nœud de résolution des noms netbios, et si le routage est activé sur le poste

```
C:\Windows\system32>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : win10-1511
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
```

ensuite pour chaque carte réseau, on récupère son adresse mac, si elle est en client dhcp ou en IP statique, son adressage IP complet, et si Netbios Over TCP-IP est maintenu ou non.

```
Carte Ethernet Ethernet 3 :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Realtek PCIe GBE Family Controller
Adresse physique . . . . . : 40-8D-5C-B1-91-28
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . : 192.168.1.170(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
NetBIOS sur Tcpip. . . . . : Activé
```

Il peut y a voir beaucoup de cartes réseaux....

ARP et l'Utilitaire ARP -a :

Les essais sur une configuration peuvent se faire à bas niveau

Permet de connaître l'adresse physique d'une machine

```
C:\Users\Administrateur>arp /?
Affiche et modifie les tables de traduction d'adresses IP en adresses
physiques utilisées par le protocole de résolution d'adresses ARP.
```

ARP est un protocole permettant la résolution adresse Ip => adresse physique. ARP est mis en oeuvre automatiquement lors de toute requête IP, et typiquement lors d'un ping....

Arp -a

En tapant **ARP -a** on affiche le contenu du cache actuellement présent sur notre machine. Sur une machine que l'on démarre, le cache peut être vide.

```
C:\WIN98>arp -a
Aucune entrée ARP n'a été trouvée
```

après un coup de voisinage réseau, le master browse ayant répondu, le cache contient désormais son adresse IP et son adresse physique

```
C:\WIN98>arp -a
Interface : 192.168.0.4 on Interface 0x2000003
  Adresse Internet      Adresse physique      Type
  192.168.0.1           00-50-04-52-09-14    dynamique
```

si on attend, le cache va finir par se vider et de nouveau on aura

```
C:\WIN98>arp -a
Aucune entrée ARP n'a été trouvée
```

Si on fait un **ping** sur une machine donnée, alors son "entrée" dans la table est effectuée dès que la réponse est obtenue...

```
C:\WIN98>ping 192.168.0.3
Envoi d'une requête 'ping' sur 192.168.0.3 avec 32 octets de données
Réponse de 192.168.0.3 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<10 ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<10 ms TTL=128
Réponse de 192.168.0.3 : octets=32 temps<10 ms TTL=128
```

ce qui donne ensuite

```
C:\WIN98>arp -a
Interface : 192.168.0.4 on Interface 0x2000003
  Adresse Internet      Adresse physique      Type
  192.168.0.3           00-20-af-c4-6a-98    dynamique
```

un **F5** (pour rafraîchir l'écran du voisinage réseau) provoquerait alors une autre entrée dans le cache ARP...etc, etc...

```
C:\WIN98>arp -a
Interface : 192.168.0.4 on Interface 0x2000003
  Adresse Internet      Adresse physique      Type
  192.168.0.1           00-50-04-52-09-14    dynamique
  192.168.0.3           00-20-af-c4-6a-98    dynamique
```

Ajout –suppression d'entrée Arp

On peut rentrer une adresse statique. **ARP -s**

```
C:\WIN98>arp -s 192.168.0.1 00-50-04-52-09-14
```

ce qui donnerait dans la table l'aspect suivant

```
C:\WIN98>arp -a

Interface : 192.168.0.4 on Interface 0x2000003
  Adresse Internet      Adresse physique      Type
  192.168.0.1           00-50-04-52-09-14   statique
```

Cette entrée "statique" ne sera purgée de la table que lors d'un redémarrage du poste. Si on souhaite la modifier il suffit de rentrer de nouveau une commande du type **arp -s**

Usurpation d'adresse ARP :

Soit une adresse donnée pour une carte

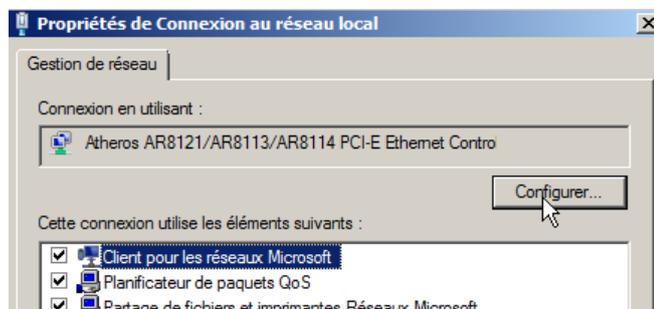
```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

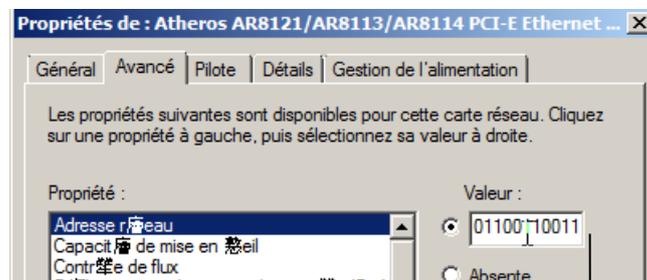
Nom de l'hôte . . . . . : POSTE13
Suffixe DNS principal . . . . . : cabare-intra.net
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: cabare-intra.net

Carte Ethernet Connexion au réseau local :
  Suffixe DNS propre à la connexion. . . : cabare-intra.net
  Description. . . . . : Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller (NDIS 6.20)
  Adresse physique . . . . . : 90-E6-B0-16-B5-2A
  DHCP activé . . . . . : Oui
  Configuration automatique activée. . . : Oui
```

Si le driver le permet, il est facile sous windows d'usurper l'adresse mac en demandant sur la carte réseau **Configurer...**



et on choisit **Adresse Réseau**

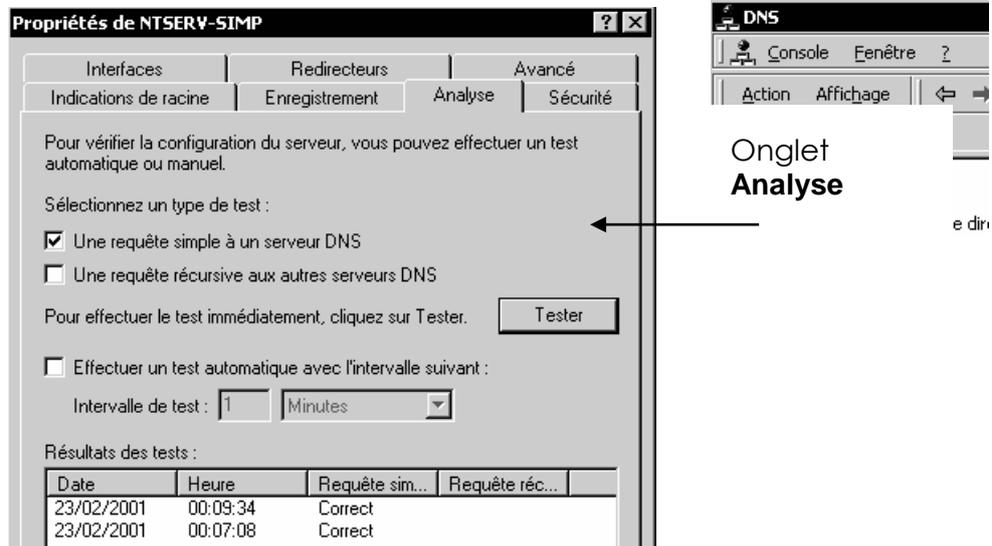


```
Carte Ethernet Connexion au réseau local :
  Suffixe DNS propre à la connexion. . . : cabare-intra.net
  Description. . . . . : Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller (NDIS 6.20)
  Adresse physique . . . . . : 00-11-00-11-00-11
  DHCP activé . . . . . : Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv4. . . . . : 192.168.1.220(préfér )
  Masque de sous-r seau. . . . . : 255.255.255.0
```

TEST DE DNS

Test DNS d'un client d'un domaine :

La bonne marche du serveur DNS peut se tester via les propriétés du Serveur DNS dans la console MMC de gestion du DNS



La bonne marche des enregistrements dans le DNS peut se tester via la commande **Nslookup**

Cet outil de diagnostic affiche des informations sur les serveurs de noms DNS (système de noms de domaine). **Nslookup** est disponible uniquement si le protocole TCP/IP est installé.

Nom d'hôte et FQDN

Soit un domaine **cabare-intra.net**, et un poste nommé **poste-10** appartenant à ce domaine. On appellera

- nom d'hôte **poste-10**
- FQDN Fully qualified Domain name **poste-10.cabare-intra.net**

De manière générale, lorsque l'on fait les tests d'un serveur DNS d'un domaine, depuis une machine du domaine, il est suffisant d'utiliser le nom d'hôte, mais si on effectue un test de DNS depuis une machine ne faisant pas partie du domaine il est alors nécessaire d'utiliser le FQDN0

Nslookup en mode interactif

Nslookup propose deux modes : interactif et non interactif.

On passe en mode inter-actif en tapant simplement **nslookup**,

On sortira du mode inter-actif en tapant **exit**.

mode interactif 1° (hors domaine – avec google – 8.8.8.8)

- En premier argument, tapez le nom ou l'adresse IP de l'ordinateur pour lequel la recherche est effectuée.
- En deuxième argument, tapez le nom ou l'adresse IP d'un serveur de noms DNS. (Si omis, le serveur de noms DNS par défaut est utilisé)

Dans les exemples ci-dessous, on est relié au **DNS** de Google : **8.8.8.8**

un **nslookup** donnera

```
C:\Users\Administrateur>nslookup
Serveur par défaut : dns.google
Address: 8.8.8.8
>
```

Au prompt de la commande **nslookup ">"**, il faut taper des résolutions à satisfaire... , jusqu'à ce que l'on en sorte, par **exit**

```
> exit
C:\Users\Administrateur>
```

Recherche d'un nom inconnu, par exemple **p1**

```
> p1
Serveur : dns.google
Address: 8.8.8.8

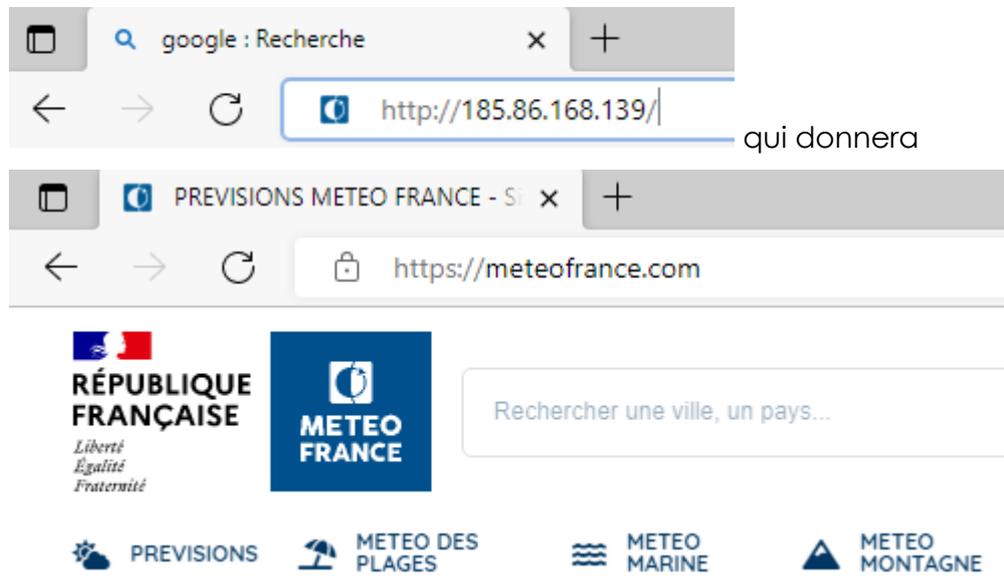
*** dns.google ne parvient pas à trouver p1 : Non-existent domain
```

Recherche d'un nom connu, par exemple **meteofrance.com**

```
> meteofrance.com
Serveur : dns.google
Address: 8.8.8.8

Réponse ne faisant pas autorité :
Nom : meteofrance.com
Addresses: 185.86.168.139
           185.86.168.140
           185.86.168.138
           185.86.168.137
```

Ce qui devrait permettre une opération du genre



mode interactif 1° (avec domaine)

- En premier argument, tapez le nom ou l'adresse IP de l'ordinateur pour lequel la recherche est effectuée.
- En deuxième argument, tapez le nom ou l'adresse IP d'un serveur de noms DNS. (Si omis, le serveur de noms DNS par défaut est utilisé)

Dans les exemples ci-dessous,

un client correct se nomme "**travail-10**",

le serveur DNS par défaut est le serveur "**srv-dc1**"

Un client incorrect se nomme "**poste-x**"

```
> travail-10 srv-dc1
*** Impossible de trouver l'adresse pour le serveur srv-dc1 : Server failed
```

Ici on ne trouve pas le serveur DNS , il faut un FQDN ?

```
> travail-10 srv-dc1.cabare-intra.net
Serveur :   srv-dc1.cabare-intra.net
Address:   192.168.1.91

*** srv-dc1.cabare-intra.net ne parvient pas à trouver travail-10 : Server failed
```

Ici on ne trouve pas de résolution pour le nom de ce client il faut un FQDN ?

```
> travail-10.cabare-intra.net srv-dc1.cabare-intra.net
Serveur :   srv-dc1.cabare-intra.net
Address:   192.168.1.91

Nom :      travail-10.cabare-intra.net
Address:   192.168.1.10
```

Ici tout est parfaitement résolu

```
> poste-x srv-dc1.cabare-intra.net
Serveur :   srv-dc1.cabare-intra.net
Address:   192.168.1.91

*** srv-dc1.cabare-intra.net ne parvient pas à trouver poste-x : Server failed
```

Ici on ne trouve pas de résolution pour le nom de ce client il faut un FQDN ?

```
> poste-x.cabare-intra.net srv-dc1.cabare-intra.net
Serveur :   srv-dc1.cabare-intra.net
Address:   192.168.1.91

*** srv-dc1.cabare-intra.net ne parvient pas à trouver poste-x.cabare-intra.net : Non-existent domain
```

Ici on ne trouve pas ce client dans le domaine, il n'y a pas d'erreur !!!

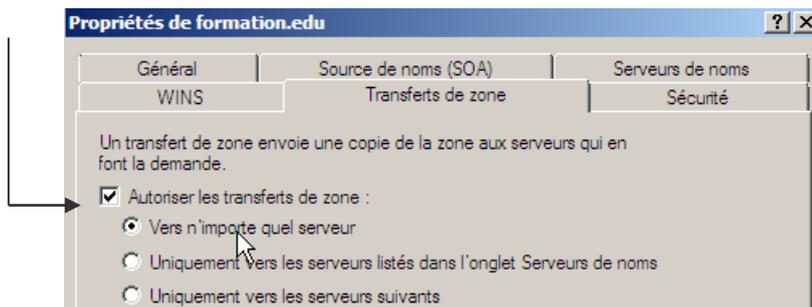
mode interactif 2°

nslookup accepte une autre commande en mode interactif, permettant de liste tous les enregistrement SRV présents dans le DNS.

N.B : un certain type de requête peut être inhibée par défaut Pour que ces commandes soient possibles, il faut en effet que le transfert de zone sur le serveur DNS soit autorisé. Par défaut depuis 2008 les transferts ne sont pas autorisés (pour des raisons de sécurité)

```
> ls -t a manuel.net
[localhost]
*** Impossible de fournir la liste du domaine manuel.net : Query refused
>
```

Pour la zone en question, on demande **propriétés**, puis **Autoriser les transferts**



avec **ls -t a** suivi de **nomdomaine** on obtient tous les enregistrement **A Hôtes du Domaine**

```
> ls -t a cabare-intra.net
[srv-dc1.cabare-intra.net]
cabare-intra.net.      A      192.168.1.91
cabare-intra.net.      A      192.168.1.90
cabare-intra.net.      NS     server = srv-dc.cabare-intra.net
cabare-intra.net.      NS     server = srv-dc1.cabare-intra.net
DESKTOP-FOAE4TI        A      192.168.1.210
DESKTOP-L214RG8        A      192.168.1.211
```

avec **set type=NS** suivit de **nomdomaine** on obtient tous les SRV correspondant a des **NS name server**

```
> set type=ns
> cabare-intra.net
Serveur :  srv-dc1.cabare-intra.net
Address:  192.168.1.91

cabare-intra.net      nameserver = srv-dc1.cabare-intra.net
cabare-intra.net      nameserver = srv-dc.cabare-intra.net
srv-dc1.cabare-intra.net  internet address = 192.168.1.91
srv-dc.cabare-intra.net internet address = 192.168.1.90
```

avec **set type=SOA** suivit de **nomdomaine** on obtient tous les SRV correspondant a des **SOA Start of Authority**

```
> set type=SOA
> cabare-intra.net
Serveur :  srv-dc1.cabare-intra.net
Address:  192.168.1.91

cabare-intra.net
  primary name server = srv-dc1.cabare-intra.net
  responsible mail addr = hostmaster
  serial = 72730
  refresh = 900 (15 mins)
  retry = 600 (10 mins)
  expire = 86400 (1 day)
  default TTL = 3600 (1 hour)
srv-dc1.cabare-intra.net  internet address = 192.168.1.91
```

mode interactif 3°

Pour vérifier l'enregistrement DNS pour tous les contrôleurs de domaine à l'invite nslookup (">"), tapez :

set type=SRV suivi de **_ldap._tcp.dc._msdcs. nomdomaine**

où **nomdomaine** est le nom DNS configuré pour être utilisé avec votre domaine Active Directory et tout contrôleur de domaine qui lui est associé.

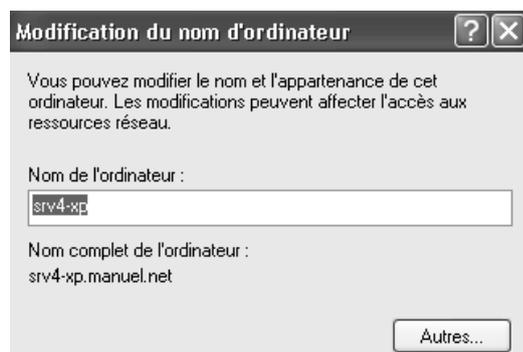
Dans l'exemple, si le nom de domaine DNS de votre domaine est **domaine1.edu**, tapez **_ldap._tcp.dc._msdcs.domaine1.edu**

```
> set type=svr
> _ldap._tcp.dc._msdcs.cabare-intra.net
Serveur :   srv-dc1.cabare-intra.net
Address:   192.168.1.91

_ldap._tcp.dc._msdcs.cabare-intra.net  SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = srv-dc.cabare-intra.net
_ldap._tcp.dc._msdcs.cabare-intra.net  SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = srv-dc1.cabare-intra.net
srv-dc.cabare-intra.net internet address = 192.168.1.90
srv-dc1.cabare-intra.net  internet address = 192.168.1.91
```

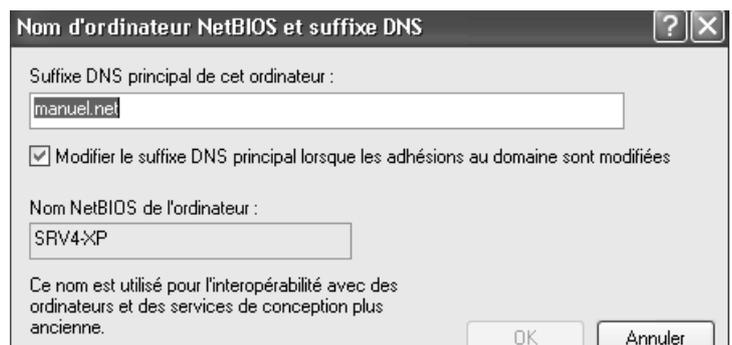
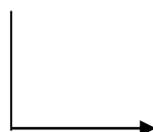
Nslookup et non-réponse de Serveur Windows :

Il peut exister un problème d'interrogation de serveur 2008 depuis un poste windows ne faisant pas partie d'un domaine. Cela arrive lorsqu'il y a des différences entre les noms netbios - nom d'hôtes des postes- ainsi que le nom DNS du domaine dont on interroge le serveur. Pour solutionner cela on peut vérifier que notre machine, dans l'onglet identification du poste de travail



Autres...

Indique bien que le DNS de rattachement est celui que l'on souhaite interroger...



Nslookup et Ping :

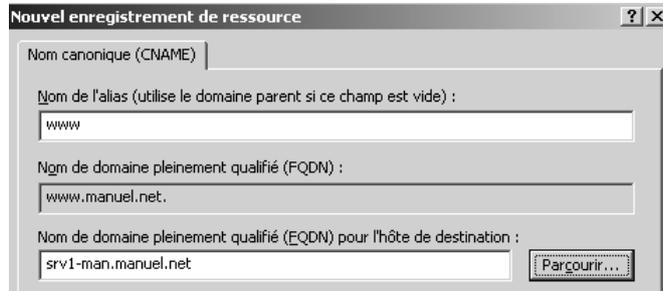
Il ne faut pas confondre les deux outils. Créons un hôte **bidon** dans le DNS

 srv1-man	Hôte (A)	192.168.1.1
 bidon	Hôte (A)	192.168.1.99

On pourra le tester avec **nslookup**,

Mais pas avec **ping**....

Créons un **Alias** « www » sur une machine existante (notre serveur)



On pourra le tester avec **nslookup**, et ici aussi utiliser **ping** !

Serveur DNS public – connus :

Si un certain nombre de Serveurs DNS public existent

✓ 8.8.8.8	google-public-dns-a.google.com
✓ 8.8.4.4	google-public-dns-b.google.com
✓ 208.67.222.222	resolver1.opendns.com
✓ 208.67.220.220	resolver2.opendns.com
✓ 1.1.1.1	1dot1dot1dot1.cloudflare-dns.com
✓ 1.0.0.1	1dot1dot1dot1.cloudflare-dns.com

On pourrait rajouter DNS Watch 84.200.69.80 et 84.200.70.40 ...

La liste des DNS des FAI est évidemment... abondante, quelques exemples

DNS de SFR  109.0.66.10 109.0.66.20	DNS Numericable  195.132.0.132 ou 89.2.0.1 ou 81.220.255.4 195.132.0.193 ou 89.2.0.2 ou 80.236.0.68	DNS Alice  212.216.212.112 212.216.172.62	DNS Bouygues Telecom  194.158.122.10 194.158.122.15
DNS Orange  80.10.246.2 80.10.246.129	DNS OVH  91.121.161.184 ou 91.121.164.227	DNS Dartybox  212.99.2.8 195.167.224.150	DNS Free  212.27.40.240 212.27.40.241

TESTER TCP-IP - NETSTAT

Netstat:

Donc **netstat** en commande de base, permet de connaître des statistiques sur les protocoles TCP-IP- UDP...

```
C:\Windows\system32>netstat

Connexions actives

Proto  Adresse locale          Adresse distante        État
TCP    127.0.0.1:50621         win10-1511:50622       ESTABLISHED
TCP    127.0.0.1:50622         win10-1511:50621       ESTABLISHED
TCP    192.168.1.170:49831    NAS-1:microsoft-ds     CLOSE_WAIT
TCP    192.168.1.170:50557    WIN10-1709:ms-wbt-server ESTABLISHED
TCP    192.168.1.170:50599    52.138.216.83:https     TIME_WAIT
TCP    192.168.1.170:50618    40.77.226.250:https     TIME_WAIT
TCP    192.168.1.170:50620    93.184.221.240:http     TIME_WAIT
TCP    192.168.1.170:50631    a23-57-82-232:http     ESTABLISHED
```

Les valeurs possibles fréquentes sont

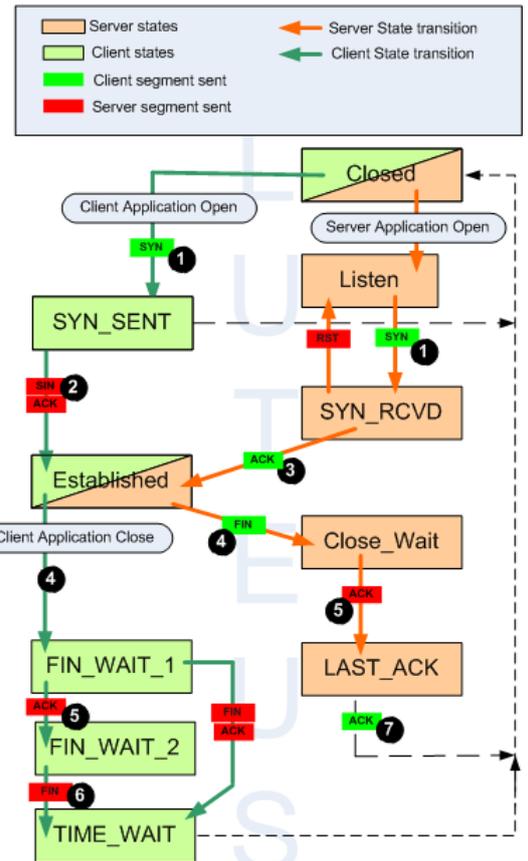
ESTABLISHED un socket de connexion est établi

TIME_WAIT la connexion est en attente après fermeture pour repasser en statut CLOSE (fermé)

CLOSE_WAIT la connexion distante est tombée, on attend les paquet de fermeture « propre »

LISTEN un socket est établi, et on attends de recevoir des paquets (il faut demander une option -l ou -a pour voir ces ports en écoute

TCP STATE TRANSITION DIAGRAM



N.B : Du coup on peut filtrer les sorties avec un `|find "mot clé"` comme dans `netstat |find « ESTABLISHED »`

```
C:\Windows\system32>netstat |find "ESTABLISHED"
TCP    127.0.0.1:50621         win10-1511:50622       ESTABLISHED
TCP    127.0.0.1:50622         win10-1511:50621       ESTABLISHED
TCP    192.168.1.170:50557    WIN10-1709:ms-wbt-server ESTABLISHED
TCP    192.168.1.170:50631    a23-57-82-232:http     ESTABLISHED
TCP    192.168.1.170:50698    par10s27-in-f3:https   ESTABLISHED
```

Netstat -a n port en écoute:

L'option **netstat -a** permet d'ajouter les ports en "ecoute" LISTENING

```
C:\Windows\System32>netstat -a

Connexions actives

Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 win10-1511:0 LISTENING
TCP 0.0.0.0:445 win10-1511:0 LISTENING
TCP 0.0.0.0:3389 win10-1511:0 LISTENING
TCP 0.0.0.0:5357 win10-1511:0 LISTENING
TCP 0.0.0.0:49664 win10-1511:0 LISTENING
TCP 0.0.0.0:49665 win10-1511:0 LISTENING
TCP 0.0.0.0:49666 win10-1511:0 LISTENING
TCP 0.0.0.0:49667 win10-1511:0 LISTENING
TCP 0.0.0.0:49668 win10-1511:0 LISTENING
TCP 0.0.0.0:49671 win10-1511:0 LISTENING
TCP 127.0.0.1:50951 win10-1511:50952 ESTABLISHED
TCP 127.0.0.1:50952 win10-1511:50951 ESTABLISHED
TCP 192.168.1.170:139 win10-1511:0 LISTENING
TCP 192.168.1.170:50222 NAS-1:microsoft-ds CLOSE_WAIT
TCP 192.168.1.170:50229 SRV-DC1:ms-wbt-server ESTABLISHED
TCP 192.168.1.170:50967 server-13-32-213-71:http ESTABLISHED
TCP [::]:135 win10-1511:0 LISTENING
TCP [::]:445 win10-1511:0 LISTENING
```

L'option **-n** affiche les n° de port IP au lieu de tenter une résolution de nom.

```
C:\Windows\System32>netstat -an

Connexions actives

Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49671 0.0.0.0:0 LISTENING
TCP 127.0.0.1:50951 127.0.0.1:50952 ESTABLISHED
TCP 127.0.0.1:50952 127.0.0.1:50951 ESTABLISHED
TCP 192.168.1.170:139 0.0.0.0:0 LISTENING
TCP 192.168.1.170:50222 192.168.1.61:445 CLOSE_WAIT
TCP 192.168.1.170:50229 192.168.1.91:3389 ESTABLISHED
TCP 192.168.1.170:50967 13.32.213.71:80 ESTABLISHED
TCP 192.168.1.170:51156 216.58.213.162:443 TIME_WAIT
TCP 192.168.1.170:51169 40.77.226.250:443 TIME_WAIT
TCP [::]:135 [::]:0 LISTENING
```

Netstat -a -p TCP port en écoute par protocole:

L'option **-p** permet de filtrer un protocole (TCP ou UDP))

```
C:\Windows\system32>netstat -n -p TCP

Connexions actives

Proto Adresse locale Adresse distante État
TCP 127.0.0.1:50621 127.0.0.1:50622 ESTABLISHED
TCP 127.0.0.1:50622 127.0.0.1:50621 ESTABLISHED
TCP 192.168.1.170:50557 192.168.1.172:3389 ESTABLISHED
TCP 192.168.1.170:50631 23.57.82.232:80 ESTABLISHED
TCP 192.168.1.170:50844 192.168.1.61:445 CLOSE_WAIT
TCP 192.168.1.170:51027 91.238.72.69:80 TIME_WAIT
TCP 192.168.1.170:51028 91.238.72.69:80 TIME_WAIT
TCP 192.168.1.170:51029 134.170.165.248:443 TIME_WAIT
TCP 192.168.1.170:51030 40.77.226.250:443 ESTABLISHED
```



Test liaison ftp – affichage dans Netstat –an :

Sur une machine ayant la possibilité de sortir, pour atteindre un poste en **62.210.16.42** (serveur **FTP** hébergeur de **ONLINE**). 1 **Tracert** permet de vérifier l'adresse **IP** du serveur **FTP**, nommé **privftp.pro.proxad.net**

```
C:\Users\Administrateur>tracert privftp.pro.proxad.net

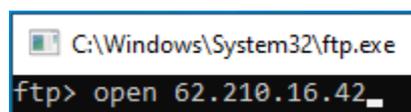
Détermination de l'itinéraire vers ftp-vit.online.net [62.210.16.42]
avec un maximum de 30 sauts :

  1  <1 ms  <1 ms  <1 ms  192.168.1.1
  2   1 ms   1 ms   1 ms  192.168.0.1
  3   3 ms   2 ms   3 ms  80.10.232.237
  4  13 ms  19 ms   9 ms  ae115-0.ncgre102.rbc1.orange.net [193.253.85.110]
  5  12 ms  12 ms  12 ms  ae43-0.nilyo202.rbc1.orange.net [193.252.101.134]
  6  11 ms  10 ms  10 ms  81.253.184.102
  7  11 ms  12 ms  10 ms  193.251.131.0
  8  11 ms  11 ms  11 ms  193.251.250.152
  9  11 ms  10 ms  10 ms  51.158.0.61
 10  11 ms  12 ms  13 ms  195.154.1.153
 11  10 ms   9 ms  10 ms  ftp.online.net [62.210.16.42]
```

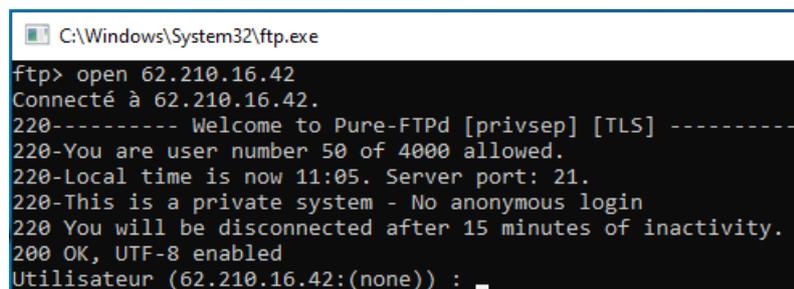
On peut lancer le client **FTP** windows natif



On demande



On est connecté, en attente du mot de passe



Un **netstat –an** affichera le connexion prise

```
C:\Users\Administrateur>netstat -an

Connexions actives

Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
TCP 192.168.1.171:139 0.0.0.0:0 LISTENING
TCP 192.168.1.171:50573 20.199.120.182:443 ESTABLISHED
TCP 192.168.1.171:50634 52.98.168.178:443 ESTABLISHED
TCP 192.168.1.171:50635 93.184.220.29:80 ESTABLISHED
TCP 192.168.1.171:50638 95.100.95.191:443 CLOSE_WAIT
TCP 192.168.1.171:50645 62.210.16.42:21 ESTABLISHED
TCP [::]:135 [::]:0 LISTENING
```

Netstat -b executable associé :

L'option **-b** permet d'afficher le nom de l'exécutable qui concerne chaque connexion ou port d'écoute.

```
C:\Windows\system32>netstat -n -p TCP -b

Connexions actives

Proto Adresse locale Adresse distante État
TCP 127.0.0.1:50621 127.0.0.1:50622 ESTABLISHED
[firefox.exe]
TCP 127.0.0.1:50622 127.0.0.1:50621 ESTABLISHED
[firefox.exe]
TCP 192.168.1.170:50557 192.168.1.172:3389 ESTABLISHED
[mstsc.exe]
TCP 192.168.1.170:50631 23.57.82.232:80 ESTABLISHED
```

Netstat -o PID correspondant :

La commande **netstat** permet donc avec les options **-ano** de connaître les n° de **pid** des processus associés aux n° de **ports**

qui utilise le port 668 ?
le PID 1984...

```
C:\Users\Administrateur>netstat -ano

Connexions actives

Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 948
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 632
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 1096
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 1164
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 688
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING 676
TCP 127.0.0.1:668 0.0.0.0:0 LISTENING 1984
TCP 127.0.0.1:668 127.0.0.1:49160 ESTABLISHED 1984
```

tasklist /svc et PID:

Par exemple **netstat -a -o** ou **netstat -a -b** sont très utiles, associées aux utilitaires **tasklists** et **taskkill**

le PID 1984...
c'est Carbonite !

```
C:\Users\Administrateur>tasklist

Nom de l'image PID Nom de la session Numéro de s Utilisation
-----
System Idle Process 0 Services 0 24 Ko
System 4 Services 0 5 784 Ko
smss.exe 448 Services 0 560 Ko
csrss.exe 580 Services 0 3 848 Ko
wininit.exe 632 Services 0 3 348 Ko
csrss.exe 644 Console 1 12 100 Ko
services.exe 676 Services 0 6 008 Ko
lsass.exe 688 Services 0 1 756 Ko
lsm.exe 696 Services 0 3 356 Ko
winlogon.exe 804 Console 1 4 564 Ko
svchost.exe 888 Services 0 4 948 Ko
svchost.exe 948 Services 0 6 096 Ko
svchost.exe 984 Services 0 16 208 Ko
svchost.exe 1096 Services 0 10 184 Ko
mdnsresponder.exe 1956 Services 0 3 824 Ko
CarboniteService.exe 1984 Services 0 18 916 Ko
FrameworkService.exe 2036 Services 0 5 128 Ko
Mcshield.exe 492 Services 0 25 936 Ko
```

et les services sont affichables, avec l'option **/SVC** par exemple ici svchost en PID **984** correspondrait à Windows defender... !

```
C:\Users\Administrateur>tasklist /svc

Nom de l'image PID Services
-----
System Idle Process 0 N/A
System 4 N/A
smss.exe 448 N/A
csrss.exe 580 N/A
wininit.exe 632 N/A
csrss.exe 644 N/A
services.exe 676 N/A
lsass.exe 688 ProtectedStorage, SamSs
lsm.exe 696 N/A
winlogon.exe 804 N/A
svchost.exe 888 DcomLaunch, PlugPlay
svchost.exe 948 RpcSs
svchost.exe 984 WinDefend
```

On peut ensuite faire le ménage, via

taskkill /f /im carbonite.exe

Ou

taskkill /PID 1984

N.B: L'argument **/f** force les processus à se terminer

N.B: l'argument **/im** spécifie le nom d'image du processus à terminer (dans l'exemple ci-dessus, le nom d'image du processus est « **carbonite.exe** »)

Nbtstat -n :

Les essais sur une configuration peuvent se faire à bas niveau, directement au niveau d'un boîte DOS

Permet de connaître des statistiques sur NETBIOS SUR TCP/IP

```
Displays protocol statistics and current TCP/IP connections using NBT(NetBIOS over TCP/IP).
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-s] [S] [interval] ]
-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                        IP address.
-c (cache)           Lists the remote name cache including the IP addresses
-n (names)           Lists local NetBIOS names.
-r (resolved)       Lists names resolved by broadcast and via WINS
-R (Reload)         Purges and reloads the remote cache name table
-S (Sessions)       Lists sessions table with the destination IP addresses
-s (sessions)       Lists sessions table converting destination IP
                        addresses to host names via the hosts file.

RemoteName  Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval    Redisplays selected statistics, pausing interval seconds
            between each display. Press Ctrl+C to stop redisplaying
            statistics.
```

TELNET TEST DE SOCKET

Installation telnet:

Le protocole **telnet** n'est pas installé par défaut... il faut l'ajouter sur notre poste Windows... **N.B** : Sous Windows 11 le client **Telnet** n'apparaît même pas dans la recherche.

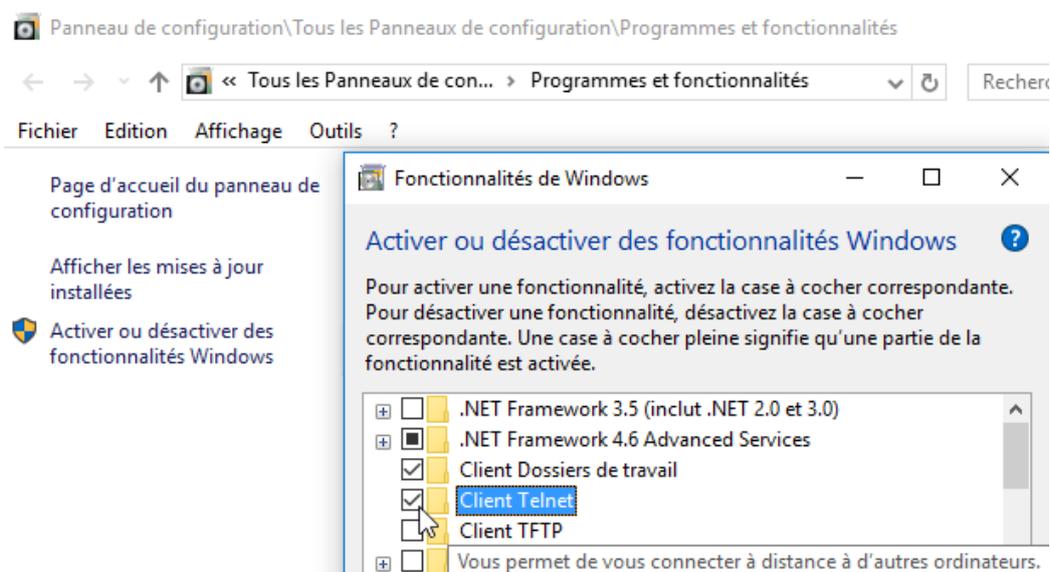
Via l'ancien **panneau configuration**

Ou – **control.exe**

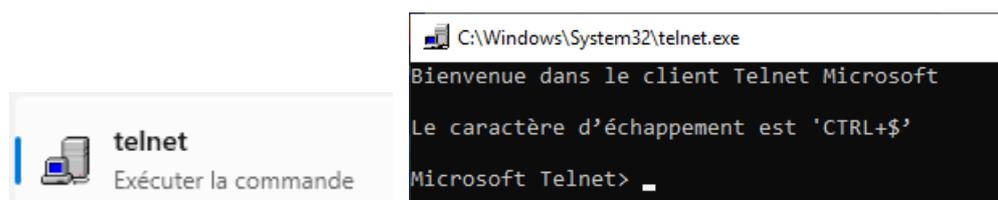


On demande **Panneaux de Configuration / Programmes et Fonctionnalités**

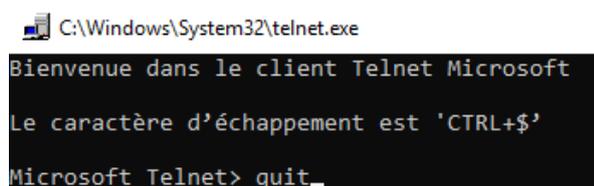
Activer ou Désactiver des fonctionnalités Windows / Client Telnet



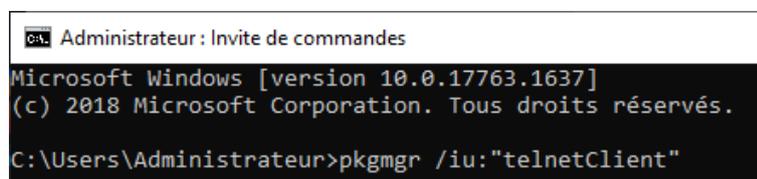
Désormais, l'application **Telnet** sera disponible.



On quittera une session Telnet par la commande **quit**



N.B: si on veut rendre **telnet** plus accessible, **pkgmgr /iu:"TelnetClient"**



Telnet - Test de Socket = @IP+ port distant:

L'utilisation de **telnet** est assez basique

```
c - close          ferme la connexion en cours
d - display       affiche les paramètres d'opération
o - open NomHôte [Port] Se connecte à l'hôte nommé (port 23 par défaut)
q - quit         quitte telnet
set - set        définit les options ('set ?' pour afficher la liste)
sen - send      envoie les chaînes au serveur
st - status     affiche les informations d'état
u - unset       annule les options ('unset ?' pour afficher la liste)
?/h - help     affiche des informations d'aide
```

On peut tester ensuite des **socket IP** (couple **Adresse Ip + N° de Port**) simplement en tapant une commande du genre

Port 3389 (RDP)

Par exemple pour le port **TCP 3389** qui correspond à du **RDP**, (Bureau à distance) que l'on peut tester sur une machine distante (activation en écoute via les propriétés du poste de travail d'une machine)

N.B: sur les anciennes versions windows on tapait directement

telnet @ip port

```
C:\Users\Administrateur>telnet 192.168.1.171 3389_
```

N.B : sur les nouvelles versions, on passe en Mode **Telnet** et ensuite on demande **Open @ip port**

```
Microsoft Telnet> open 192.168.1.10 3389
```

Si le port 3389 n'est pas ouvert sur la machine 192.168.1.171, on aura alors

```
C:\Users\Administrateur>telnet 192.168.1.171 3389
Connexion à 192.168.1.171...Impossible d'ouvrir une connexion à l'hôte, sur le port 3389
```

Si le port 3389 est en écoute, on aura RIEN... mais... cela veut dire que la connexion est établie ! (on ne peut pas établir une connexion RDP en telnet... Cela peut être une fenêtre noire, peu importe, si la connexion est prise cela veut dire que le port de la machine distante est ouvert....

Ou

```
Microsoft Telnet> open 192.168.1.10 3389
Connexion à 192.168.1.10...
```

Ne sera pas visible d'ailleurs si on fait un **netstat -na** car la **connexion RDP n'est pas montée !**

Port 22 (SFTP)

donc si on veut tester **SFTP** sur une machine distante nommée **sftp.sd6.gpaas.net** (adresse ip **155.133.142.129**) on testera le port **22**

```
C:\> Administrateur : Invite de commandes
Bienvenue dans le client Telnet Microsoft

Le caractère d'échappement est 'CTRL+$'

Microsoft Telnet> open sftp.sd6.gpaas.net 22
Connexion à sftp.sd6.gpaas.net...
```

le serveur SFTP répond...

```
C:\> Telnet sftp.sd6.gpaas.net
SSH-2.0-OpenSSH_8.4p1 Debian-2~bpo10+1
```

le port est ouvert

Visible d'ailleurs si on fait un **netstat -na**

```
C:\Users\Administrateur>netstat -na

Connexions actives

Proto Adresse locale Adresse distante État
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
TCP 192.168.1.171:139 0.0.0.0:0 LISTENING
TCP 192.168.1.171:50528 152.199.19.161:443 CLOSE_WAIT
TCP 192.168.1.171:50541 20.199.120.151:443 ESTABLISHED
TCP 192.168.1.171:50542 95.100.95.191:443 CLOSE_WAIT
TCP 192.168.1.171:50544 152.199.21.118:443 CLOSE_WAIT
TCP 192.168.1.171:50563 155.133.142.129:22 ESTABLISHED ←
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
```

Port 21 (FTP)

donc si on veut tester FTP sur une machine distante 88.190.253.101 on tentera le port 21

```
C:\Users\Administrateur>telnet 88.190.253.101 21
Connexion à 88.190.253.101...
```

Et si on obtient

```
C:\> Telnet 88.190.253.101
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 153 of 2048 allowed.
220-Local time is now 11:58. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
_
```

On sait que l'on a ouvert une connexion, ...

Si le port 21 est fermé, on aura

```
C:\Users\Administrateur>telnet 88.190.253.101 21
Connexion à 88.190.253.101...Impossible d'ouvrir une connexion à l'hôte, sur le port 21
```

TESTER TCP/IP - COMPLEMENTS

Test MTU ping -l -f:

Dans un **ping**, l'option **-l** permet de spécifier la taille des paquets

Dans un **ping**, l'option **-f** demande de ne pas fractionner le paquet

	Network	MTU (bytes)
Ping -l taille -f	-----	
	16 Mbps Token Ring	17914
	4 Mbps Token Ring	4464
	FDDI	4352
	Ethernet	1500
	IEEE 802.3/802.2	1492
	PPPoE (WAN Miniport)	1480
	X.25	576

A **512 octets**, cela marche, pour tout le monde en général

```
C:\Windows\system32>ping -l 512 -f 192.168.1.171

Envoi d'une requête 'Ping' 192.168.1.171 avec 512 octets de données :
Réponse de 192.168.1.171 : octets=512 temps<1ms TTL=128
```

A **1500 octet** cela ne marche plus... pourquoi ?

Car chaque protocole ajoute des octets par rapport aux octets de data "pur", c'est le principe d'encapsulation. Et donc un paquet de 1500 octets utiles, spécifié par **-l 1500** nécessite en fait l'envoi d'une trame de plus de 1500 octets, qui dépassera du coup la limite maximale.

```
C:\Windows\system32>ping -l 1500 -f 192.168.1.171

Envoi d'une requête 'Ping' 192.168.1.171 avec 1500 octets de données :
Le paquet doit être fragmenté mais paramétré DF.
```

N.B: comme on ne sait pas par quel routeur on va passer, ni quel protocole on peut prendre à un moment donné, il vaut mieux fixer la taille maximale avec un seuil de sécurité !

Constat de la valeur MTU 1500 en Wan

Ainsi une trame **Ethernet** comme la commande **Ping** qui possède 1 en-tête de **28 octets** (20 pour entête Ip et 8 pour entête ICMP) va avoir une taille maximale transmissible de $1500 - 28 = 1472$ **octets**.

Donc 1472 octets à transmettre via la commande ICMP ping cela marche

```
C:\Windows\system32>ping -l 1472 -f 192.168.1.171

Envoi d'une requête 'Ping' 192.168.1.171 avec 1472 octets de données
Réponse de 192.168.1.171 : octets=1472 temps<1ms TTL=128
Réponse de 192.168.1.171 : octets=1472 temps<1ms TTL=128
```

Mais 1473 octets cela ne marche plus !

```
C:\Windows\system32>ping -l 1473 -f 192.168.1.171
Envoi d'une requête 'Ping' 192.168.1.171 avec 1473 octets de données :
Le paquet doit être fragmenté mais paramétré DF.
Le paquet doit être fragmenté mais paramétré DF.
```

Evidemment sans **/f**, cela marche car le paquet sera fragmenté.

```
C:\Windows\system32>ping -l 1473 192.168.1.171
Envoi d'une requête 'Ping' 192.168.1.171 avec 1473 octets de données :
Réponse de 192.168.1.171 : octets=1473 temps<1ms TTL=128
Réponse de 192.168.1.171 : octets=1473 temps<1ms TTL=128
```

Si on doit transmettre la même quantité d'octet, via **FTP**, (qui n'est pas **ICMP** mais qui est un protocole applicatif, surcouche **IP**) il faut comprendre que en plus de **l'entête IP et TCP**, il faudrait rajouter les informations liées au **protocole TFTP**...). Pour faire simple, dès que l'on prend une connexion physique autre que la liaison **Ethernet 802.3 Lan** (par exemple **ADSL, FIBRE, 4G/LTE**) alors la taille en octets de données réellement émissible sans fragmentation varie et diminue. **TCP-IP** peut modifier dynamiquement au cours d'un échange la taille **MTU** à travers un mécanisme nommé **MSS maximum Segment size**.

Pour information en **LAN** : **netsh interface ipv4 show interfaces**

```
C:\Windows\system32>netsh interface ipv4 show interfaces
```

Idx	Mét	MTU	État	Nom
1	50	4294967295	connected	Loopback Pseudo-Interface 1
10	10	1500	connected	Ethernet 3

et en **WAN** : **netsh interface ipv4 show destinationcache**

```
C:\Windows\system32>netsh interface ipv4 show destinationcache
```

```
Interface 1 : Loopback Pseudo-Interface 1
```

PMTU	Adresse de destination	Adresse de saut suivant
1500	127.0.0.1	127.0.0.1

```
Interface 10 : Ethernet 3
```

PMTU	Adresse de destination	Adresse de saut suivant
1456	8.8.8.8	192.168.1.1
1500	10.3.0.1	192.168.1.1

Ainsi une trame **Ethernet 802.3** comme la commande **Ping** qui possède 1 entête de 28 **octets** (20 pour entête Ip et 8 pour entête ICMP) va avoir une taille maximale transmissible ici de $1456 - 20 - 8 = 1428$ **octets**

Une **MTU** est posée à 1428 pour **Windows** des que l'on "sort"

```
C:\Windows\system32>ping -l 1428 -f 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 1428 octets de données :
Réponse de 8.8.8.8 : octets=1428 temps=13 ms TTL=57
Réponse de 8.8.8.8 : octets=1428 temps=13 ms TTL=57
Réponse de 8.8.8.8 : octets=1428 temps=13 ms TTL=57
Réponse de 8.8.8.8 : octets=1428 temps=14 ms TTL=57
```

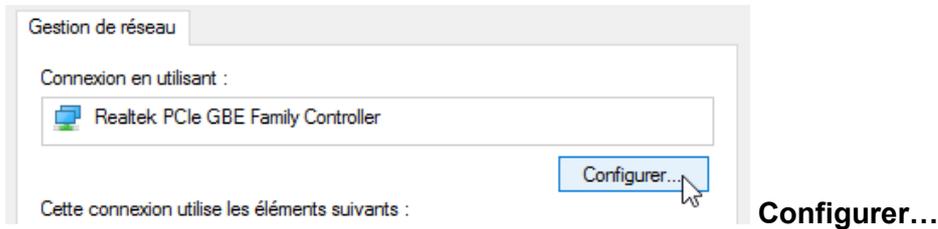
et

```
C:\Windows\system32>ping -l 1429 -f 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 1429 octets de données :
Réponse de 192.168.0.1 : Le paquet doit être fragmenté mais paramétré DF.
```

Jumbo Frames - MTU en Lan

Si on modifie la taille des paquets **MTU** dans les paramètres de la carte réseau



Et on demande des frames dites **Jumbo Frame** maxi **MTU de 4ko**



On devrait pouvoir faire un ping avec un paquet de 4 kilo...

Ping 192.168.1.114 -l 4000 -f

Si cela ne marche pas, c'est que entre les 2 postes un appareil (hub, switch) n'accepte pas ces frames agrandies... on peut essayer directement avec un câble croisé.

```
C:\Users\Administrateur>ping 192.168.1.114 -l 4000 -f

Envoi d'une requête 'Ping' 192.168.1.114 avec 4000 octets de données :
Réponse de 192.168.1.114 : octets=4000 temps<1ms TTL=128
Réponse de 192.168.1.114 : octets=4000 temps<1ms TTL=128
Réponse de 192.168.1.114 : octets=4000 temps<1ms TTL=128
```

Routage route print netstat -r :

On est sur une machine en 192.168.1.100 sans indication de
La commande **route print**, ou **netstat -r** donne l'affichage suivant

```
C:\Windows\system32>route print
=====
Liste d'Interfaces
10...40 8d 5c b1 91 28 .....Realtek PCIe GBE Family Controller
1.....Software Loopback Interface 1
=====
```

Et la table par défaut étant

```
IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
127.0.0.0             255.0.0.0        On-link            127.0.0.1         306
127.0.0.1             255.255.255.255 On-link            127.0.0.1         306
127.255.255.255      255.255.255.255 On-link            127.0.0.1         306
192.168.1.0           255.255.255.0   On-link            192.168.1.100    266
192.168.1.100        255.255.255.255 On-link            192.168.1.100    266
192.168.1.255        255.255.255.255 On-link            192.168.1.100    266
224.0.0.0             240.0.0.0        On-link            127.0.0.1         306
224.0.0.0             240.0.0.0        On-link            192.168.1.100    266
255.255.255.255      255.255.255.255 On-link            127.0.0.1         306
255.255.255.255      255.255.255.255 On-link            192.168.1.100    266
=====
Itinéraires persistants :
Aucun
```



Destination Réseau	Masque Réseau	Adr. Passerelle	Adr. interface	Métrique
Vers ou veut on aller	permet de définir une plage étendue de destination	Adresse /carte par laquelle on doit passer	à partir de quelle adresse / carte on part	Cout. plus il est petit, plus la route est prioritaire

- On-link** = aucun routage nécessaire, on est directement relié au réseau
- 192.168.1.100 / 255.255.255.255** : Route de l'ordinateur vers lui-même, "Destination réseau" et "Adresse interface" ont la même valeur. le masque entièrement à 255 qui permet de désigner une plage limitée à une seule adresse.
- 192.168.1.0 / 255.255.255** permet d'indiquer les adresses du même réseau IP (pas de routage nécessaire, forcément)
- 192.168.1.255 / 255.255.255.255** permet d'indiquer l'adresse de broadcast

Toutes les autres entrées servent à indiquer les adresses le multidiffusio. (127.0.0.0 = localhost – 127.255.255.225 etc etc)

L'ordre de traitement de la table de routage va des masques les plus longs aux plus petits. C'est à dire que le routeur va d'abord comparer les sous-réseaux avec le masque 255.255.255.255 pour finir par comparer les sous-réseaux avec le masque 0.0.0.0. Il peut y avoir plusieurs routes possibles, mais elles n'ont pas la même métrique

Si on ajoute une passerelle en 192.168.1.1 alors

```

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
0.0.0.0              0.0.0.0          192.168.1.1        192.168.1.100     266
127.0.0.0            255.0.0.0        On-link            127.0.0.1         306
127.0.0.1            255.255.255.255  On-link            127.0.0.1         306
127.255.255.255      255.255.255.255  On-link            127.0.0.1         306
192.168.1.0          255.255.255.0    On-link            192.168.1.100     266
192.168.1.100        255.255.255.255  On-link            192.168.1.100     266
192.168.1.255        255.255.255.255  On-link            192.168.1.100     266
224.0.0.0            240.0.0.0        On-link            127.0.0.1         306
224.0.0.0            240.0.0.0        On-link            192.168.1.100     266
255.255.255.255      255.255.255.255  On-link            127.0.0.1         306
255.255.255.255      255.255.255.255  On-link            192.168.1.100     266
=====
Itinéraires persistants :
Adresse réseau    Masque réseau    Adresse passerelle    Métrique
0.0.0.0           0.0.0.0          192.168.1.1           Par défaut

```

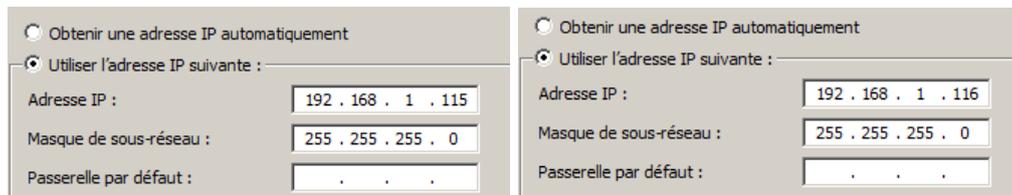
Route par défaut **0.0.0.0/0.0.0.0** : c'est la route utilisée si aucune autre route possible n'a été trouvée dans la table de routage

Test routage route add :

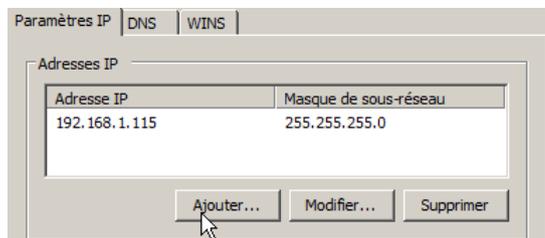
soit 2 machines respectivement communiquant

en 192.168.1.115/24

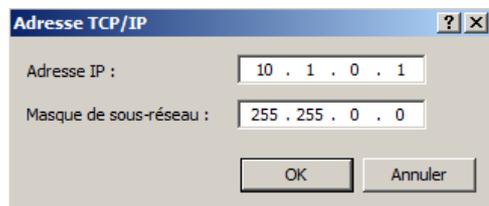
et 192.168.1.116/24



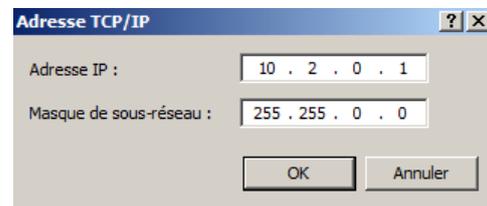
on ajoute sur chaque poste une 2° @ IP respectivement en 10.1.0.1 et 10.2.0.1. donc via **Avancé/ Ajouter**



Donc a joute sur la 1° machine



et sur la 2° machine



On aura donc pour la 1° machine



Et pour la 1° machine on peut vérifier

```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : POSTE15
Suffixe DNS principal . . . . . : cabare-intra.net
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS : cabare-intra.net

Carte Ethernet Connexion au réseau local :
Description . . . . . : Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller(NDIS6.20)
Adresse physique . . . . . : 90-E6-BA-16-B5-38
DHCP activé . . . . . : Non
Configuration automatique activée . . . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::3909:f763:8ab1:fea2%11<préféré>
Adresse IPv4 . . . . . : 10.1.0.1<préféré>
Masque de sous-réseau . . . . . : 255.255.0.0
Adresse IPv4 . . . . . : 192.168.1.115<préféré>
Masque de sous-réseau . . . . . : 255.255.255.0
```

Ping en 192.168.1.116 marche, bien sur

```
C:\Users\Administrateur>ping 192.168.1.116

Envoi d'une requête 'Ping' 192.168.1.116 avec 32 octets de données :
Réponse de 192.168.1.116 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.116:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Ping en 10.2.0.1 échoue

```
C:\Users\Administrateur>ping 10.2.0.1

Envoi d'une requête 'Ping' 10.2.0.1 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.

Statistiques Ping pour 10.2.0.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Si on ajoute une route, il faut connaître l'adresse ip en 192.168.1.116 de la machine d'à coté, que l'on utilisera comme moyen d'accès...

Route add 10.2.0.0 mask 255.255.0.0 192.168.1.116

```
C:\Users\Administrateur>route add 10.2.0.0 mask 255.255.0.0 192.168.1.116
OK!
```

Et on vérifie notre table

```
IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
-----
10.0.0.0                255.0.0.0     On-link         10.1.0.1        266
10.1.0.1                255.255.255.255 On-link         10.1.0.1        266
10.2.0.0                255.255.0.0   192.168.1.116  10.1.0.1        11
10.255.255.255          255.255.255.255 On-link         10.1.0.1        266
127.0.0.0              255.0.0.0     On-link         127.0.0.1       306
127.0.0.1              255.255.255.255 On-link         127.0.0.1       306
127.255.255.255        255.255.255.255 On-link         127.0.0.1       306
192.168.1.0            255.255.255.0 On-link         10.1.0.1        266
```

Maintenant cela marche

```
C:\Users\Administrateur>ping 10.2.0.1

Envoi d'une requête 'Ping' 10.2.0.1 avec 32 octets de données :
Réponse de 10.2.0.1 : octets=32 temps<1ms TTL=128
```