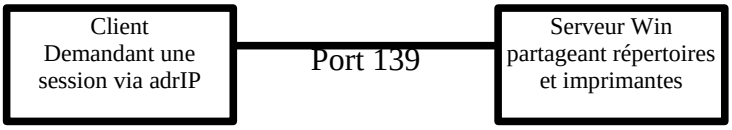
1.6 Service session

Reprécisons que **ce n'est pas NetBIOS** lui même **qui ne passe pas les routeurs mais la diffusion NetBIOS**. Quand on recherche une machine par son adresse IP en utilisant la fonction Rechercher sous Windows, on ne fait que demander à notre client NetBIOS de se connecter via un **port** à la machine Windows. Une fois la connexion de socket établie, on peut accéder aux partages de la machine distante. C'est pour cette raison que les postes Windows et les serveurs Samba qui ont des partages mal protégés sont particulièrement vulnérables.



Le service de session NetBIOS utilise donc le port TCP139. **Une session s'établit comme suit** :
- Résolution du **nom** NetBIOS **en adresse IP**;
- Résolution de **l'adresse IP** en adresse **MAC**;
- Établissement d'une **session TCP** de la station au **serveur** sur le **port 139**;
- La station fait sa demande d'établissement de **session NetBIOS** sur le nom du serveur, par-dessus la connexion TCP. Si le serveur est effectivement à l'écoute sur ce nom, il répond par l'affirmative et la session NetBIOS s'établit.

Un fois établie, le client et la station SMB négocient le niveau de protocole SMB qu'ils vont utiliser par dessus NetBIOS. On notera que le nombre de sessions NetBIOS se limite à 254 par machine.

!!! Si une machine exploite son fichier "**lmhosts**" (expliqué au §2.2) pour la résolution de nom, et qu'il y a une différence entre le contenu de ce fichier et le nom NetBIOS du serveur, alors la station contactera le serveur (via adr IP) mais celui-ci refusera la session et retournera une erreur 51 "remote computer not listening".

1.7 Service datagramme sous NetBIOS

Il fonctionne lui avec le **port 138** et permet d'envoyer un message à un nom de groupe ou à un nom unique.
Cf commande 'net' . Exemple : [net send machine "contenu du message"] ou encore [net send /domain: "message"]

La machine **émettrice** va **envoyer** un **paquet unicast** (pour un nom unique) **ou de broadcast** (pour un nom de groupe) **sur le nom** se **finissant** par le seizième caractère **<03>**.

1.8 Le Maître Explorateur : maître du réseau.

L'explorateur réseau sur chaque machine NetBIOS est le service qui :
- **rassemble, organise** et **mémorise** la **liste des ordinateurs** NetBIOS et les domaines
- **permet de savoir** à tout moment quels sont les ordinateurs exécutant NetBIOS sur le même réseau IP sans le demander

On peut imaginer qu'à tous moments les ordinateurs peuvent s'activer, se désactiver, communiquer, se déconnecter, se reconnecter... Et que chaque ordinateur devrait actualiser sa propre liste "image du réseau NetBIOS" à tout instant (BOF).

En fait, il y a **un ordinateur** précis qui tient la liste la plus à jour possible de tout ce qui est présent. Il est **appelé** "**Maître Explorateur**" (master Browser). Les **ordinateurs présents lui demanderont** la **liste** d'exploration à afficher dans le voisinage réseau.

1.8.1 Enregistrement des noms, actualisation de la liste

Toutes les **12 minutes**, les **ordinateurs annoncent** leur **présence** au **maître explorateur**. Trame : "nomNetBIOS<grp/domain><1D>".
À partir de ces diffusions, le **maître** explorateur **crée** donc une **liste d'exploration**. Dans le même temps, il **s'attribue l'enregistrement** <01><02>__MSBROWSE__<02><01>, et **l'annonce** au réseau. Grâce à ce système, les **maîtres** explorateurs des autres grp/domain **savent à qui demander** les listes d'exploration pour ces grp/domain d'ordinateurs. En fait, **chaque maître explorateur** sur chaque groupe de machine d'un même réseau IP **possède** aussi une **liste d'exploration des autres groupes** de ce réseau IP.
Si le **nombre d'ordinateurs croît**, le **maître explorateur** commence à **répliquer** sa liste sur des **explorateurs de secours** (Backup Browsers). Les **explorateurs de secours contactent** le **maître explorateur** pour mettre leur liste à jour toutes les **15 minutes**.

1.8.2 Réponse du maître explorateur aux requêtes des clients

Lorsqu'une **demande d'exploration** est faite par un client, celle-ci est faite directement auprès du **maître explorateur**, qui **retourne** la **liste** des **ordinateurs du réseau**. Le service d'exploration du **client garde** pour un usage futur les **noms de 3 explorateurs** du réseau.
Sous Windows, un **client commence** par **demander la liste** des enregistrements <01><02>__MSBROWSE__<02><01>. Il obtient les noms des maîtres explorateurs pour chaque groupe et les ordinateurs dans chaque groupe.
Lorsqu'un **utilisateur entre dans un groupe**, le **client** fait sa **demande** au **maître explorateur** du groupe choisi (<domaine><1D>). Dans le cas où il n'y a pas de réponse, il fait la même requête auprès du maître explorateur du groupe qu'il souhaite explorer.

1.9 Maître explorateur du Domaine

On parle de **domaine de sécurité**. Dans le cas ou plusieurs ordinateurs du domaine sont sur des réseaux séparés par routeurs, il existe un super maître explorateur du domaine dont son rôle est dévolu au **Contrôleur Principal de Domaine** qui permettra de les rendre communiquants.
Le **maître explorateur du Domaine fusionne** les **listes d'exploration locales** en une **seule** grande **liste**, et les **redistribue** à chaque **maître explorateur local**, qui à son tour les réplique sur les explorateurs de secours.
Il y a 2 possibilités : soit le Contrôleur Principal de domaine est multirésident (à cheval sur plusieurs réseaux), soit on utilise un serveur WINS (§2.1).

1.10 Élection du maître explorateur

Parmi ceux qui ont toutes les chances d'être **élus maître explorateur**, on trouve les **Contrôleurs Principaux de Domaine** (100%).

En fait la **première machine** sur le réseau NetBIOS **devient Maître Explorateur** si elle ne trouve pas de maître explorateur au démarrage. Ou si elle détecte la disparition d'un maître explorateur.

Vient ensuite des ordres de priorité :
Un **serveur l'emporte** sur un **station**,
Un **contrôleur de domaine l'emporte sur un serveur** membre.

Il est possible **d'éviter** d'engendrer des **problèmes** avec des **élections successives** en paramétrant une machine maître explorateur et paramétrer les autres pour qu'elle ne se présentent pas aux élections.

Des machines démarrées ne sont pas vues immédiatement dans le voisinage réseau (idem pour sa disparition) . Les causes :
- Toutes les listes d'exploration sont à refaire parce qu'une élection a eu lieu
- Les ordinateurs viennent tous d'envoyer leur nom NetBIOS au maître explorateur, et que l'explorateur de sauvegarde vient juste de recevoir la liste. Il va donc s'écouler 12 minutes
- le maître explorateur attend 3 mises à jour de la liste avant de considérer un ordinateur éteint

1.11 Remarques

L'avantage de **NetBEUI** est sa **petite pile de protocoles**, ce qui explique qu'il trouve son emploi principalement sur des ordinateurs fonctionnant sous **MS-DOS** (léger, rapide et peu exigeant en ressources).

NetBIOS et **NetBEUI** sont des plus **faciles** à mettre en **oeuvre**. Plus souvent utilisés sur des **petits LAN** "égal à égal" (peer to peer).

Il a été fortement décrié pour la charge induite sur les réseaux, mais c'est aussi un système puissant et fonctionnel dès lors qu'il est paramétré avec soin sur un système stable et bien protégé.

Le grand **désavantage** est qu'il n'est **pas routable** et que son application se **limite**, par conséquent, à **un segment** de réseau. Certains routeurs transmettent, à la totalité de leurs segments, les paquets NetBEUI. Mais le résultat est une nette augmentation de la charge réseau alors que le routeur est censé la réduire.

<table>
<tr><td>Application</td><td colspan="2">Applications NetBIOS (Voisinage réseau, explorer ...)
Interface NetBIOS (netbios.dll)</td></tr>
<tr><td>Transport</td><td rowspan="2">NetBEUI</td><td>NetBIOS sur TCP/IP
(NetBT)</td></tr>
<tr><td>Réseau</td><td>TCP/IP</td></tr>
<tr><td>Matériel</td><td colspan="2">NDIS</td></tr>
</table>

2 Résolution de nom : Wins, lmhosts D, type de noeuds

Microsoft a cherché des **méthodes** pour **pallier** aux **limitations** du fonctionnement par **diffusions**.
Au niveau de **Internet**, la **résolution** de nom se fait avec **DNS** (système éprouvé). Microsoft a donc cherché à faire la même chose que DNS, mais pour environnements de type PME. Ne pouvant concevoir un système aussi rigide que DNS **il créa WINS** pour système compatible NetBIOS avec **mise à jour automatique** de la **base** de données de **noms** de machines.

2.1 WINS

Le **Windows Internet Name Service** fût implanté sur Win3.5. C'est un système de **centralisation dynamique** des listes **des noms** des machines. On précise aux **ordinateurs** du réseau **d'inscrire** leur **nom au serveur Wins**, et de lui **demander** de **résoudre un nom** NetBIOS en **adresse IP**.
Ce système permet de **limiter** grandement les **diffusions** et permet en plus de **fonctionner** en **environnement routé** car un client s'adressera à une adresse IP (celle du serveur WINS).
Fonctionnement :

- Les ordinateurs **s'initialisent** et s'ils sont paramétrés pour **s'inscrire** sur un **serveur WINS**, vont enregistrer leur nom et son adresse dans la base du serveur.
- Le serveur **WINS construit** sa liste et quand une machine inscrite a besoin de **résoudre** un **nom** NetBIOS, il lui donne.
- Lorsqu'un ordinateur **s'éteint**, il se **désinscrit**.
- Si un **ordinateur n'a pas l'adresse IP du serveur WINS** :
  - Et si le **client** est sur le **même réseau** IP que le serveur, alors le serveur recevra par diffusion ses : nom et adresse tôt ou tard.
  - Et si le **client n'est pas sur le même réseau** IP, alors on peut installer un **proxy-WINS** (ordinateur interceptant les diffusions et les transmettant au serveur WINS). C'est le serveur proxy-WINS qui inscrira auprès du serveur WINS les machines et c'est aussi lui qui demandera à WINS de transmettre la réponse quand un ordinateur non inscrit fera une diffusion pour résoudre un nom.

WINS peut être très utile pour joindre un ordinateur à un domaine n'étant pas sur le même réseau IP.

2.2 Fichiers LMHOSTS

Dans le cas où une **machine** est **séparée** par un routeur et qu'il **n'y a pas** de serveur **WINS**, il est toujours possible de **configurer** le **fichier** équivalent à "/etc/hosts" sur UNIX : le fichier **LMHOSTS**.
Exemple du fichier "C:\WINDOWS\system32\drivers\etc\lmhosts.sam" ou "C:\winnt\system32\drivers\etc\" pour w2k.

```
192.168.1.2     GE209-02        #PRE    #DOM:GE209
ADR_IP          NomNetBIOS      Paramètres
```

#PRE ->charge le nom dans le cache NetBIOS (visible avec la commande nbstat)
#DOM:<domaine> ->Indique que c'est un contrôleur du domaine "domaine"

Il est aussi possible d'indiquer qu'il faut utiliser le fichier "lmhosts" d'un autre ordinateur.
"#INCLUDE <nom_de_fichier>"
TP2 NetBIOS ici

2.3 Types de noeuds

Grâce au type de noeud paramétré, un ordinateur va savoir dans quel ordre utiliser les ressources. On entend par type de noeud, l'ordre de résolution de nom. Il y a 4 types de noeuds(nodes) :

- **B node** : Broadcast – La résolution de nom se fait uniquement par **diffusion**;
- **P node** : Point to point – La résolution de nom se fait uniquement avec le **serveur WINS**;
- **H node** : Hybride - La résolution de nom se fait **d'abord** avec le serveur **WINS puis** s'il ne répond pas, par **diffusion**;
- **M node** : Miste - La résolution de nom se fait **d'abord** par **diffusion**, **puis** avec **WINS**.

Lorsque la **carte réseau** est **configurée manuellement** alors le **type** de noeud est configuré en **Hybride**.
Lorsque la **carte réseau** est **configurée** avec **DHCP** alors le **type** de noeud doit être renseigné dans les **options DHCP** du serveur.

3 IPX/SPX

L'Internetworking Packet Exchange fût la réponse **Novell** à la complexité de IP. Conçu au début des année 80, est un protocole relativement efficace dont les fonctions contentent les administrateurs réseaux :

- Contrairement à IP, IPX peut **configurer sa propre adresse**. Particulièrement utile lors **d'installation de multiples machines**.
- IPX est un protocole "**bavard**". Il signale sa présence sur le réseau. Cette caractéristique est intéressante sur des réseaux aux frontières bien délimitées dont la bande passante n'est pas trop mauvaise. Sur un réseau étendu (comme WAN), la nature de IPX devient gênante, car elle peut **surcharger** les connexions de faible bande passante.

IPX est **facile à installer** et à **utiliser**. Malheureusement, ce n'est pas une **norme** ouverte car sous **contrôle de Novell** qui a reconnu que IPX cédera la place à IP.