

PROTOCOLES

Le protocole SMB

Server Message Bloc

C. Drocourt

LE PROTOCOLE SMB

Modèle OSI

7	Application	HTTP, SSH, SMB, ...
6	Présentation	Unicode, MIME, HTML, XML, XDR
5	Session	NetBios, SIP, H323, ...
4	Transport	TCP, UDP, ICMP, SPX, ...
3	Réseau	NetBEUI, IPv4, IPv6, IPX, ...
2	Liaison	Ethernet, token ring, fddi, wifi, ppp, ...
1	Physique	

LE PROTOCOLE SMB

Le protocole SMB signifie **Server Message Bloc**. Il est utilisé pour le partage de fichiers et d'imprimantes entre ordinateurs. Son histoire remonte à 1985 et a été défini au départ par IBM. On le connaît mieux maintenant sous le nom de **CIFS** (Common Internet File System).

Le protocole SMB peut être utilisé sur de nombreux autres protocoles de niveaux inférieurs, mais son utilisation la plus courante reste avec **NETBIOS** (NETwork Basic Input Output System), lui-même utilisant **TCP/IP**, dans ce cas on le nomme **netbt** (NETBIOS over TCP/IP).

Un bon point de départ pour l'étude de ce protocole se trouve à l'adresse suivante : <http://www.samba.org/cifs/docs/what-is-smb.html>.

LE PROTOCOLE SMB

NETBIOS

Le protocole **NETBIOS** sur **TCP/IP** est défini dans les rfc1001 et rfc1002. Il est utilisé pour le nommage des ressources réseaux et l'accès à ces dernières. Il utilise les ports suivants :

- Netbios Name Service (port udp 137),
- Netbios Datagram Service (port udp 138),
- Netbios Session Service (port tcp 139).

Sur un réseau **NETBIOS**, chaque ressource possède un nom limité à 16 caractères, dont le dernier est utilisé pour déterminer la nature de la ressource. Il y a deux types de ressources : celles associées au nom de l'ordinateur (unique dans ce cas), et le nom du groupe auquel il appartient (multiple). Des informations sur ce dernier caractère peuvent être trouvées à l'adresse : <http://support.microsoft.com/kb/q163409/>.

LE PROTOCOLE SMB

NETBIOS

<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<\\--__MSBROWSE__>	01	G	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 Interchange(MSMail 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 Administrators Remote Control Tool
<computername>	45	U	SMS Clients Remote Chat
<computername>	46	U	SMS Clients Remote Transfer
<computername>	4C	U	DEC Pathworks TCPIP service on Windows NT

LE PROTOCOLE SMB

NETBIOS

<computername>	42	U	mccaffee anti-virus
<computername>	52	U	DEC Pathworks TCPIP service on Windows 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>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<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
IRISMULTICAST	[2F]	G	Lotus Notes
IRISNAMESERVER	[33]	G	Lotus Notes
Forte_\$ND800ZA	[20]	U	DCA IrmaLan Gateway Server Service

LE PROTOCOLE SMB

NETBIOS

Pour effectuer une association entre un nom NETBIOS et une adresse IP un ordinateur à deux solutions :

- Effectuer une diffusion sur le réseau (broadcast) et attendre une réponse, dans ce cas la limite du réseau NETBIOS est celle du LAN, puisque la diffusion ne passera pas au travers des équipements de niveau 3 (routeurs),
- Utiliser un serveur capable de lui fournir une réponse (serveur WINS), dans ce cas il n'y a pas de limite théorique sur l'étendue du réseau NETBIOS, mais cela nécessite l'utilisation d'un service actif sur un serveur.

Dans les deux cas, la méthode retenue est utilisée aussi bien pour :

- S'annoncer (enregistrement de son nom netbios),
- Effectuer une résolution (demander une IP à partir d'un nom NETBIOS).

LE PROTOCOLE SMB

NETBIOS

Pour les raisons précédentes, il existe plusieurs types de noeuds NETBIOS:

- B-noeud (Broadcast) : L'ordinateur effectue un broadcast pour enregistrer et résoudre les requêtes DNS,
- P-noeud (Point-to-Point) : L'ordinateur interroge un serveur de résolution de noms netbios (WINS),
- M-noeud (Mixed) : L'ordinateur se comporte comme un B-noeud et s'il ne trouve pas de réponses, il bascule en mode P-noeud,
- H-noeud (Hybrid) : L'ordinateur se comporte comme un P-noeud et s'il ne trouve pas de réponse, il bascule en mode B-noeud.

Le type de noeud par défaut est le H-noeud, mais il peut être modifié dans la base de registre ou via un paramètre du serveur DHCP.

LE PROTOCOLE SMB

NETBIOS : Les outils

La première commande à connaître sous Windows est **nbtstat** qui permet l'utilisation de la couche **NETBIOS** directement sur la ligne de commande, la commande équivalente sous Linux est **nmblookup**.

Exercice :

Sous Windows :

Affichez la table de noms netbios de la machine locale,

Affichez la table de noms netbios d'une machine de la salle,

Affichez les statistiques de sessions netbios par adresse IP toutes les 5 secondes,

Sous Linux :

Testez la commande findsmb,

A l'aide de la commande nmblookup interrogez votre machine windows,

LE PROTOCOLE SMB

NETBIOS : Les outils

Pour lister les ressources disponibles sur un ordinateur, on utilisera sous Windows la commande **net view**, et sous Linux la commande **smbclient** (avec l'option -L).

Exercice :

Sous Windows :

*Testez les ressources partagées par votre machine windows,
Testez les ressources partagées par la machine 172.20.0.24.*

Sous Linux :

*Testez les ressources partagées par votre machine windows,
Testez les ressources partagées par la machine 172.20.0.24.*

LE PROTOCOLE SMB

NETBIOS : Les outils

Une fois le partage identifié, il est possible de l'utiliser à condition de posséder les autorisations nécessaires. Sous windows on pourra utiliser la commande **net use** pour « mapper » un chemin réseau sur un lecteur virtuel. Sous Linux, on peut utiliser **smbmount** (ou **mount**) pour monter le système de fichier distant, ou simplement **smbclient** qui est l'équivalent d'un client ftp adapté au protocole SMB.

Exercice :

Sous Windows :

*Utilisez la commande `net use` pour mapper le partage **public_profs** de la machine 172.20.0.24.*

Sous Linux :

Utilisez `smbclient` pour naviguer dans ce même partage, et récupérer un fichier (commande `get`).

LE PROTOCOLE SMB

Sans NETBIOS

A partir de Windows 2000, le protocole SMB est implémenté directement sur TCP/IP et ne passe plus par la couche NETBIOS mais utilise le service standard de nommage internet : le DNS. Ce nouveau service utilise le **port 445** en TCP et en UDP (qui remplace donc l'utilisation des ports 137, 138 et 139).

Toutefois, afin de garder une compatibilité avec les versions précédentes de Windows, le support de NETBIOS est encore actif, et il est utilisé si la résolution DNS échoue.

Si le réseau de l'entreprise n'utilise plus de versions de Windows antérieures à 2000, ce support peut être désactivé dans les options TCP/IP. Avec SAMBA, on ajoutera l'option « disable netbios = yes » dans son fichier de configuration.

LE PROTOCOLE SMB

Sans NETBIOS

Exercice :

- *Désactivez le support NETBIOS sous Windows,*
- *Que se passe t'il dans le voisinage réseau ?*
- *Interrogez votre cache local avec nbtstat, conclusion ?*
- *Interrogez votre machine Windows à partir de Linux avec nmblookup, alors ?*