Réseau

AB – v3.28 (22/10/2022)

Nommage des systèmes

- Chaque système possède :
  - Un nom de machine
  - Un nom de groupe pouvant être :
    - Un WORKGROUP (entrée déclarative, annuaire réparti)
    - Un DOMAINE (annuaire centralisé)
- Ces noms sont sous deux formats :
  - Le format **NetBios** (maximum 15 caractères)
  - Le format **DNS** (*hostname* & FQDN)

NetBios

NetBios

- Protocole historique (années 80), toujours supporté sous Windows via *NetBIOS over TCP/IP* (NetBT ou NBT)

- NetBios offre trois services :
  - NetBIOS Name Service (**NBNS**) : **TCP/UDP 137**
  - NetBIOS Datagram Service (**NBDS**) : **UDP 138**
  - NetBIOS Session Service (**NBSS**) : **TCP 139**

- RFC 1001 (03/1987) : *Concepts and methods*
- RFC 1002 (03/1987) : *Detailed specifications*

NetBIOS Name Service (NBNS)

- NBNS permet l'enregistrement, la libération et la résolution d'un nom NetBios sur un réseau local
- Format nom NetBios : 15 caractères + 1 (NetBIOS *suffix*)
- Les 3 commandes sont :
  - **`Registration`** (*claim*) : permet de s'assurer que le nom n'est pas déjà utilisé et d'enregistrer un nom
  - **Release** : permet de libérer un nom
  - **`Query`** (*resolution* ou *discovery*) : permet de résoudre un nom
- Repose massivement sur l'utilisation de messages en *broadcast*

Windows Networking
(WNet)

Mise en œuvre

- WNet permet l'accès et la gestion des systèmes de fichiers réseau
- Il est mis en œuvre par :
  - L'**API WNet** qui permet la gestion des ressources réseau (énumération des ressources réseau, connexion à un réseau, authentification, association d'un partage à une lettre)
  - **Multiple Provider Router (MPR)** qui permet de déterminer quel fournisseur (***Network providers***) doit être invoqué lorsque l'API WNet est sollicitée
  - **Multiple UNC Provider (MUP)** (dans le noyau) qui permet de déterminer vers quel redirecteur réseau (***Network redirectors***) doit être redirigée une requête UNC

UNC et WNet

- La notation **UNC** (*Uniform Naming Convention*) permet d'identifier une ressource réseau (partage, fichier, imprimante) accessible via un système de fichiers réseau :

```
\\Serveur\Partage\Chemin\Fichier
```

- Exemple de **systèmes de fichiers réseau** :
  - Natifs : Lanman, WebDav, TS, (NFS)
  - Tiers : VirtualBox, VMWare, etc.

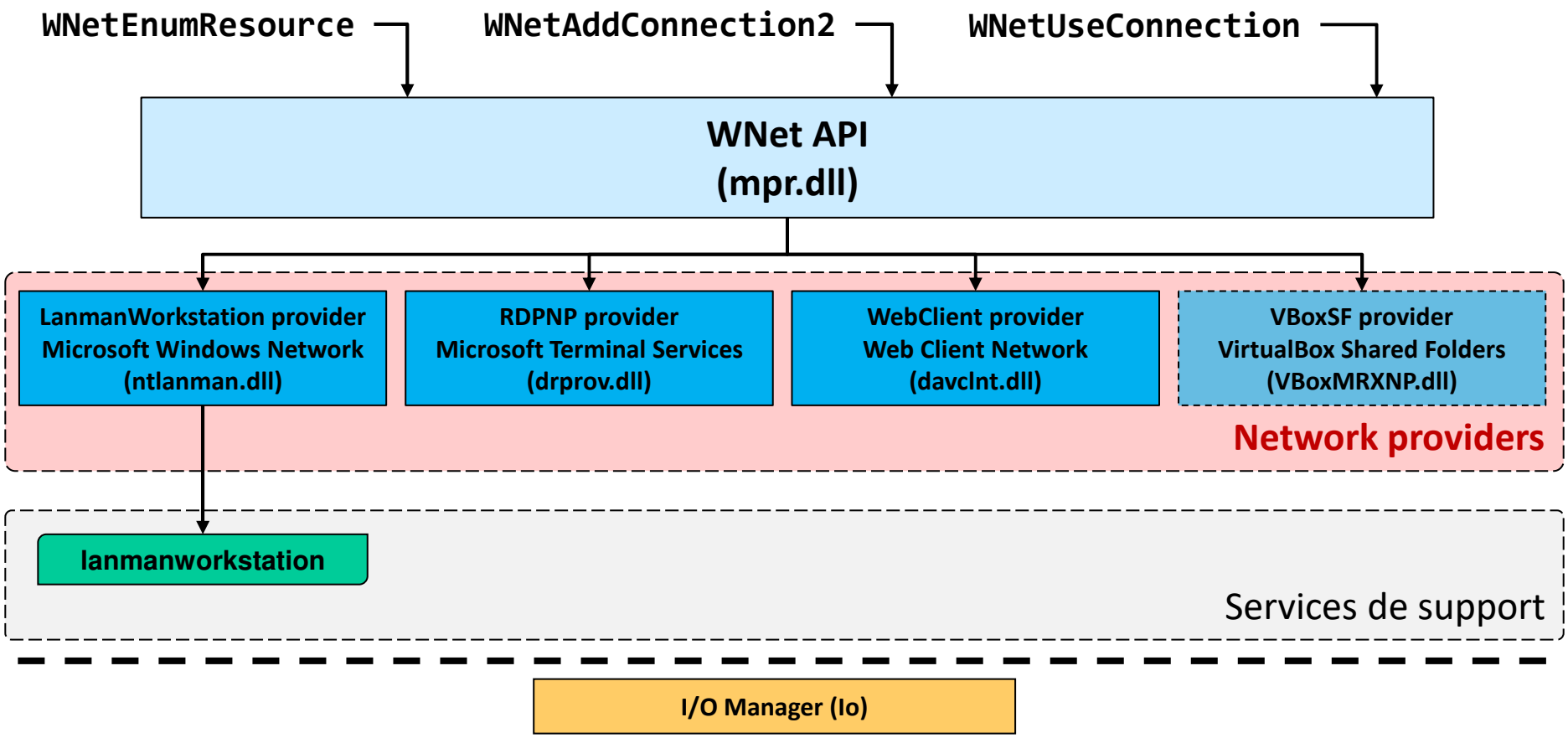
Notations UNC

`\\ Serveur \ Partage \ Chemin \ vers \ fichier`

- **Serveur** : nom de la machine distante :
  - **.** : machine locale
  - Adresse IP
  - Nom NetBios (devant être résolu par NBNS)
  - FQDN (devant être résolu par DNS)
- **Partage** : nom du partage
  - C$, ADMIN$, répertoire

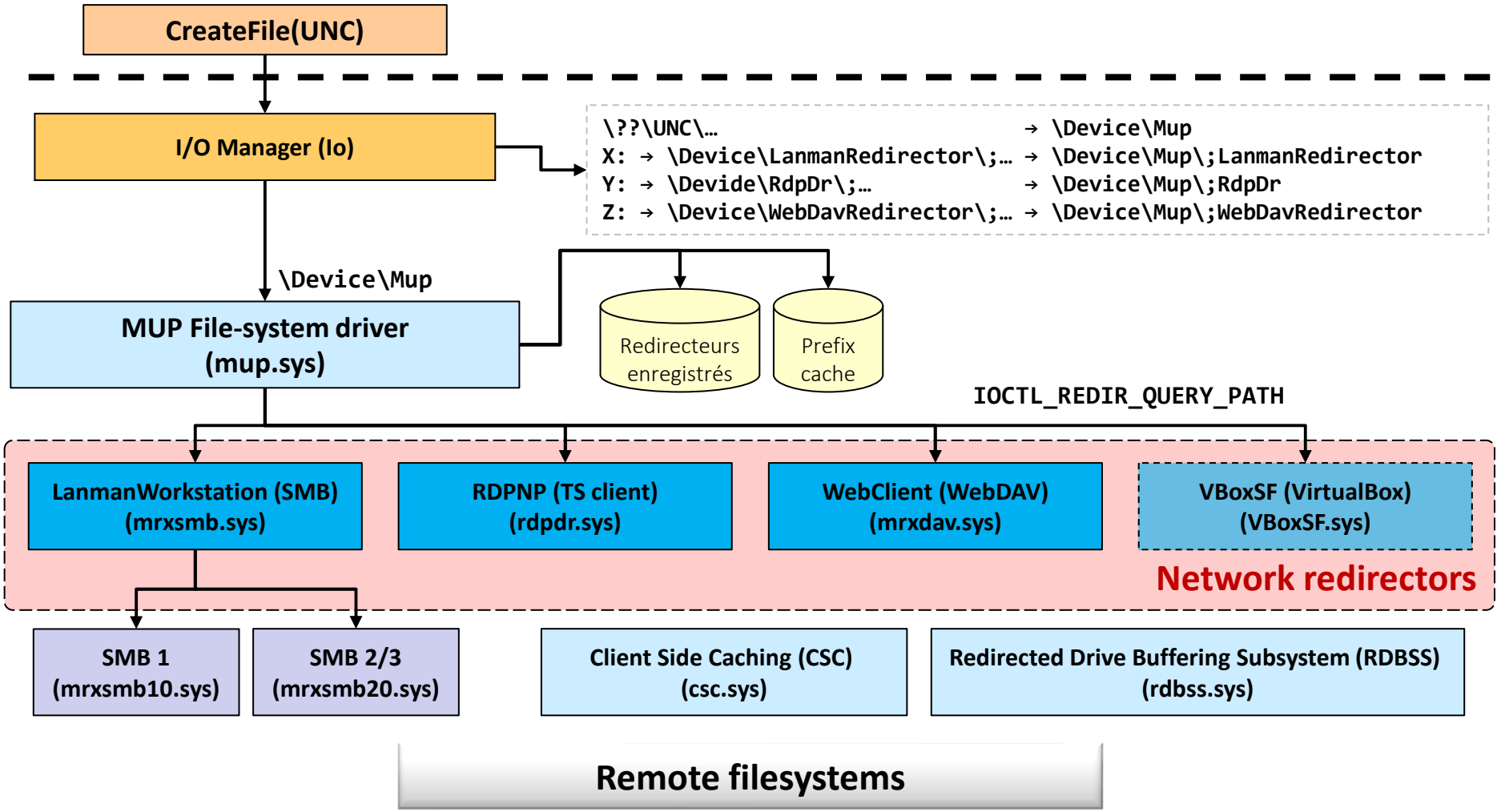
Multiple Provider Router (MPR)

HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\HwOrder



Multiple UNC Provider (MUP)

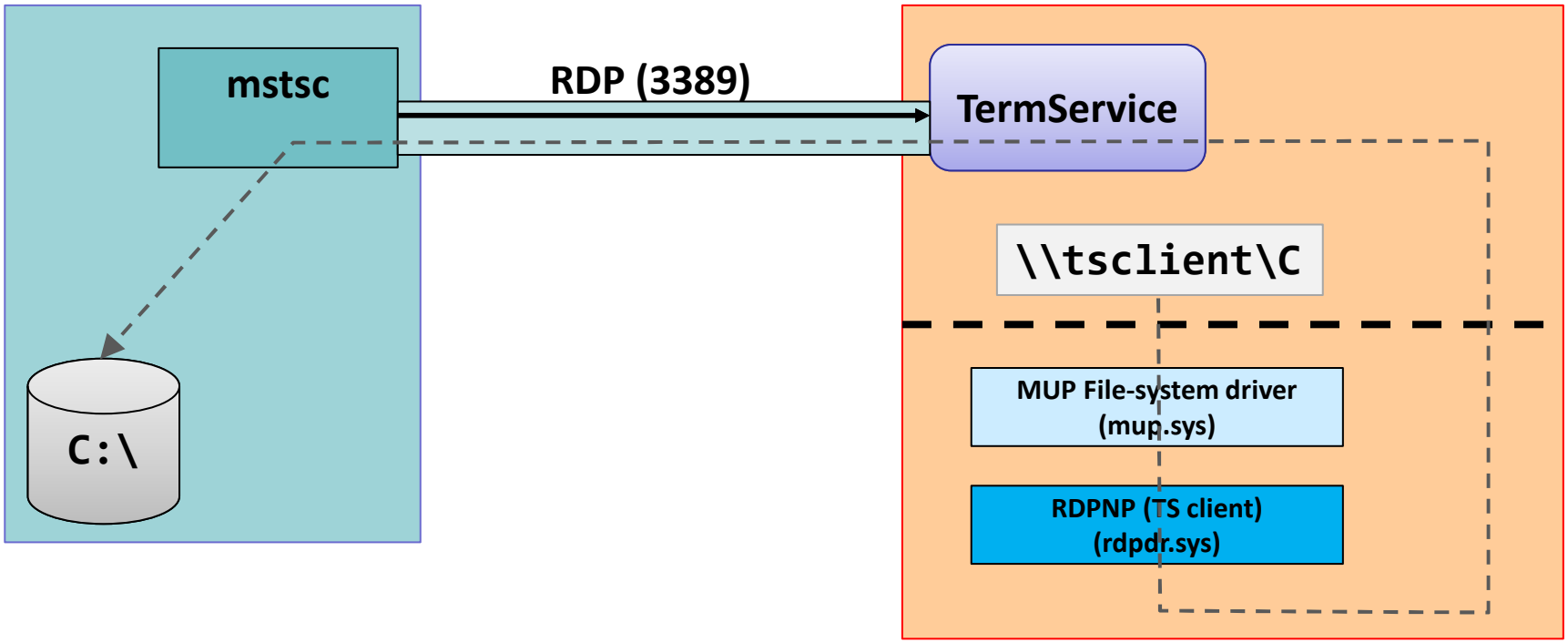
HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order



Redirecteur RDPNP (TS client)

- Utilisé par le service Terminal Services pour l'accès aux ressources de type disque du client
- Exemples :
  - \\tsclient\D

Redirecteur RDPNP (TS client)



Redirecteur WebClient (WebDAV)

- Permet l'accès à des fichiers via HTTP(S) et les extensions WebDAV (COPY, MOVE, LOCK, UNLOCK, PROPFIND, PROPPATCH et MKCOL)
- Exemples :
  - http(s)://server/share/ → \\server\share\
  - \\server@SSL\
  - \\server@Port\
  - \\server\ → \\server\DavWWWRoot\
  - net use z: https://live.sysinternals.com/tools

Redirecteur LanmanWorkstation (SMB)

- Permet l'accès à un système de fichiers via le protocole SMB
- Exemple :
  - net use \\localhost\c$

Redirecteur Plan 9 Network

- Apparu avec Windows 10 1903
- Basé sur le protocole « Plan 9 Filesystem »
- Permet l'échange de fichiers entre Windows et des conteneurs Linux WSL
- Repose sur les sockets Windows de type `AF_UNIX` et un serveur 9P dans les instances WSL

- Utilise le partage `\\wsl$`

Autres redirecteurs non Microsoft

- VirtualBox (`\\vboxsrv`)
- WinFsp (*Windows File System Proxy*)
  - SSHFS-Win (*SSHFS for Windows*)
    - `\\sshfs\[LOCUSER=]REMUSER@HOST[!PORT][\PATH]`
    - `\\sshfs.r\[LOCUSER=]REMUSER@HOST[!PORT][\PATH]`
    - `\\sshfs.k\[LOCUSER=]REMUSER@HOST[!PORT][\PATH]`
    - `\\sshfs.kr\[LOCUSER=]REMUSER@HOST[!PORT][\PATH]`

SMB

(*Server Message Block*)

Historique et contexte de SMB

- Protocole de **partage de fichiers** apparu dans les années 80 où de nombreuses implémentations ont coexisté (DOS, draft-leach-cifs-v1-spec-01, Unix, etc.)
- Apparition avec Windows NT 4 d'une évolution baptisée **CIFS** (*Common Internet File System*) (`draft-leach-cifs-v1-spec-01`)
- Nouvelle évolution avec Windows 2000 où le nom CIFS disparaît au profit d'un retour du nom **SMB**
- Refonte complète avec Windows Vista/2008 avec l'apparition de SMB2 puis de SMB3 avec Windows 8/2012
- Supporté maintenant par de nombreux constructeurs ou éditeurs : Apple, EMC, NetApp, Samba, etc.

Évolution de SMB

- Avec Vista, Microsoft a introduit **SMB2** (SMB 2e génération)
- **SMB2** est désormais décliné en 3 familles (*Dialect Family*) et 5 versions de dialectes (*Dialect Revisions*)

Famille	Révision	Code	Système
SMB 2.0.2	SMB 2.0.2	0x0202	Windows Vista SP1 / 2008
SMB 2.1	SMB 2.1	0x0210	Windows 7 / 2008 R2
SMB 3.X	SMB 3.0	0x0300	Windows 8 / 2012
	SMB 3.0.2	0x0302	Windows 8.1 / 2012 R2
	SMB 3.1.1	0x0311	Windows 10 / 2016

Apports de SMB2

- SMB2 apporte de nombreux changements :
  - Signature toujours supportée (mais pas imposée)
  - Abandon du transport par NetBios
  - Changement complet du format après la phase de validation
  - Performance (*pipeline* des commandes)
  - Sécurité (signature sur 16 octets)
  - Simplification (passage de 100 à ≈20 commandes)
  - Support des liens symboliques, des *handles* persistants

SMB 3.0 (Windows 8 / 2012)
SMB 3.0.2 (Windows 8.1 / 2012R2)

- SMB 3.0
  - Chiffrement via AES-128-CCM (confidentialité et signature)
  - Signature avec AES-128-CMAC
  - Négociation sécurisée des dialectes entre v2/v3 (mais pas entre v2/v3 et v1)
  - Désactivation possible de SMB1
- SMB 3.02 :
  - amélioration des opérations de connexion et d' I/O, partage de disque VHD
- Administration avec PowerShell

SMB 3.1.1 (Windows 10)

- Amélioration de la négociation :
  - *Extensible Negociation*
  - *Negotiate Contexts*
- *Pre-Authentication Intregrity*
- *SMB Encryption Improvements*
  - Support d'AES-128-GCM
- Possibilité pour le client à forcer le chiffrement
- *Cluster Dialect Fencing* et *Cluster Failover* v2

Désactivation de SMB1

- SMB1 est maintenant considéré comme obsolète et dangereux et doit être désactivé

https://support.microsoft.com/fr-fr/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
https://learn.microsoft.com/fr-fr/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

- Commandes :
  - `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`
  - `Set-SmbServerConfiguration -EnableSMB1Protocol $false`
  - `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
    - `SMB1 -> 0`
  - `sc.exe config lanmanworkstation depend= browser/mrxsmb20/nsi`
  - `sc.exe config mrxsmb10 start= disabled`

- SMB1 est désactivé par défaut depuis Windows 10 1709

Principales opérations SMB

- Négociation génération/dialecte/révision
- Authentification de l'utilisateur
- Connexion à un partage SMB (*tree connect*)
- Accès aux ressources du partage :
  - Fichiers
  - Répertoires
- Déconnexion

- Diverses opérations (Lock, IOCTL, Echo, Query info, etc.)

Commandes SMB2

- **Négociation du dialecte :**
  - NEGOTIATE
- **Authentification de l'utilisateur :**
  - SESSION_SETUP, LOGOFF
- **Connexion à un partage :**
  - TREE_CONNECT, TREE_DISCONNECT
- **Accès aux fichiers :**
  - CREATE, CLOSE, READ, WRITE, LOCK, IOCTL, QUERY_INFO, SET_INFO, FLUSH, CANCEL
- **Accès aux répertoires :**
  - QUERY_DIRECTORY, CHANGE_NOTIFY
- **Requête d'état :**
  - ECHO

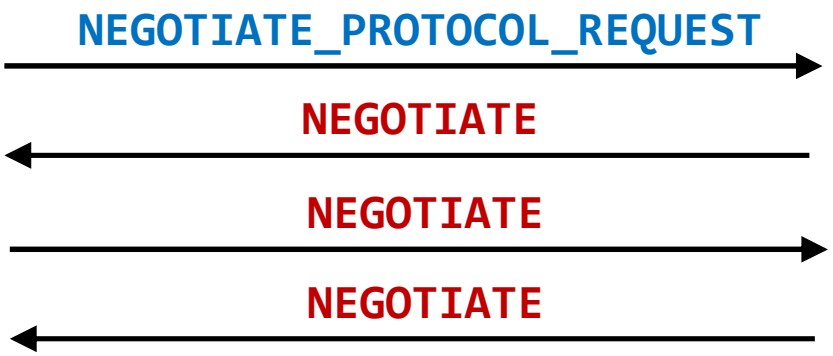
Échanges classiques

Négociation du dialecte

Négociation des dialectes :

- PC NETWORK PROGRAM 1.0
- LANMAN1.0
- Windows for Workgroups 3.1a
- LM1.2X002
- LANMAN21
- NT LM 0.12

SMB1



1re négociation (dialectes textes) :

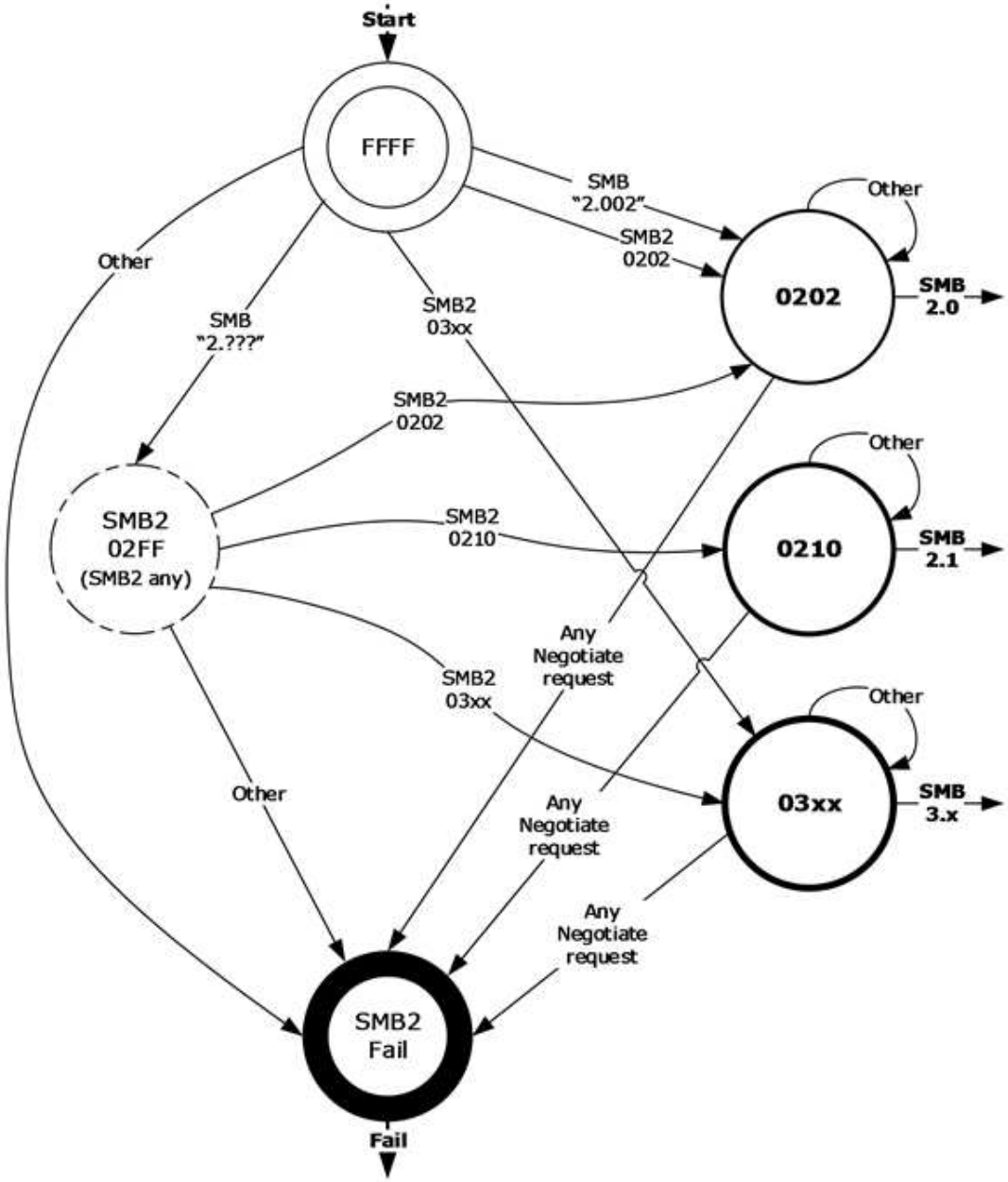
- SMB1 + SMB2.002 et SMB 2.???

2e négociation (dialectes binaires) :

- 0x0202
- 0x0210
- 0x0300
- 0x0202
- 0x3011

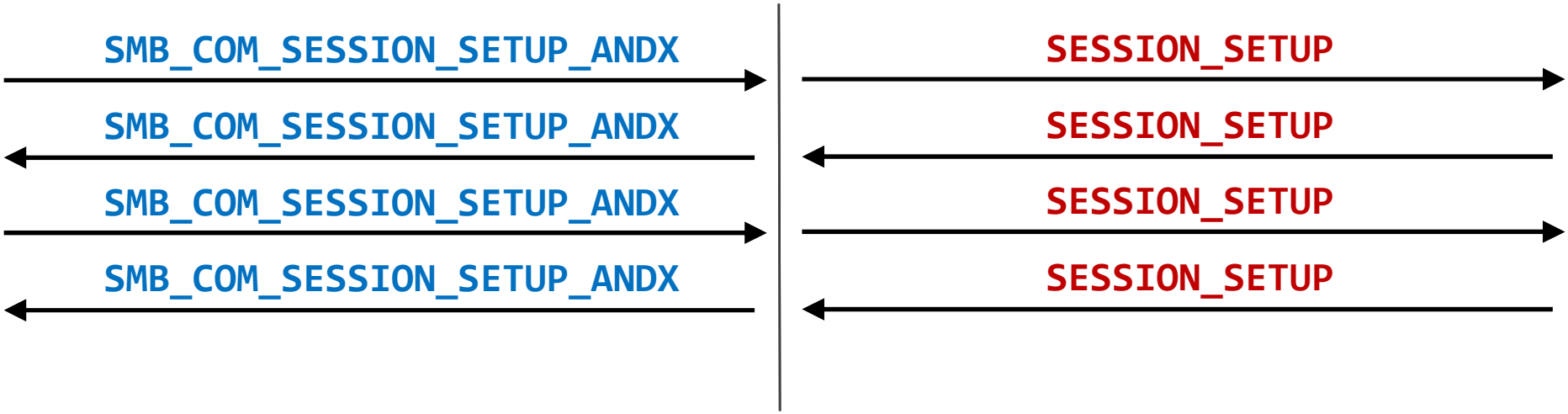
SMB2/3

SMB2 : négociation du dialecte



Échanges classiques

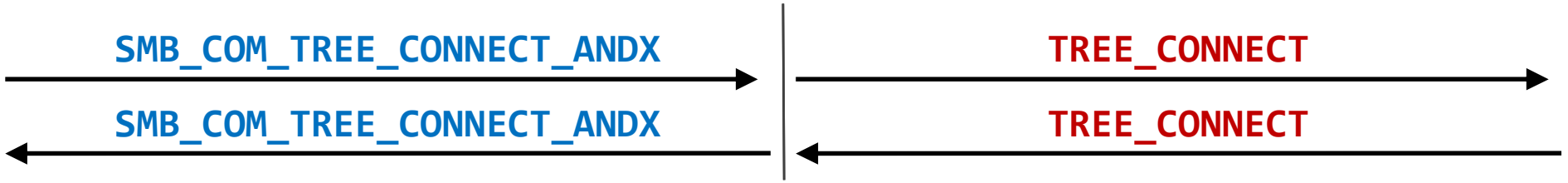
Authentification de l'utilisateur



- L'authentification repose sur GSS-API et met en œuvre le SSP SPNEGO (NTLM ou Kerberos). Voir cours sur l'authentification pour les détails
- Cette étape permet aux participants de générer une clé de session (*session key*) partagée entre les deux parties

Échanges classiques

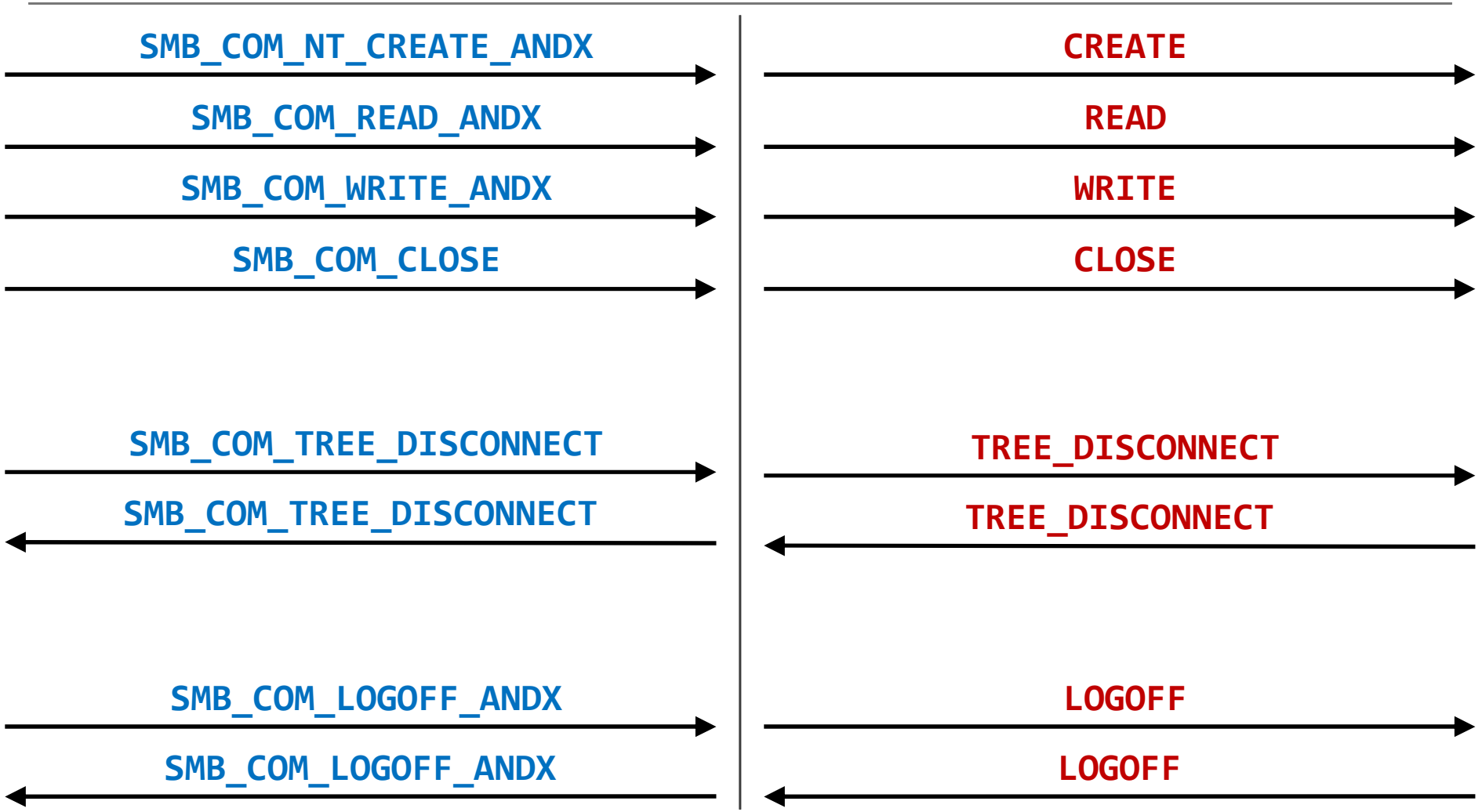
Connexion à un partage



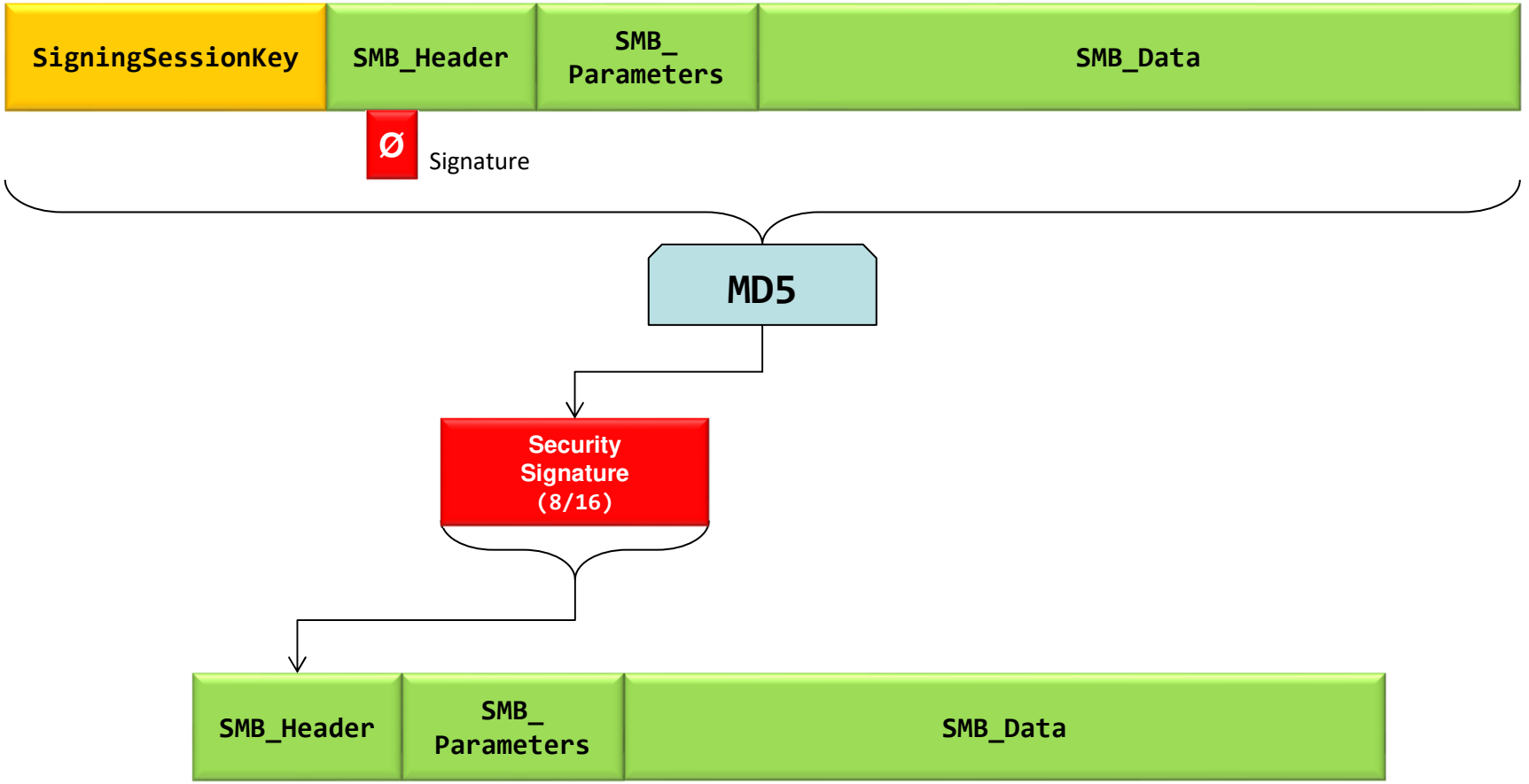
- L'opération de connexion à un partage s'appelle ***tree connect***
- Un partage peut-être :
  - Défini manuellement depuis un répertoire
  - Créé automatiquement (partage administratif) :
    - Racine des disques (C$, D$, etc.)
    - %SYSTEMROOT% (ADMIN$)
  - Créé pour l'impression
  - Dédié au mécanisme des canaux nommés (IPC$)
- Chaque partage possède un descripteur de sécurité

Échanges classiques

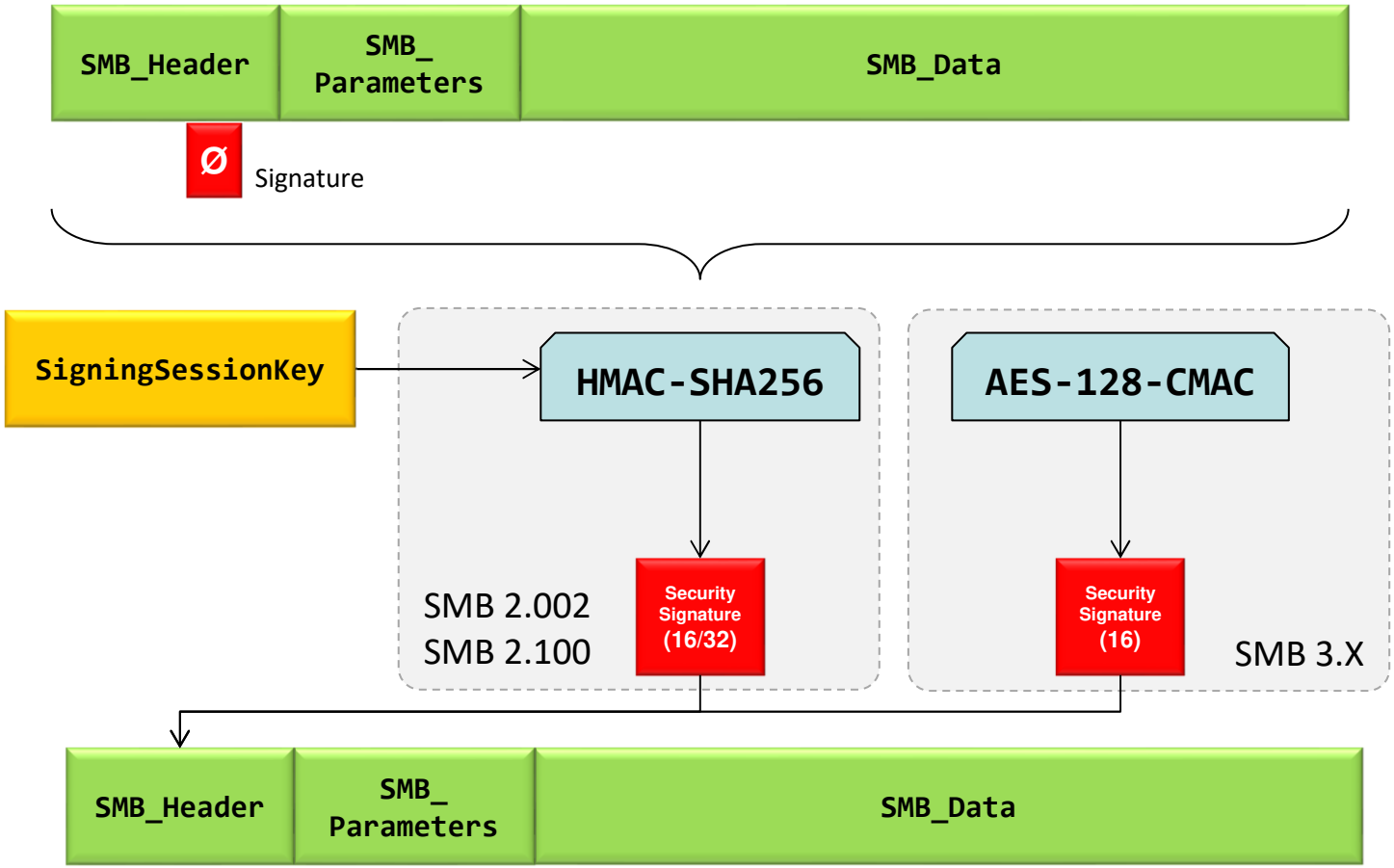
Opérations sur les fichiers



Signatures SMB1



Signatures SMB2



Configuration de la signature SMB1

Client signing state	Server signing state			
	Disabled (XP/2003)	**Declined** (Vista/2008)	Enabled	Required
Disabled (XP/2003)	Unsigned	Unsigned	Unsigned	Blocked
Declined (Vista/2008)	Unsigned	Unsigned	Unsigned	Signed
Enabled	Unsigned	Unsigned	Signed	Signed
Required	Blocked	Signed	Signed	Signed

Configuration de la signature SMB2

Client signing state	Server signing state	
	Not required	Required
Not required	Not signed	Signed
Required	Signed	Signed

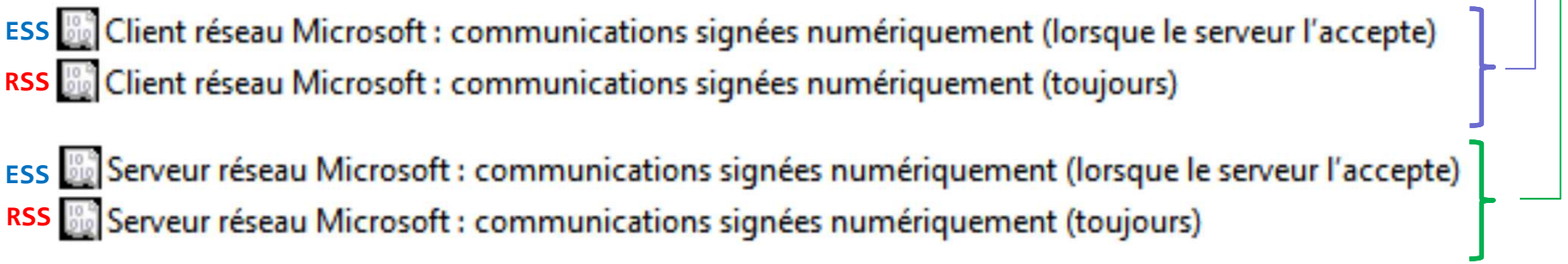
Paramètres de configuration de la signature SMB

Article de référence :
http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx
https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102

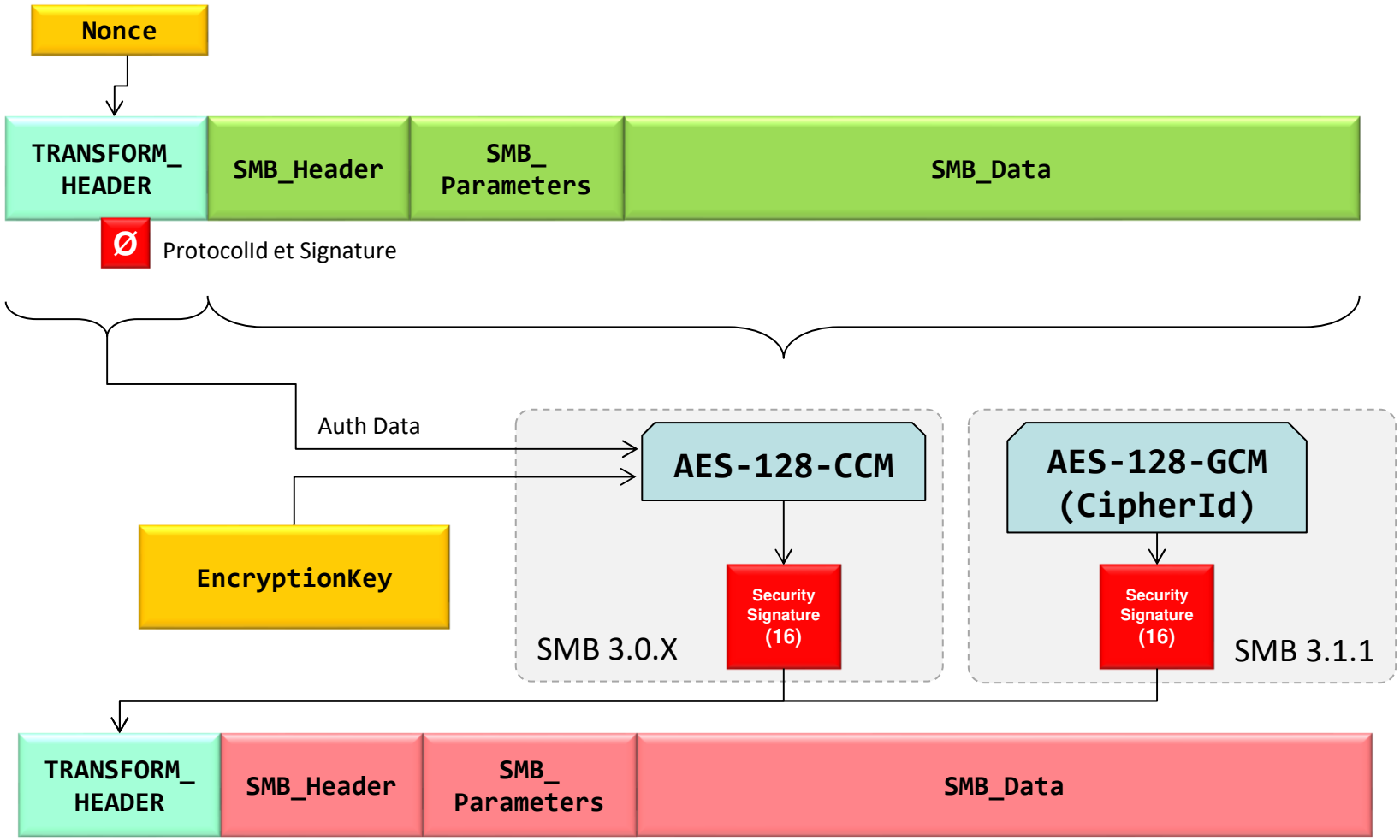
ESS (SMB1 seulement) **RSS**

Paramètres (**`EnableSecuritySignature`** / **`RequireSecuritySignature`**) :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters



Chiffrement SMB3



Paramètres de configuration du chiffrement SMB

- Le chiffrement peut être activé globalement ou pour un partage spécifique
- Le chiffrement peut être obligatoire (par défaut) ou facultatif

- `Set-SmbServerConfiguration –EncryptData $true`
- `Set-SmbShare –Name <sharename> -EncryptData $true`

- `Set-SmbServerConfiguration –RejectUnencryptedAccess $false`

UNC Hardened Access
KB 3000483

- Jusqu'à présent, la configuration côté client de la signature ou du chiffrement était binaire (activée ou désactivée globalement pour le système)
- Le KB 3000483 a introduit *UNC Hardened Access* qui permet aux clients de définir une politique plus fine
- La politique permet d'imposer (et donc d'activer) :
  - La signature : **`RequireIntegrity`**
  - L'authentification mutuelle : **`RequireMutualAuthentication`**
  - Le chiffrement : **`RequirePrivacy`**

Paramètres
UNC Hardened Access

- Software\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths
- [GPO] Ordinateur
  - Modèles d'administration
    - Réseau
      - Fourniseur réseau
        - » Chemins d'accès UNC renforcés (Hardened UNC Paths)
- Exemple :
  - *\SYSVOL → RequireMutualAuthentication=1, RequireIntegrity=1
  - \\FILER → RequirePrivacy=1

- Depuis Windows 10, si aucune politique n'est définie, une politique implicite est mis en œuvre qui permet d'assurer la protection de la récupération des GPO :
  - *\NETLOGON et *\SYSVOL
    - RequireMutualAuthentication=1, RequireIntegrity=1

Partages administratifs (*Administrative shares*)

- Par défaut, le service serveur partage :
  - %SystemRoot% → ADMIN$
  - C: → C$
  - D: → D$
  - …
- Ces partages peuvent être désactivés via les attributs `AutoShareWks` et `AutoShareServer` de la clé :

`HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters`

Compression SMB

- Windows 10 1903 apporte le support de la compression SMB
- Encapsulation dans un en-tête `SMB2 COMPRESSION_TRANSFORM_HEADER`
  - ProtocolId : 0xFC, 'S', 'M', 'B’
  - CompressionAlgorithms :
    - LZNT1
    - LZ77
    - LZ77+Huffman
    - Pattern_V1

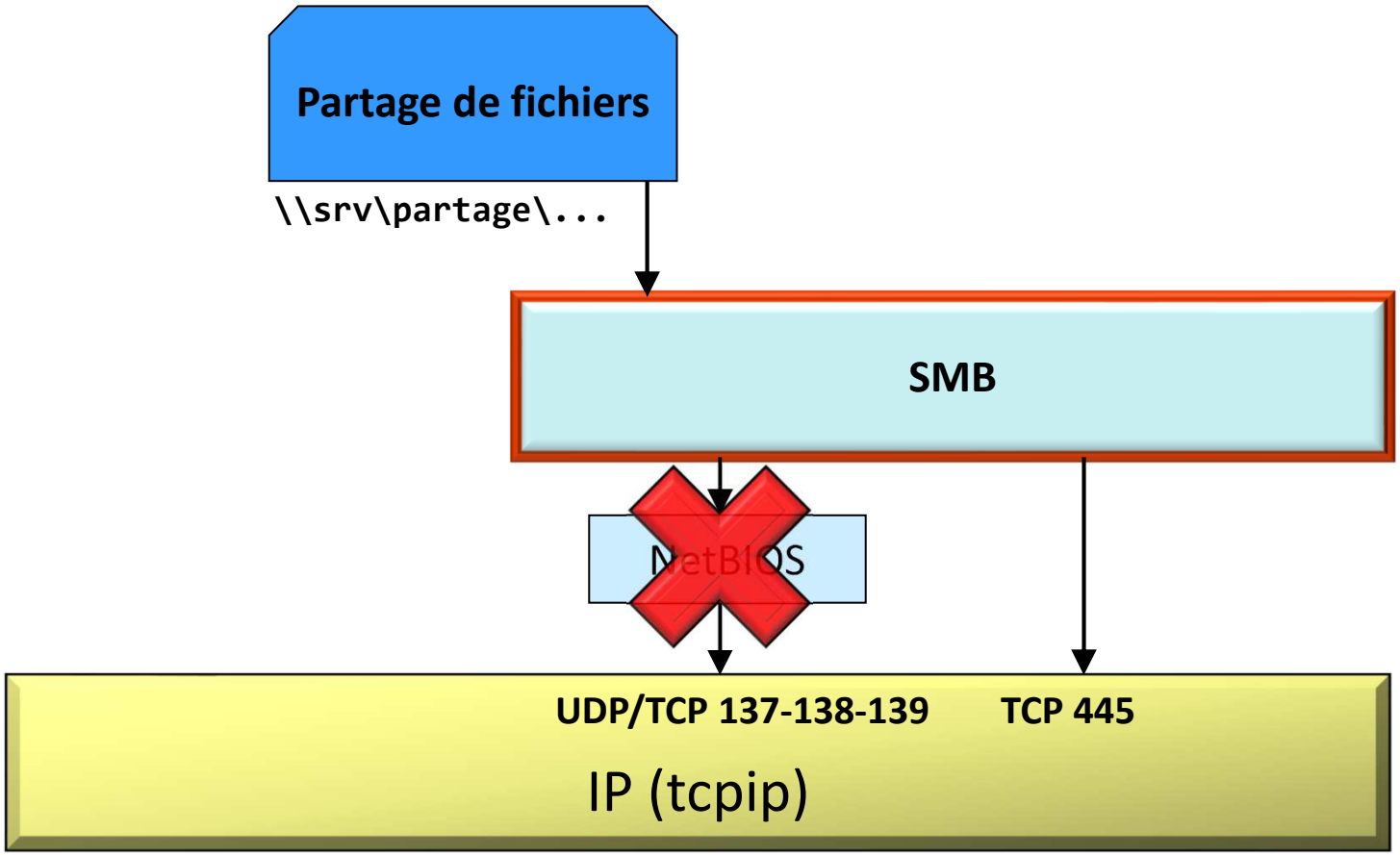
- Windows 10 2004 apporte le support de la compression chainée

Transport de SMB

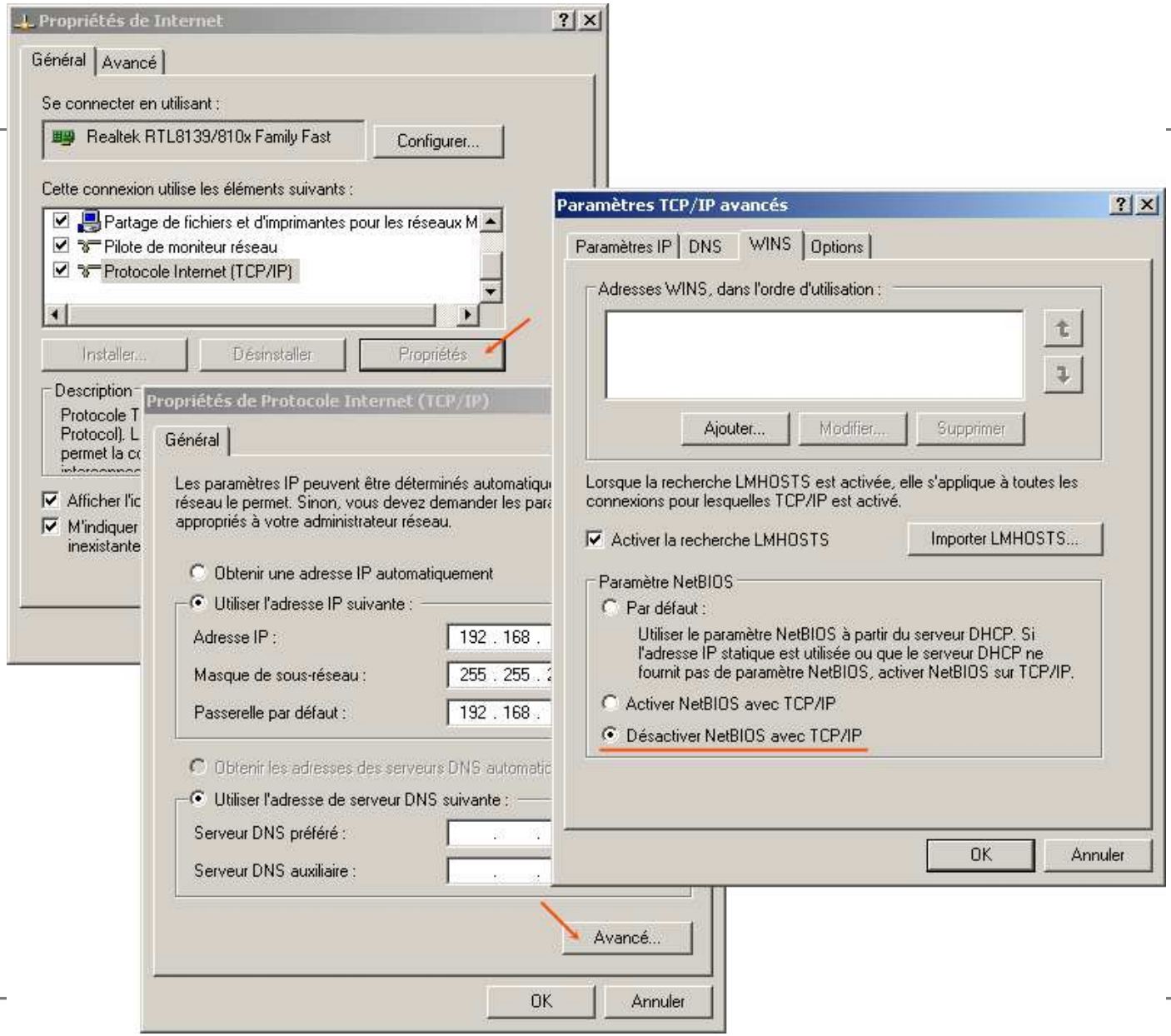
Transport de SMB

- Tout système Windows :
  - NetBIOS Session Service (**TCP 139**)
    - OBSOLÈTE → Doit être désactivé
- À partir de Windows 2000 :
  - *Direct Hosting* (**TCP 445**)
- SMB 3.x :
  - RDMA (*Remote Direct Memory Access*)
- Windows 10 21Hx, Windows 11, Windows Server 2022 :
  - QUIC (**UDP 443**)

IP & SMB


Partage de fichiers
\\srv\partage\...
SMB
NetBIOS
UDP/TCP 137-138-139
TCP 445
IP (tcpip)

Désactiver NetBios sur TCP/IP



Scripts pour désactiver NetBios/TCP sur toutes les interfaces

Visual Basic :

```
Option Explicit
On Error Resume Next

Dim objWMIService
Dim colNetAdapters
Dim objNetAdapter

Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
Set colNetAdapters = objWMIService.ExecQuery("Select * from
  Win32_NetworkAdapterConfiguration where IPEnabled=TRUE")

For Each objNetAdapter in colNetAdapters
    objNetAdapter.SetTcpipNetbios(2)  ' 2 = Disable Netbios
Next
```

PowerShell :

```
$adapters = (Get-WmiObject Win32_NetworkAdapterConfiguration)
Foreach ($adapter in $adapters)
{
  $adapter.SetTcpipNetbios(2)
}
```

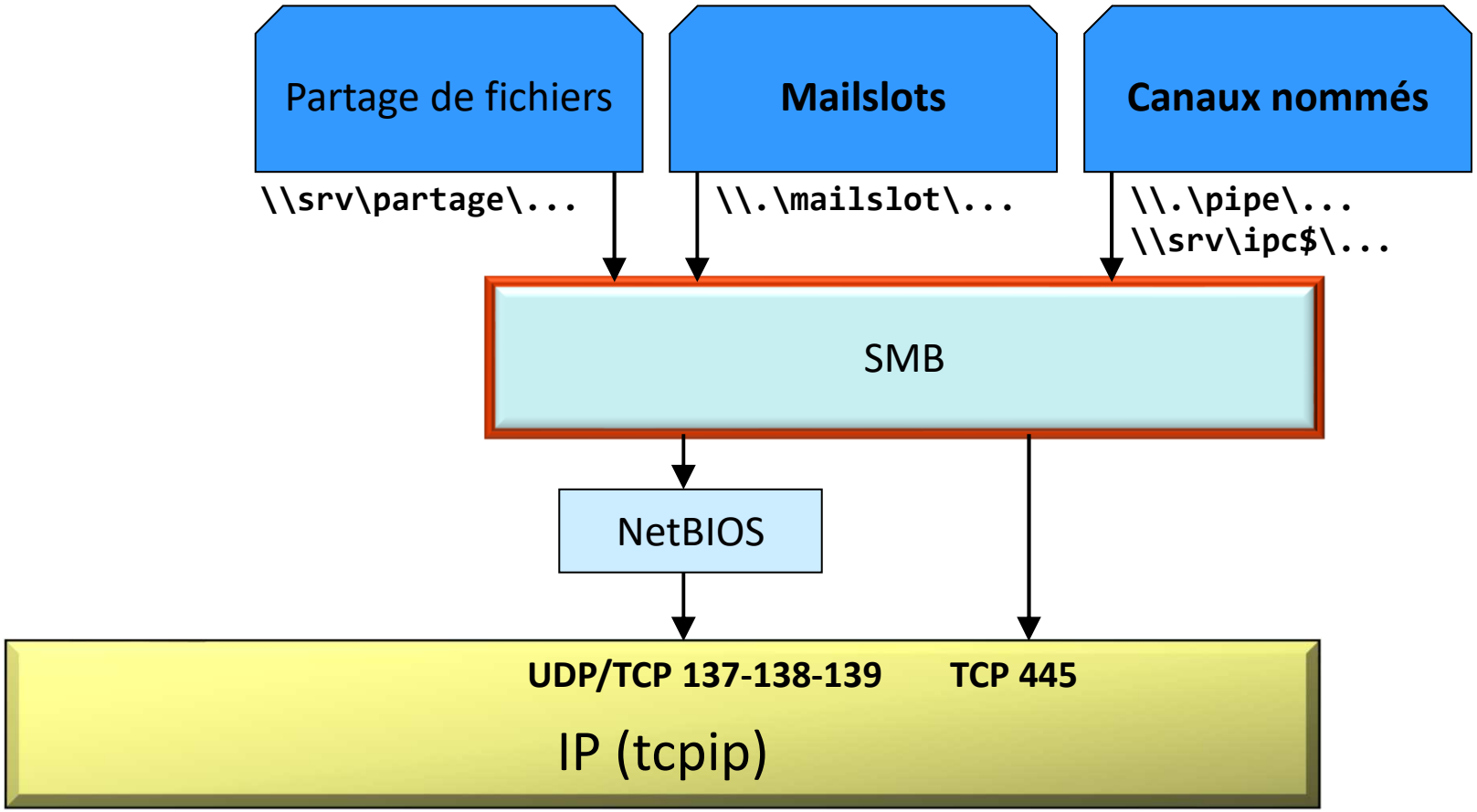
Communications IPC
Mailslots

- Permet une communication asynchrone entre deux machines via l'envoi de message dont la taille est limitée à 424 octets
- Portée des messages :
  - Local : **\\.\mailslot\[path\]name**
  - Machine : **\\ComputerName\mailslot\[path\]name**
  - Groupe de machines : **\\DomainName\mailslot\[path\]name**
  - Le sous-réseau : ***\mailslot\[path\]name**
- Les messages sont envoyés dans un paquet SMB via un paquet *NetBIOS Datagram Service* (UDP 138)

Communications IPC
Pipes

- **anonymes** : permet une communication entre deux processus sur une même machine
- **nommés** (*named pipe*) : permet une communication entre processus éventuellement sur deux machines différentes
  - Le partage SMB est **`IPC$`**
  - Chemin SMB : (insensible à la casse) **`\\ServerName\pipe\PipeName`**
  - Le canal nommé possède un descripteur de sécurité
  - Utilisation possible d'alias : **`HKLM\SYSTEM\CurrentControlSet\Services\Npfs\Aliases`**

Mailslots et Named Pipes



Remote Procedure Call (RPC)

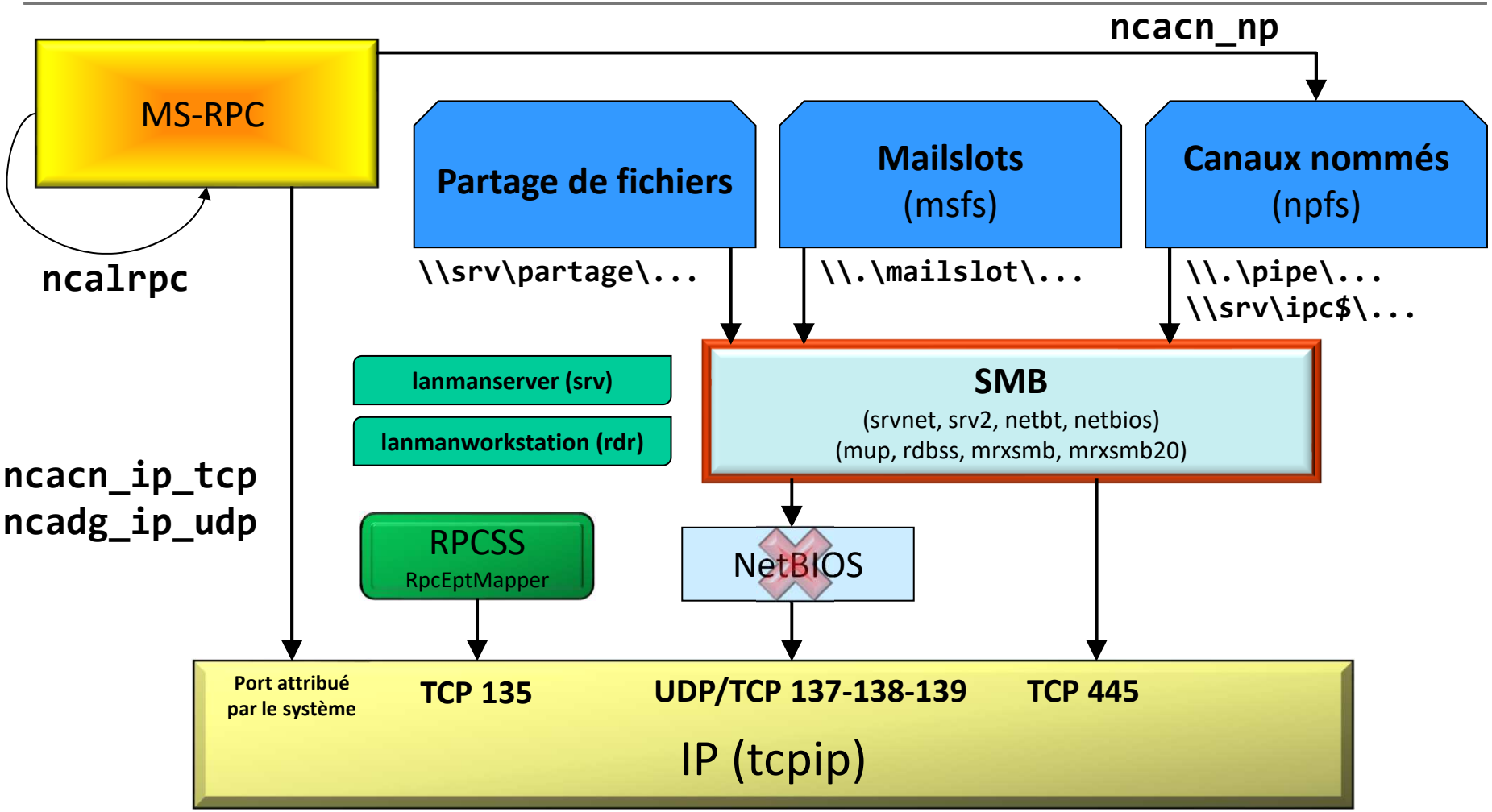
- Mécanisme de gestion d'un modèle client/serveur réparti : fonctions exportées par un serveur et appelées par un client
- La gestion des communications réseau est effectuée par le système d'exploitation
- Chaque interface RPC est identifiée par :
  - un UUID (*Universal Unique Identifier*) de type GUID
  - un numéro de version
- Les fonctions sont ensuite identifiées par un numéro d'*opcode*

Principaux protocoles réseau RPC

- **`ncacn_ip_tcp`** : protocole TCP
- **`ncadg_ip_udp`** : protocole UDP
- **`ncacn_np`** : canal nommé
- **`ncacn_http`** : HTTP via IIS
- **`ncalrpc`** : *Local Inter-Process Communication port* (LPC)

- **LPC** : port de communication mis en œuvre par le noyau et permettant une communication rapide entre deux processus au sein d'une même machine
- Remplacé par **ALPC** depuis Vista (*Advanced LPC*)

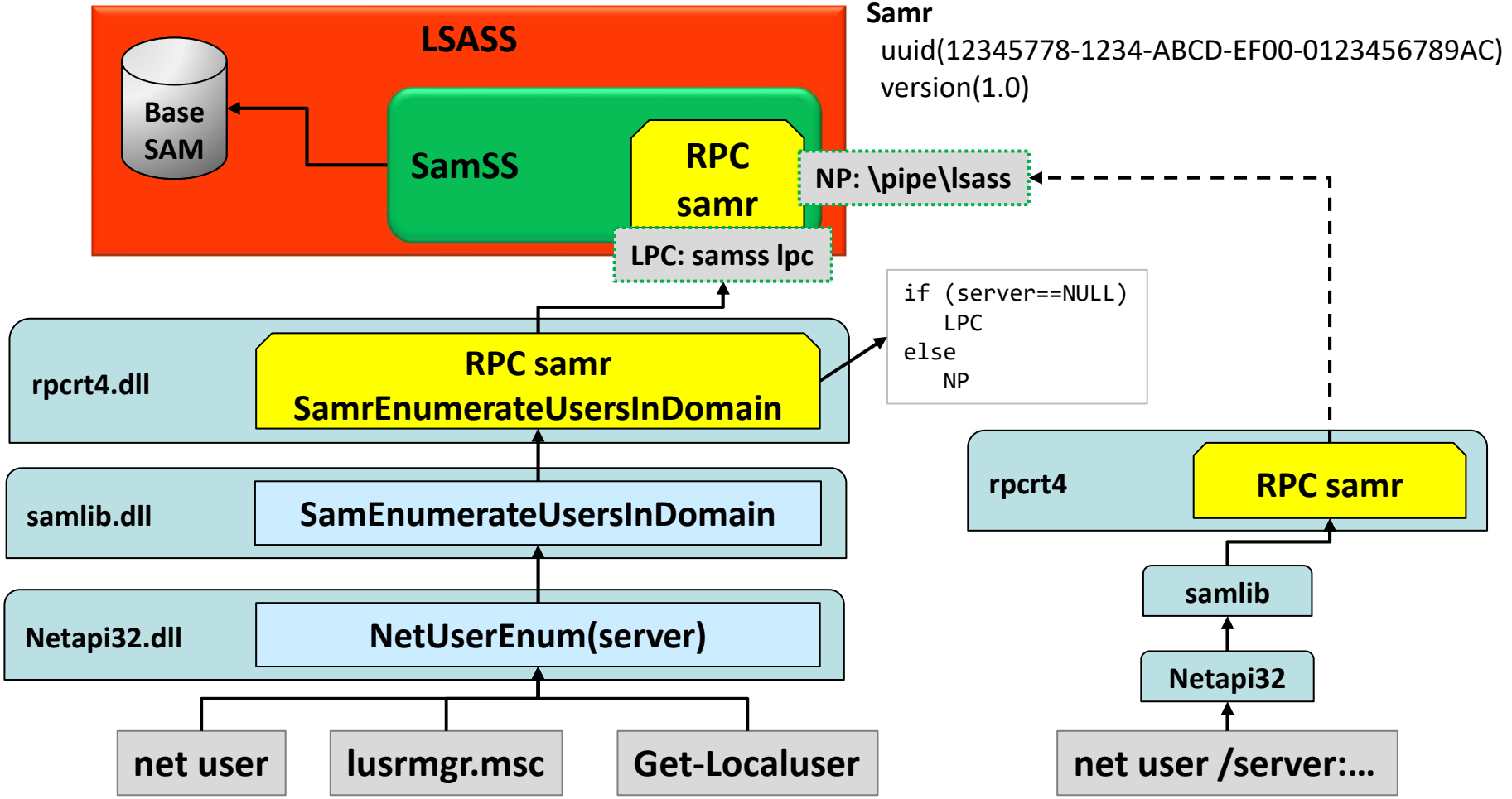
RPC


ncacn_np
MS-RPC
ncalrpc
Partage de fichiers
Mailslots
(msfs)
Canaux nommés
(npfs)
\\srv\partage\...
\\.\mailslot\...
\\.\pipe\...
\\srv\ipc$\...
lanmanserver (srv)
lanmanworkstation (rdr)
SMB
(srvnet, srv2, netbt, netbios)
(mup, rdbss, mrxsmb, mrxsmb20)
ncacn_ip_tcp
ncadg_ip_udp
RPCSS
RpcEptMapper
NetBIOS
Port attribué
par le système
TCP 135
UDP/TCP 137-138-139
TCP 445
IP (tcpip)

Services RPC Microsoft sur canaux nommés

- De nombreuses interfaces RPC du système sont accessibles via un canal nommé (`\pipe\nom_canal`) :
  - **`atsvc`** : planificateur de tâches
  - **`browser`** : explorateur d'ordinateur (*browser*)
  - **`epmapper`** : *Endpoint Mapper*
  - **`eventlog`** : journaux d'évènements
  - **`lsarpc`** : politique LSA
  - **`ntsvcs`** : *plug and play* (plugplay sous Vista)
  - **`samr`** : base SAM
  - **`spoolss`** : imprimantes
  - **`srvsvc`** : service serveur (*lanmanserver*)
  - **`svcctl`** : gestionnaire de services (SCM)
  - **`winreg`** : accès distant au Registre
  - **`wkssvc`** : service client (*lanmanworkstation*)

Mise en œuvre de RPC



Autres protocoles réseau d'administration à distance

- **RDP** : Bureau à distance (*Terminal Service*)
  - tcp/3389 et udp/3389
- **WinRM** : *Remote Shell*, *Remote PowerShell*
  - tcp/5985 et tcp/5986 (TLS)
- **SSH** : *Built-in OpenSSH Server* (Windows 10 1809)
  - tcp/22