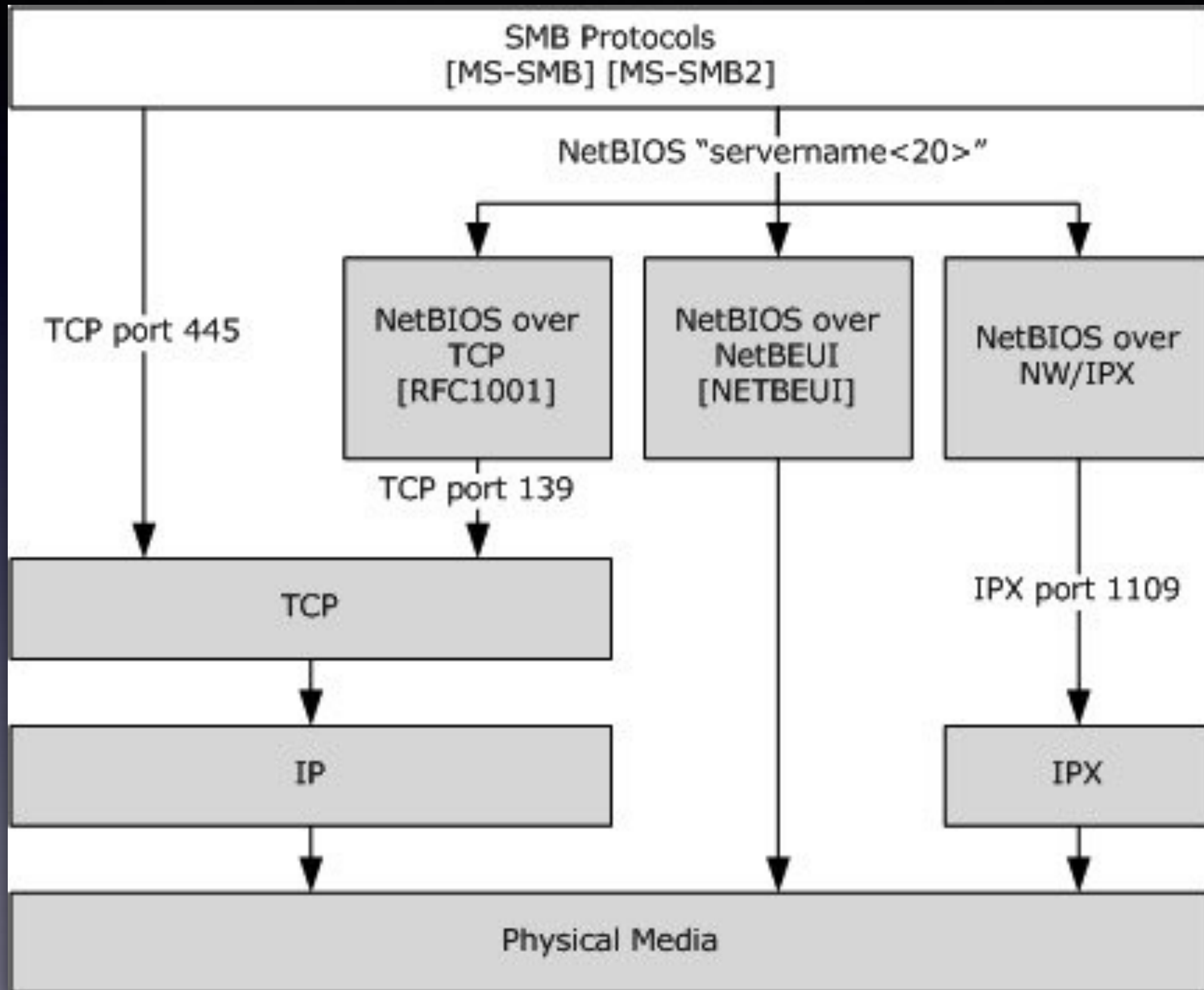


# Sessions SMB



# Sessions nulles

- Connexion TCP au port 445 ou 139
- Etablissement d'une session SMB avec identifiant et mot de passe vides
  - Seule étape d'authentification
- Connexion au partage IPC\$
- Ouverture d'un tube nommé
- Association à une interface RPC
- Chaque interface RPC (remote procedure call) est identifiée par un identifiant (UUID) (Universal Unique Identifier)
- Lancement de requêtes RPC