

Utilisation de données distantes

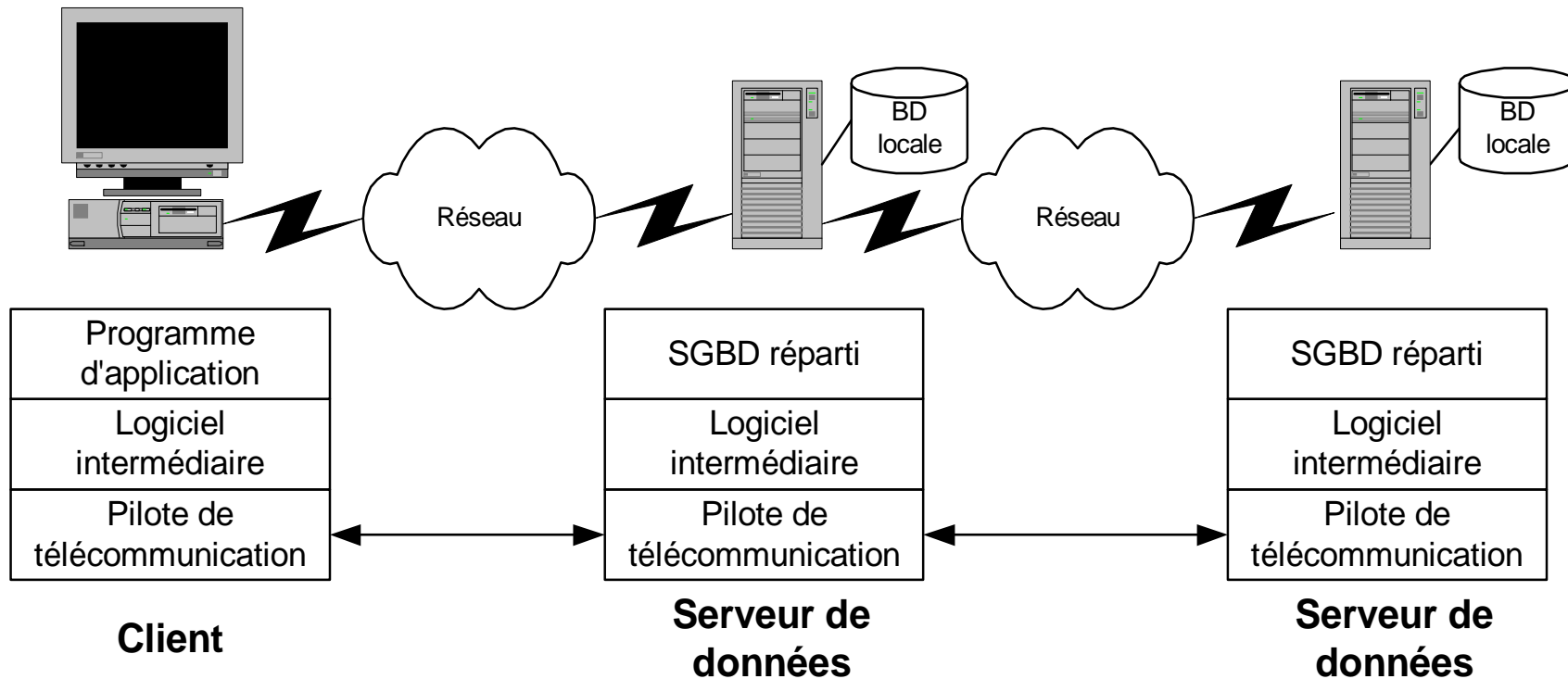
Force probante des travaux de l'expert

Prof. F. Castanié
Expert près la Cour d'Appel de Toulouse

Problématique des données distantes :

- ✓ *Serveurs distants (sic)*
- ✓ *Serveurs répartis: Grille, Cloud Computing, ...*
- ✓ *Base de données Réparties ou Distribuées avec **SGBDR**
ou **D***
- ✓ *Hébergements dynamiques des BD : réallocation des
hébergeurs, fragmentation des BD, ...*

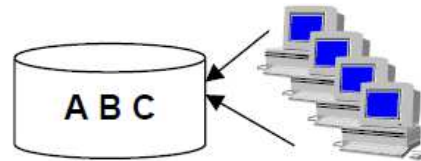
Base de données distribuées



Grande multiplicité de topologies de BDR ou D, en croissance constante.

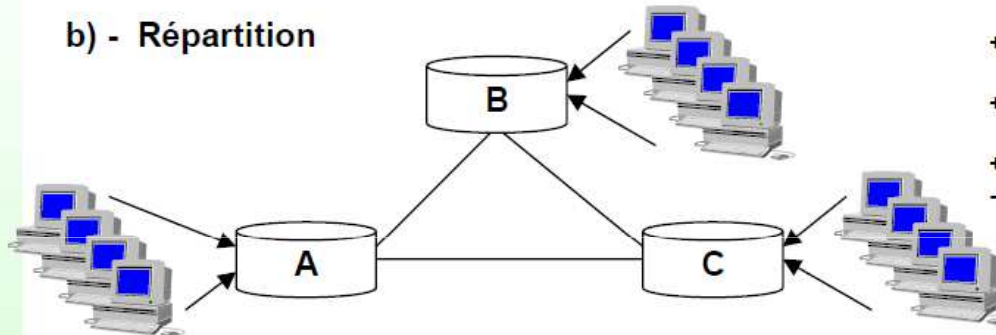
Exemples de topologies de BDR ou D

a) - Cas centralisé



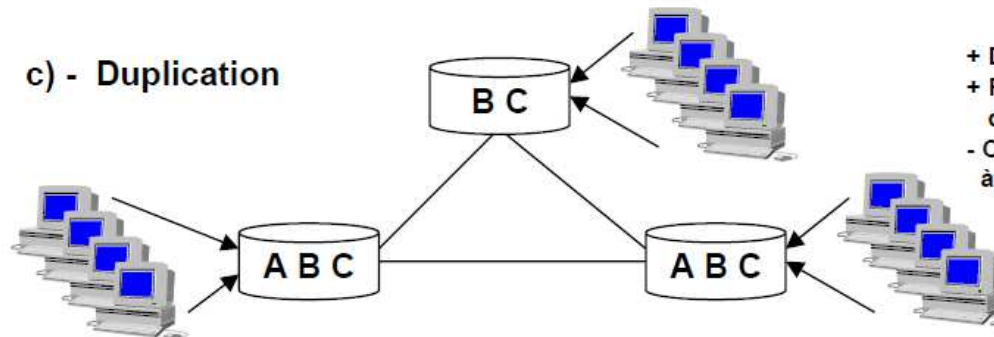
- + Égalité des accès
- + Facilité de gestion
- Contention sur la BD

b) - Répartition



- + Rapidité d'accès au données locales
- + Autonomie locale de chaque site
- + Accès possible aux autres sites
- Gestion globale de la BD

c) - Duplication



- + Disponibilité des données
- + Rapidité d'accès aux données locales
- Coordination des mises à jour

Typologie des problèmes

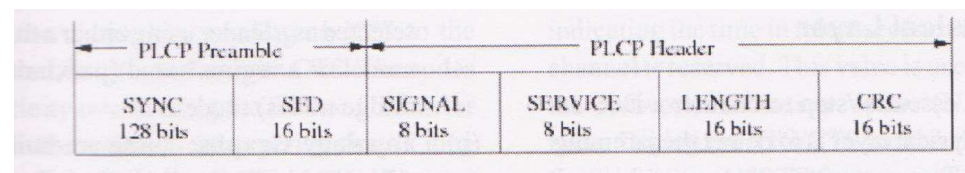
- ✓ *Authentification de la BD : notion d'annuaire intègre*
- ✓ *Identification et/ou localisation du Serveur
(hétérogénéité de réglementations **internationales**)*
- ✓ *Intégrité des canaux de communication*
 - ❑ *Types de réseaux : privés, avec segments IP, MANETs, satellites, ...*
 - ❑ *Niveaux d'attaques : PHY, MAC, Réseau*

Typologie des attaques

- ✓ *Intentionnelles ou non*
- ✓ *Niveau technique de l'attaquant*
- ✓ *Moyens techniques de l'attaquant et ses accès*

Cibles

- ✓ *Authentification des Serveurs : 'spoofing'; etc.*
- ✓ *Détournement de paquets (black holes, wormholes, ...)*
- ✓ *Sur le routage (ex: Réseaux MANETs)*
- ✓ ...



Niveau des attaques (Ex: IEEE 802.11)

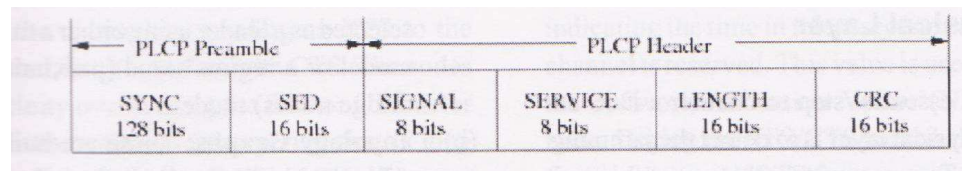
✓ *Couche PHY*

- *Segments radio (WiFi, WiMax, ...)*
- *Tapping sur lignes filaires*

✓ *Couche MAC*

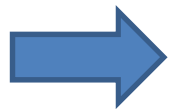
✓ *Couches Réseau*

➔ *Refus de Service (DoS)*



Existence de mécanismes de protection des données

- ✓ *Tunnels (SSH, etc.) et encapsulations*
- ✓ *Différents niveaux de chiffrage*
- ✓ *Sécurisation des annuaires (Ex: LDAP, ...)*



Impossibilité d'affirmation absolue d'intégrité

Conclusions

- ✓ *Existence de multiples possibilités de niveaux d'attaques*
- ✓ *Fragilité plus ou moins grande selon le type de connections (en particulier Radio)*
- ✓ *Impossibilité actuelle de garantir l'authenticité et l'intégrité absolues des données distantes*
- ✓ *Possibilité d'évaluer la probabilité d'authenticité et d'intégrité des données*
- ✓ *... pédagogie en regard des interlocuteurs juridiques*

Bibliographie succincte

- ✓ R. Santanam, et al. , « *Cyber Security, Cyber Crime and Cyber Forensics* » Information Science Reference, 2011
- ✓ T. Ebrahimi et al. « *Cryptographie et sécurité des systèmes et réseaux* » Hermès Lavoisier, Traité IC2 2005
- ✓ ... et plusieurs autres références du même traité IC2