Architectures de registre avancées
&
Opérations de registre fiable, robuste et résiliente

Rappels sur les Registres

Qu'est-ce qu'un registre de ccTLD

- Publie une ou plusieurs zones (TLD / SLD)
- Gère les délégations
- Publies des informations publiques (whois)
- Peut percevoir un montant pour effectuer ces opérations.

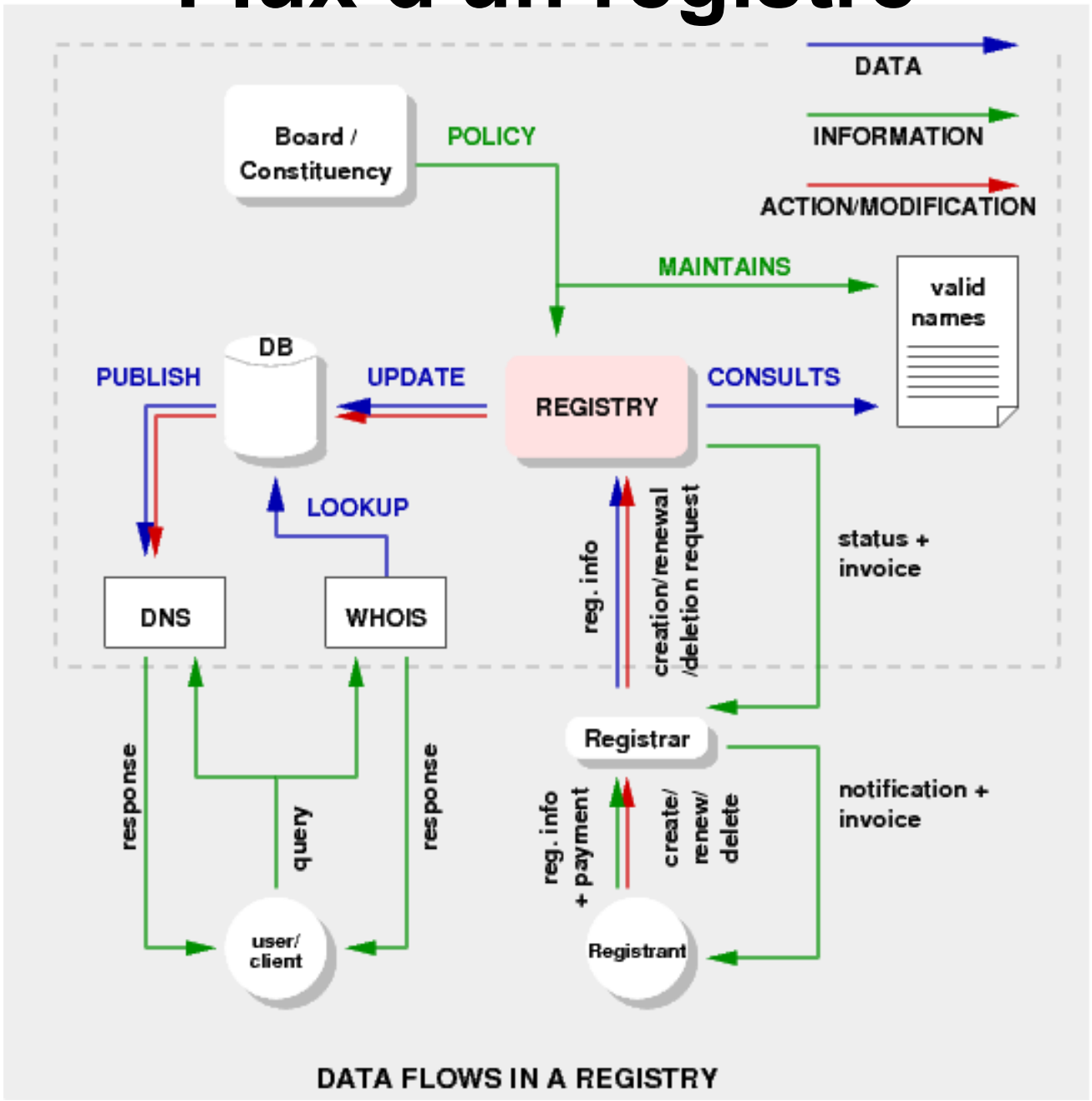
Flux de données

- En entrée
  - Demande d'enregistrement de nom
  - Demande de création/suppresion/modification de noms de domaine
  - Ajout de serveur de noms (nom + IP)
  - Informations administratives (dépositaire, contact technique, contact de facturation, ...)

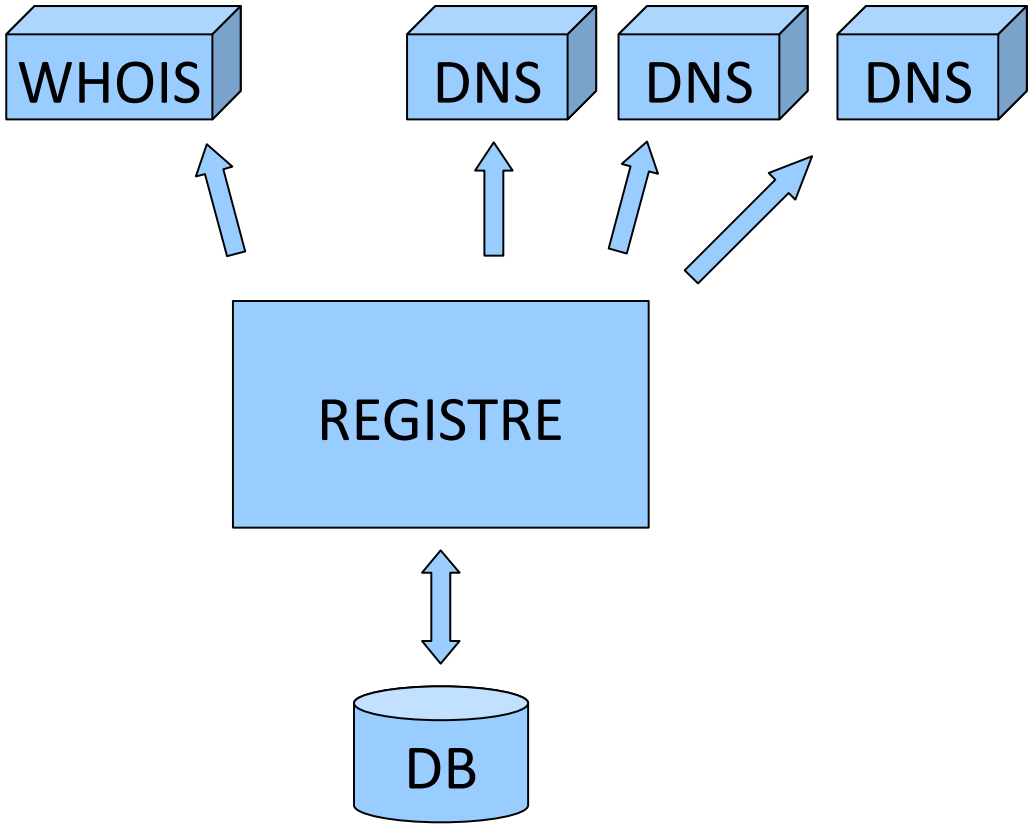
Flux de données

- En sortie:
  - Réponse aux requêtes DNS
  - Zones avec délégation (publication)
  - Enregistrements de glu (NS faisant partie de la zone déléguée)
  - Publication du WHOIS

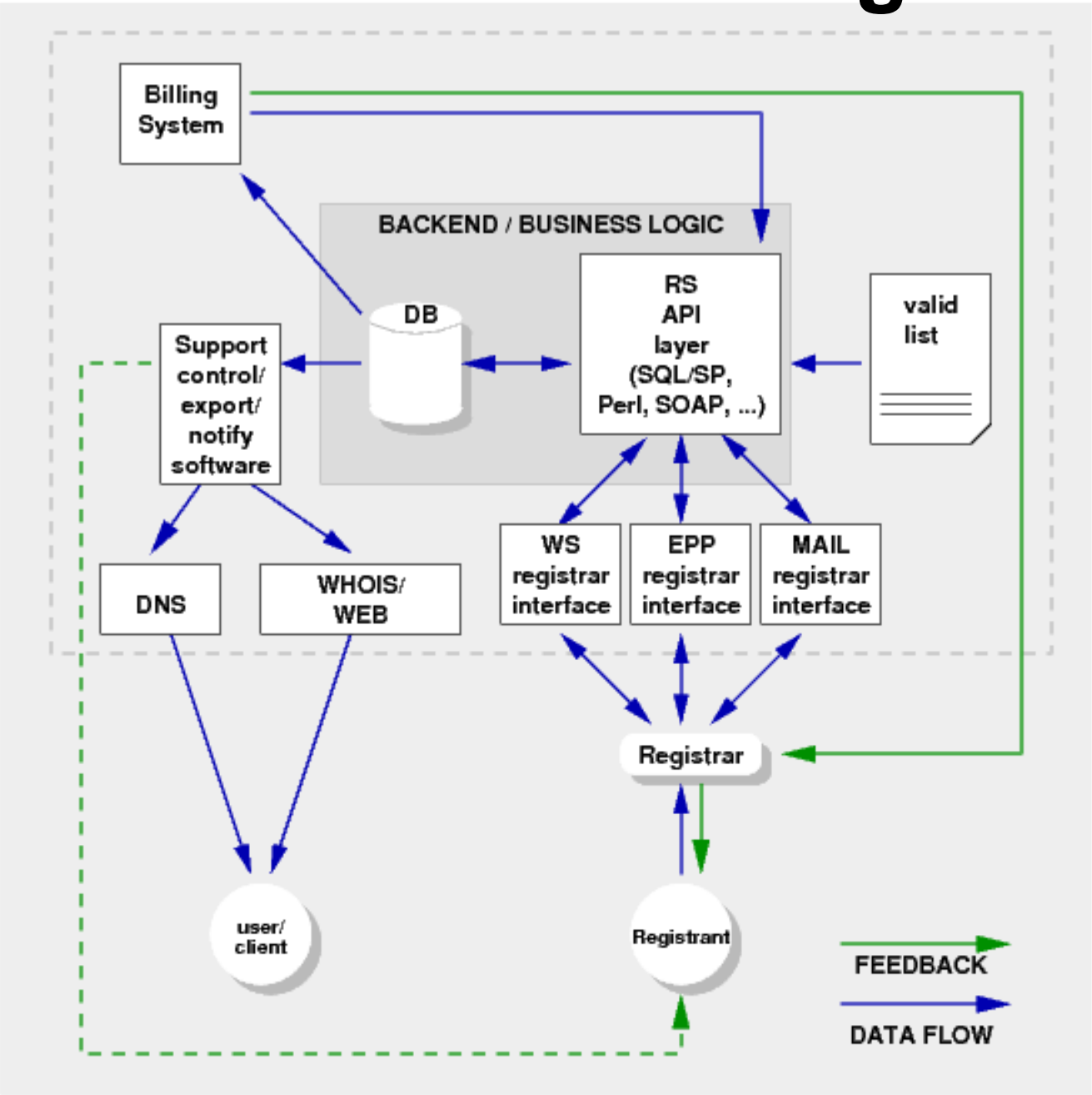
Flux d'un registre



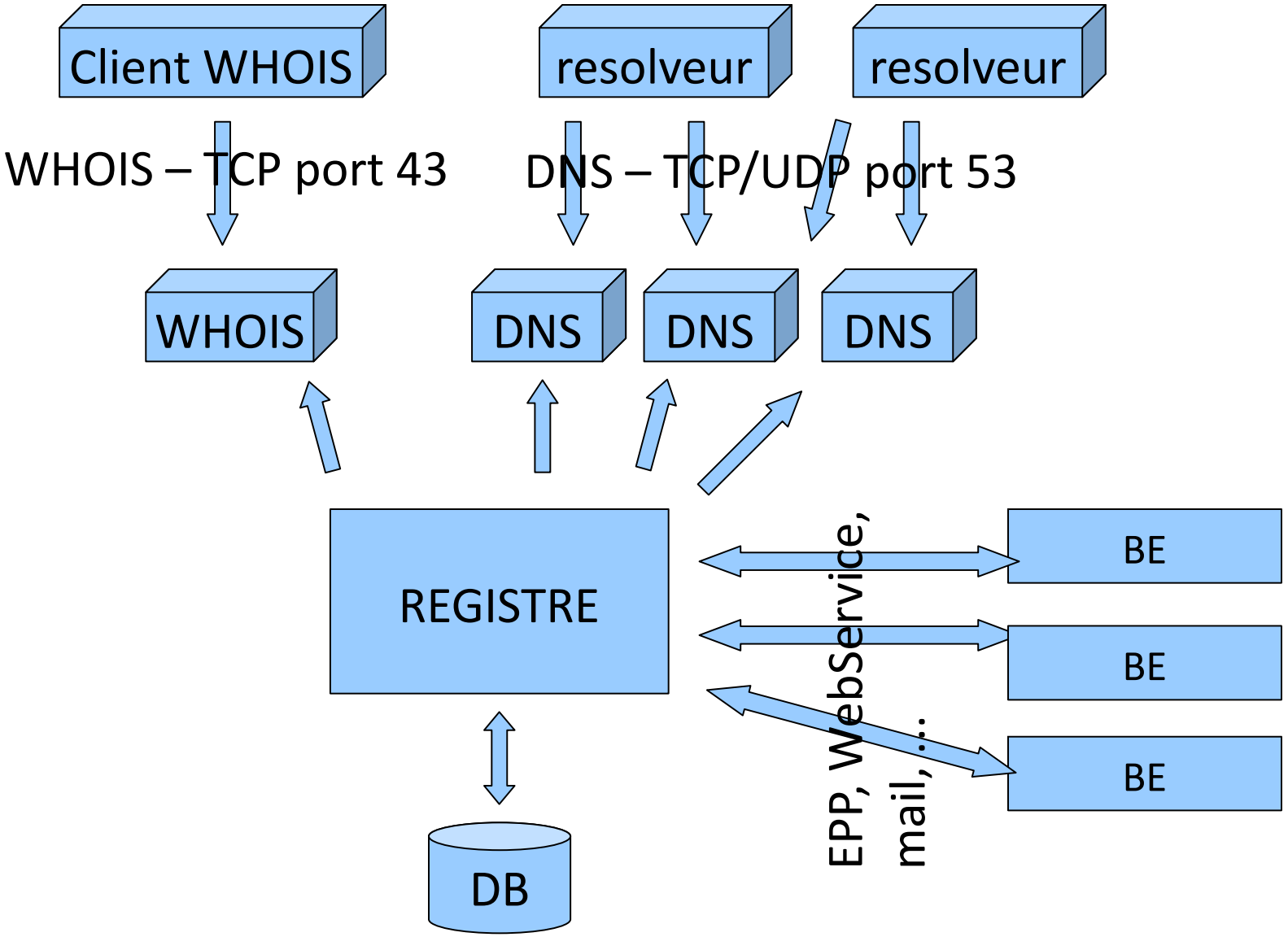
Architecture



Architecture d'un registre



Interfaces extérieures



Quels opérations ?

- Ajout et suppression d'enregistrements (redélégation)
- Ajout/modification/suppression de serveurs de noms (la modification étant une redélégation)
- Mise à jour des données administratives (infos WHOIS)

Quel niveau de complexité ?

- Aussi simple qu'un fichier texte avec des commentaires
- Maintenu via l'interfaces des Dix Doigts

```
...
; Société Machin
; contact Jean Dupont, +33 1 1234 4567, ;
  jean@masociete.fr
masociete      NS       ns1.autreTLD.org.
               NS       ns.masociete
ns.masociete    A       1.2.3.4
...
```

Modèle opérationnel plutôt simple

- Ajout d'une délégation
  - Creation d'un domaine
- Changement de délégation
  - Redélégation d'un domaine
- Suppression d'une délégation
  - Destruction d'un domaine
- Toute opération peut affecter les délégations existanttes, les enregistrements de glu, les données WHOIS

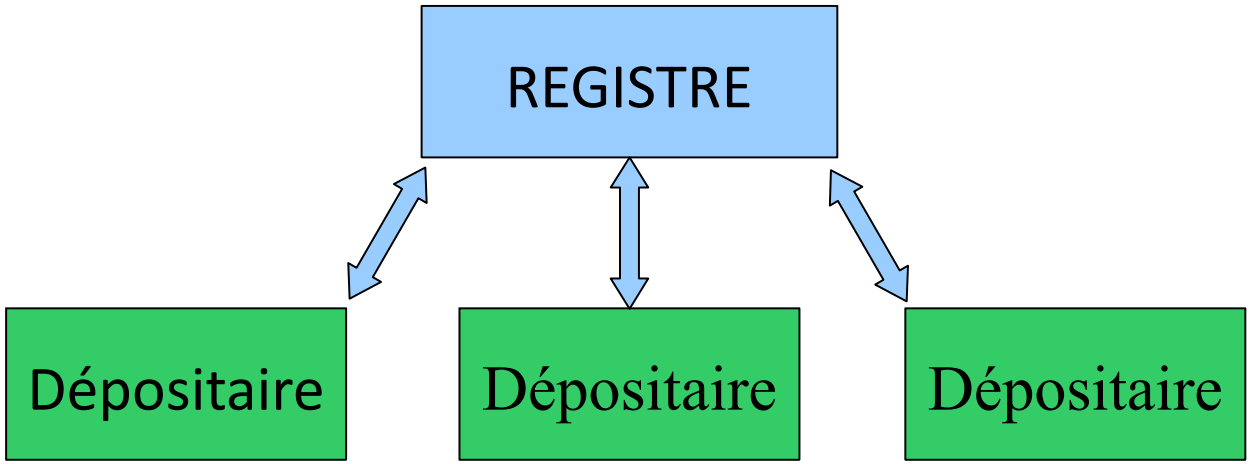
Vocabulaire

- ”Registre” - Institution ou organisation qui maintient la zone et les données administratives/nominatives qui y sont associées.
- ”Registrant” (dépositaire) – Personne physique ou morale responsable du domaine
- ”Registrar” (BE) - Organisation gérant les enregistrements de domaine pour le compte des dépositaires.

Différent modèles: 2R

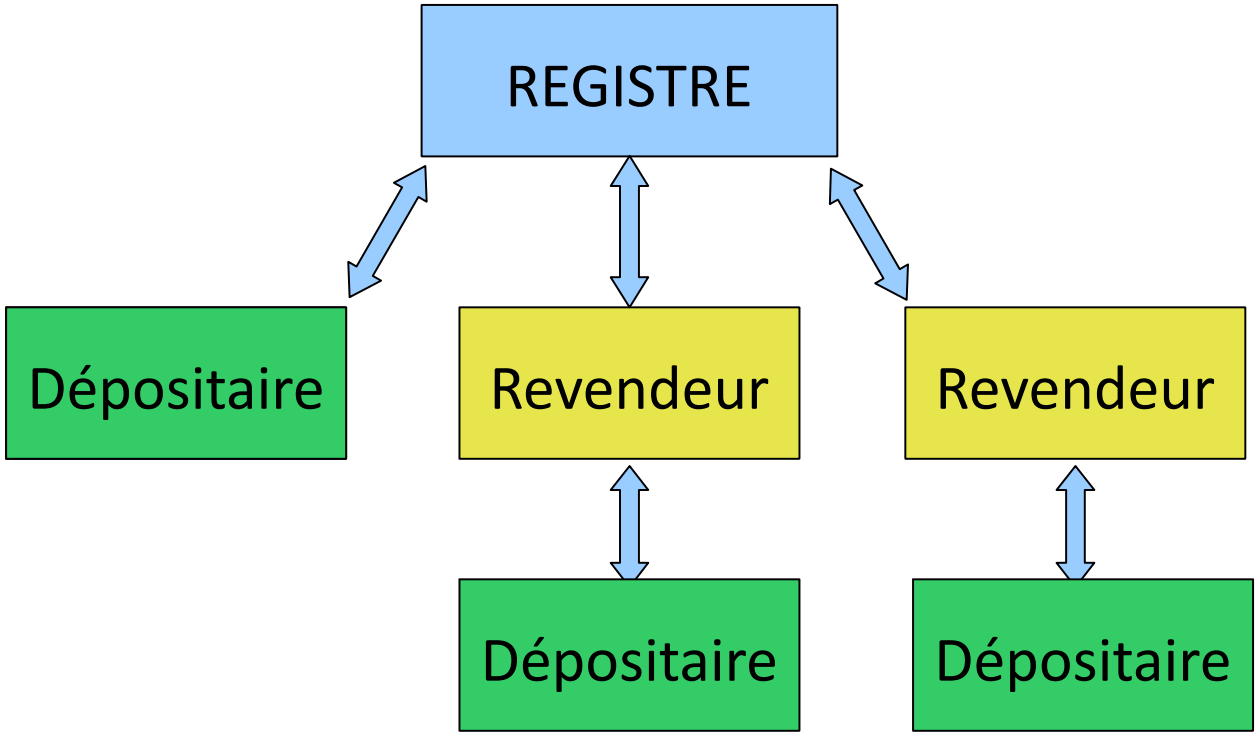
- Modèle de registre simple – pas de BE

Le dépositaire est en contact direct avec le registre. Également appelée registre à ”accès unique”.



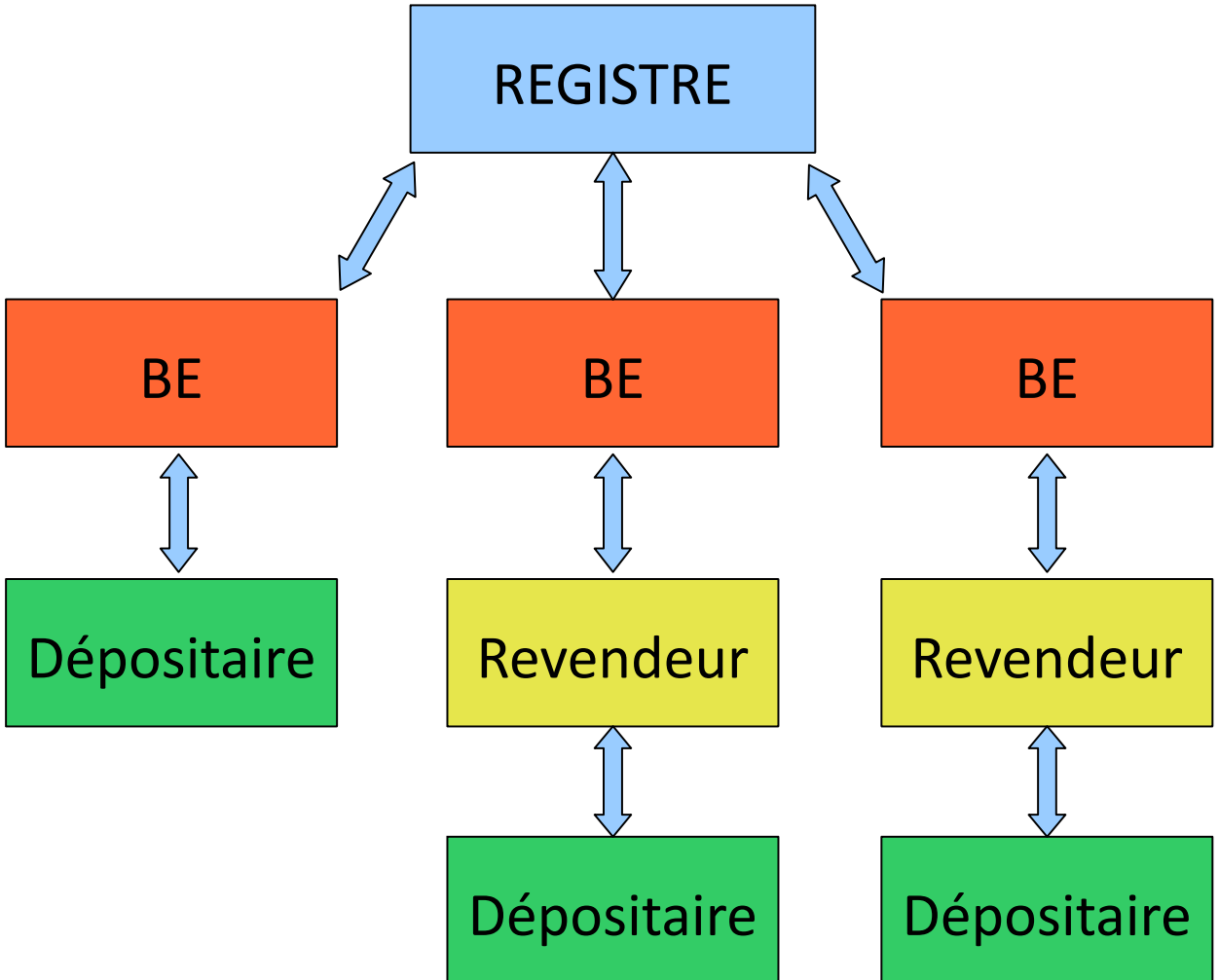
Différent modèles: 2R

- Cela reste un registre à accès unique, même si il autorise des revendeurs:



Différent modèles: 3R

- Registre à accès partagé



Épais vs Mince

- Indique comment le WHOIS is placé/ distribué
- Dépend de l'emplacement de la base de données:
  - Mince: .COM, .NET: données administratives réparties sur plusieurs BE
  - Épais: .INFO – the les données administratives sont centralisées chez le registre

Plat ou hiérarchique ?

- Plat
  - Une politique ”aplatie” permet l'enregistrement de noms directement au sommet du TLD, comme par exemple example, nsrc.org .
- Hiérarchique
  - Une conception hiérarchique offre des catégories ou des groupement logique par intérêt ou activité au second niveaul. Par exemple, mycollege.ac.uk, ou alors ministere.gouv.fr

Évolution d'un registre

- Du plus simple...
  - Fichier texte avec commentaires
  - Demande d'enregistrement par email
  - Pas de whois, ou mise à jour manuelle
  - Pas de revendeurs ou de BE - 2R.
- … au plus avancé
  - DB relationnelle et transactionnelle, facturation automatique, WHOIS, EPP, interface Web
  - Mise à jour dynamique / automatique
  - 3R avec de multiples BE
  - Anycasting des serveurs DNS

EPP

- RFC3730
- Succède à RRP (RFC2832)
- Extensible Provisioning Protocol
- Basé sur XML
- Utilisé par un nombre grandissant de BE et de registres.
- Pas tous les registres ”moderne” l'ont encore adapté!
- RFC4310 décrit les extensions de sécurité pour EPP

WHOIS

- Rapatrier des informations administratives concernant un domaine, y compris le nom, l'adresse, no. de téléphone, ---
- RFC 954
  - Protocole pas formellement spécifié
  - Les données issues de différents BE et Registres peuvent avoir un format différent (et c'est souvent le cas)
- RFC 3912
  - TCP port 43

Relation Registre-Registrar (BE)

Relation Registre – BE – l'accréditation

- Souvent la relation entre le BE et le registre est contractuelle

- Certains registres requièrent que les société souhaitant devenir BE suivent un processus d'accréditation.

- Critères pouvant faire l'object d'une accréditation
  - Stabilité technique
  - Forme de société
  - Stabilité financière & organisationnelle
  - Autre

Relation Registre – BE – quelques aspects contractuels

Quand la relation entre le registre et les BE est basée sur un contrat, le registre doit prendre en compte certains aspects:

- Transfert du contrat et transfert des domaines associés
- Procédures de sauvetage pour les dépositaires (et leurs domaines!) si leur BE fait faillite ou ”disparaît”
- Pénalité quand le BE n'est pas à jour avec les paiements dûs au registre
- Modèle de facturation (prépayé, facture, ...)

Relation BE – Registre: code de bonne conduite

- **Code de bonne conduite**
  - Afin d'assurer que le dépositaire du nom de domaine puisse attendre un service fiable, et des informations correctes, certains registres ont proposé un code de bonne conduite des BE
  - La plupart de ces codes sont basés sur des principes volontaires, mais sont conçus pour **aider les utilisateurs à avoir confiance dans le processus d'enregistrement dans son ensemble**

Relation BE – Registre: Méthodes de communication

- **Outils de communication**
  - Listes de diffusion
  - Réunions fréquentes
  - Service d'assistance
  - Lettre d'annonce
  - Interfaces web dédiées

Relation BE – Registre: Les interfaces web

Interfaces web:

- Facilité d'accès très souhaitable (simplicité)
- Systèmes basés sur EPP

Souvent, divisée en deux sous-parties

- Informations publiques
- Informations restreintes à l'attention des FAI et BE.

Bases de données relationnelles

Pourquoi utiliser une base de données?

Comparons l'utilisation d'un fichier texte feuille de tableur avec un SGBD:

BD	Feuille tableur/fichier texte
Accès multi-utilisateur	Accès utilisateur unique
Rapidité et complexité des requêtes possibles	Mises à jour lentes
Facile à étendre	Besoin langage de script
Permet un accès sécurisé aux données	Permissions fichier (tout ou rien)
Maintient de l'intégrité	”Protection” cellules

Quel problèmes ?

Quels problèmes essayons nous de résoudre, ou d'éviter ?

- Maintenance d'un très gros fichier de zone
- Comptabilité client (dépositaire ou BE)
- Service clientèle et marquetique (profils)
- S'assurer de l'exactitude des données
- Sécuriser les données
  - Enregistrements clients
  - Enregistrements comptabilité

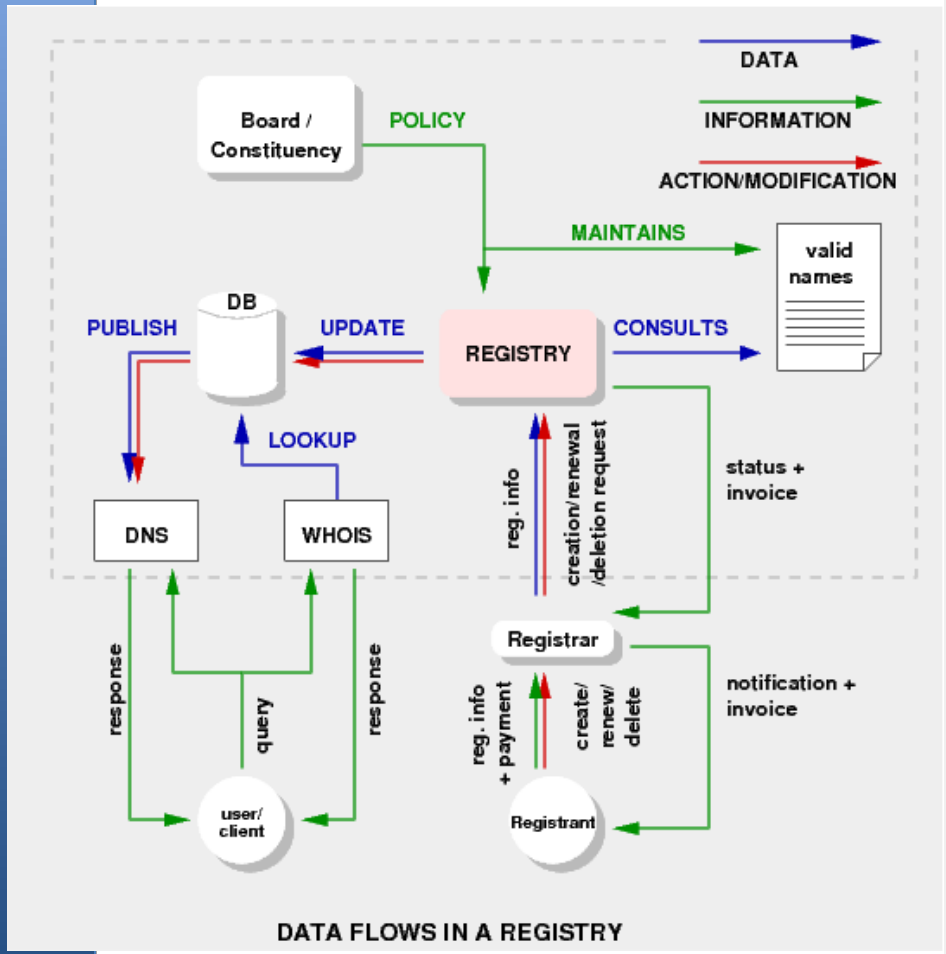
Accès multi-utilisateur

- Un fichier plat (feuille tableur / texte) ne peut être manipulé que par un utilisateur à la fois
- Votre organisation grandit, vous allez avoir le besoin de mises à jour simultanées par plusieurs personnes (fiches client, DNS, ...)
- Accès multi-utilisateur => meilleur service clientèle, plus d'efficacité et un risque moindre de perte de l'intégrité (mise à jour simultanée d'un enregistrement par deux employés)

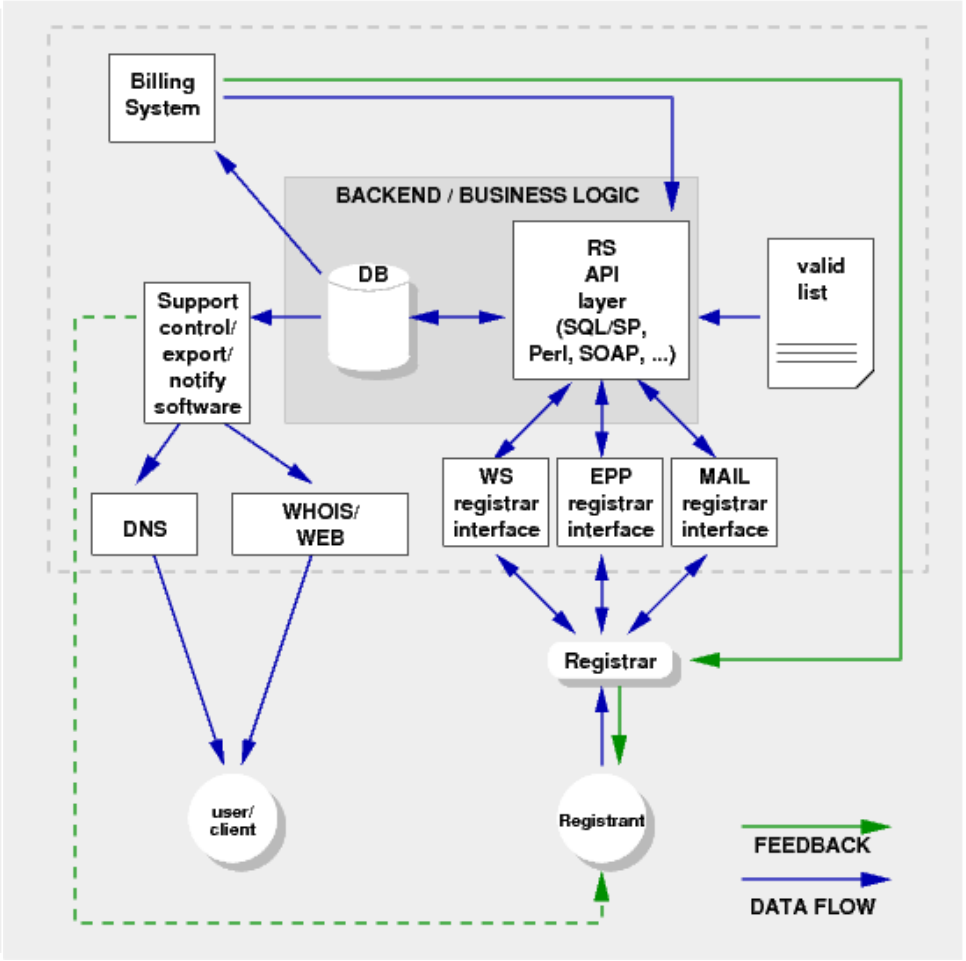
Accès multi-utilisateur (2)

- L'accès multi-utilisateur est un prérequis pour étendre les activités d'un registre:
  - Les département marketing et commerciaux voudrons des rapports (noms les plus populaires, temps moyen d'enregistrement, etc...)
  - Le service facturation aura besoin de metre à jour la BD (directement ou non) pour marquer les délégation pour lesquelles il n'a pas été payé de renouvellement (modèle 2R souvent)

Rappel



DATA FLOWS IN A REGISTRY



BD: Facile à étendre

• Multiples utilisateurs en accès concurrent sur une zone via la BD:

- Interface logicielle pour produire le fichier de zone (BD → fichier)
- Fichier de zone exporté automatiquement à intervalles réguliers, sans intervention humaine
- La BD enforce la nécessité que certaines informations soient unique, pour garantir un fichier de zone qui soit valide.
- Le schéma BD lui-même peut être modifié pour permettre les évolutions

BD: maintien de l'intégrité

- Vous voulez être certain que vos données ne sont pas corrompues, et ceci doit rester le cas.
- Une BD bien conçue peut aider à “forcer” une sasie correcte des informations par votre organisation.
- Un SGBD peut vérifier les relations et l'intégrité de vos données.
- Les SGBD ont un grand nombre d'outils pour la sauvegarde, la récupération, le nettoyage et la vérification.

BD: requêtes relationnelles

- Impossible dans un tableur – très limité.
- Un modèle relationnel vous laisse créer de multiples tables avec des enregistrements, et les interconnecter.
- Données visible sous une multitude d'angles
- Trouver des relations, effectuer des requêtes sur celle-ci, et obtenir des résultats, sont une des fonctionalités les plus puissantes des SGBD relationnelles.

Rapidité et complexité des requêtes

- Une base bien conçue autorise des requêtes précises et détaillées sur des gros volumes de données. Ces requêtes pourront être:
  - Rapides
  - Logiquement correctes (l'arithmétique booléenne garantit l'exactitude des requêtes)
  - Les résultats seront garantis dans leur intégrité
  - Tres rapides

SGBD publiques

Par “publiques”, cela signifie:

- SGBD disponibles sous une license logicielle “libre”
- SGBD développés dans un forum publique
- Les SGBD commerciaux doivent être achetées
- Les SGBD commerciaux nécessitent un support payant continu pour les mises à jour
- Il est toutefois possible d'acheter du support payant dans les deux cas (publique & commercial)
- Les bases de données publiques ont un support communautaire souvent tout aussi réactif que certaines solutions commerciales.
- ...

MySQL et PostgreSQL

Les deux SGBDR libres les plus populaires.

Lequel choisir ?

MySQL remplit la plupart des besoins des utilisateurs.

Si vous voulez bénéficier des fonctionnalités SQL avancées, ou voulez un SGBD qui implémente ”ACID” → PostgreSQL!

MySQL progresse en permanence, mais son futur est difficile à prévoir – plusieurs versions, plusieurs moteurs de stockage, …

Les types de données stockées

- **Client:**
  - Enregistrements comptabilité
  - Transactions
  - Support
- **Fichier de zone**:
  - Enregistrements de délégation
- **Relations**:
  - Clients
  - Domaines

Prodution du fichier de zone depuis la base

- **Langage de programmation au choix:**
  - PHP, Perl, Python, ...
  - C, C++
  - etc...

- Besoin de produire une zone ***valide***
- Validation des données en entrée **ET** en sortie de la BD.
- Parcourir TOUS les enregistrements (garantir la totalité)

- Construite dynamiquement pour pouvoir agir sur la zone et les données client simultanément.

Exemple de schema

```
create table data (
  zone      text,    - ”nsrc.org.”
  name      text,    - ”www”
  ttl       text,    - ”3600”
  rdtype    text,    -  ”A”
  rdata     text,    -  ”128.223.157.19”
  locked    bool,    - ”t”
  comments  text,    - ”Website for NSRC.org”
  dynamic   bool,    - ”f”
);
```

Exemple de schema

Le fichier de zone ne contient qu'un *sous ensemble* des données dans la BD

Par exemple, les informations sur les dépositaires, les commentaires, les dates d'enregistrement, etc... ne sont PAS exportés vers le fichier de zone.

Pareillement, un serveur WHOIS ne montre pas les informations appartenant à la zone – sauf peut-être quels NS sont publiés pour la zone concernée

Quelques outils de gestion de registre

CoCCA http://sourceforge.net/projects/coccaopenreg/
Consortium, Council of Country Code Administrators

CodevNIC http://codev-nic.generic-nic.net/
.fr project, Co-developped NIC

DNRS http://sourceforge.net/projects/dnrs/
.nz, Domain Name Registry System

FRED http://fred.nic.cz/
.cz, Free Registry for ENUM and Domains

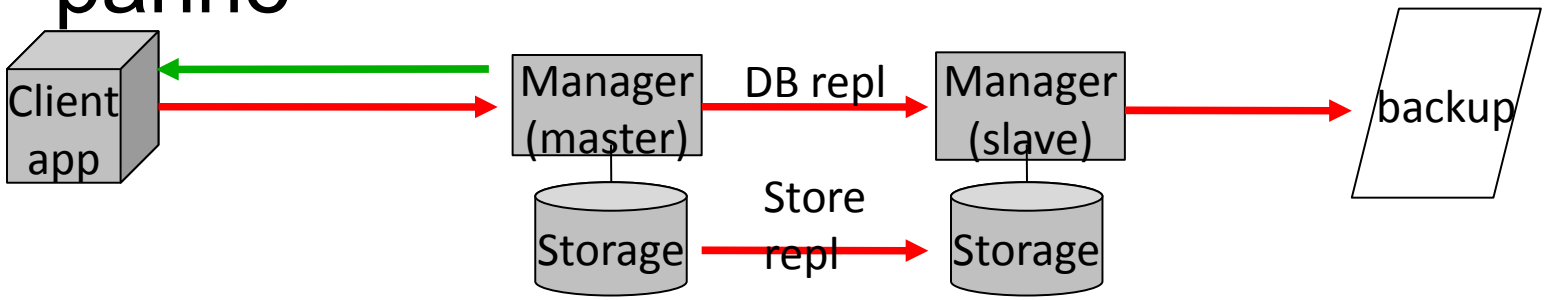
Opérations de registre fiable, robuste et résiliente

Disponibilité bases de données

Les BD sont plus complexes que les fichiers texte ou les feuilles tableur Excel

Corruption, erreurs de manipulation, vandalisme: tous peuvent rendre une BD inutilisable

La sauvegarde est bien sûr obligatoire, mais on peut contempler la réplication de BD ou de stockage pour minimiser les temps de panne



Disponibilité services registre

Il est tentant de profiter de la BD pour faire une publication ”temps réel” de la zone et du whois (requêtes DNS WHOIS → DB)

Il y a des risques dans cette approche, cf. les points évoqués sur la page précédente.

La DB devient le maillon le plus faible dans la chaîne (les systèmes complexes tombent plus souvent en panne que les plus simples), comparé au serv. DNS ou whois

Contempler le découplage du stockage de la zone et sa publication.

Disponibilité services registre (2)

i.e.: re-publier la zone à intervalles réguliers.

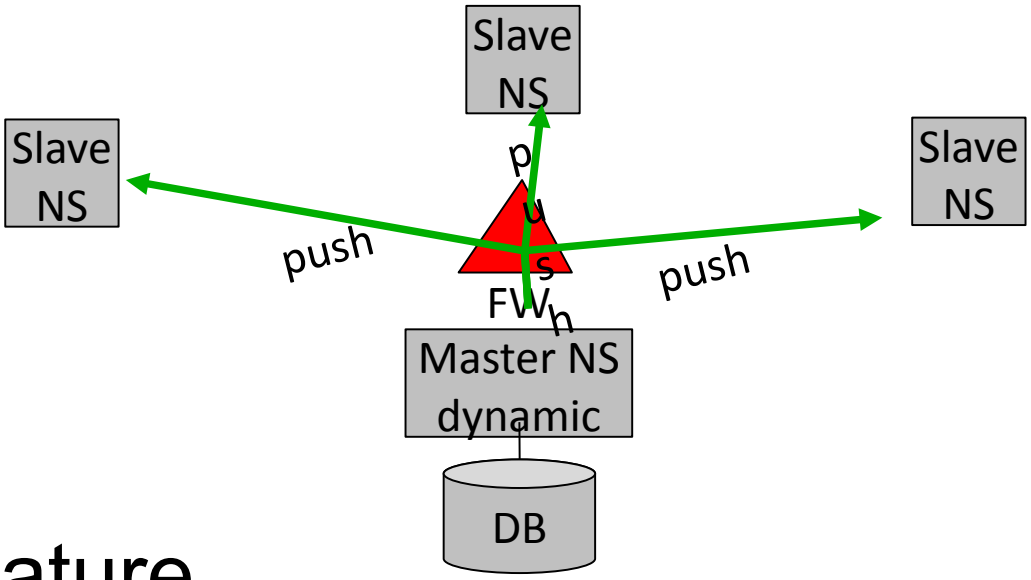
Ceci est en ligne avec par exemple DNSSEC, ou les groupes d'enregistrements (RRsets) doivent être re-signés régulièrement

Même approche pour les données WHOIS:

Avoir un processus distinct pour générer le fichier de zone et le WHOIS depuis la BD. Le service peut ainsi continuer à fonctionner dans le pire des scénarion catastrophe (crash BD)

Disponibilité services registre (3)

Une autre solution est d'avoir un ”maître caché”. Il peut parler directement à la base, mais les serveurs publiques sont des copies esclaves de ce serveur maître.



La signature

DNSSEC: autre facteur à prendre en compte.

Disponibilité services registre (4)

Les services d'enregistrement peuvent continuer de tourner même en cas de panne BD.

Les protocoles comme EPP ont besoin de la BD pour effectuer les changements.

Mais on peut aussi mettre en file d'attente les requêtes jusqu'à disponibilité de la base (certaines opérations deviennent impossible)

La méthode est une question de choix politique

Conserver une trace des changements

Quand la zone est dans un fichier texte ou un tableur, il est facile de garder un historique des sauvegardes:

- Copie de la zone avec la date dans le nom du fichier après chaque changement.
- Facile à automatiser.

Comment faire avec une BD ?

Quand on exporte la zone vers un fichier texte, versionnez le (nous évoquerons ceci) ou bien implémenter le versionnage dans la BD (plus compliqué, mais très utile)

Quelle granularité ? (date, transaction)

Anycast des serveurs DNS

Services DNS

- Multitudes de secondaires pour les ccTLD
  - Redondance
  - Distribution de charge
  - Meilleurs temps de réponse

Les serveurs DNS secondaires doivent se situer à des emplacements topologiquement et géographiquement distincts sur l'Internet.

- RFC 2182
- AfriNIC, RIPE, ISC, PCH, PSG.COM, etc... offrent du service secondaire pour les ccTLD

Anycast du service DNS

Bénéfices de l'anycast

- Basculement en cas de panne transparent et automatique (routage)
- Équilibrage/répartition de charge
- Réduction de la latence (l'instance la plus “proche” est ”choisie”)
- Mitigation de l'attaque (plein de machines partout)
- Configuration simplifiée pour les utilisateurs (une seule IP dans tout le réseau pour la récursion)

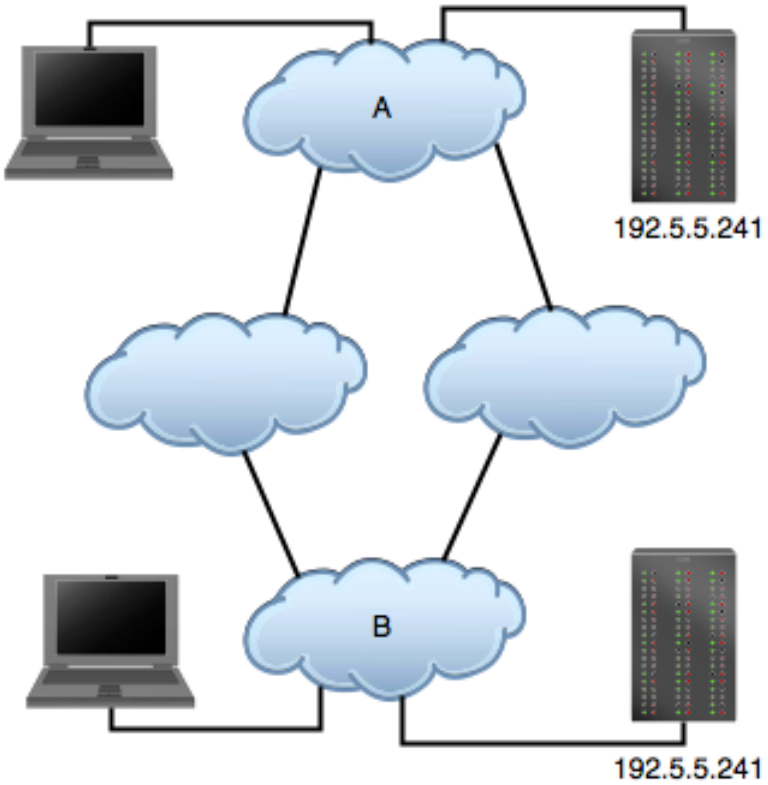
Certains des opérateurs précités offrent un service anycast.

On peut payer pour un service anycast avec support

Serveurs DNS Anycast

- Une IP publique IPv4 / IPv6 unique
- Les requêtes destinées à ces adresses sont acheminées (routées) à des serveurs différents en fonction de l'origine de la requête.
- Ce comportement est transparent pour les mécanismes qui envoient les requêtes

Routage anycast

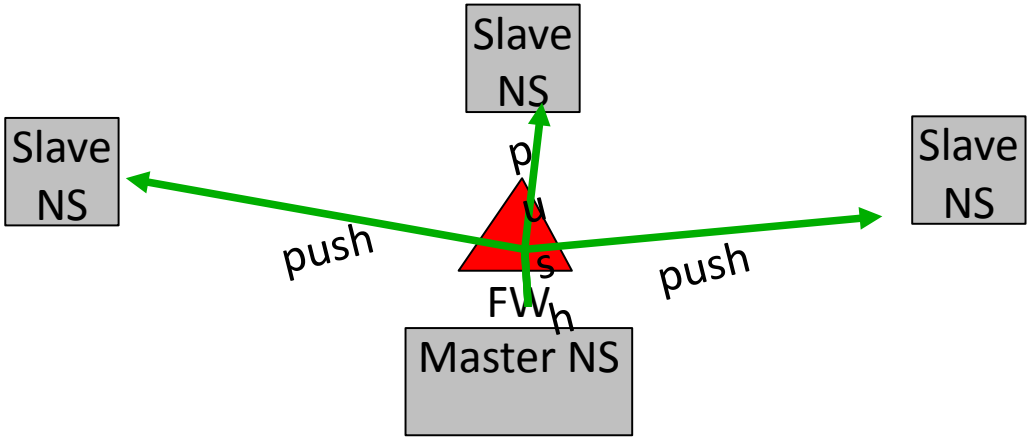


Anycast hiérarchique

- Certains noeuds anycast servent tout l'Internet (noeuds globaux)
  - Gros, bien connectés, sécurisés et beaucoup de capacité en surplus.
- D'autres peuvent fournir un noeud pour une région particulière (plus petits)
- Le routage de chaque noeud est tel que dans des conditions normales, il n'attirera jamais le trafic / fournira de service pour des clients ailleurs dans le monde – que du trafic local

Intégrité des données secondaires

Rappel



Contempler l'utilisation de communication sécurisée entre les maîtres et esclaves par exemple avec TSIG, ou utiliser un mécanisme de réplication comme SSH/rsync pour distribuer les zones.

Questions ?