

DNS

Domaine Name System
Port : 53

[RFC 1032 à 1035, 1987]
Plus de 110 autres documents

1

DNS - Généralité

- Espace de nom **mondiale et cohérent**
- Accès à **toutes** les ressources d'Internet
- Gestion **décentralisée**
- **Indépendant** aux types de machines, aux types de réseaux et aux protocoles de la couche « transport »

2

Nom

Noms de domaines
structure hiérarchique

3

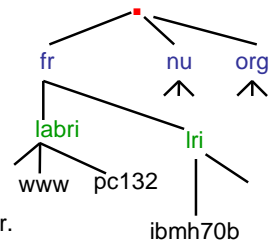
Hiérarchie des noms = arborescence

Root « . »

Premier niveau : fr. de.

Deuxième niveau : labri.fr.

Troisième niveau : www.labri.fr.



4

Domaines du premier niveau

- Domaine géographique – ccTLD - (274) :
uk., it., us., au., ir., iq., ...
- domaines génériques - gTLD - (21):
aero., biz., coop., edu., gov., info., int., net., ...
- Arpa. : résolution de nom inversée
(adresse IP – nom)

5

Nouveau gTLD

- le 20 juin 2011 Réunie à Singapour pour sa 41ème réunion, l'ICANN vient de confirmer le lancement du processus des « nouveaux gTLD » amorcé il y a trois ans à Paris : ainsi, d'ici un ou deux ans, plusieurs centaines de nouveaux TLD pourraient venir s'ajouter aux plus de 300 TLD existants
- Ex .Bordeaux,
- Dépôt des candidatures avant fin 2012

6

Délégation d'autorité

7

Délégation

- Le système DNS est entièrement décentralisé au niveau planétaire
- Le mécanisme sous-jacent est la délégation de domaine
- A tout domaine est associé une organisation responsable qui peut
 - découper le domaine en sous-domaines
 - déléguer la gestion des sous-domaines à d'autres organisations

8

Délégation

- [ICANN](#) - Internet Corporation for Assigned Names and Numbers – a autorité pour le niveau racine « . »
- [AFNIC](#) a autorité pour le domaine « fr. » et « re. »

9

Serveur de noms

10

Les serveurs de noms

- Les serveurs de nom
 - enregistrent les données propres à une zone (une partie de l'espace « nom de domaine »)
 - répondent aux requêtes concernant leur zone d'autorité
 - transmettre les requêtes auxquels il ne peuvent répondre à un autre serveur DNS

11

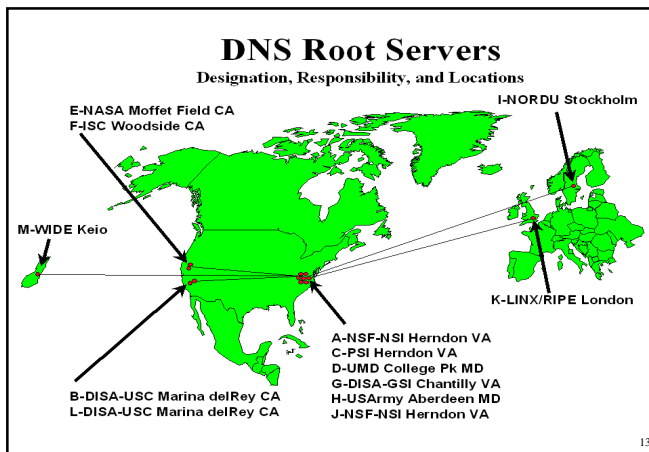
Serveurs racine

- Les serveurs « racine » connaissent les autres serveurs « racine »
- Les serveurs « racine » connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (org., mil., kr., be., ...)



Pierre angulaire du système DNS
si les serveurs « racine » ne sont pas opérationnels
==> plus de communication sur l'Internet

12



Serveur Logique/physique

La technique du « anycast », permettent que les 13 serveurs DNS racines correspondent en fait à plus de 120 de serveurs physiques éparpillés dans le monde entier.

deux de ces serveurs "physiques" sont en France:

- Copie du serveur F maintenu par « ISC ».
- Copie du serveur M maintenu par "WIDE Project".

14

Types de serveurs de nom

- Un Serveur de nom primaire
- Des Serveurs de nom secondaire :
 - interroge périodiquement son serveur de nom primaire et met à jour ses données

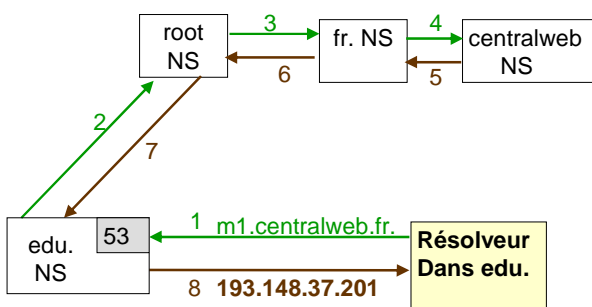
La redondance permet de garantir le service en cas de défaillance éventuelle du serveur primaire et/ou du (des) secondaire(s)

15

Fonctionnement

16

Mode récursif



Configuration des serveurs sous Linux/Unix

/etc/bind/named.conf
/etc/bind/db-xxx

18

Extrait du fichier /etc/bind/named.conf

```
zone "maison.net" {
    type master;
    file "/etc/bind/db-maison";
};
```

nom de la zone

type du serveur (master/slave)

fichier stockant les données

19

Extrait du fichier /etc/bind/named.conf

```
zone "2.4.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db-2.4.10";
};
```

Résolution inverse pour les adresses commençant par 10.4.2 :
serveur primaire
les données sont stockées dans le fichier /etc/bind/db.2.4.10

20

Fichier : /etc/bind/db-maison

```
@ IN SOA wallace.maison.net. admin.maison.net. (
    2 ; Serial ;
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

@ IN NS wallace
@ IN NS mcgraw
@ IN MX 10 wallace
@ IN MX 20 mcgraw
```

21

Fichier : /etc/bind/db-maison (suite)

```
wallace IN A 10.4.2.254
mcgraw IN A 10.4.2.3

www IN CNAME wallace

attic IN NS 10.4.2.1
```

22

Explications

```
@ IN SOA wallace.maison.net. admin.maison.net. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
```

Domaine courant : maison.net
Serveur DNS primaire du domaine courant : wallace
Boîte aux lettres de l'admin : admin@maison.net
augmenter le « serial number » après chaque modification du fichier

23

Explications (2)

```
@ IN NS wallace
@ IN NS mcgraw
```

« @ = Domaine Courant »
Domaine courant a 2 serveurs DNS de nom wallace et mcgraw

```
@ IN MX 10 wallace
@ IN MX 20 mcgraw
```

« @ = Domaine Courant »
Domaine courant a 2 serveurs SMTP de nom wallace et mcgraw

24

Explication (3)

wallace IN A 10.4.2.254

wallace a pour adresse IPv4 10.4.2.254

www IN CNAME wallace

www est un synonyme de wallace

attic IN NS 10.4.2.1

attic est un sous domaine du domaine courant, son serveur DNS primaire est 10.4.2.1

25

Fichier : /etc/bind/db-2.4.10

@ IN SOA wallace.maison.net.
admin.maison.net. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

254 IN PTR wallace

3 IN PTR mcgraw

26

Configuration des clients sous Linux/Unix

/etc/bind/named.conf
/etc/bind/db-xxx

27

Configuration des clients

fichier /etc/resolv.conf

search maison.net

nameserver 10.4.2.254

Extrait du fichier /etc/nsswitch.conf

hosts files dns

28