Un livre de Wikilivres.

Système de noms de domaine

Le_modèle_hiérarchique

Le DNS possède un modèle hiérarchique. Dans cette partie, nous allons partir de la racine de l'arbre et aller vers les différentes branches de l'arbre. Nous n'allons pas ou très nous préoccuper des implémentations au niveau de serveurs. C'est essentiellement le modèle qui nous intéresse ici.

Historique

Le fichier unique Hosts au SRI (Stanford research Institute)

La structure arborescente du DNS

Les RFC de référence sont les RFC 1034 et RFC 1035 (en remplacement des RFC 882 et RFC 883). Ces RFC décrivent un modèle arborescent. Ils restent plus de 20 ans après la base du DNS aujourd'hui.

Concepts de base

- Domaine
- Sous-Domaine
- Zone
- Délégation

Similitude avec les autres annuaires

Un annuaire est un système qui centralise les informations concernant les utilisateurs et les services pour en simplifier l'administration. Un annuaire est une base de données, cependant la réciproque est fausse. En effet, un annuaire possède certaines particularités : il est plus sollicité en lecture qu'en écriture et les transactions gérées sont de nature simple (pas de transactions en concurrence ou de gros volume de données).

Le modèle arborescent n'est pas unique au DNS. Au contraire, il est même courant dans le monde des annuaires. D'autres annuaires utilisent donc un modèle similaire. On peut citer plusieurs exemples :

- *X500* le modèle de l'annuaire
- *LDAP* simplification du modèle X500
- *Active Directory* de Microsoft (basé sur LDAP)
- *UDDI* annuaire de services web

UDDI

UDDI est un annuaire des services web. Sa version 3 (la dernière) prévoit un structure hiérarchique.

Monde de Microsoft et le DNS

WINS et DNS

Les anciens réseaux Microsoft utilisent le protocole NetBEUI. Dans ces réseaux les machines sont identifiées par un nom NetBIOS et l'adresse physique de la carte réseau. NetBEUI ne passe pas les routeurs. Et NetBEUI est remplacé par des protocoles plus modernes.

WINS signifie Windows Internet Naming Service. Il va faire le lien entre l'adresse IP et les noms NetBEUI.

- Serveur DNS : FQDN (hostname) <--> adresse IP
- Serveur WINS : nom NetBIOS <--> adresse IP

Contrairement au DNS statisque, WINS est dynamique. Dans certains cas, un serveur WINS peut cohabiter avec un serveur DNS.

Active Directory et le DNS

Voir l'article de Wikipédia : http://fr.wikipedia.org/wiki/Active_Directory

Voir également la présentation d'Active Directory http://manu.all-3rd.net/docs/hsc/docs/publications/ad/print/main.pdf

Active Directory est le service d'annuaire mis en place par Microsoft dans les derniers Windows (2000 et suivants). Il remplace le service d'annuaire de Windows NT4 qui souffre de nombreuses limites. Ainsi dans NT4 la base des utilisateurs était limitée à 40 000 entrées. AD s'inspire de LDAP et intègre le DNS. C'est donc un système assez complexe.

Active Directory est basé sur la notion de domaine (Windows). Ces domaines s'organise en arbres et en forêts. Un arbre est un ensemble de domaines composant une structure hiérarchique où un domaine fait office de domaine racine : exemple stagiaires.soc.fr, techniciens.soc.fr et soc.fr. La notion de forêt est un

ensemble de domaine qui ne sont pas sous-domaines les uns des autres, mais liés par une relation de confiance bidirectionnelle transitive.

DDNS pour (Dynamique Domain Name Service) est l'implémentation DNS de Microsoft. Son but est notamment de remplacer l'ancien WINS (Windows Internet Naming Service). DDNS est donc lié à Active Directory, il profite des mécanismes de réplication et du système de permissions via les ACL d'Active Directory.

DDNS interopère avec BIND version 8.2 et supérieur. Il a besoin, pour pouvoir fonctionner correctement, d'un DNS supportant les enregistrement SRV (RFC 2782), les mises a jour dynamiques (RFC 2136) et les transferts de zone.

DDNS supporte le transfert de zone incrémental (RFC 1995) et DNSSEC.

Contraintes sur les noms

Il existe deux types de contraintes :

- des contraintes syntaxiques (liées à l'historique et à la mise en œuvre du DNS)
- des contraintes issues des décisions des acteurs dans les chartes de nommage

Exemple dans le cadre du .fr, l'AFNIC maintient une charte de nommage qui dans son article 21 reprend les contraintes syntaxiques et dans son article 20 décrit une liste de termes fondamentaux (interdits et réservés). Les termes interdits sont liés à des crimes et délits. Les termes réservés protègent notamment les termes géographiques comme les villes et les professions.

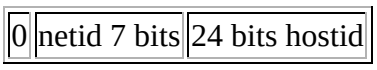
La correspondance inverse

Il s'agit de faire la correspondance entre les adresses IP et les noms de serveurs.

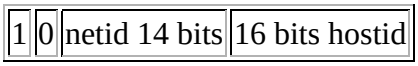
Rappel sur les adresses IPv4

Initialement les adresses IP étaient réparties en 5 classe (de A à E) basé sur des blocs de 8 bits.

Classe A



Classe B



Classe C

Classe D

Classe E

1	1	1	1	0	réservé à usage futur 27 bits

Classe	Espace
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Par la suite, ce modèle de classes A, B et C a été incapable de répondre à la demande des adresses IP. Les classes A gaspillent de nombreuses adresses. CIDR (classless Inter Domain Routing, RFC 1517) permet un découpage plus fin qui ne dépend pas des frontières de 8 bits. La notation est alors <adresse> / <nombre de bits significatifs>. Ainsi 192.0.0.0/8 peut être noté 193/8. On peut imaginer un fournisseur d'accès à Internet gérant les adresses 192.168.0/22. Il peut repartir sa plage d'adresses entre 4 entreprises A, B, C et D : 192.168.0/24, 192.168.1/24, 192.168.2/24, 192.168.3/24.

Le RFC 1918 définit les plages d'adresse IPv4 réservées pour IPv4. Ce sont :

- 10/8 (10.0.0.0 - 10.255.255.255)
- 172.16/12 (172.16.0.0 - 172.31.255.255)
- 192.168/16 (192.168.0.0 - 192.168.255.255)

Les RIR

Association regroupant des informations communes http://www.nro.net

La gestion des adresses IPv4 est une fonction de l'IANA, donc maintenant de l'ICANN. L'ICANN attribue une partie de l'espace d'adressage des registres régionaux ou RIR (Regional Internet Registries). Il existe 5 RIR :

- l'APNIC (Asia Pacific Network Information Centre) pour la zone Asie - Pacifique
- l'ARIN (American Registry for Internet Numbers) pour la zone Amérique du nord
- le RIPE NCC (Réseaux IP Européens - Network Coordination Centre) pour l'Europe, le Moyen-Orient
- l'AfriNIC (African Regional Network Information Centre) pour l'Afrique
- le LACNIC (Latin American and Caribbean IP address Regional Registry) pour l'Amérique latine

Les RIR les attribuent à des registres locaux ou LIR qui sont parfois des fournisseurs d'accès à Internet. L'allocation des adresses IP est décrite dans le RFC 2050. Cette RFC est un peu ancienne et l'IANA maintient sur son site la répartition des adresses IPv4 http://www.iana.org/assignments/ipv4-address-space.

Correspondance des adresses IPv4

Cette correspondance utilise le TLD technique arpa. Dans ce domaine, in-addr.arpa est le sous domaine reservé pour la gestion des adresses IPv4.

Ainsi la recherche de l'adresse IP 192.0.2.1 correspond à la recherche du nom de domaine 1.2.0.192.in-addr.arpa.

Correspondance inverse et CIDR

Voir RFC 2317

La racine du DNS

L'ICANN

C'est une association californienne sans but lucratif. Elle gère notamment la racine du DNS.

Modèle de racine unique

Le DNS se base sur un modèle avec une racine "logique" unique. Ce modèle est décrit dans la RFC 2826. Cela signifie qu'il existe qu'une seule source de données. Ce modèle est repris dans le document ICP-3 de l'ICANN "A Unique, Authoritative Root for the DNS" http://www.icann.org/icp/icp-3.htm. ICP signifie Internet Coordination Policy.

Par contre physiquement, il existe plusieurs serveurs redondant qui implémentent la racine.

Les serveurs root

Treize serveurs root, cette limite évite d'avoir des messages DNS trop long.

Répartition spatiale :

- 10 aux États-Unis
- 2 en Europe
- 1 en Asie (Japon)

La gestion correcte des serveurs racines est décrite dans le RFC 2870 (http://www.ietf.org /rfc/rfc2870.txt) [archive].

La technique Anycast

La technique anycast va permettre d'associer à une adresse IP plusieurs machines éloignées physiquement. Une seule machine parmi le groupe va réponse au datagramme IP. Anycast est prévu dans le cadre de IPv6. Cette technique a été reprise dans le cadre de IPv4.

L'application d'anycast au DNs est décrite dans le RFC 3258 (avril 2002). Actuellement, cette technique permet de passer de 13 serveurs root à environ 60. Par contre, il n'y a que 13 adresses IPv4 pour ces serveurs.

Les TLD

TLD signifie Top Level Domain ou en français noms de domaine de premier niveau.

On distingue dans un premier niveau d'abstraction :

- les *gTLD* de type générique
- les *ccTLD* liés à un pays ou plus généralement à un territoire

Un second niveau de détails ajoute les sTLD et le TLD technique ".arpa".

Les gTLD

Ce sont les très connus .com .net et .org. A partir de 2001, l'ICANN a introduit des TLD de seconde génération comme le .biz et le .info.

Les sTLD

sTLD sont une variante des gTLD. Il s'agit des TLD "sponsorisés". Cette notion apparaît dans le RFC 3071.

La définition en anglais selon l'ICANN est la suivante : *The Sponsored Top Level Domain (sTLD) is a TLD that is delegated to an organization that has responsibility for the formulation and enforcement of certain policies that would normally be formulated and enforced by ICANN (Internet Corporation for Assigned Names and Numbers). The Sponsoring Organization represents the interests of the TLD community.*

Donc la notion de sTLD fait apparaitre la notion de sponsor qui représente les intérets de la communauté liée au TLD. Les exemples des sTLD sont les ".aero" et ".museum".

Les ccTLD

Ce sont les .fr .be ... Ces noms suivent la norme ISO 3166-1. Environ 240 sont définis.

le TLD infrastructure (arpa)

C'est le ".arpa". Il gère la résolution inverse et toutes les extensions du DNS. les détails de TLD infrastructure est décrit dans le RFC 3172 (septembre 2001) qui définit les sous-domaines "in-addr.arpa", "ip6.arpa" et "e164.arpa". L'IANA gère ce domaine http://www.iana.org/arpa-dom/. Dans la pratique ce TLD est un véritable racine technique et se trouve sur les serveurs racine.

La gestion des adresses IP (résolution inverse) se fait en liaison avec les RIR (regional IP registries exemple RIPE) avec les sous-domaines suivant :

- in-addr.arpa (adresses IPv4)
- ip6.arpa (adresses IPv6)

Autres fonctions

- e164.arpa ENUM
- iris.arpa destiné à IRIS le successeur de WHOIS
- uri.arpa
- urn.arpa

Le domaine iris.arpa est destiné à la mise en œuvre de IRIS le successeur de WHOIS. Ce sous-domaine est prévu dans le RFC 4698 (page 32).

Actualités récentes concernant les TLD

L'attitude de l'ICANN reste assez prudente sur l'ouverture de nouveaux TLD. Cependant, l'importance commerciale et stratégique de l'Internet alimente les projets de nouveaux TLD. L'actualité récente le prouve.

Selon les sources, le coût de la création d'un TLD à l'ICANN s'élève entre 40 000 et 80 000 euros.

Les TLD lancés en 2006

- Le .cat pour la communauté catalane (sTLD).
- Le .eu pour la communauté européenne (ccTLD).

- Le .mobi pour téléphonie mobile (sTLD)

Le .cat pour la communauté catalane a eu impact énorme sur les projets de TLD régionaux (Bretagne, Écosse, Galice). En effet, la situation actuelle avec les ccTLD donne des TLD pour des petits territoires comme le territoire des taaf qui ne l'utilise même pas pour son site officiel. Par contre elle ignore les grandes régions, ou les subdivisions des états fédéraux.

Le .mobi est l'un des derniers nouveaux sTLD qui semble comme les autres s'ouvrir à tous. Il va peut-être tuer dans l'œuf le projet du .tel prévu en 2007.

Le .eu est considéré par l'IANA comme un ccTLD. Il est actuellement le seul TLD à l'échelle d'un continent, au détail près qu'il s'agit bien de la communauté Européenne et non l'Europe en tant que telle. D'autres auteurs espèrent créer des TLD à l'échelle du continent ou de large communauté.

Les ouvertures prévues en 2007

- .tel
- .asia dotasia (http://www.dotasia.org/) [archive]

Le .tel accepté par l'ICANN en mai 2006 sera lancé en 2007. Le site officiel est http://www.telname.com.

Le .asia est le TLD pour l'Asie. Ce projet est très intéressant car il s'agira du second TLD au niveau d'un continent. Mais contrairement au .eu, il n'y a pas d'organisation de type étatique comme la communauté européenne. Le siège prévu du gestionnaire se trouve à Hong-Kong. Le second intérêt est la volonté d'utiliser à large échelle les IDN (nom de domaines internationalisé), dans une zone géographique très favorable à son utilisation.

Les TLD en projet

- projets bien avancés
  - .berlin
- projets à l'état d'ébauche
  - .bzh projet à l'état d'ébauche mais commence à
  - et bien d'autres (.gal .sco)

Le projet d'un TLD au niveau d'une ville n'est pas illogique. En effet de TLD au niveau des villes existent déjà pour les cités-état comme Hong-Kong, Singapour car elles bénéficient d'un ccTLD. De plus, le phénomène de ccTLD "markétés" c'est à dire des ccTLD détournés de leur usage initial en ajoute quelques uns comme le .la pour Los Angeles (mais aussi le Laos).

Notons enfin le rejet régulier du .xxx pour l'industrie pornographique sous la pression du gouvernement des Etats-Unis d'Amérique.

L'avenir

On peut imaginer à l'avenir des TLD à tous les niveaux géographiques : continent, pays, région et ville.

Niveau géographique	TLD actifs	TLD en projet
Continent	ccTLD .eu	sTLD .asia
Pays	ccTLD classiques	

Région	sTLD .cat	.sco (Ecosse), .cym (Pays de Galle), .bzh (Bretagne)
Ville	ccTLD des cités etat (.hk .sg) ccTLD markété .la	.berlin .london .nyc .tokyo

Les sLD

sLD signifie domaine de second niveau. Ce sont les domaines définis sous les TLD. On prendre par exemple le ".asso" existant sous le ".fr". Le domaine complet de mon association sera donc "monassociation.asso.fr".

Selon les choix des acteurs appelés souvent registre en français ou registry en anglais, l'utilisation des sLD est soit imposée soit possible. Ou bien encore la notion de sLD est complètement inexistante.

sLD imposés

Pour les registres des ".uk" pour le Royaume-Uni et ".au" pour l'Australie, l'utilisation des sLD est imposée. Donc le nom de domaine de ma société internationale sera pour ces pays "magrandesociete.co.uk" et "magrandesociete.com.au".

sLD proposés

Deux exemples

- .fr avec les .asso.fr .presse.fr
- .us voir le RFC 1480 (juin 1993)

Dans ce cas le l'utilisation des sLD tend à stagner voir diminuer. le RFC 1480 proposait un sLD par états ou territoire membre des États-Unis. Par exemple pour la Californie, il propose le sLD ".ca" soit le domaine ".ca.us". Dans la pratique, ces sLD sont presque tous abandonnés.

sLD inexistants

C'est le cas du ".com". Le nom de ma grande société sera "magrandesociete.com". Le TLD ".com" est le TLD le plus peuplé. Il contient plus presque 50 millions de noms de domaine. Cette situation montre que le DNS pour des raisons commerciales s’éloigne de son modèle initiale hiérarchique.

Il faut remarquer un mouvement progressif vers la suppression de ces sLD. En mai 2006, le registre de la Corée du Sud a annoncé la suppression des sLD sous le le "kr".

Les acteurs du monde du DNS

- L'ICANN
- Registry ou en français registre (ex AFNIC EURID)
- Registrar (exemple GANDI)
- Registrant (le client)

La distinction entre registre et registrar est apparu vers 1999. Cette distinction sépare la partie technique de la partie commerciale et évite de placer les registres en situation de monopole.

Les registres

Les termes de registre, de registry et de NIC sont synonymes. Ils représentent des organismes gérant les TLD. Ce sont soit des organismes de recherche, soit des associations à but non lucratif, soit des sociétés commerciales.

Par exemple en France, le registre du domaine fr était d'abord un service de l'INRIA un organisme de recherche très reconnu dans le monde informatique. Maintenant, l'AFNIC association loi 1901 a repris la gestion du ccTLD ".fr". Par contre le ".tf" pour les "Terres Australes et Antarctiques françaises" étaient géré par la société commerciale AdamsNames. A la demande du gouvernement français ce ccTLD est passé sous la responsabilité de l'AFNIC (1994 voir le document de l'IANA http://www.iana.org/reports/tf-report-05aug05.pdf).

On distingue deux types de politique parmi les registres, des politiques restrictives et des politiques libérales. Ainsi, la politique du registre .com a une politique très libérale qui se traduit par "premier arrivé premier servi". Par contre les registres des ccTLD choisissent ou plutôt choisissaient des politiques restreintes. Ainsi un nom dans le domaine du .fr étaient très lié à la France. Progressivement les politiques se libéralisent. Un exemple récent est l'ouverture aux particuliers du domaine fr (juin 2006).

L'AFNIC

L'AFNIC (http://www.afnic.fr) est une association loi 1901 qui gère le .fr et le .re. Elle est en charge d'autres ccTLD liés au DOM-TOM français : tf, wf, pm et yt même si seul le tf est réellement "peuplé". Elle fournit de nombreuses documentations concernant le DNS en français.

Remarque : pour vérifier que l'AFNIC gère bien un tld, on peut regarder la base Whois de l'IANA. Mais on peut utiliser également la commande *dig SOA tld.* comme par exemple :

```
dig SOA yt.
; <<>> DiG 9.3.2 <<>> @192.168.1.1 SOA yt.
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 966
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;yt. IN SOA

;; ANSWER SECTION:
yt. 172780 IN SOA nsmaster.nic.fr. hostmaster.nic.
fr. 2006022800 3600 1800 3600000 5400

;; Query time: 1625 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Tue Jun 27 21:44:14 2006
;; MSG SIZE rcvd: 82
```

nic.fr = AFNIC ...

On peut retrouver le rapport d'activité de l'association sur son site http://www.afnic.fr/afnic/presentation/activite. Elle emploie 40 personnes et gère un budget 4,5 millions d'euros. Elle ne touche que très peu de subventions.

L'actualité récente de l'AFNIC est l'ouverture aux particuliers du .fr fin juin 2006. Pour cette opération, l'AFNIC a ouvert un nouveau site qui apparaît beaucoup moins "sérieux" que son site officiel : http://www.faites-vous-un-nom.fr/. Un autre site effectue le suivi technique de cette ouverture http://open.nic.fr/. Il est encore trop tôt à l'heure actuelle pour voir le succès de cette opération.

L'EURID

L'EURID est l'association qui gère le .eu le nouveau ccTLD pour l'Union Européenne.

Whois et IRIS

Présentation de Whois

Whois = Who is (qui est-ce ?). Ce protocole donne les correspondants techniques et administratifs associés à nom de domaine

IRIS le successeur d'IRIS

IRIS est décrit dans le RFC 3981 et son application au registre (ou registry en anglais) est décrit dans le RFC 3982

Un blog concernant IRIS avec un exemple d'application http://iris.verisignlabs.com/blojsom/blog/iris/about/

Les racines alternatives

Plusieurs raisons :

- Raisons idéologiques
- Raisons commerciales

Expériences terminées :

- Alternic (arrêté en 1997)
- eDNS (arrêté en 1998)

Mise_en_œuvre

Types de serveurs

- Serveurs primaires
- Serveurs secondaires
- Serveurs cache.

Serveurs primaires et secondaires

Les serveurs primaires possèdent les données de la zone en local. Les serveurs secondaires se connectent à un serveur primaire pour copier les données de la zone. Un primaire n'envoie pas les données aux secondaires.

Le RFC 2182 définit les bonnes pratiques de gestion des serveurs autoritaires. Il impose plus d'un serveur autoritaire par zone.

Recherches récursives et recherches non récursives.

Gestion du cache dans le DNS

Un cache est un niveau intermédiaire d'accès rapide, en ll lieu de stockage d'une information et celui de son utilisation. La notion de cache ne concerne pas uniquement le DNS mais toute l'informatique.

Dans le cadre du DNS le cache est non seulement positif mais aussi négatif (RFC 2308). Dans le cadre du DNS, une réponse négative peut représenter soit l'absence du domaine (NXDOMAIN), soit l'absence de données (No Data) le domaine est valide mais il n'y a pas d'enregistrements ou de type associé à ce nom.

Les durées de mise dépendent de durée appelée TTL pour Time To Live. Ces durées peuvent atteindre 41 jours sur les enregistrements sur les noms de serveurs de la racine.

BIND et ses alternatives

Présentation

Pour plus de détails voir : ***Le système d'exploitation GNU-Linux/Le serveur de noms BIND***.

BIND est la référence de l'implémentation d'un serveur DNS, il est d'ailleurs le serveur DNS le plus utilisé sur Internet(Référence nécessaire).

- Historique JEEVES implémentation par Paul Mockapetris d'un serveur DNS (1983)
- Depuis 1995 BIND

Deux principales versions de BIND sont maintenues.

- BIND 8
- BIND 9

Pendant longtemps il existait une autre version : BIND version 4. Elle n'est plus maintenue et donc ne doit plus être utilisée.

BIND a connu de nombreuses alertes de sécurité, a tel point que certains acteurs utilisent d'autres logiciels.

Alternatives à BIND

- NSD
- PowerDNS
- MaraDNS
- djbDNS
- myDNS

Les types d'enregistrements

Pour plus de détails voir : ***w:Liste des enregistrements DNS***.

Le type SOA

SOA définit la zone. Il contient notamment un numéro de série. Ce numéro doit toujours être augmenté en cas d'évolution de la zone. Le format conseillé est AAAAMMJJNN.

- AAAA année
- MM mois de 01 à 12
- JJ jour de 01 à 31
- NN numéro de changement du jour de 00 à 99

Exemple de SOA avec les durées conseillées par le RIPE (http://www.ripe.net/ripe/docs/dns-soa.html).

```
example.com. 3600 SOA dns.example.com. hostmaster.example.com. (
                        1999022301   ; serial YYYYMMDDnn
                        86400        ; refresh (  24 hours)
                        7200         ; retry   (   2 hours)
                        3600000      ; expire  (1000 hours)
                        172800 )     ; minimum (   2 days)
```

Le type A

A associe le nom d'hôte à l'adresse IP.

Le type PTR

PTR associe l'adresse IP au nom (conversion inverse).

Il n'est généralement utilisé que pour vérifier les serveurs qui envoient des emails (dans la lutte antispam).

Le type NS

NS donne la liste les serveurs autoritaires pour la zone.

Le type CNAME

CNAME définit des alias de nom de serveur.

Le type DNAME

Ce type est très proche de CNAME. Il définit des alias de noms de domaine, tandis que CNAME définit des alias de nom de serveur. Il est définit dans le RFC 2672.

Il est relativement rare. Il a été utilisé lors de la refonte de certains domaines, lors du passage de ip6.int à ip6.arpa par exemple. Ces domaines sont utilisés lors de la conversion inverse des adresses IPv6 en noms de domaine. Voir le document http://www.isc.org/index.pl?/pubs/tn/index.pl?tn=isc-tn-2002-1.html

Le type MX

Il est utilisé pour la messagerie électronique. Les enregistrements MX définissent les hôtes "Mail eXchanger". Il permet de définir des serveurs principaux et de serveurs de secours. Dans l'exemple suivant le serveur de messagerie sera de préférence celui avec le poids le plus petit donc rex1.ouaf.com.

```
petit-teckel.fr IN MX 0 rex1.ouaf.com
petit-teckel.fr IN MX 10 rex2.ouaf.com
petit-teckel.fr IN MX 30 rex3.ouaf.com
```

Auparavant, il existait deux types d'enregistrement MD (Mail Destination) et MF (Mail Forwarder). MD

représentaient les machines principales et MF les machines de secours. Le RFC 973 dans sa page 4 explique la raison du changement de gestion : une gestion plus efficace du cache.

Maintenant le type SRV généralise la notion de MX à tout type de service lié au domaine.

Le type HINFO

Cet enregistrement donne des informations sur le matériel et le système d'exploitation utilisé. Il est généralement masqué pour des raisons de sécurité.

Le type TXT

Il contient tout texte descriptif, notamment les règles SPF.

Il n'est généralement utilisé que pour vérifier les serveurs qui envoient des emails (dans la lutte antispam).

Le type SRV

Il s'agit d'une généralisation du type MX. Il est définit dans le RFC 2782, mais pour avoir des exemples supplémentaires on peut également regarder l'ancien RFC 2052. Il s'agit de définir les liens entre services et noms de machine.

Les enregistrements SRV peuvent permettre de retrouver la liste des serveurs HTTP ou bien encore des contrôleurs de domaines. Il est possible de donner une priorité différente à chaque enregistrement SRV. Ce type d'enregistrement est utilisé par le DNS dans le cadre d'Active Directory.

Le type WINS

WINS et WINS-R sont deux types d'enregistrement qui permettent la cohabitation entre WINS et un serveur DNS.

WINS : les enregistrements de ressources de type WINS indiquent au serveur DNS l'adresse IP d'un serveur WINS a contacter en cas d'échec lors de la résolution de nom d'hôte. Les enregistrements WINS ne peuvent être crée que dans une zone de recherche directe.

WINS-R : les enregistrements de ressources de type WINS-R ne peuvent être crée que dans une zone de recherche inversée.

Type LOC

Voir la RFC 1876 (expérimental). Ce type définit la position géographique (longitude, latitude et altitude) du serveur. Il est très peu utilisé. le seul cas d'utilisation est sur le site : http://www.ckdhr.com/dns-loc

Le message DNS

le DNS utilise UDP par défaut sauf si le message est supérieur à 512 octets. Dans ce cas, il utilise TCP. Ceci est un argument pour limiter le nombre de serveurs racine à treize.

Outils d'interrogation du DNS

- nslookup
- dig

La commande nslookup existe sous Windows, mais elle n'est pas pratique ni complète. Dig est conseillé pour travailler avec le DNS, mais elle n'existe pas par défaut sous Windows. Pour avoir cette commande sous ce système il faut récupérer la version pour Windows de BIND (http://www.isc.org/index.pl?/sw/bind/bind9.php).

Nslookup

```
nslookup
```

Dig

Cette commande est très riche. La page "man" est ici http://www.bind9.net/dig.1.

la commande "dig @192.168.1.11 txt chaos version.bind nom_serveur" permet de connaitre la version du serveur BIND. En général, cette version est masquée. Il s'agit un des rare cas où on utilise un classe différente de IN.

```
dig @192.168.1.11 txt chaos version.bind

; <<>> DiG 9.3.2 <<>> @192.168.1.11 txt chaos version.bind
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 582
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind. CH TXT

;; ANSWER SECTION:
version.bind. 0 CH TXT "9.3.2"

;; AUTHORITY SECTION:
version.bind. 0 CH NS version.bind.

;; Query time: 1265 msec
;; SERVER: 192.168.1.11#53(192.168.1.11)
;; WHEN: Thu Jun 29 20:54:52 2006
;; MSG SIZE rcvd: 62
```

Pour masquer cette version, il faut modifier le fichier named.conf

```
options {
../..
version "le numero de version est masque";
../..
};
```

L'option x de commande dig (ex dig -x adresse_ip) permet de faire la recherche inverse simplement, sans utiliser le in-addr.arpa.

```
dig -x 81.91.232.1
; <<>> DiG 9.3.2 <<>> @192.168.1.1 -x 81.91.232.1
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 404
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;1.232.91.81.in-addr.arpa. IN PTR

;; ANSWER SECTION:
1.232.91.81.in-addr.arpa. 86400 IN CNAME 1.0-127.232.91.81.in-addr.arpa.
1.0-127.232.91.81.in-addr.arpa. 86400 IN PTR ben02.gouv.bj.
```

L'option +trace de commande dig permet de faire la recherche en parcourant l'arborescence depuis la racine jusqu'à la réponse.

```
dig @192.168.1.1 +trace www.tiscali.co.uk

; <<>> DiG 9.3.2 <<>> @192.168.1.1 +trace www.tiscali.co.uk
; (1 server found)
;; global options: printcmd
. 142221 IN NS B.ROOT-SERVERS.NET.
. 142221 IN NS C.ROOT-SERVERS.NET.
. 142221 IN NS D.ROOT-SERVERS.NET.
. 142221 IN NS E.ROOT-SERVERS.NET.
. 142221 IN NS F.ROOT-SERVERS.NET.
. 142221 IN NS G.ROOT-SERVERS.NET.
. 142221 IN NS H.ROOT-SERVERS.NET.
. 142221 IN NS I.ROOT-SERVERS.NET.
. 142221 IN NS J.ROOT-SERVERS.NET.
. 142221 IN NS K.ROOT-SERVERS.NET.
. 142221 IN NS L.ROOT-SERVERS.NET.
. 142221 IN NS M.ROOT-SERVERS.NET.
. 142221 IN NS A.ROOT-SERVERS.NET.
;; Received 228 bytes from 192.168.1.1#53(192.168.1.1) in 2218 ms

uk. 172800 IN NS NS1.NIC.uk.
uk. 172800 IN NS NS2.NIC.uk.
uk. 172800 IN NS NS3.NIC.uk.
uk. 172800 IN NS NS4.NIC.uk.
uk. 172800 IN NS NS5.NIC.uk.
uk. 172800 IN NS NS6.NIC.uk.
uk. 172800 IN NS NS7.NIC.uk.
uk. 172800 IN NS NSA.NIC.uk.
uk. 172800 IN NS NSB.NIC.uk.
uk. 172800 IN NS NSC.NIC.uk.
uk. 172800 IN NS NSD.NIC.uk.
;; Received 497 bytes from 192.33.4.12#53(C.ROOT-SERVERS.NET) in 171 ms

tiscali.co.uk. 172800 IN NS ns0.tiscali.co.uk.
tiscali.co.uk. 172800 IN NS ns0.as9105.com.
;; Received 97 bytes from 195.66.240.130#53(NS1.NIC.uk) in 78 ms

www.tiscali.co.uk. 300 IN A 212.74.99.30
tiscali.co.uk. 3600 IN NS ns0.as9105.com.
tiscali.co.uk. 3600 IN NS ns0.tiscali.co.uk.
;; Received 129 bytes from 212.74.114.132#53(ns0.tiscali.co.uk) in 62 ms
```

Extensions

Les problèmes de sécurité et DNSSEC

Attaques spécifiques au DNS

Les serveurs DNS sont succeptible de subir les attaques classiques à tous serveurs. Mais ce système peut subir des attaques spécifiques que nous allons détailler ici.

Attaques de type DoS sur les serveurs root

Il s'agit d'une attaque de type DoS sur l'ensemble des serveurs pour bloquer complétement le système DNS. Une attaque de ce type à eu lieu le 21/10/2002, pendant laquelle 7 serveurs sur les 13 sont tombés. Cependant cette attaque n'a pas eu d'impact réel sur les utilisateurs.

La sécurisation du DNS avec TSIG et DNSSEC

Rappel sur la cryptographie

La sécurisation du DNS va se baser sur la cryptographie.

Les services de sécurité sont :

- la confidentialité
- l'intégrité
- l'authentification
- la non répudiation

Le RFC 3833 fait une analyse des menaces concernant le DNS et explique ce DNSSEC tente d'améliorer. Dans le cadre du DNS avec des données publiques, les services utiles sont l'authentification et l'intégrité des données :

- L'authenticité : la donnée est-elle publiée par l'entité autoritaire
- L'intégrité : la donnée est-elle conforme à celle publiée

La cryptographie va permettre de signer des messages ou de les crypter. Il existe deux types d'algorithme :

- des algorithmes à clés secrètes ou symétriques
- des algorithmes à clés publiques ou asymétrique

Dans les algorithmes à clés secrètes, la clé de chiffrement ou de signature est la même que la clé de déchiffrement ou de vérification. Dans ce cas, on utilise un secret partagé. Il faut noter que la cryptographie symétrique est plus rapide que l'asymétrique.

Dans le cas des algorithmes asymétrique la clé de chiffrement est publique tandis que la clé de déchiffrement est gardée secrète, ou plutôt la clé de signature est secrète tandis que la clé de vérification est publique. Un exemple connu d'algorithme asymétrique est RSA.

Enfin, un dernier point utile pour la notion de signature est la notion de fonctions de hachage. Elles permettent l’obtention d'une empreinte numérique de taille fixe à partir d'un message de taille variable. Un fonction de hachage utilisable dans la sécurité est celle qui engendre de faibles collisions (empreinte identique pour des messages distincts) et qui est en sens unique (difficulté de retrouver le message

d'origine).

TSIG et SIG(0)

TSIG = transaction Signature (RFC 2845). La liste des algorithmes utilisés par TSIG est maintenue par l'IANIA http://www.iana.org/assignments/tsig-algorithm-names

SIG(0)

NTP

TSIG et SIG0 signent avec un tampon de temps. Donc une synchronisation par NTP est nécessaire. Voir la présentation de NTP http://alexandre.alapetite.net/iup-gmi/ntp/ et http://fr.wikipedia.org /wiki/Network_Time_Protocol.

Une version simplifiée de NTP existe. Il s'agit de SNTP qui est notamment utilisé par Windows pour se synchroniser avec le "temps internet".

DNSSEC

DNSSEC est un ensemble d'extensions pour sécuriser le système DNS.

le projet initial (2004) de mise en place de l'infrastructure DNSSEC en France est ici : http://www.idsa.prd.fr

document de présentation de dnssec : http://ws.edu.isoc.org/workshops/2005/ccTLD-Dakar/jour4/dnssec-dakar-francais-updated.pdf

IDN

Noms de domaines dits internationaux. L'implémentation actuelle est IDNA (International Domain Name for Application). Le nom de domaine enregistré dans le dns reste écrit avec les caractères autorisés par le DNS (une partie de l'ASCII). Les applications interprête ce nom de domaine pour l'afficher les bons caractères. Pour savoir que le nom est un IDN, il commence par xn--. C'est pourquoi, il est interdit dans la plupart des cas d'enregistrer des noms de domaines commençant par cette chaine.

Attention les idn concernent également les adresses mails

Les premiers tests datent de 1998. Mais en pratique les IDN avancent lentement.

L'AFNIC n'autorise pas d'enregistrement d'IDN.

Notion de "babel name"

Exemple xn--NomDuMarqueConnue.com peut faire croire que la marque détient le domaine, alors que le préfixe laisserait supposer le contraire.

Les IDN et les TLD

Deux types d'IDN

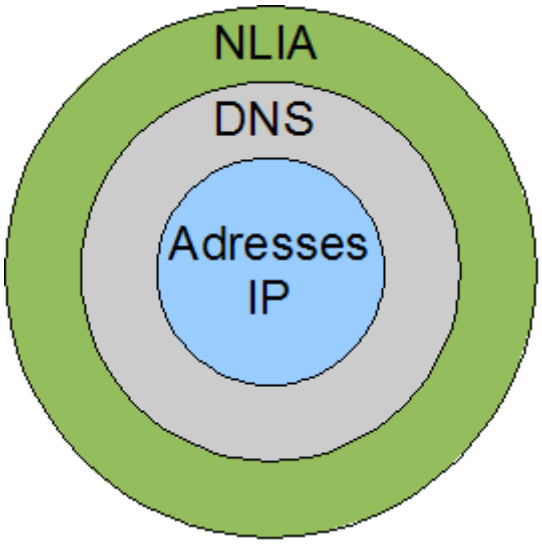
- IDN hybride idn.ascii
- IDN complet idn.idn (en fait n'existe pas encore)

Alternative aux IDN

Certains acteurs considèrent que l'IDN n'est pas satisfaisant pour permettre à accès multilingue à l'Internet. La société Netpia, http://e.netpia.com propose par exemple un système de serveurs de mots clefs, similaires au des pages jaunes ou des moteurs de recherche. Ce système est appelé "Native Language Internet Address". Les serveurs servent une zone géographique donnée utilisant la même langue ou le même système d'écriture. L'intégration du système se fait soit au niveau du navigateur (plug-in) soit au niveau du FAI (ou par la modification du serveur DNS). Le système est parti de Corée, puis s'est entendu à d'autres pays comme le Japon, pour toucher actuellement 95 pays, selon la société qui commercialise le système.

Dans ce modèle, on ajoute au dessus du DNS un système non hiérarchique. Il existe un draft de RFC datant de 2001, mais apparemment pas de RFC : http://tools.ietf.org/html/draft-jhbae-nliasa-00 . Attention, ce draft ne peut pas servir de référence. Simplement, on monte en abstraction et on se rapproche des utilisateurs finaux en passant successivement :

- Des adresses IP
- Des noms de domaine
- Des noms de domaine partiellement internationalisés
- Des noms de domaine complètement internationalisés (avec TLD internationalisés)
- Native Language Internet Address ou NLIA (mots clés internationalisés)



Il imagine un système de serveurs NLIA fonctionnant à côtés des serveurs DNS. Une requête devrait comporter trois éléments :

- Native Language Internet Address
- Informations concernant l'application
- Informations concernant la langue

La réponse dépend de l'application concernée, exemple demande sur le mot Netpia (exemple pris dans le draft) :

- Navigateur web, www.netpia.com
- client news, news.netpia.com
- client mail, webmaster@netpia.com
- client telnet, telnet.netpia.com
- client FTP, ftp.netpia.com
- Téléphone, 82 2 3665 0123

Le serveur DNS de Neptia a pour adresse IP 211.106.67.202. Certaines réponses DNS sur ce serveur sont

assez surprenantes comme le montre cet exemple.

```
dig @211.106.67.202 A ibm.

; <<>> DiG 9.3.2 <<>> @211.106.67.202 A ibm.
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 225
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;ibm. IN A

;; ANSWER SECTION:
ibm. 86400 IN A 211.106.67.202

;; AUTHORITY SECTION:
realname. 86400 IN NS update-kt.netpia.com.

;; ADDITIONAL SECTION:
update-kt.netpia.com. 102 IN A 211.106.67.221

;; Query time: 2265 msec
;; SERVER: 211.106.67.202#53(211.106.67.202)
;; WHEN: Sun Jun 25 15:46:25 2006
;; MSG SIZE rcvd: 95
```

ENUM

ENUM permet de placer les numéros de téléphone dans le DNS. Après un certaine activité au cours des années 2004 2005, les projets liés à ENUM semblent diminuer.

Le projet français Numerobis

Projet terminé ? Il a eu lieu entre 2002 et 2004.

IPv6 et le DNS

Ajout des types d'enregistrement AAAA et A6.

IPv6 commence à avancer dans de nombreux TLD. Pour le constater, on peut regarder les nombreux enregistrements de type AAAA dans le fichier root.zone disponible sur le site de le ftp de l'internic ftp://rs.internic.net/domain. On trouve environ une vingtaine de TLD en IPv6 (AT BE BIZ BR CH CN DE FR IE IT JP LU KR NET ORG PL PR PT SE TH TN TW UK).

La sécurisation de la messagerie électronique

Le courrier électronique est peu sécurisé. Les RFC 2821 et RFC 2822 qui le spécifient ne permettent pas une authentification même faible de l'émetteur. Ceci explique les nombreuses manipulations sur les en-têtes des mails.

De nombreux RFC récentes proposent des mécanismes d'authentification faible du courrier électronique. Concrètement, il indique comment définir les adresses IP ayant le droit d'émettre des mails au nom du nom de domaine. donc on authentifie uniquement le domaine et non l'émetteur complet. Il existe d'autres

mécanismes de sécurisation de la messagerie électronique qui sortent du cadre du DNS (exemple S/MIME). Deux propositions concurrentes existent : Sender ID et SPF. Ils utilisent tous les deux l'enregistrement de type TXT sur le domaine.

Sender ID

RFC 4408. Le contenu de l'enregistrement TXT commence par "spf2.0/".

SPF

RFC 4406. Le contenu de l'enregistrement TXT commence par "spf1".

Exemples d'application

AOL a mis en place SPF et Sender ID.

```
dig TXT aol.com

; <<>> DiG 9.3.2 <<>> TXT aol.com
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 684
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 2

;; QUESTION SECTION:
;aol.com. IN TXT

;; ANSWER SECTION:
aol.com. 300 IN TXT "v=spf1 ip4:152.163.225.0/24 ip4
:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.0/24
 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
aol.com. 300 IN TXT "spf2.0/pra ip4:152.163.225.0/24
 ip4:205.188.139.0/24 ip4:205.188.144.0/24 ip4:205.188.156.0/23 ip4:205.188.159.
0/24 ip4:64.12.136.0/23 ip4:64.12.138.0/24 ptr:mx.aol.com ?all"

;; AUTHORITY SECTION:
aol.com. 1071 IN NS dns-01.ns.aol.com.
aol.com. 1071 IN NS dns-02.ns.aol.com.
aol.com. 1071 IN NS dns-06.ns.aol.com.
aol.com. 1071 IN NS dns-07.ns.aol.com.

;; ADDITIONAL SECTION:
dns-01.ns.aol.com. 15742 IN A 64.12.51.132
dns-02.ns.aol.com. 15742 IN A 205.188.157.232

;; Query time: 31 msec
;; WHEN: Thu Jun 29 15:42:53 2006
;; MSG SIZE rcvd: 512
```

Microsoft a mis en place SPF.

```
dig TXT microsoft.com

; <<>> DiG 9.3.2 <<>> TXT microsoft.com
; (10 servers found)
;; global options: printcmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1548
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5

;; QUESTION SECTION:
;microsoft.com. IN TXT

;; ANSWER SECTION:
microsoft.com. 3600 IN TXT "v=spf1 mx include:_spf-a.micros
oft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com ~all"

;; AUTHORITY SECTION:
microsoft.com. 98386 IN NS ns1.msft.net.
microsoft.com. 98386 IN NS ns2.msft.net.
microsoft.com. 98386 IN NS ns3.msft.net.
microsoft.com. 98386 IN NS ns4.msft.net.
microsoft.com. 98386 IN NS ns5.msft.net.

;; ADDITIONAL SECTION:
ns1.msft.net. 92291 IN A 207.68.160.190
ns2.msft.net. 162045 IN A 65.54.240.126
ns3.msft.net. 92291 IN A 213.199.144.151
ns4.msft.net. 92291 IN A 207.46.66.126
ns5.msft.net. 162045 IN A 65.55.238.126

;; Query time: 46 msec
;; WHEN: Thu Jun 29 15:47:14 2006
;; MSG SIZE rcvd: 323
```

Et il est obligatoire d'en avoir pour pouvoir écrire à ses domaines : Hotmail, Outlook et Live[1]. Éventuellement les emails doivent contenir une signature DKIM correspondant aux DNS.

> **Remarque :** Si les règles IN TXT sont invisibles (ex : avec `dig -t txt domaine.com`) après le TTL, il suffit de retirer la règle posant problème (IN SPF).

Références

1. http://www.zebulon.fr/questions-reponses/ecrire-a-des-gens-chez-hotmail-live-133814.html

Exercices

TP

TP 1 : Programmation en java

La programmation java se base sur le package java.net.*. Voici un court programme en java effectuant une recherche d'adresse à partir d'un nom d'hôte, puis effectuant la recherche inverse.

```
import java.net.*;

public class Test1 {

        public static void main(String[] arg)
```

```
        {
                try {
                        if(arg.length<1)
                                System.out.println("Utilisation: java Test1 nom_hote\n");
                        else
                        {
                                InetAddress IPAddresse= InetAddress.getByName(arg[0]);
                                System.out.println("Adresse IP : "+IPAddresse.getHostAddr

                                InetAddress IPAddresse2=
 InetAddress.getByAddress(IPAddresse.getAddress());
                                System.out.println("Adresse Nom d'hote : "+IPAddresse2.ge
                        }

                } catch (UnknownHostException e) {
                        // TODO Auto-generated catch block
                        e.printStackTrace();
                }
        }
}
```

L'usage sera : java Test1 nom_hote

Il est naturellement possible de l'améliorer, notamment en ce qui concerne la gestion de l'erreur.

TP 2 : Utilisation simple de BIND

BIND peut avec ses fichiers de configuration comme un peu archaïque. Mais finalement, c'est le serveur DNS libre pouvant fonctionner sous Windows. En plus, il est la référence pour ce genre de logiciel. Donc, il est le plus adapté pour ce TP.

Installation de BIND sous Windows

Il est possible d'installer BIND sous Windows même sur les versions familiales de XP. Naturellement, il ne s'agit pas d'en faire un serveur de production, mais de manipuler concrètement les fichiers zones. BIND est disponible sur le site de ISC (http://www.isc.org) [archive]. Pour ce TP, je suis parti de la version 9.3.3, l'archive compressée ne fait que 3.4 Mo. En décompressant, l'archive on trouve un executable BINDInstall.exe qu'il faut lancer. L'installation va se faire dans le répertoire c:\Windows\System32\DNS (il peut toujours avoir des variantes suivant la version de Windows). Je conseille de pas cocher lors de l'installation BIND en tant que service "Start BIND Service after Install".

Maintenant BIND installé, il faut pouvoir le démarrer. Il faut ajouter au "path" le répertoire de destination des binaires de BIND. Il comporte notamment dig.exe et named.exe. Ce chemin est probablement "C:\Windows\System32\DNS\bin". Pour l'ajouter au "path", il faut aller dans le panneau de configuration, choisir "système", aller dans l'onglet "avancé" et cliquer sur le bouton "variables d'environnement". A ce niveau, il faut ajouter à la fin du path "c:\Windows\System32\DNS\bin". A la fin de cette opération, en mode dos, les commandes dig et named doivent fonctionner. La commande named se plante au bout de quelques secondes. Pour voir la log du serveur, il faut le lancer avec l'option "-g" soit "named -g". La log indique qu'il manque des fichiers de configuration.

Installation Sous Linux

Sous fedora

```
yum install bind9
```

Sous ubuntu

```
apt-get install bind9
```

Présentation du réseau

Par la suite, nous allons étudier un réseau simple d'un particulier ayant un fixe relié à l'Internet avec un boîtier du style "livebox" et un portable relié également à ce boîtier. Nous allons installer le serveur BIND sur le portable en tant que serveur primaire et sur le fixe en tant que serveur secondaire.

Notre réseau se compose :

- D'un fixe avec l'adresse ip 192.168.1.11
- D'un portable avec l'adresse ip 192.168.1.10
- Du boîtier avec l'adresse ip 192.168.1.1

L'objectif est de définir une zone tld1 et une zone sld1.tld1.

Première configuration du primaire

Il faut créer dans le répertoire "C:\Windows\System32\DNS\etc", le fichier named.conf. Ce fichier contient la liste des zones et où les trouver. Pour commencer, nous allons simplement déclarer la zone "0.0.127.in-addr.arpa" qui permet d'associer à l'adresse 127.0.0.1, le nom "localhost".

```
options {
directory "c:/windows/system32/dns/etc/namedb"; // répertoire de travail
};

//adresse 127.0.0.1
zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};
```

Maintenant, il faut définir le fichier zone "db.127.0.0". Dans le répertoire "c:/windows/system32/dns/etc /namedb".

```
$TTL 3h
0.0.127.in-addr.arpa. IN SOA portable.tld1. postmaster.tld1. (
        1; numero de serie
        1h; rafraichissement
        3h; nouvel essai
        1w; expiration
        1h; ttl negatif
        )

0.0.127.in-addr.arpa.   IN      NS      portable.tld1.

1.0.0.127.in-addr.arpa. IN      PTR     localhost.
```

A ce niveau, la commande named -g doit fonctionner correctement.

Définition de la zone "tld1" sur le primaire

Cette zone se compose des éléments :

- livebox, adresse 192.168.1.1, alias routeur
- portable, serveur primaire, adresse 192.168.1.10, alias beau-portable
- fixe, serveur secondaire, adresse 192.168.1.11, alias vieux-fixe

On modifie le fichier named.conf pour ajouter la déclaration de la zone "tld1".

```
options {
directory "c:/windows/system32/dns/etc/namedb";
};

zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};

zone "tld1" in {
type master;
file "db.tld1";
notify yes;
};
```

Et maintenant, il faut décrire notre zone "tld1" dans le fichier "db.tld1". Cette zone est composée d'un enregistrement SOA, de deux enregistrements déclarant les deux serveurs de noms, des adresses IP et enfin des alias.

```
$TTL 3h
tld1. IN SOA portable.tld1. postmaster.tld1. (
        1; numero de serie
        1h; rafraichissement
        3h; nouvel essai
        1w; expiration
        1h; ttl negatif
        )

tld1.                   IN      NS      portable.tld1.
tld1.                   IN      NS      fixe.tld1.

localhost.tld1.         IN      A       127.0.0.1
portable.tld1.          IN      A       192.168.1.10
fixe.tld1.              IN      A       192.168.1.11
livebox.tld1.           IN      A       192.168.1.1

beau-portable.tld1.     IN      CNAME   portable.tld1.
vieux-fixe.tld1.        IN      CNAME   fixe.tld1.
routeur.tld1.           IN      CNAME   livebox.tld1.
```

La zone "sld1.tld1" et délégation

Nous allons imaginer une zone "sld1.tld1" composée des éléments :

- livebox, adresse 192.168.1.1 (le nom complet est livebox.sld1.tld1)
- portable, serveur primaire, adresse 192.168.1.10 (le nom complet est portable.sld1.tld1)
- fixe, serveur secondaire, adresse 192.168.1.11 (le nom complet est fixe.sld1.tld1)

Il faut donc modifier le fichier zone "db.tld1" pour prendre en compte cette délégation. Il s'agit de déclarer les serveurs de noms pour la zone "sld1.tld1".

```
$TTL 3h
tld1. IN SOA portable.tld1. postmaster.tld1. (
        2; nouveau numero de serie
        1h; rafraichissement
        3h; nouvel essai
        1w; expiration
        1h; ttl negatif
        )

tld1.                   IN      NS      portable.tld1.
tld1.                   IN      NS      fixe.tld1.

localhost.tld1.         IN      A       127.0.0.1
portable.tld1.          IN      A       192.168.1.10
fixe.tld1.              IN      A       192.168.1.11
livebox.tld1.           IN      A       192.168.1.1

beau-portable.tld1.     IN      CNAME   portable.tld1.
vieux-fixe.tld1.        IN      CNAME   fixe.tld1.
routeur.tld1.           IN      CNAME   livebox.tld1.

sld1.tld1.              IN      NS      portable.tld1.
sld1.tld1.              IN      NS      fixe.tld1.
```

Le nouveau fichier de configuration "named.conf" comporte la déclaration d'une zone supplémentaire.

```
options {
directory "c:/windows/system32/dns/etc/namedb";
};

zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};

zone "tld1" in {
type master;
file "db.tld1";
notify yes;
};

zone "sld1.tld1" in {
type master;
file "db.sld1.tld1";
notify no;
};
```

Il faut maintenant définir le fichier zone "db.sld1.tld1", suivant la configuration de notre zone.

```
$TTL 3h
sld1.tld1. IN SOA portable.sld1.tld1. postmaster.tld1. (
```

```
        1; numero de serie
        1h; rafraichissement
        3h; nouvel essai
        1w; expiration
        1h; ttl negatif
        )

sld1.tld1.              IN      NS      portable.sld1.tld1.
sld1.tld1.              IN      NS      fixe.sld1.tld1.

localhost.sld1.tld1.    IN      A       127.0.0.1
portable.sld1.tld1.     IN      A       192.168.1.10
fixe.sld1.tld1.         IN      A       192.168.1.11
livebox.sld1.tld1.      IN      A       192.168.1.1
```

Ajout du lien avec la racine du DNS

Notre serveur répond bien aux requêtes correspondant aux éléments de notre réseau, mais il est incapable de répondre aux requêtes correspondant avec des éléments extérieurs. Nous allons ajouter un lien avec la racine du DNS. Le fichier named.conf devient :

```
options {
directory "c:/windows/system32/dns/etc/namedb";
};

zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};

zone "tld1" in {
type master;
file "db.tld1";
notify yes;
};

zone "sld1.tld1" in {
type master;
file "db.sld1.tld1";
notify no;
};

zone "." in {
type hint;
file "db.cache";
};
```

Il faut définir le fichier db.cache. Attention, il n'a pas de rapport avec la notion de cache du DNS. Son contenu est l'ensemble des serveurs racine et les adresses IP associées.

```
. 518400 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 IN A 198.41.0.4

. 518400 IN NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 IN A 192.228.79.201

. 518400 IN NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 IN A 192.33.4.12
```

```
. 518400 IN NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 IN A 128.8.10.90

. 518400 IN NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 IN A 192.203.230.10

. 518400 IN NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000 IN A 192.5.5.241

. 518400 IN NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000 IN A 192.112.36.4

. 518400 IN NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000 IN A 128.63.2.53

. 518400 IN NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000 IN A 192.36.148.17

. 518400 IN NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000 IN A 192.58.128.30

. 518400 IN NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000 IN A 193.0.14.129

. 518400 IN NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000 IN A 198.32.64.12

. 518400 IN NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000 IN A 202.12.27.33
```

Fichier zone pour la résolution inverse

Pour la résolution inverse. Il faut définir la zone "1.168.192.in-addr.arpa.". Il faut donc ajouter une dernière zone au fichier "named.conf".

```
options {
directory "c:/windows/system32/dns/etc/namedb";
};

zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};

zone "tld1" in {
type master;
file "db.tld1";
notify yes;
};

zone "sld1.tld1" in {
type master;
file "db.sld1.tld1";
notify no;
};

zone "." in {
type hint;
file "db.cache";
};
```

```
zone "1.168.192.in-addr.arpa" in {
type master;
file "db.192.168.1";
notify no;
};
```

Maintenant le contenu du fichier zone "db.192.168.1" est assez proche de "db.127.0.0". Il simplement garder à l'esprit que chaque élément possède en fait deux noms. Ce qui donne donc :

```
$TTL 3h
1.168.192.in-addr.arpa. IN SOA portable.tld1. postmaster.tld1. (
        1; numero de serie
        1h; rafraichissement
        3h; nouvel essai
        1w; expiration
        1h; ttl negatif
        )

1.168.192.in-addr.arpa. IN NS portable.tld1.
1.168.192.in-addr.arpa. IN NS fixe.tld1.

10.1.168.192.in-addr.arpa. IN PTR portable.tld1.
10.1.168.192.in-addr.arpa. IN PTR portable.sld1.tld1.

11.1.168.192.in-addr.arpa. IN PTR fixe.tld1.
11.1.168.192.in-addr.arpa. IN PTR fixe.sld1.tld1.

1.1.168.192.in-addr.arpa. IN PTR livebox.tld1.
1.1.168.192.in-addr.arpa. IN PTR livebox.sld1.tld1.
```

Configuration du secondaire

Le secondaire ne va pas avoir en local les fichiers zones mais va les récupérer lors du démarrage sur le primaire. Les zones concernés sont "tld1", "sld1.tld1" et la zone inverse "1.168.192.in-addr.arpa". Une petite adaptation sera à faire sur le fichier "db.127.0.0". Le nouveau fichier de configuration named.conf est donc :

```
options {
directory "c:/windows/system32/dns/etc/namedb";
};

zone "0.0.127.in-addr.arpa" in {
type master;
file "db.127.0.0";
notify no;
};

zone "tld1" in {
type slave;
file "db.bak.tld1";
masters {192.168.1.10; };
};

zone "sld1.tld1" in {
type slave;
file "db.bak.sld1.tld1";
masters {192.168.1.10; };
};

zone "." in {
type hint;
```

```
file "db.cache";
};

zone "1.168.192.in-addr.arpa" in {
type slave;
file "db.bak.192.168.1";
masters {192.168.1.10; };
};
```

Si tout se passe bien, les fichiers sont transféré et sont visible sur le secondaire. Lorsqu'on les regarde, on constate qu'ils utilisent un notation simplifiée avec la directive "$ORIGIN". Les noms sont des noms relatifs non terminés par un point. On a par exemple pour "db.bak.tld1" :

```
$ORIGIN .
$TTL 10800      ; 3 hours
tld1                    IN SOA  portable.tld1. franck.tld1. (
                                2 ; serial
                                3600 ; refresh (1 hour)
                                10800 ; retry (3 hours)
                                604800 ; expire (1 week)
                                3600 ; minimum (1 hour)
                                )
                        NS      fixe.tld1.
                        NS      portable.tld1.
$ORIGIN tld1.
beau-portable           CNAME   portable
fixe                    A       192.168.1.11
livebox                 A       192.168.1.1
localhost               A       127.0.0.1
portable                A       192.168.1.10
routeur                 CNAME   livebox
sld1                    NS      fixe
                        NS      portable
vieux-fixe              CNAME   fixe
```

Enfin, les serveurs peuvent être testés avec la commande Dig.

TP 3 : QCM de l'AFNIC

L'AFNIC a mis en place un très bonne présentation d'une DNS. Chaque partie se termine par un questionnaire. je propose donc de bien lire l'intégralité de ce cours et de faire les questionnaires. Attention certaines questions ne sont évidentes pour les personnes débutantes dans le DNS. Le site est http://www.afnic.fr/ext/dns/.

TP 4 : Quand wanadoo.fr devient orange.fr

En juin 2006, Wanadoo.fr devient orange.fr. Mais pour les clients la messagerie et le site web doivent toujours fonctionner avec la nouvelle adresse et l'ancienne adresse.

Regardons en détail la zone orange.fr

```
dig ANY orange.fr

; <<>> DiG 9.3.2 <<>> ANY orange.fr
; (10 servers found)
;; global options: printcmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 442
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 18

;; QUESTION SECTION:
;orange.fr. IN ANY

;; ANSWER SECTION:
orange.fr. 473 IN MX 10 smtp-in.orange.fr.
orange.fr. 2153 IN NS ns2.wanadoo.fr.
orange.fr. 2153 IN NS ns.wanadoo.fr.

;; AUTHORITY SECTION:
orange.fr. 2153 IN NS ns.wanadoo.fr.
orange.fr. 2153 IN NS ns2.wanadoo.fr.

;; ADDITIONAL SECTION:
smtp-in.orange.fr. 473 IN A 193.252.23.110
smtp-in.orange.fr. 473 IN A 193.252.22.56
smtp-in.orange.fr. 473 IN A 193.252.22.65
smtp-in.orange.fr. 473 IN A 193.252.22.78
smtp-in.orange.fr. 473 IN A 193.252.22.79
smtp-in.orange.fr. 473 IN A 193.252.22.80
smtp-in.orange.fr. 473 IN A 193.252.22.81
smtp-in.orange.fr. 473 IN A 193.252.22.82
smtp-in.orange.fr. 473 IN A 193.252.22.83
smtp-in.orange.fr. 473 IN A 193.252.22.89
smtp-in.orange.fr. 473 IN A 193.252.22.92
smtp-in.orange.fr. 473 IN A 193.252.22.107
smtp-in.orange.fr. 473 IN A 193.252.22.110
smtp-in.orange.fr. 473 IN A 193.252.22.116
smtp-in.orange.fr. 473 IN A 193.252.22.123
smtp-in.orange.fr. 473 IN A 193.252.23.67
ns.wanadoo.fr. 1441 IN A 80.12.255.24
ns2.wanadoo.fr. 304 IN A 80.12.255.159

;; Query time: 62 msec
;; WHEN: Thu Jun 29 10:46:45 2006
;; MSG SIZE rcvd: 410
```

Elle pointe bien vers wanadoo.fr. Regardons en détail la zone wanadoo.fr.

```
dig ANY wanadoo.fr

; <<>> DiG 9.3.2 <<>> ANY wanadoo.fr
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 206
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;wanadoo.fr. IN ANY

;; ANSWER SECTION:
wanadoo.fr. 158 IN NS ns11.wanadoo.fr.
wanadoo.fr. 158 IN NS ns.wanadoo.fr.
wanadoo.fr. 158 IN NS ns2.wanadoo.fr.
wanadoo.fr. 158 IN NS ns10.wanadoo.fr.
wanadoo.fr. 356 IN SOA ns.wanadoo.fr. postmaster.wanado
o.fr. 2006062801 21600 7200 604800 600
wanadoo.fr. 2471 IN MX 10 smtp.wanadoo.fr.

;; AUTHORITY SECTION:
```

```
wanadoo.fr. 158 IN NS ns10.wanadoo.fr.
wanadoo.fr. 158 IN NS ns11.wanadoo.fr.
wanadoo.fr. 158 IN NS ns.wanadoo.fr.
wanadoo.fr. 158 IN NS ns2.wanadoo.fr.

;; ADDITIONAL SECTION:
ns.wanadoo.fr. 1318 IN A 80.12.255.24
ns2.wanadoo.fr. 181 IN A 80.12.255.159
ns10.wanadoo.fr. 2498 IN A 80.12.255.23
ns11.wanadoo.fr. 1318 IN A 80.12.255.152

;; Query time: 15 msec
;; WHEN: Thu Jun 29 10:48:49 2006
;; MSG SIZE rcvd: 289
```

Visiblement wanadoo.fr ne donne pas beaucoup de renseignements. Nous allons l'interroger directement sur l'enregistrement MX.

```
dig MX wanadoo.fr

; <<>> DiG 9.3.2 <<>> MX wanadoo.fr
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1163
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 16

;; QUESTION SECTION:
;wanadoo.fr. IN MX

;; ANSWER SECTION:
wanadoo.fr. 2226 IN MX 10 smtp.wanadoo.fr.

;; ADDITIONAL SECTION:
smtp.wanadoo.fr. 82 IN A 193.252.22.56
smtp.wanadoo.fr. 82 IN A 193.252.22.65
smtp.wanadoo.fr. 82 IN A 193.252.22.78
smtp.wanadoo.fr. 82 IN A 193.252.22.79
smtp.wanadoo.fr. 82 IN A 193.252.22.80
smtp.wanadoo.fr. 82 IN A 193.252.22.81
smtp.wanadoo.fr. 82 IN A 193.252.22.82
smtp.wanadoo.fr. 82 IN A 193.252.22.83
smtp.wanadoo.fr. 82 IN A 193.252.22.89
smtp.wanadoo.fr. 82 IN A 193.252.22.92
smtp.wanadoo.fr. 82 IN A 193.252.22.107
smtp.wanadoo.fr. 82 IN A 193.252.22.110
smtp.wanadoo.fr. 82 IN A 193.252.22.116
smtp.wanadoo.fr. 82 IN A 193.252.22.123
smtp.wanadoo.fr. 82 IN A 193.252.23.67
smtp.wanadoo.fr. 82 IN A 193.252.23.110

;; Query time: 62 msec
;; WHEN: Thu Jun 29 10:52:53 2006
;; MSG SIZE rcvd: 305
```

Donc les deux zones semblent bien pointer pour les serveurs de messagerie vers les même machines. Apparemment, il s'agit d'un important cluster. Regardons maintenant la correspondance inverse, je prends l'adresse 193.252.22.100.

```
dig -x 193.252.22.110
```

```
; <<>> DiG 9.3.2 <<>> -x 193.252.22.110
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1129
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;110.22.252.193.in-addr.arpa. IN PTR

;; ANSWER SECTION:
110.22.252.193.in-addr.arpa. 86315 IN PTR smtp.orange.fr.

;; Query time: 0 msec
;; WHEN: Thu Jun 29 10:59:12 2006
;; MSG SIZE rcvd: 73
```

Elle répond smtp.orange. Ce qui semble logique : orange.fr remplace wanadoo.fr. Maintenant regardons le site web. Le site www.wanadoo.fr pointe sur le site de www.orange.fr.

```
dig A www.wanadoo.fr

; <<>> DiG 9.3.2 <<>> A www.wanadoo.fr
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 816
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 6

;; QUESTION SECTION:
;www.wanadoo.fr. IN A

;; ANSWER SECTION:
www.wanadoo.fr. 2539 IN CNAME www.wanadoo.fr.multis.x-echo.com
.
www.wanadoo.fr.multis.x-echo.com. 61 IN A 193.252.122.103
www.wanadoo.fr.multis.x-echo.com. 61 IN A 193.252.149.30

;; AUTHORITY SECTION:
multis.x-echo.com. 168757 IN NS ns2.bavoila.net.
multis.x-echo.com. 168757 IN NS ns3.x-echo.com.
multis.x-echo.com. 168757 IN NS ns3.bavoila.net.
multis.x-echo.com. 168757 IN NS ns1.x-echo.com.
multis.x-echo.com. 168757 IN NS ns1.bavoila.net.
multis.x-echo.com. 168757 IN NS ns2.x-echo.com.

;; ADDITIONAL SECTION:
ns1.x-echo.com. 11250 IN A 195.101.94.10
ns1.bavoila.net. 5134 IN A 193.252.118.130
ns2.x-echo.com. 61990 IN A 195.101.94.1
ns2.bavoila.net. 5134 IN A 193.252.122.34
ns3.x-echo.com. 62625 IN A 193.252.148.142
ns3.bavoila.net. 784 IN A 193.252.122.36

;; Query time: 62 msec
;; WHEN: Thu Jun 29 11:07:43 2006
;; MSG SIZE rcvd: 325
```

Et www.orange.fr ???

```
dig A www.orange.fr
```

```
; <<>> DiG 9.3.2 <<>> A www.orange.fr
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 436
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 6

;; QUESTION SECTION:
;www.orange.fr. IN A

;; ANSWER SECTION:
www.orange.fr. 339 IN CNAME www.orange.fr.multis.x-echo.com.

www.orange.fr.multis.x-echo.com. 182 IN A 193.252.122.103
www.orange.fr.multis.x-echo.com. 182 IN A 193.252.149.30

;; AUTHORITY SECTION:
multis.x-echo.com. 168707 IN NS ns1.bavoila.net.
multis.x-echo.com. 168707 IN NS ns2.x-echo.com.
multis.x-echo.com. 168707 IN NS ns2.bavoila.net.
multis.x-echo.com. 168707 IN NS ns3.x-echo.com.
multis.x-echo.com. 168707 IN NS ns3.bavoila.net.
multis.x-echo.com. 168707 IN NS ns1.x-echo.com.

;; ADDITIONAL SECTION:
ns1.x-echo.com. 11200 IN A 195.101.94.10
ns1.bavoila.net. 5084 IN A 193.252.118.130
ns2.x-echo.com. 61940 IN A 195.101.94.1
ns2.bavoila.net. 5084 IN A 193.252.122.34
ns3.x-echo.com. 62575 IN A 193.252.148.142
ns3.bavoila.net. 734 IN A 193.252.122.36

;; Query time: 31 msec
;; WHEN: Thu Jun 29 11:08:33 2006
;; MSG SIZE rcvd: 323
```

Nous allons regarder qui se cache derrière 193.252.122.103 et 193.252.149.30

```
dig -x 193.252.122.103

; <<>> DiG 9.3.2 <<>> -x 193.252.122.103
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2015
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;103.122.252.193.in-addr.arpa. IN PTR

;; ANSWER SECTION:
103.122.252.193.in-addr.arpa. 3600 IN PTR hpwoo.wanadooportails.com.

;; AUTHORITY SECTION:
103.122.252.193.in-addr.arpa. 86400 IN NS ns.x-echo.com.
103.122.252.193.in-addr.arpa. 86400 IN NS ns1.x-echo.com.
103.122.252.193.in-addr.arpa. 86400 IN NS ns1.bavoila.net.
103.122.252.193.in-addr.arpa. 86400 IN NS ns2.bavoila.net.

;; ADDITIONAL SECTION:
ns.x-echo.com. 53003 IN A 195.101.94.1
ns1.x-echo.com. 10262 IN A 195.101.94.10
```

```
ns1.bavoila.net. 4148 IN A 193.252.118.130
ns2.bavoila.net. 4148 IN A 193.252.122.34

;; Query time: 46 msec
;; WHEN: Thu Jun 29 11:24:01 2006
;; MSG SIZE rcvd: 238
```

```
dig -x 193.252.149.30

; <<>> DiG 9.3.2 <<>> -x 193.252.149.30
; (10 servers found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1066
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;30.149.252.193.in-addr.arpa. IN PTR

;; ANSWER SECTION:
30.149.252.193.in-addr.arpa. 3600 IN PTR vip10-junon-vlan32.x-echo.com.

;; AUTHORITY SECTION:
149.252.193.in-addr.arpa. 3600 IN NS ns.x-echo.com.
149.252.193.in-addr.arpa. 3600 IN NS ns1.x-echo.com.
149.252.193.in-addr.arpa. 3600 IN NS ns1.bavoila.net.
149.252.193.in-addr.arpa. 3600 IN NS ns2.bavoila.net.

;; ADDITIONAL SECTION:
ns.x-echo.com. 52963 IN A 195.101.94.1
ns1.x-echo.com. 10222 IN A 195.101.94.10
ns1.bavoila.net. 4108 IN A 193.252.118.130
ns2.bavoila.net. 4108 IN A 193.252.122.34

;; Query time: 78 msec
;; WHEN: Thu Jun 29 11:24:41 2006
;; MSG SIZE rcvd: 234
```

On peut également pour continuer faire des "zonecheck" pour wanadoo.fr et orange.fr http://www.afnic.fr /outils/zonecheck. La zone wanadoo.fr passe le test sans problème tandis qu'orange.fr pose problème :

La valeur du champ 'retry' est de 7200 sec, et devrait être inférieure au 'refresh' (3600 sec). La référence est le RFC1912 (p.4) "The 'retry' value is typically a fraction of the 'refresh'". L'erreur est considérée comme fatale. Dans le cas présent la zone orange.fr fonctionne en fait correctement. Il est vrai que les TTL sont assez petit.

Un dernier point serait de faire une interrogation des bases Whois pour regarder les contacts techniques (http://www.afnic.fr/outils/whois). En fait dans ce cas le contact technique ne donne pas de renseignements supplémentaires. En effet il s'agit d'une trop grande structure et en général le site web et la gestion de la messagerie sont gérés par des entités différentes.

Annexes

Rappel des liens vers Wikipédia

- BIND
- ICANN
- Anycast
- DNS
- TLD
- Serveurs DNS Racine
- Liste des Internet TLD
- DNSSEC
- Nom de domaine
- Nom de domaine internationalisé
- ENUM
- NTP
- Le fichier hosts

Commandes

- whois
- nslookup
- dig
- host

Principaux RFC

En principe les RFC sont en anglais. Cependant, certains sont traduits en français. le site suivant propose la traduction certains http://abcdrfc.free.fr/

Il existe certainement plus de 114 RFC concernant le DNS. Le site http://www.dns.net/dnsrd/rfc rassemble une majorité des RFC concernés. Cependant cette liste n'est plus mise à jour.

Les RFC historiques suivantes décrivent la situation avant la mise en place du DNS tel qu'on le connait actuellement soit avant 1983.

- RFC 606
- RFC 608
- RFC 811

Les principes du DNS se trouvent dans les RFC 1034 et RFC 1035. Ils remplacent les RFC originaux RFC 882 et RFC 883.

Mails

- RFC 2821
- RFC 2822
- RFC 4871
- RFC 5322
- RFC 5617

Sites notables

Blog

- http://www.bortzmeyer.org/

Wiki

- http://www.icannwiki.org/ (anglais)

Dictionnaire

- http://www.dicofr.com/
- http://fr.wiktionary.org/wiki/Catégorie:Lexique_en_français_des_réseaux_informatiques

Formation

- http://www.afnic.fr/doc/lexique/ lexique de l'AFNIC
- http://www.afnic.fr/doc/formations/supports autoformation à l'AFNIC
- http://www.afnic.fr/ext/dns/index.html : CD-ROM Auto-formation au DNS de l'AFNIC

Chiffres et statistiques sur les noms de domaines

- http://www.domainesinfo.fr
- http://www.commentcamarche.net/faq/1496-serveurs-dns-des-principaux-fai

Outils en ligne

- http://www.ripe.net/data-tools autorité pour les reverses DNS
- Zone-check de l'AFNIC http://www.zonecheck.fr/
- Dig en ligne http://www.galacsys.net/?fmh=T3V0aWxz&fcf=b3V0aWxzX2RpZw==
- Outils de calcul des dépendances http://www.dns.pl/cgi-bin/dnsexplorer.pl
- Convertisseur punycode http://www.nameisp.com/puny.asp
- Nombreux outils http://dns-tools.domaintools.com/
- http://www.openspf.org/Tools

Organisations importantes

- http://www.icann.org
- http://www.iana.org
- http://www.isc.org l'ISC maintient le logiciel BIND

Alternative : le projet CoDoNS

Le projet CoDoNS http://www.cs.cornell.edu/people/egs/beehive/codons.php. Le principe de ce projet est de remplacer le système de serveur DNS en utilisant la technologie peer to peer. Ce projet reprend les annuaires distribués de certains réseaux pair à pair (ou peer to peer) pour l'appliquer au DNS. Dans ce modèle, on a une séparation complète entre l'espace de noms et la mise en œuvre. Concrètement, l'annuaire utilise une "table de hachage distribuée" (voir l'article Wikipédia Table de hachage distribuée).

Pour rappel le terme *pair à pair* désigne un modèle distribué où les entités appelées pairs jouent le double rôle de client et serveur et interagissent afin d'offrir à un communauté un service de manière décentralisée. Ces réseaux utilisent comme annuaire, soit des annuaires centralisés, soit une propagation par inondation, soit des annuaires basés sur des tables de hachage distribuées.

Récupérée de « https://fr.wikibooks.org/w/index.php?title=Système_de_noms_de_domaine/Version_imprimable&oldid=442684 »

Dernière modification de cette page le 1 mars 2014 à 23:42.

Développeurs