Domain Name Service

cours@urec.cnrs.fr

DNS

- 1993: Création - Bernard Tuy -
- Modifications
  - 1997: Bernard Tuy
  - 1998: P.Leca

Plan

- Généralités
- Domain Name System : la théorie
- et ... la pratique

Nommage des Ressources Réseau

- Les équipements communiquent grâce à leur adresse IP.
- Seules les applications utilisent les noms des équipements
  - *pour certaines on peut utiliser les adresses: ftp, telnet,..*
  - *pour d'autres les noms sont indispensables: www,..*
- A une adresse IP peut correspondre un ou plusieurs noms (alias)
- Un nom doit être unique au monde

Les Correspondances Nom - Adresse IP

- Fichier /etc/hosts
  - fichier ASCII
  - mise à jour manuelle
  - gestion manuelle des ressources non locales
- NIS (Yellow Pages)
  - fichier ndbm
  - créé à partir du fichier /etc/hosts du "maître"
  - gestion manuelle des ressources non locales
- Domain Name System (DNS)
  - ensemble de fichiers ASCII
  - organisation hiérarchique et mondiale des ressources
  - mémorisation des informations recueillies (cache)

DNS : généralités (1)

- RFC 1032, 1033, 1034 et 1035
- Les Objectifs :
  - Espace de Noms mondial, cohérent, indépendant des protocoles et du système de communication sous-jacents
  - Gestion décentralisée des informations de la base de données globale
  - Usage général indépendant des types d'applications
  - ...et du type de machines : du micro au main frame !

DNS : généralités (2)

- Avantages :
  - Gestion décentralisée :
    - *administration des seules ressources locales*
    - *mais accès à toutes les ressources de l'Internet*
  - Système de "cache" :
    mémoriser les résolutions précédentes :
    - gain de temps
    - pas de surcharge inutile du réseau
  - DNS : système largement répandu, bien rôdé et standard

DNS : généralités (3)

- Inconvénients :
  - Problème de certification de l'information :
    - *les données changent lentement*
      - les couples (noms, @IP)
    - *priorité à l'accès à l'information sur les mises à jour* ***et la garantie de cohérence***

DNS : la théorie (1)

- Constituants du DNS :
  - L'Espace des Noms de domaines et les informations afférentes (*Resource Records* ou RR)
  - Les Serveurs de Noms
  - Les "Resolvers"

DNS : la théorie (2)

- L'espace des Noms est arborescent (// UFS)
- Il est divisé en niveaux de domaines :
  - Root ("")
  - Top Level Domain (com, mil, net, edu, fr, uk, de ...)
  - Secondary Level domain, ...
- A chaque Noeud ou Feuille de l'arborescence :
  - est associé un ensemble de Ressources
  - et un Nom (63 caractères maximum !)
    - *Ex.: EDU, JUSSIEU, FR, CNRS*
- Le *nom de domaine* d'un noeud :
  - suite des noms de domaines en remontant du noeud vers la racine (Root)
  - les noms de domaine de cette suite sont séparés par un "."
    - *Ex.: edu. Jussieu.fr. fr. cnrs.fr.*

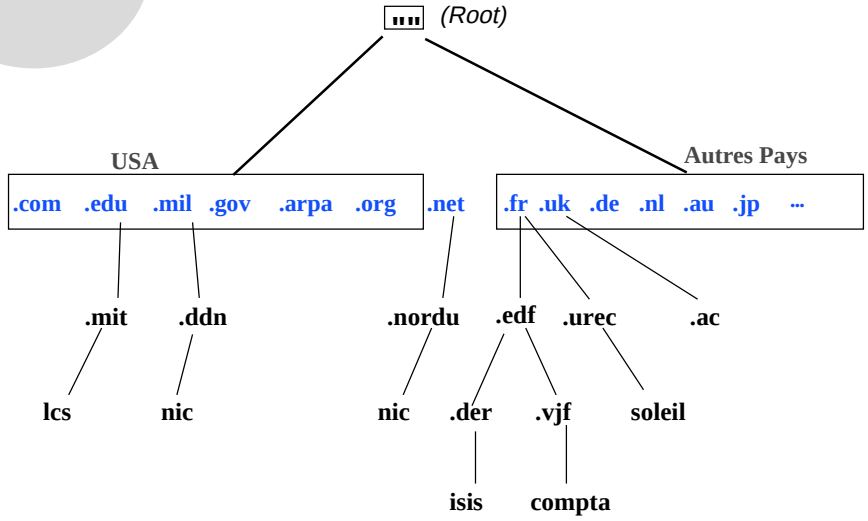
DNS : la théorie (3)

- Le nommage peut aussi être relatif
  - cela suppose que l'ORIGINE soit connue
  - Ex.: shiva.jussieu est un nom relatif au du domaine FR.
    - *on dit que FR. est l'origine courante*
- un nom de domaine (relatif ou absolu) est "limité" à 255 caractères
- un domaine est identifié par un Nom de domaine
  = c'est la sous arborescence qui a pour origine ce nom de domaine
- Un domaine inclus dans un autre est un *sous domaine*
  - Ex.: prep.ai.mi t.edu. est sous domaine de :
    - *ai.mit.edu.*
    - *mit.edu.*
    - *edu.*
    - *""*

DNS : la théorie (4)

- Quel Nom de Domaine choisir ?
  - RFC 1032
  - 63 caractères max. (conseillé : 12 caractères max)
  - A-Z, a-z, 0-9, -
  - *doit commencer par une lettre !*
- le gérant du domaine englobant le vôtre doit assurer l'unicité des noms de domaine !
  - l'UREC pour un sous-domaine de CNRS.FR.
  - le AFNIC pour un sous-domaine de FR.
  - ...

L'Espace des Noms



DNS : administration (1)

- L'administration des noms de domaine est hiérarchisée :
  - Le NIC (Network Information Center) aux Etats Unis est responsable de la ccordination mondiale : *AUTORITE*
- et décentralisée :
  - Le NIC a donné délégation à RIPE-NCC pour la gestion des Noms de Domaine en Europe :
    - *RIPE-NCC a autorité pour l'Europe*
  - RIPE-NCC a donné délégation a l 'AFNIC pour la gestion des noms de domaine en France :
    - *le AFNIC (Association Française pour le nommage internet en coopération - http://www.nic.fr) a autorité en France*
  - ...

DNS : administration (2)

- L ' AFNIC enregistre tous les noms de sous- domaine du domaine .FR.
  - avec un gérant pour chaque domaine (délégation d'autorité) :
    - *edf.fr,. est géré par la Direction de l'EDF*
    - *urec.fr. et cnrs.fr. sont gérés par l'UREC*
    - *...*
- Le gérant du domaine X.fr est responsable:
  - de la délégation des noms de domaines de la forme Y.X.fr
  - de la désignation d' un administrateur du domaine Y.X.fr

DNS : administration (3)

- Il faut contacter l 'AFNIC (http://www.nic.fr)
  - Pour faire enregistrer un nom de domaine sous .fr
  - Pour faire ouvrir la zone correspondante
- Contacter le GIP Renater (dnssvp@renater.fr ou www.renater.fr)
  - pour les entités relevant de la communauté Enseignement / Recherche
- Il faut contacter l'UREC (dnsmaster@urec.cnrs.fr ou www.urec.cnrs.fr)
  - Pour faire enregistrer un nom de domaine sous cnrs.fr
  - Pour faire ouvrir la zone X.cnrs.fr.

DNS : la théorie (6)

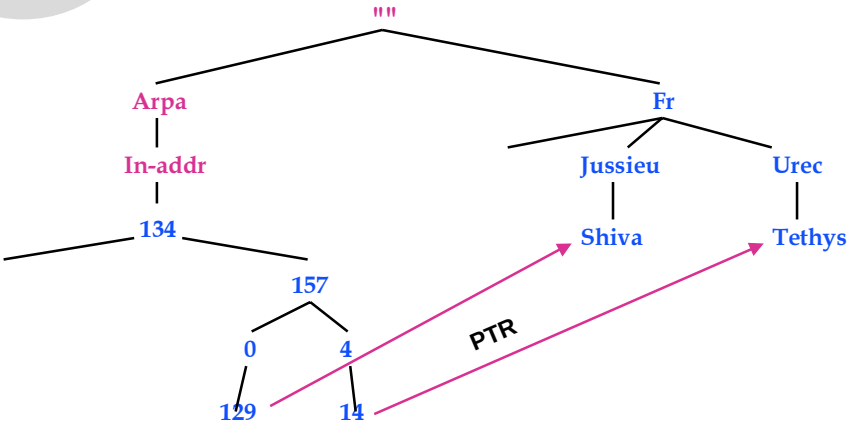
- Il n'y a pas de correspondance systématique entre un nom de domaine et une adresse de réseau IP
  - Le nom est une notion "administrative"
  - Le domaine cnrs-dir.fr regroupe 2 sites à Paris et 1 site à Toulouse
- Il y a une hiérarchie des noms de domaines
- contrairement aux adresses de réseaux

DNS : la théorie (7)

L'espace des Noms et les requêtes inverses

- réaliser la correspondance @IP -> nom
  - (nom de machine ou de réseau)
- le pseudo-domaine in-addr.arpa. et des pointeurs
  - représentation de l'espace des adresses sous forme de domaines :
  - ex: *134.157.0.129* et *134.157.4.14*

Le pseudo domaine in-addr.arpa.



DNS : la théorie (8)

Les "Resource Records" (RRs)

- Un nom de Domaine identifie un noeud de l'arbre des Noms
- 1 noeud => un ensemble d'informations (Ressources)
- Cet ensemble est décrit par des RRs
- Il peut y avoir plusieurs RRs
  - leur ordre est indifférent

Sructure d'un RR

Propriétaire	TTL	CLASSE	TYPE	RDATA f(TYPE, CLASSE)
Nom de Domaine (implicite)	Nb entier (secondes)	IN	A	@IP (32 bits)
			PTR	Nom_Dom.
		CH	SOA	
			NS	Nom_host
			MX	Nom_host
			CNAME	Nom_host
	durée de vie dans le cache		*HINFO*	Texte
			WKS	Services
			...	

DNS : la théorie (10)

- Exemples de Resource Records :

Propriétaire	Classe	Type		RDATA
ISI.EDU.	IN	MX	10	VENERA.ISI.EDU.
VENERA.ISI.EDU.		A		128.9.0.32
		A		10.1.0.52

Alias et noms canoniques

Propriétaire	Classe	Type	RDATA
Laforia.ibp.fr	IN	A	132.227.60.10
Kleio.ibp.fr		CNAME	Laforia.ibp.fr.
tethys.urec.fr		A	134.157.4.16
ns.urec.fr		CNAME	tethys.urec.fr.
ftp.urec.fr		CNAME	tethys.urec.fr.

DNS : la théorie (12)

Alias et noms canoniques :

- Un nom de Domaine ne doit jamais pointer sur un alias mais sur un Nom canonique

- Ex.:
  - 10.60.227.132.in-addr.arpa IN PTR Laforia.ibp.fr.

DNS : la théorie (13)

- ***Paramètres du SOA (RFC 1035) :***
  - ***Serial*** *No de version*
  - ***Refresh*** *Intervalle entre 2 polling des serveurs 2daires*
  - ***Retry*** *Intervalle si polling infructueux*
  - ***Expire*** *Durée de l'autorité sur la zone*
  - ***Minimum*** *Durée de vie (TTL) des RR dans un cache*
- **Exemple:**

```
1999011902      ; Version
21600           ; Refresh (6h)
3600            ; Retry   (1h)
604800          ; Expire  (7j)
86400           ; Minimum (1j)
```

DNS : Les ZONES (1)

- **Espace des Noms de Domaine est découpé en ZONES administratives**
- **Une Zone est sous l'autorité d'un Name Server (NS)**
- **Un Name Server peut avoir autorité sur plusieurs Zones**

DNS : les ZONES (2)

Définitions :

- une ZONE est délimitée par les parties contigües de l'arbre des noms de domaine sur lesquelles un NS possède une information complète.
- c'est le sous-arbre géré par une entité administrative particulière. L'autorité sur ce sous-arbre (cette Zone) lui a été déléguée.
- la délégation est totale :
  - peut changer l'organisation du sous-arbre dont il a la charge sans préavis
  - peut déléguer une partie de la Zone à une autre entité : sous-zone

DNS : les ZONES (3)

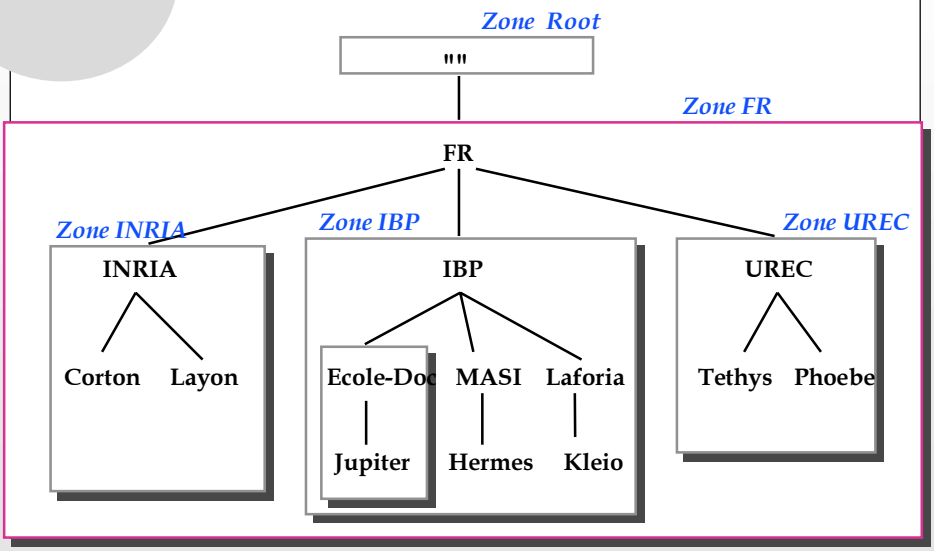
- Le nom de la Zone = Nom du noeud sommital
  - noeud sommital = noeud le plus élevé de la sous-arborescence
- coupure (entre 2 zones) :
  - n'importe où entre 2 noeuds adjacents de l'arbre
  - tous les noeuds d'une zone doivent être reliés entre eux

  => fragmentation de la base de donnée générale

  => plus grande facilité d'administration

  => mais ...

DNS : les ZONES (4)



DNS : les ZONES (5)

Création d'une nouvelle Zone (RFC 1033)

- obtenir la délégation de cette nouvelle zone
  - auprès du gérant de la "zone-mère"
  - zone-mère : zone qui inclut la nouvelle zone (1er niveau)
- Offrir un service de noms redondant
  - backup "éloigné"
- Ajouter les informations ad hoc dans la zone-mère
  - glue data

DNS : Les Serveurs de Noms (1)

- Name Servers (NS)
- Origine : BIND (Berkley Internet Name Daemon)
- Basé sur le mode client-serveur
  - Utilise une connexion TCP (port 53 pour le serveur)
  - Unix : in. Named, Windows NT: MS name server:
    - *répond aux requêtes des clients*
    - *résoud les correspondances :*
      - Nom --> @ IP
      - @IP -> Nom ...

DNS : Les Serveurs de Noms (2)

- Fonctions :
  - Répondre aux requêtes reçues concernant des ressources de sa (ses) zone(s)
  - Eventuellement répondre à des requêtes concernant d'autres zones (*cached data*)
- Il connait :
  - les @IP et les noms des ressources de sa zone
  - les @IP des NS des zones incluses (sous-zones)
  - les @IP des NS de la zone Root

    qui connaissent l'@IP des NS des sous-zones adjacentes : EDU, NET, COM, FR, UK, NL ...

DNS : Les Serveurs de Noms (3)

Résolutions des requêtes :

- mode itératif (minimal et obligatoire) :
  => Réponse = { Data | Erreur | Pointeur }
- mode récursif (facultatif, précisé par le flag RA/RD) :
  => Réponse = { Data | Erreur }

DNS : Les Serveurs de Noms (4)

- Lorsqu'un serveur reçoit une requête :
  - il répond au client si :
    - *il a l'information dans ses tables*
    - *ou dans son cache*
  - sinon, il construit une (des) requêtes pour les NS successifs (en commencant par ceux de la zone Root), et
    - soit transmet la réponse à l'auteur de la requête (mode récursif)
    - soit transmet l'@ IP du NS à interroger.
    - l'auteur de la requêtedevra interroger ce nouveau serveur (mode itératif)
- Sur chaque machine un cache mémorise toutes les résolutions précédentes

DNS : les serveurs de noms (5)

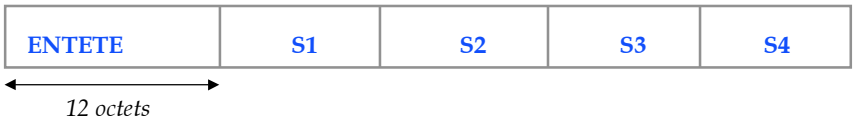
- Redondance des serveurs
  - Un serveur appelé primaire :
    - *Base d'informations d'un domaine.*
    - *Cette base est mise à jour manuellement*
    - *seule autorité sur les informations du domaine*
  - Des serveurs secondaires
    - *copie, avec mise à jour automatique, de la base d'informations du serveur primaire.*
    - *sollicitation à intervalle régulier du serveur primaire*
    - *stockent dans leur cache.*

DNS : les serveurs de noms (6)

- Remarques
  - *Il faut bien choisir son serveur primaire et ses serveurs secondaires*
  - *Penser au "." en fin des noms qui désignent un domaine absolu*
  - *Attention à modifier le numéro de version dans les tables à chaque mise à jour*

Les Requêtes et les réponses (1)

- les formats sont standardisés :
  - UDP (Port 53)
  - 512 octets maximum



Entête => Opcode : type de requête

S1 : Qname, Qtype, Qclass → Qname = Nom "canonique"
Qtype = A, PTR, MX, SOA ...
Qclass = IN, CH

S2 : RRs répondant à la requête reçue
S3 : RRs pointant vers d'autres NS
S4 : RRs "en prime"

DNS : Les Requêtes (2)

Exemple :
Requête = IBP.FR, MX ?

- S1 =
  - Qname = IBP.FR.
  - Qtype = MX
  - Qclass = IN
- S2, S3 et S4 = vides

DNS : Les Requêtes (3)

Réponse :

- S1 = d° requête
- S2 =
  - IBP.FR. MX 10 Pascal.ibp.fr.
- S3 = vide
- S4 =
  - Pascal.ibp.fr. A 132.227.60.30

DNS : Les Requêtes (4)

Remarque :

- Pour la résolution @IP -> Nom de Machine on n'utilise pas un format de requête inverse
- mais le pseudo-domaine IN-ADDR.ARPA. (RFC 1035)

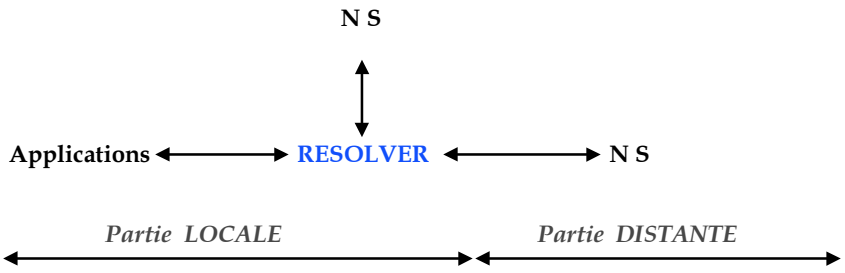
DNS : Les "Resolvers" (1)

- Fonctions :
  - Correspondance Nom -> @IP
    => RRs de type A
  - Correspondance @IP -> Nom
    => RRs de type PTR
    @IP = x.y.z.t => requête: t.z.y.x.IN-ADDR.ARPA.
  - Recherche de toute information dans la base de données de l'espace des Noms
    - *utilisation du cache*

- Objectifs :
  - réduire les délais et la charge du réseau
  - réduire le travail des NS

DNS : Les "Resolvers" (2)

- Le Resolver est une interface :



DNS : Mise en Oeuvre (1)

Les types de Serveurs de Noms :

- Pas de serveur du tout mais un Resolver !
  - pas de résolution des noms des ressources locales
  - résolution des noms des ressources distantes
- Serveur secondaire
  - l'administration des ressources locales est assurée par un tiers
- Serveur primaire
  - administration des ressources locales
  - autorité sur ces informations
- Serveur cache
  - mémorise les requêtes précédentes
  - aucune table locale
- Serveur "forwarding"
  - enrichi le cache d'un (ou plusieurs) autre(s) NS

DNS : Mise en Oeuvre (2)

Les Fichiers à configurer :

- /etc/named.boot (version bind < = 4.9.7)
- ou /etc/named.conf (version Bind > 8.0)

- /etc/resolv.conf

- "Répertoire"/root.ns
- "Répertoire"/resources
- "Répertoire"/reverse
- "Répertoire"/localhost

"Répertoire" : défini dans /etc/named.boot

DNS : Mise en Oeuvre (3)

Pour tester un NS :

- nslookup
  - *nslookup ressource*
  - *nslookup*
    > ?
  - *nslookup -type=mx ressource*

- hosts