Master d'Informatique – 1ère année

Réseaux et protocoles

DNS

Bureau S3-354
mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M1/rezo

Domain Name System

Le fonctionnement d'un réseau IP est basé sur l'adressage et le routage. En théorie, cela suffit pour pouvoir accéder à tout service disponible sur le réseau. En fait, il est fort utile (voire indispensable) de pouvoir désigner ces services par des noms.
On a donc un système de noms, réparti dans le réseau. Il permet de désigner les domaines, les machines.
Les URLs l'utilisent et permettent de préciser le protocole utilisé, la ressource précise demandée, ...

Interrogations

Le but est de convertir les noms en adresses, ou parfois l'inverse.
Dans le premier cas, on sollicitera le serveur de noms de la zone concernée (exemple info.unicaen.fr), mais dans le second celui de la zone reverse correspondante. Exemple 128.55.193.in-addr.arpa en v4,
1.0.1.7.0.6.6.0.1.0.0.2.ip6.arpa en v6
Il peut y avoir plusieurs zones reverse par zone directe (si on possède plusieurs réseaux)

Domain Name System

Rappel : structure de noms de domaine hiérarchique en arbre (ex : info.unicaen.fr. , ibm.com., ...).
Indispensable à cause de la répartition des responsabilités.

IP ne fonctionne qu'avec des adresses.
==> nécessité de conversion nom --> adresses (et inv.)

La gestion de cette conversion est aussi répartie.

Resolver

Une application qui doit convertir un nom en adresse (ou inversement) fait un appel au resolver.
Ce dernier recherche l'information demandée :

- dans un fichier local (par ex. /etc/hosts)
- dans sa mémoire cache (si déjà résolu récemment)
- en faisant appel au service d'un serveur de noms (dont l'adresse est connue du système de la machine – dans le fichier /etc/resolv.conf par exemple)

Serveur de noms

Chaque domaine (ou sous, sous-sous, ... domaine) doit en posséder un (en fait deux au moins, par sécurité).
Ce serveur contient les données concernant le domaine, sous la responsabilité de l'administrateur du domaine.
Il doit pouvoir être interrogé par tout resolver (donc par n'importe qui).

Le dialogue resolver / serveur utilise un protocole de niveau application spécifique.

Types de données

Resolver et serveur échangent donc des données relatives à un domaine. Les données sont organisées en "enregistrements" (Rrs=Ressource Records) comportant :

- un nom
- un type
- une classe
- une durée de vie
- une longueur de la partie données
- les données.

Ces enregistrements figurent dans la base de données des serveurs et peuvent être envoyés aux clients.

Le protocole du DNS

La plupart des requêtes / réponses utilisent UDP.
(le plus souvent, un seul datagramme)

Le port "bien connu" des serveurs est le 53 (décimal)

Les serveurs qui ne connaissent pas la réponse deviennent client d'un autre serveur de noms. Ils utilisent aussi le port 53 pour cela.

Le protocole permet également la mise à jour des données entre serveurs secondaires et primaire (en utilisant TCP à cause de la longueur).

Implémentation & détails

Un logiciel domine très largement : BIND
Simple au départ, assez complexe à présent.
Causes : NATs, vues internes / externes, ...

Bases de données dans fichiers textes :
Zone et Rev

Fichier de config named.conf pour déclarer les zones (direct, reverse; local, ...)

Zones

Zone pour conversion noms-->adresses (essentiellement)
ex info.unicaen.fr

Zone reverse v4 : xx.xx.in-addr.arpa
Zone reverse v6 : x.x.x.....x.ip6.arpa

Zone locale : localhost
Zone reverse locale v4 : 127.in-addr.arpa
Zone reverse locale v6 : 1.0....0.ip6.arpa

Zone "." (racine) de type hint pour récursion

Types et classes

Classe IN : internet

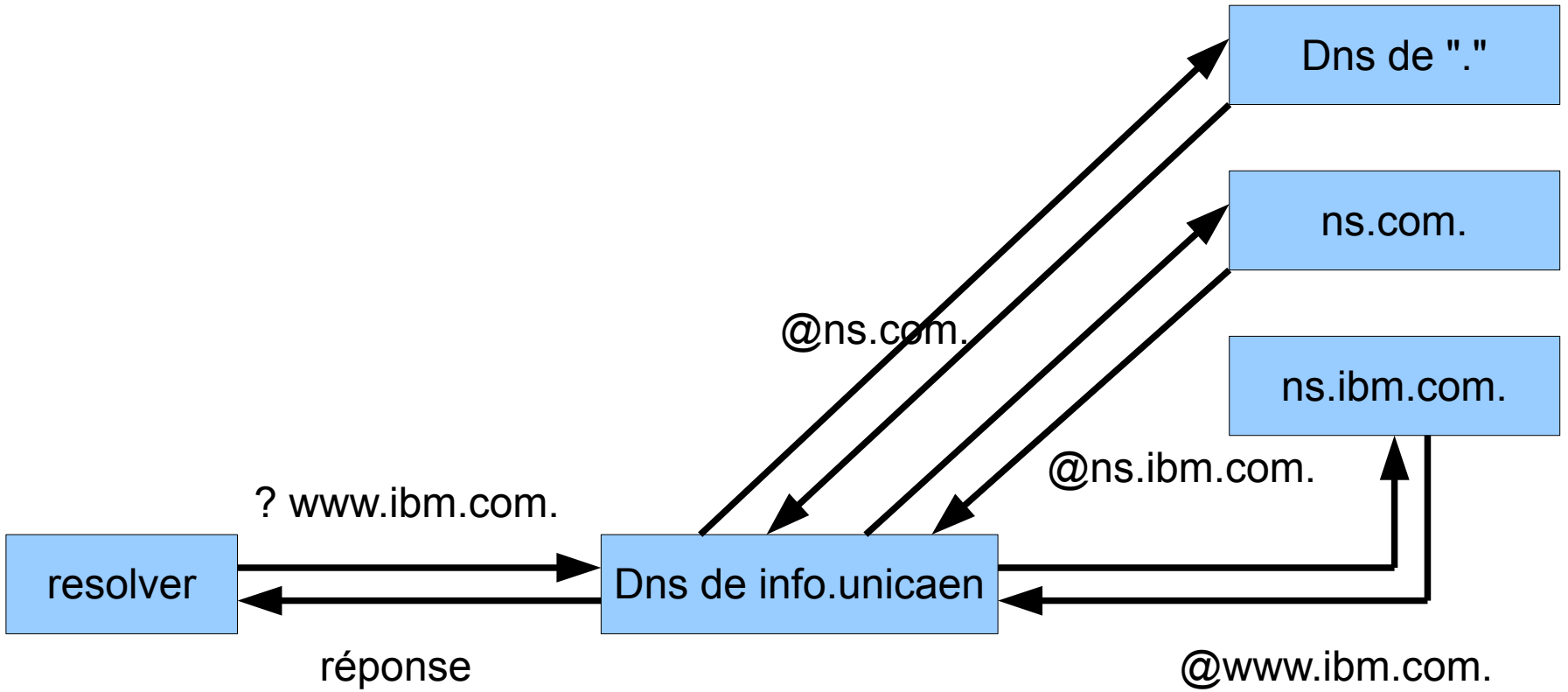
Principaux types:
A ou AAAA : adresses
PTR : pointeur (reverse)
NS : Name Servers
MX : Mail recorder
CNAME : aliases
INFO : information
TXT : texte
SOA : Start Of Authority

Fonctionnement

Le NS répond directement à toute question dont il connaît la réponse
Sinon, il recherche un serveur la connaissant,
en s'adressant d'abord à un serveur "racine" (zone ".")
(comportement par défaut) ou à un autre serveur défini par un "forwarders".

Les serveurs racine sont déclarés dans un fichier spécifique, fourni avec la distribution, pouvant être mis à jour.

Fonctionnement (exemple)



Autres RRs

Position géographique (longitude, latitude, altitude)
Permet les traceroute graphiques

Divers essais plus ou moins obsolètes

en v6 : A6 et DNAME : définition "répartie" des adresses

Interrogations

Le plus souvent records A ou AAAA ou PTR

Mais aussi :
SOA (serveur ayant autorité sur le domaine)
MX (serveur mail du domaine)
NS (serveurs de noms du domaine)
CNAME (nom canonique)

Voir l'utilisation de Host ou Dig

UDP ou TCP ?

Le plus souvent UDP, mais :

Passage en TCP si réponse trop longue
exemple : liste d'une zone complète

Pas toujours autorisé par config DNS ou firewall

TCP utilisé pour communication serveur primaire / secondaire

Champ SOA

Définit :
Le serveur ayant autorité sur le domaine
L'adresse du "postmaster"
Des paramètres de temps pour la mise à jour des serveurs secondaires, et le TTL par défaut
Le numéro de version des données
(le plus souvent sous la forme YYYYMMJJVV)

Champs courants

Nom class type donnée

Exemples :
www IN CNAME panoramix
panoramix IN A 193.55.128.30
info.unicaen.fr IN MX 10 averell
info.unicaen.fr IN NS calvin

Serveur DNS en pratique

Nous utiliserons le logiciel BIND.
Les fichiers de configuration se trouvent dans : /etc/bind

Il y a en particulier le fichier principal : named.conf à NE PAS modifier, on utilisera named.conf.local.
Il y a également des fichiers db.xx, qui nous servirons de base pour ceux qu'on ajoutera.

Localisation du serveur

On installera le serveur dns sur une machine interne, dont l'adresse DEVRA être :
192.168.xx.2 en v4
2001:660:7101:XX::2

ATTENTION ! Le XX est compris entre 10 et 1F en héxadécimal pour l'adresse v6, mais il faut le convertir en décimal pour v4.

Zone directe

Dans named.conf.local, il faut définir les zones gérées par notre serveur, par exemple :

```
zone "zonexx.tp.info.unicaen.fr" {
        type master;
        file "/etc/bind/db.zonexx";
};
```

où xx est votre numéro attribué (entre 10 et 1F, mais CONVERTI en décimal ! - ex 17 pour 11)

Zones reverses

Il faut aussi définir les zones reverse :

```
zone "xx.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.XX";
};
zone "X.X.0.0.1.0.1.7.0.6.6.0.1.0.0.2.ip6.arpa" {
        type master;
        file "/etc/bind/db.XX";
};
```

Les deux fichiers sont distincts car xx en décimal, XX en hexa !

Fichiers de données

Les données d'une zone seront précisées dans le fichier correspondant, annoncé dans le fichier named.conf.local (instruction file...).
Ces fichiers devront donc être crées, et remplis avec les données nécessaires.
Les fichiers fournis dans /etc/bind pourront être utilisés comme base (les copier vers le fichier dont le nom est celui de l'instruction file)

Fichiers de données : règles

Chaque fichier de données comportera un enregistrement SOA
Le signe « @ » remplace le nom de la zone tel que défini dans named.conf.local.
(zone directe ou reverse selon le cas)
Ce nom de zone sera automatiquement ajouté à tout nom ne se terminant pas par le signe « . »

Données à renseigner

Dans tout fichier de données : le nom du serveur de noms (choisir « ns »), enregistrement de type « NS ».
Dans le fichier de zone directe, les correspondances noms- adresse des machines (enregistrements A ou AAAA). Exemple :
www IN A 192.168.xx.3
Dans le reverse :
3 IN PTR www.zonexx.tp.info.unicaen.fr.

Remarques sur les données

Dans le fichier de zone directe, le nom « www » est automatiquement complété par le nom de la zone : tp.info.unicaen.fr.

Dans le reverse, c'est le « 3 » qui est complété par xx.168.192.in-addr.arpa., le nom correspondant (www.zonexx.tp.info.unicaen.fr.) doit être renseigné en entier car sinon le « www » serait complété par xx.168.192.in-addr.arpa.

Données : autres champs

Dans la zone directe, on pourra ajouter des alias (enregistrements CNAME), des champs d'information (TXT, HINFO).

Pour chaque modification de données, relancer le serveur pour qu'elles soient lues !
(/etc/init.d/bind restart)