Serveur DNS

- **Plan :**
  - Objectifs
  - Architecture DNS
  - La résolution des noms
  - Les requêtes récursives
  - Les requêtes itératives
  - Les types de recherches
  - Installation du service et configuration
  - Création et configuration des zones

Serveur DNS

- Objectifs
  - Sur internet les machines sont connues par leur adresse IP :
    - 32 bits en IPv4
    - 128 bits en Ipv6
  - Il est difficile voire impossible pour un être humain de mémoriser ces chiffres :
    - 2^{32} adresses en Ipv4
    - 2^{128} adresses en Ipv6
  - Il faut plutôt utiliser des noms symboliques faciles à retenir :
    - www.google.cm
    - www.cameroon-info.net

Serveur DNS

- Objectifs
  - Un serveur DNS maintient une table de correspondance entre :
    - Les adresses numériques des ordinateurs
    - Les noms symboliques utilisés par les humains
  - Il peut alors faire une résolution de noms :
    - On lui donne un nom symbolique d'une machine
    - Il retourne l'adresse numérique de cette machine
  - Il peut faire la résolution inverse de noms
    - On lui donne une adresse numérique de machine
    - Il retourne le nom symbolique de cette machine

Serveur DNS

- Architecture du DNS :
  - Elle est hiérarchique et se présente sous forme d'arbre n-aire.
  - La racine de l'arbre est appelée domaine racine et est représenté par un point :
    - Il y a treize serveurs DNS à ce niveau
  - Chaque nœud interne de l'arbre est un domaine et porte un nom différent de celui de ses frères :
    - Il y a en général un serveur DNS dans un domaine
  - Les feuilles de l'arbre sont les ordinateurs
  - **NB :** la notion de domaine est logique et ne correspond pas à une machine.

Serveur DNS

- Architecture du DNS :
  - Les nœuds de niveau 1 (fils de la racine) sont appelés TOP LEVEL DOMAIN. On y trouve :
    - Les domaines de chaque pays :
      - .cm, .ci, .cn, .fr, .us, .uk
    - Les domaines correspondant aux grands secteurs d'activités sur le plan mondial :
      - .com, .net, .org, .mil, .gov, .edu
  - Chaque nœud de niveau 1 peut avoir des nœud enfants du niveau 2
  - Chaque nœud de niveau i, peut avoir un nœud enfant de niveau i+1

Serveur DNS

- Architecture du DNS :
  - Le nom complètement qualifié (Fully Qualified Domain Name FQDN) d'un nœud feuille (machine) est tout simplement une chaîne composée du nom du nœud et de l'ensemble des noms des nœuds parents séparés par des points :
    - WWW.ISESTMA.CAMTEL.CM
  - Un FQDN tient au plus sur 255 caractères.
  - Un serveur DNS ne gère pas toute l'arborescence. Il gère en général seulement son domaine et délègue le domaine enfant à un autre serveur DNS.

Serveur DNS

- L'arbre des noms de domaines d'internet est généralement organisé en zones.
- Une zone est le sous arbre géré par une autorité administrative donnée :
  - Elle peut comporter plusieurs domaines.
  - Elle peut aussi n'être qu'une partie d'un domaine.
  - Elle peut enfin correspondre à un domaine.
  - Elle est gérée par un serveur de noms.
  - Son nom est donné par le nom du noeud le plus élevé dans la hiérarchie de l'arbre de noms.

Serveur DNS

- La résolution de noms :
  - Dans la configuration d'un hôte il est en général indiqué l'adresse IP de son serveur de noms.
  - Il s'adresse à ce dernier pour obtenir l'adresse d'un hôte à partir de son nom symbolique complètement qualifié (interrogation récursive).
  - Si le serveur DNS peut résoudre le nom, alors il envoie l'adresse IP à l'hôte.
  - Sinon il interroge itérativement :
    - Un serveur racine
    - Et éventuellement tous les serveurs des domaines indiqués dans son FQDN autres que son serveur DNS.
    - Si l'un d'eux a le nom, il le retrourne au serveur DNS de l'hôte qui la remet en définitive à l'hôte.

Serveur DNS

- La résolution de noms :
  - Elle peut être récursive ou itérative :
    - Dans la recherche itérative, le serveur à qui on demande de faire une résolution, s'il n'a pas la réponse, indique un autre serveur à qui demandé
    - Dans la recherche récursive, le serveur à qui on demande de faire une résolution, doit retourner l'information recherché ou une réponse négative au demandeur.

Serveur DNS

- La résolution de noms :
  - En général, un hôte intérroge son serveur DNS de façon récursive.
  - Le serveur DNS d'un domaine interroge les serveurs DNS des autres domaines de façon itérative.
- Un serveur DNS qui gère une zone connaît :
  - les adresse IP et les noms des ressources de sa zone
  - les adresses IP des serveurs de noms des zones incluses (sous-zones)
  - les adresses IP des serveurs de noms de la zone racine.

Serveur DNS

- La résolution inverse de noms :
  - Il s'agit de trouver un nom symbolique d'hôte, connaissant son adresse IP.
  - Un domaine spécial appelé in-addr.arpa a été créé au niveau 1 de l'arbre des domaines DNS
  - Ce domaine contient des références vers les domaines à qui on a alloué un certain bloc d'adresses.
  - Les adresses sous forme pointée forme un arbre que l'on utilise comme lors de la recherche directe.
- **NB :** La résolution inverse apporte un peu plus de sécurité. Elle peut permettre de détecter un hôte qui usurpe l'identité d'un autre hôte.

Serveur DNS

- Différents types de serveurs :
  - serveur de noms primaire : il maintient les données maîtres sur une zones. Il charge ces données à partir des fichiers de zones édités par l'administrateur manuellement ou à l'aide d'un outil de configuration, ou suite à des mises à jour automatique.
  - Serveur de noms secondaire: il charge les informations sur la zone à partir d'un transfert de données détenues par un autre serveur (qui en général est primaire, mais qui peut être aussi secondaire).
- **NB :** les serveurs primaires et secondaires ont chacun un enregistrement de type NS dans la zone mère ainsi que dans la zone sur laquelle ils ont autorité.

Serveur DNS

- Différents types de serveurs :
  - « stealth name server » ou serveur de noms furtif :
    - Il se comporte comme l'un ou l'autre des serveurs précédents,
    - mais il n'a pas reçu de délégation de la zone mère.
    - Il n'apparaît pas dans les fichiers de zones de la zone mère.
  - **Serveur cache:** Il s'agit de serveurs de noms qui gardent les informations de résolution en mémoire, pour une éventuelle autre résolution plus tard.

Serveur DNS

- Installation du service DNS :
  - Sous linux :
    - sudo apt-get install bind9
    - Les fichiers de configuration se retrouvent dans :
      - /etc/bind/named.conf // fichier principal
      - /etc/bind/named.conf.default-zones
      - /etc/bind/named.conf.local // es configurations locales ici
      - /etc/bind/named.conf.options
      - /etc/bind/db.root // la base des serveurs racine
    - Chez le client configurer le resolveur. C'est le logiciel qui fait la resolution de noms. Il recupère l'adresse du serveur dans /etc/resolv.conf
    - Créer les fichiers de zones directe et les fichiers de zones inverses

Serveur DNS

- Installation du service DNS :
  - Sous windows server :
    - Installer windows server
    - Ajouter le rôle dns
    - Ajouter le rôle active directory
    - Autoriser le service dns dans active directory
    - Création des zones directe et indirecte

Serveur DNS

- Les enregistrements (ressources) d'un fichier de zone directe
- La forme générale d'un enregistrement est la suivante :
  - **[owner] [ttl] [class] type data**
  - Où :

owner : identifie le domaine ou le nom d'hôte associé à l'enregistrement. Si pas donné, l'enregistrement se rapporte au nom donné dans l'enregistrement précédent

ttl : indique le temps de validité de l'info, une fois obtenu la réponse du serveur DNS. Si pas donné, la valeur du dernier enregistrement Start Of Authority (SOA) est utilisée.

class : spécifie une classe d'adresse, par exemple IN pour TCP/IP

type : liste de types de l'enregistrement. Ce champ est obligatoire (par exemple NS, A, SOA,...etc).

data : spécifie les données associées à l'enregistrement . Ce champ est obligatoire.

Serveur DNS

- Enregistrement de type SOA (Start Of Autority) :

@ IN SOA dm1.dm. root.dm1.dm. (

20160311001 ; serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

NB : on peut commencer par @ à la place de dm1.dm.

Serveur DNS

- Enregistrement de type SOA (Start Of Autority) :

Il indique toutes les informations sur le domaine :

- le nom de la zone

- le numéro de série incrémenté à chaque mise à jour de la zone

-le délai de mise à jour des bases de données entre serveurs de noms primaires et secondaires

- le nom du responsable du domaine

- le délai avant un nouvel essai de récupération des données

- le temps pour l'expiration des données

Serveur DNS

- Autres enregistrements :

enregistrement de type NS (name server) : il donne l'adresse d'un serveur de nom pour le domaine

```
dm1.dm.      IN    NS    monDNS.dm1.dm1.
Dm1.dm.      IN    NS    monDNSSec.dm1.dm.
```

Le «. » final signifie que le nom est pleinement qualifié. On aurait pu mettre :

```
@            IN    NS    monDNS.dm1.dm.
             IN    NS    monDNSSec.dm1.dm.
```

Serveur DNS

- Autres enregistrements :

enregistrement de type A (adresse): il donne l'adresse d'un hôte du domaine

machine1.dm1.dm.IN A 192.168.20.1

machine2.dm1.dm.IN A 192.168.20.2

localhost.dm1.dm. IN A 127.0.0.1

….. autres machines ici

Serveur DNS

- Autres enregistrements :

enregistrement de type CNAME (canonical name): il permet de définir des alias pour certains hôtes permettant ainsi qu'ils soient désignés par des noms différents :

```
www     IN    CNAME    monDNS.dm1.dm.
ftp     IN    CNAME    monDNS.dm1.dm.
```

Serveur DNS

- Autres enregistrements :

enregistrement de type MX (mail exchanger): il permet d'indiquer quel hôte est le serveur de messagerie :

@ IN MX Nbre mail

mail.dm1.dm. IN A 192.168.20.10

NB : Nbre est une priorité associée au serveur de messagerie. Le serveur de plus petit numéro est le plus prioritaire.

Serveur DNS

- Enregistrements d'un fichier de zone inverse :
  - L'enregistrement SOA est le même
  - L'enregistremen NS est le même
  - **Enregistrement de type PTR (pointer):** il permet la résolution de noms inverse dans le domaine

    in-addr.arpa :

1.20.168.192.in-addr.arpa. INPTR monDNS.dm1.dm.

2.20.168.192.in-addr.arpa. IN PTR monDNSSec.dm1.dm.

10.20.168.192.in-addr.arpa. IN PTR mail.dm1.dm1.

Serveur DNS

- Exemple de fichier de configuration :

```
zone "isestma.cm" in {
        notify no;
        type master;
        file "/etc/bind/db.isestma";
};

zone "20.168.192.in.addr.arpa" in {
        notify no;
        type master;
        file "/etc/bind/db.isestma.rev";
};
```

Serveur DNS

- $TTL 854600
- isestma.cm. IN SOA dns.isestma.cm. gtindo.isestma.cm. (
- 2016032201;
- 604000;
- 84600;
- 2419600;
- 604000;
-)
- isestma.cm. IN NS dns.isestma.cm.
- www IN CNAME dns.isestma.cm.
- ftp IN CNAME dns.isestma.cm.
- dns.isestma.cm. IN A 192.168.20.1
- localhost.isestma.cm. IN A 127.0.0.1
- machine1.isestma.cm.IN A 192.168.20.2
- machine2.isestma.cm.IN A 192.168.20.3

Serveur DNS

- Exemple de fichier de zone inverse:

```
$TTL  854600
@   IN    SOA   dns.isestma.cm. gtindo.isestma.cm. (
2016032201;
604000;
84600;
2419600;
604000;
)

@   IN   NS     dns.isestma.cm.
1  IN    PTR    dns.isestma.cm.
2  IN    PTR    machine1isestma.cm.
3  IN    PTR    machine2.isestma.cm.
```

Serveur DNS

DELEGATION:On considère la sous zone ebages.isestma.cm

Pour configurer la délégation, dans le fichier de zone directe de isestma.cm on met des enregistrements décrivant les serveurs de ebages :

```
ebages          64600   NS      serveur1.ebages.isestma.cm.
                64600   NS      serveur2.ebages.isestma.cm.
serveur1.ebages.isestma.cm. IN      A       192.168.30.1
serveur2.ebages.isestma.cm. IN      A       192.168.30.2
```

Dans le fichier de zone inverse il faut faire aussi une délégation:

```
ebages                  IN   NS    serveur1.ebages.isestma.cm.
                        IN   NS    serveur2.ebages.isestma.cm.
1.30.168.192.in-addr.arpa   64400  IN  PTR  serveur1.ebages.isestma.cm.
2.30.168.192.in-addr.arpa   64400  IN  PTR  serveur2.ebages.isestma.cm.
```