

Fiche : DNS/DHCP.

DNS.

Le service DNS était fait pour Internet mais il s'est démocratisé sur les réseaux locaux.

On va centraliser l'information grâce aux Active Directory (annuaire).

Le DNS (**Domain Name System**) est un service permettant d'établir une correspondance » entre un nom de domaine et une adresse IP.

Créé par **Paul MOCKAPETRIS** en 1983, ce protocole est un des piliers d'Internet et des réseaux locaux maintenant.

Ce type de serveur fonctionne **en UDP** et utilise le **port 53** par défaut.

Fonctionnement du service DNS.

A l'heure actuelle même sur les réseaux d'entreprise, le service DNS est utilisé :

- Pour affecter des noms aux machines en local.
- Pour établir un relai vers les serveurs DNS d'internet et des FAI.

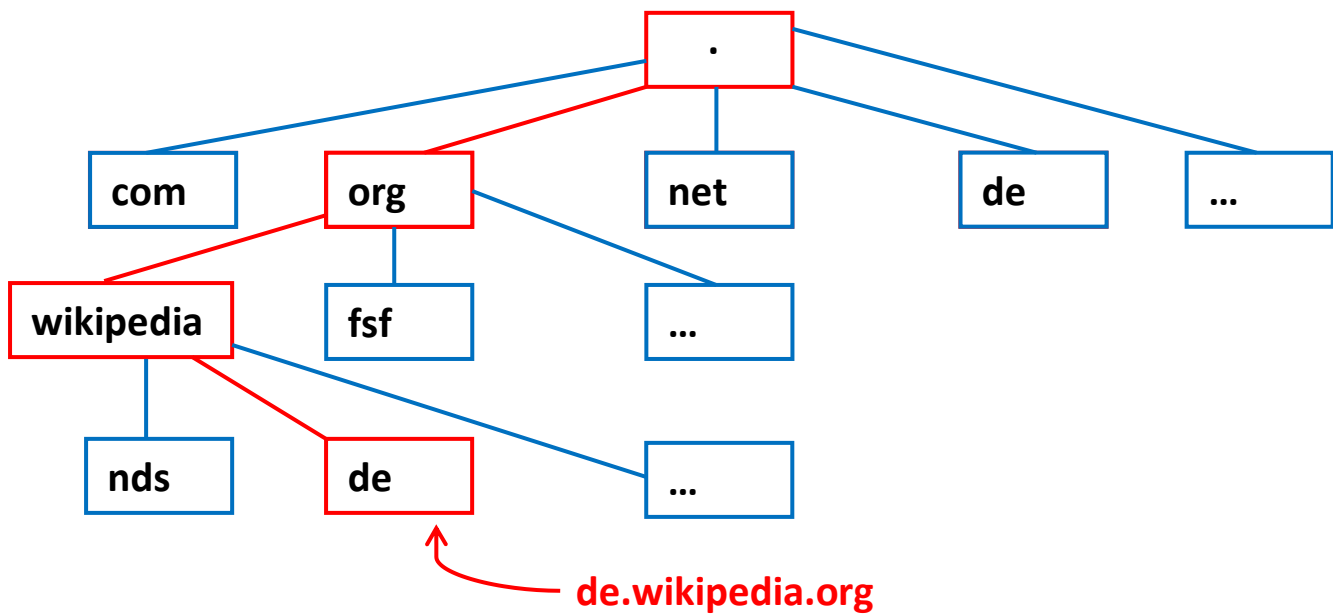
Ainsi une IP sur Internet peut correspondre à un nom de domaine. En local, on utilisera souvent des noms de domaines fictifs : stesio.local accessible uniquement à l'intérieur du réseau de l'entreprise.

Ce système fonctionne de manière hiérarchique sous forme d'arborescence. Le sommet de cette arborescence est appelé la « racine » (analogie avec le système Unix).

Ensuite, il est possible de créer des sous-domaines.

On peut également réaliser une résolution inverse CIDR d'une adresse IP vers un nom.

En termes de sécurité, le protocole DNSSEC a été développé sur le même modèle que le système VPN IPSEC.



A : record ou address record qui fait correspondre un nom d'hôte à une adresse IPv4.

AAAA : record ou IPv6 address record.

CNAME: record ou canonical name record qui permet de faire d'un domaine un alias, (ex : www.monpingouin.fr CNAME monpingouin.fr).

MX : record ou mail exchange record qui définit les serveurs de courriel pour ce domaine.

PTR : record ou pointer record qui associe une adresse IP à un enregistrement de nom de domaine(ex : 88.10.0.1 PTR monpingouin.fr).

NS : record ou name server record qui définit les serveurs DNS de ce domaine (ex : ns1 monpingouin.fr NS).

SOA : record ou Start Of Authority record qui donne les informations générales de la zone.

Questions sur le DNS :

Quelle solution de nom de domaine peut-on proposer à quelqu'un qui possède une adresse IP publique dynamique (qui change régulièrement) ? **On demande à avoir un service d'adresses IP fixe.**

Que doit-on privilégier dans le cas d'une entreprise ?

Les commandes de diagnostic DNS sur les machines clientes :

Si vous voulez réaliser un **ping** google.fr, la translation se réalisera naturellement si votre configuration DNS est correcte.

La commande **dig** permet d'obtenir des informations précieuses sur un serveur DNS.

La commande **whois** est un outil permettant d'interroger des bases d'informations (appelées registres) concernant les noms de domaines et adresses IP.

Lorsque vous êtes sur un poste client penser à vérifier le bon fonctionnement de DNS en cas de problème.

Commandes de gestion de cache DNS sous Windows et Linux :

Ipconfig suivi des options suivantes :

- **/flushdns.**
- **/displaydns.**
- **/registerdns.**

Par défaut sous Linux, le cache n'est pas géré, il faut installer l'utilitaire nscd pour changer cela.

Configuration DNS des machines clientes.

Sur Windows en cas d'adresses statiques, les serveurs DNS sont à préciser dans les propriétés TCP/IP de la carte réseau. Pourquoi y-a-t-il deux serveurs DNS à spécifier ? Il y en a un de secours.

Sur Linux, il faut éditer le fichier `/etc/resolv.conf` et ajouter la ligne :

```
Nameserver x.x.x.x
```

```
Search nomdudomaine.com
```

Que se passe-t-il lorsque l'on fonctionne en adressage automatique ? On précise qu'il doit attribuer une passerelle et un DNS.

Serveur DNS.

Sous UNIX, un service appelé BIND utilisé principalement sur Internet et dans les entreprises ayant les compétences nécessaires.

Sous Windows 2003, 2008 Server, un service DNS intégré utilisé avant tout sur des réseaux locaux.

Bind est beaucoup plus optimisé et complet que l'outil microsoft mais demande de la rigueur puisqu'il est configurable à l'aide de fichiers de configuration.

DHCP.

Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station.

On peut attribuer aux clients :

- Une adresse IPv4 ou IPv6.
- Un masque.
- Une passerelle.
- Un serveur DNS.
- Un bail pour l'adresse.

Fonctionnement de DHCP :

BOOTP est l'ancêtre de DHCP, vous pouvez trouver ce protocole sur certain matériel mais il est vivement conseillé de privilégier DHCP qui est plus récent et plus stable.

Le client envoie au démarrage une requête de diffusion de type DHCP sur le port 67 de n'importe quel serveur.

Tout serveur DHCP ayant reçu la requête renvoie une réponse sur le port 68 du client de type DHCP OFFER.

Le client répond au DHCP OFFER par une requête de type DHCP REQUEST pour donner des informations au serveur nécessaires à l'attribution d'adresses.

Enfin, le serveur attribue les paramètres suite à une requête de type DHCP Ack.

Gestion DHCP sur des machines clientes :

Sous Windows, à l'aide de la commande ipconfig :

- /renew.
- /release.
-

Sous Unix en général, le service client DHCP se nomme dhclient :

Pour l'ensemble des options consulter les manpages.

Questions sur DHCP :

- Si un serveur DHCP est placé derrière un routeur, comment les clients font-ils pour obtenir leurs adresses IP ? **Sur le routeur on va pouvoir configurer un agent pour laisser passer les requêtes de diffusion.**
- Si le serveur DHCP tombe en panne quelle est l'adresse attribuée par le système statique ?
- Quels sont les avantages et les inconvénients d'un système d'adressage automatique par rapport un système statique ? **On gagne en simplicité mais moins de lisibilité.**

CONCLUSION.

DHCP Et DNS sont des protocoles liés aux postes de travail clients. Sans eux, ces postes peuvent connaître des problèmes.

Vous devrez être en mesure dans un cadre professionnel, d'intervenir sur ce type de machine. Vous devrez diagnostiquer le problème et connaître les commandes permettant de résoudre.