Présentation

Qu’est-ce que le DNS ?

Le **DNS**, ou *Domain Name System*, est un système indispensable au fonctionnement d’Internet. Son rôle est de traduire les **noms de domaine** que l’on utilise tous les jours (comme `google.com`, `rakouns.bzh`, ou `wikipedia.org`) en **adresses IP** compréhensibles par les machines.

En effet, les ordinateurs, les serveurs et tous les équipements réseau communiquent entre eux à l’aide d’adresses IP. Mais pour les humains, il serait difficile de mémoriser une série de chiffres pour chaque site. Grâce au DNS, on peut simplement taper un nom lisible dans le navigateur, et celui-ci sera automatiquement converti en adresse IP en arrière-plan.

À quoi ça sert ?

Le DNS joue un rôle de **répertoire téléphonique** d'Internet. Lorsqu'on entre une adresse web dans un navigateur, ce dernier interroge un serveur DNS pour demander : "À quelle adresse IP correspond ce nom de domaine ?"

Le serveur répond avec l'adresse IP du site, et le navigateur peut ensuite établir la connexion. Ce processus est invisible pour l'utilisateur, mais il se produit à chaque requête, souvent en quelques millisecondes.

Sans DNS, il faudrait connaître et entrer manuellement l'adresse IP de chaque site ou service en ligne. Ce serait non seulement fastidieux, mais quasiment inutilisable à grande échelle.

Comment ça fonctionne, en pratique ?

Dès qu'un appareil tente de se connecter à un nom de domaine, il envoie une **requête DNS** à un serveur spécifique. Ce serveur peut être :

- celui fourni par la box ou le fournisseur d'accès Internet,
- un service public comme **Cloudflare (1.1.1.1)** ou **Google DNS (8.8.8.8)**,
- ou un serveur DNS interne, dans les réseaux professionnels.

Si le serveur a déjà la réponse en mémoire (ce qu'on appelle le cache DNS), il répond immédiatement. Sinon, il interroge d'autres serveurs dans une chaîne hiérarchique, jusqu'à obtenir une réponse fiable.

Une fois l'adresse IP récupérée, elle est utilisée pour établir la communication avec le site demandé.

Et dans un réseau local ?

Dans un réseau d'entreprise, il est courant d'utiliser un **serveur DNS interne**. Celui-ci peut résoudre des noms comme `serveur-fichiers.local` ou `intranet.entreprise` en adresses IP locales. Cela facilite la gestion du parc informatique, la maintenance des services, et améliore la lisibilité pour les utilisateurs et les administrateurs.

Le DNS interne peut aussi être couplé à d’autres services comme **Active Directory**, pour gérer dynamiquement les machines et les comptes utilisateurs dans un environnement Windows.

Le DNS, un maillon critique

Parce qu’il intervient dans toutes les connexions, le DNS est aussi une **cible privilégiée des attaques**. Il existe des solutions pour sécuriser son usage, comme :

- le **DNSSEC**, qui garantit l’intégrité des réponses,
- le **DoH (DNS over HTTPS)** ou **DoT (DNS over TLS)**, qui chiffrent les requêtes pour éviter qu’elles soient espionnées.

Certaines solutions comme **AdGuard Home** ou **Pi-hole** utilisent aussi le DNS comme point de contrôle, pour bloquer les publicités, les malwares ou les services indésirables.

En résumé

Le DNS est un service invisible mais essentiel. Il rend le web lisible, accessible et fluide pour les utilisateurs, tout en restant extrêmement puissant et flexible pour les administrateurs réseau. Chaque fois qu’on accède à un site, qu’on envoie un mail ou qu’on utilise une application connectée, le DNS est là, en arrière-plan, pour faire le lien entre les noms et les adresses.

Revision #1
Created 2025-10-29 12:40:41 UTC
Updated 2025-10-29 12:40:42 UTC