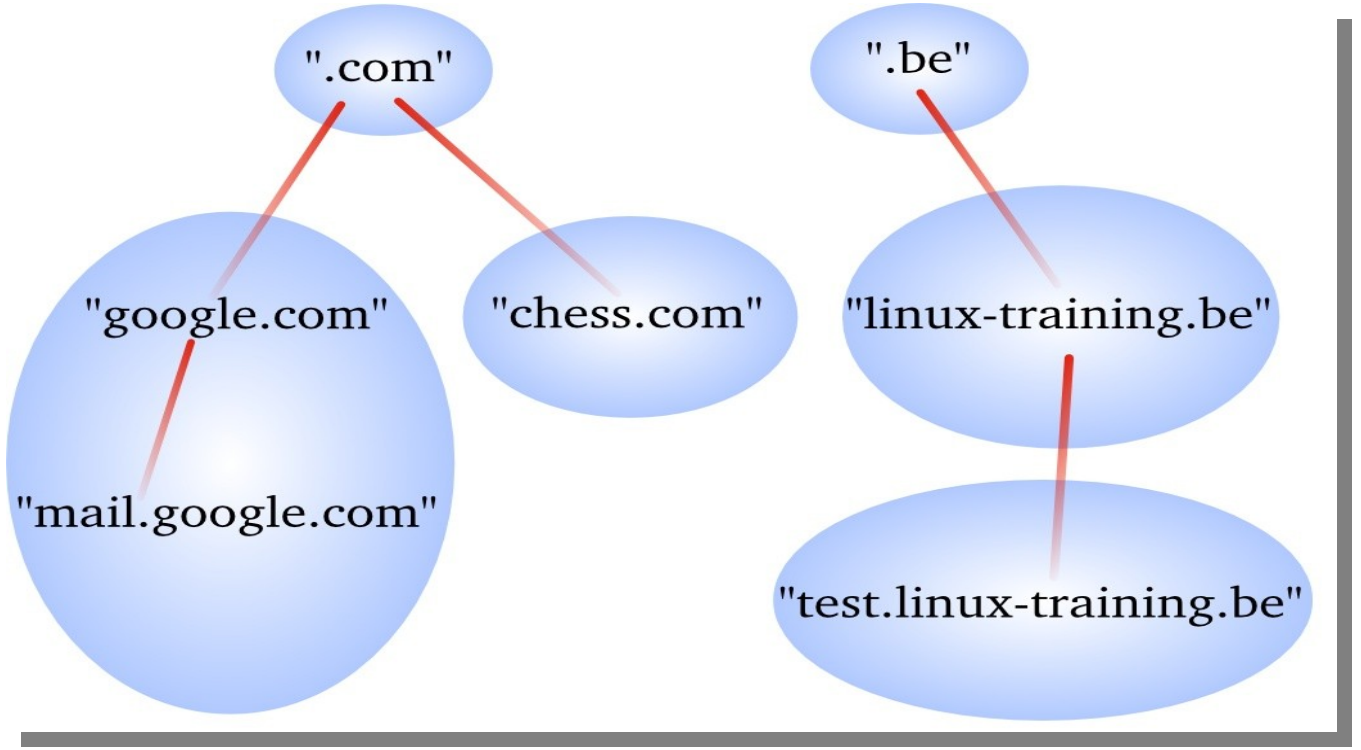
COURS THEORIQUE – SERVICE DNS SUR WINDOWS SERVER 2025

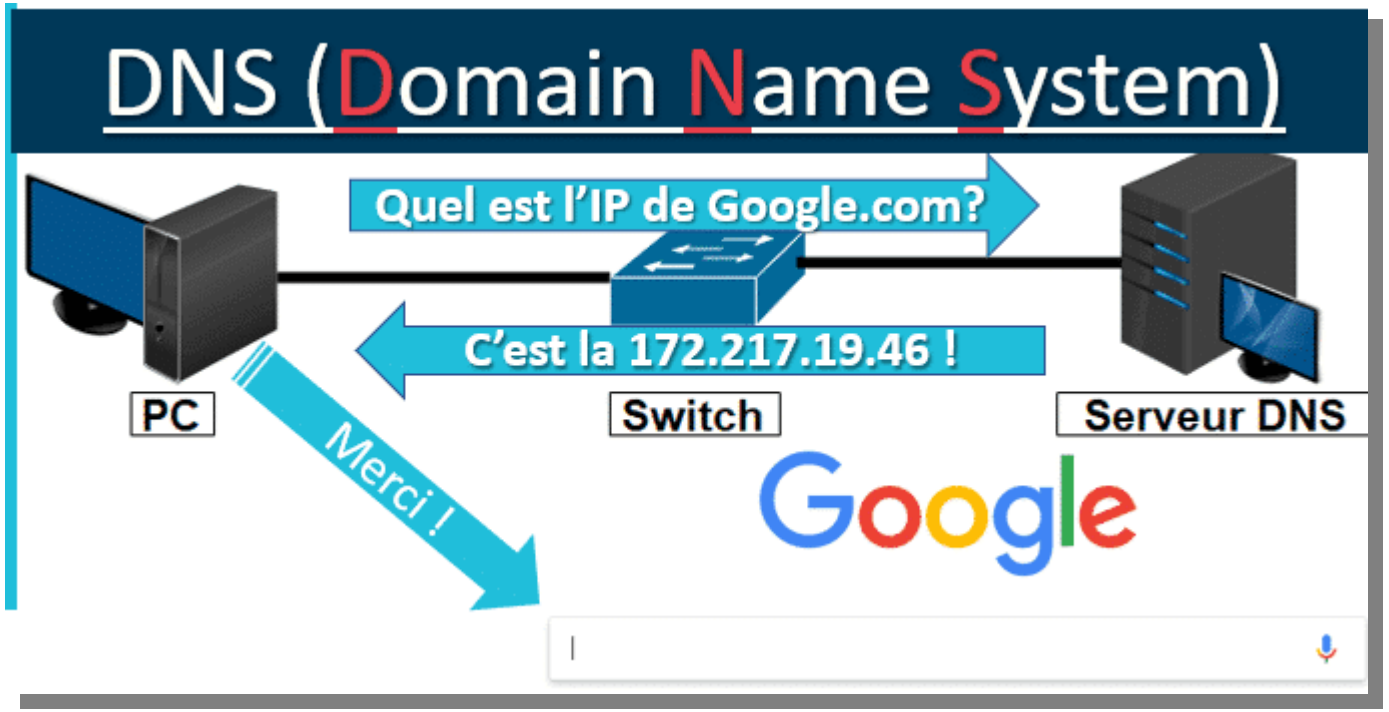
Introduction au DNS

- Le DNS (Domain Name System) est un service essentiel qui permet de résoudre les noms de domaine en adresses IP.
- Il fonctionne comme un annuaire distribué hiérarchique sur Internet et au sein des réseaux privés.



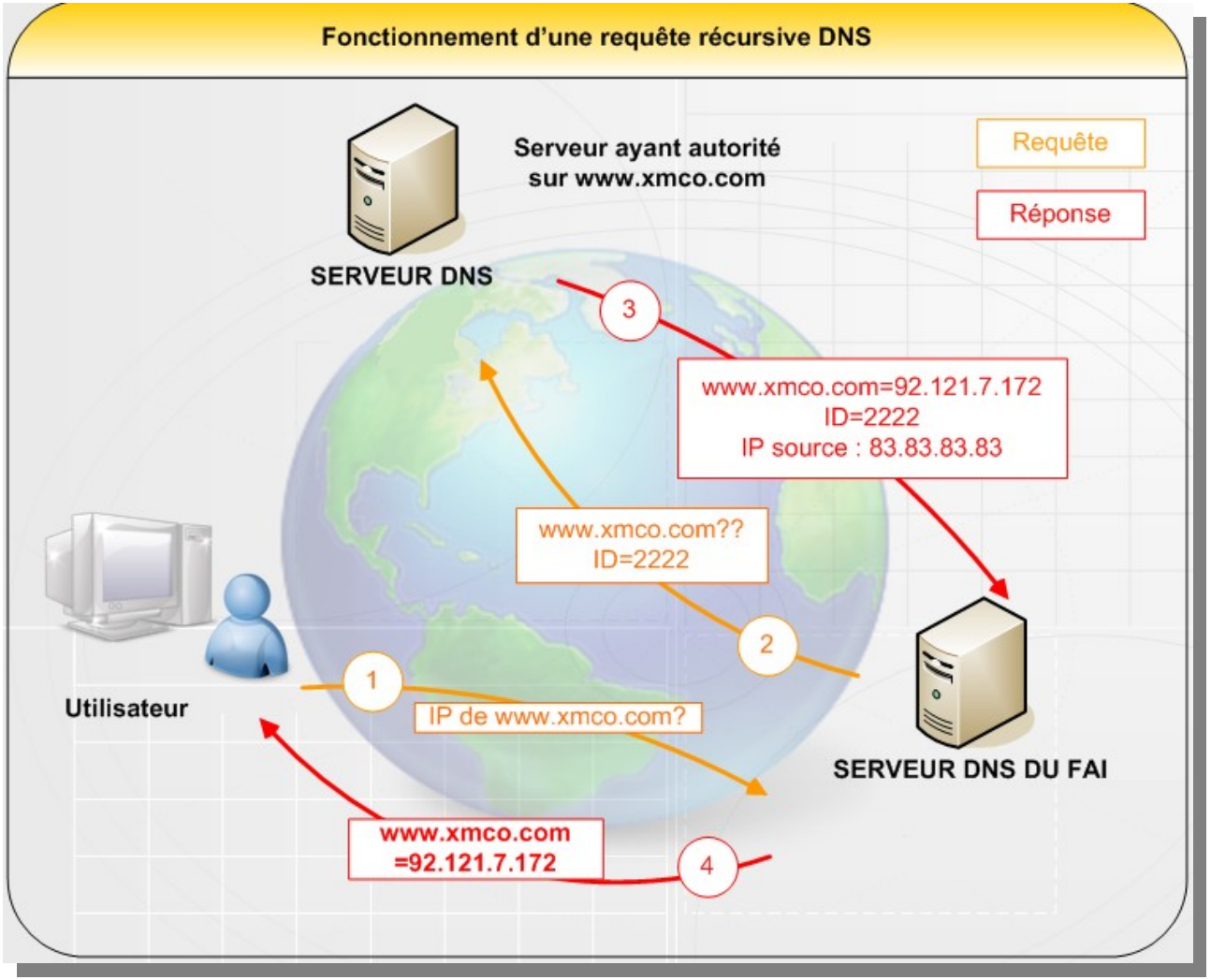
Objectifs du DNS

- Traduire les noms lisibles par l’homme (ex : www.exemple.local) en adresses IP (ex : 192.168.1.10).
- Faciliter la communication entre machines.
- Centraliser la gestion des noms dans un domaine d’entreprise.



Fonctionnement du DNS

- Client DNS (resolver) envoie une requête au serveur DNS.
- Le serveur DNS retourne l’adresse IP associée au nom (enregistrements A ou AAAA).
- Système hiérarchique : racine (.), TLD (.com, .org), domaines (exemple.com).



Types d’enregistrements DNS

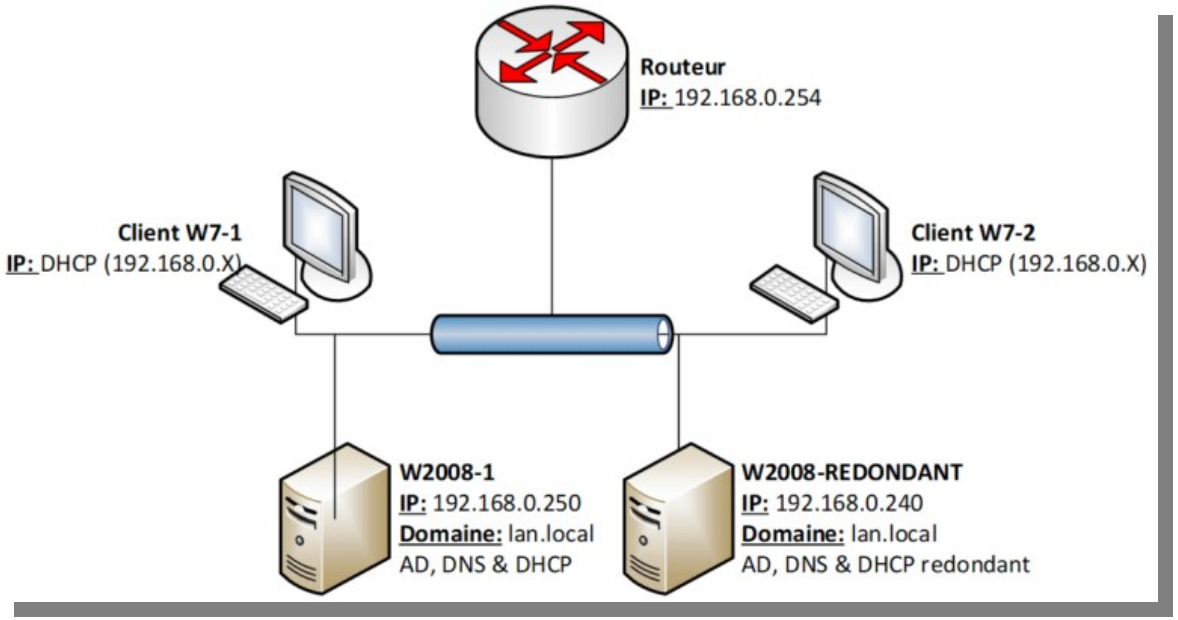
- **A** : il s’agit des enregistrements d’adresses faisant correspondre un nom d’hôte à une adresse IPv4 de 32bits. En IPv6, on utilise des enregistrements AAAA codés sur 128bits.
- **CNAME** : il s’agit d’enregistrements canoniques créant un alias d’un domaine vers un autre. L’alias hérite de tous les sous-domaines de l’original.
- **MX** : définit les serveurs de messagerie pour le domaine.
- **PTR** : associe une adresse IP à un enregistrement de nom de domaine (on parle de reverse puisqu’il s’agit du contraire de l’enregistrement A).
- **NS** : définit les serveurs DNS du domaine (primaire et secondaire).
- **SOA** : fournit les informations générales de la zone : serveur principal, contact, délai d’expiration, n° de série de la zone.
- **SRV** : généralise la notion d’enregistrement MX en proposant des fonctions avancées : taux de répartition de charge (décrit dans la RFC2782).
- **NAPTR** : donne accès aux règles de réécriture de l’information permettant de lier le nom de domaine et une ressource (RFC3403).
- **TXT** : permet à l’administrateur d’insérer un texte quelconque pour un enregistrement DNS.

Implémentation du DNS sur Windows Server 2025

- Ajout du rôle DNS : Ouvrir le Gestionnaire de serveur > Ajouter des rôles > DNS Server. L’installation est souvent automatique avec le rôle AD DS.
- Création d’une zone de recherche directe : Exemple : domaine.local. Ajout d’enregistrements A pour les postes. Optionnel : autorisation de mise à jour dynamique (sécurisée recommandée).
- Création d’une zone de recherche inversée : Exemple : 192.168.1.0/24 => permet de résoudre une IP vers un nom. Ajout automatique des enregistrements PTR si activé dans DHCP.
- Configuration DNS côté clients : Via DHCP (option 006 DNS Server). Ou manuellement dans les paramètres TCP/IP.
- Outils de verification: `nslookup`: tester les résolutions DNS. `ping`: tester la connectivité et la résolution. `ipconfig /all`: vérifier les serveurs DNS utilisés.

Haute Disponibilité et Redondance du DNS

- Installer au moins deux serveurs DNS pour tolérance de panne.
- Le DNS secondaire peut être configuré avec une réplication de zone.
- Dans Active Directory, les zones DNS peuvent être stockées dans AD et répliquées automatiquement entre contrôleurs de domaine.



Avantages du stockage DNS dans AD

- Sécurité renforcée.
- Réplication automatique.
- Gestion centralisée.

Cybersécurité et DNS – Recommandations ANSSI

- Le DNS est souvent ciblé par les attaques réseau (spoofing, cache poisoning, exfiltration). Voici les bonnes pratiques de cybersécurité recommandées par l’ANSSI.

https://cyber.gouv.fr/publications/recommandations-relatives-aux-architectures-des-services-dns

Recommandations ANSSI (1/2)

- Utiliser les mises à jour dynamiques sécurisées : N’autoriser que les mises à jour DNS authentifiées via Kerberos.
- Isoler le serveur DNS dans un VLAN ADMIN : Restreindre l’accès au serveur DNS au réseau interne.
- Configurer les ACLs DNS : Contrôler qui peut effectuer des requêtes ou des mises à jour.
- Utiliser des zones de transfert sécurisées : Transfert de zones DNS uniquement entre serveurs autorisés.

Recommandations ANSSI (2/2)

- Surveillance et Logging : Activer les journaux DNS dans l'observateur d’événements. Utiliser un SIEM pour surveiller les requêtes anormales.
- Mitiger le cache poisoning : Limiter la durée de vie des enregistrements en cache (TTL). Utiliser DNSSEC si possible pour authentifier les réponses.

Ressources

- ANSSI : "Guide des bonnes pratiques DNS"
- Microsoft : "DNS Security Best Practices"
- RFC 1034, 1035, 4033 à 4035 (DNSSEC)

Commandes PowerShell Utiles

- Installer DNS: `Install-WindowsFeature -Name DNS -IncludeManagementTools`
- Créer une zone directe: `Add-DnsServerPrimaryZone -Name "domaine.local" -ZoneFile "domaine.local.dns`
- Ajouter un enregistrement A: `Add-DnsServerResourceRecordA -Name "srv1" -ZoneName "domaine.local" -IPv4Address "192.168.1.10`
- Créer une zone inversée: `Add-DnsServerPrimaryZone -NetworkId "192.168.1.0/24" -ZoneFile "1.168.192.in-addr.arpa.dns`

Conclusion

- Le service DNS est un pilier des réseaux informatiques.
- Une mauvaise configuration peut causer de graves problèmes de connectivité ou exposer l’infrastructure à des attaques.
- En combinant les fonctionnalités de Windows Server 2025 avec les recommandations de l’ANSSI, il est possible de bâtir une infrastructure DNS fiable, résiliente et sécurisée.

FIN DU COURS