

# **Module 5:**

## **Service de répertoire de noms**

- **Problématique**

- Nom d'ordinateur, d'utilisateur, de service sous forme textuelle à traduire en identificateur binaire et éventuellement en identificateur de bas niveau (nom/adresse IP/adresse Ethernet, nom de fichier/capacité/serveur-fichier).
- Base de donnée de paires nom-attributs.
- Service de consultation, recherche, découverte, modification, effacement, enregistrement.
- Serveurs hiérarchiques, répliqués.
- Doit fonctionner à l'échelle planétaire (nom des ordinateurs, utilisateurs...).
- Exemples: DNS, X500, CORBA Naming Service, Portmap, LDAP.

## • Organisation

- Domaine de nom: niveau dans la hiérarchie pour lequel une autorité gère les noms mais peut déléguer son autorité pour un sous-domaine.
- Pour chaque nom une série de paires <type, valeur> est stockée: <usager, nom/téléphone/adresse...>, <service, adresse/version>, <ordinateur,architecture/OS/adresse IP/propriétaire>, <groupe,liste de noms>, <alias, nom>, <répertoire, liste de noms>.
- Services: AttributeSequence Lookup(String name, AttributeType t), Bind(String name, AttributeSequence attr), UnBind(String name).
- Noms hiérarchiques (division physique ou organisationnelle) avec différents niveaux de répertoires qui peuvent être servis et gérés de manière répartie.
- Une composante d'un nom peut mener à un autre contexte. La recherche d'un nom peut donc se faire de manière itérative ou récursive en partant du contexte racine dont la localisation doit être bien connue.
- Cache: <nom, attributs>, ou <Préfixe,nom de serveur>
- Différents espaces de noms: ordinateurs, usagers, services, fichiers...

- **Discussion**

- Noms relatifs.
- Fusion d'espaces de noms.
- Alias pour aider restructuration.
- URI, URL and URN.
- Le nom peut être un des attributs avec recherche possible sur tous les attributs: quel est le nom de l'utilisateur dont le numéro de téléphone est X. (Pages jaunes au lieu de simples pages blanches).

- **Différents services**

- Domain Name Service (DNS)
- Hesiod (Projet Athena au MIT)
- NIS (Sun Yellow Pages)
- Netinfo (NeXT)
- Banyan VINES
- NT Domains (avant Active Directory)
- X.500 (OSI)
- LDAP (simplification de X.500)
- Active Directory (Microsoft, basé sur LDAP)
- SLP, Jini, CORBA naming service, Portmap...

- **DNS**

- Avant 1987, chacun prenait une copie d'un monstrueux fichier /etc/hosts par ftp.
- Convertir les noms en adresses IP.
- Trouver le serveur de courriel pour un domaine.
- Informations sur chaque ordinateur.
- Alias pour services courants (www.polymtl.ca, ntp.polymtl.ca, ftp.polymtl.ca).
- Trouver le nom pour une adresse IP.

- **Organisation de DNS**

- Serveur avec: attributs pour les noms d'un domaine, noms et adresses des serveurs en autorité pour le domaine et pour les sous-domaines dont l'autorité a été déléguée, paramètres pour la zone comme le TTL (Time To Live).
- Chaque zone doit être servie par au moins deux serveurs en autorité qui présentent des modes de défaillance non corrélés.
- Le logiciel de serveur Bind peut être configuré en serveur primaire, secondaire ou cache seulement.
- La librairie client contacte par UDP les serveurs qui s'occupent de maintenir une cache en utilisant les valeurs de TTL.
- Peut avoir plusieurs IP (avec TTL très court) pour un nom, de manière à répartir des requêtes sur plusieurs ordinateurs.

- **Serveurs DNS de départ**

- Le service officiel est géré par le Internet Corporation for Assigned Names and Numbers (ICANN), anciennement sous le USA Department of Commerce et, depuis octobre 2016, après 18 ans de débats, sous une gouvernance plus neutre.
- OpenNIC offre des serveurs racine alternatifs avec beaucoup plus de liberté sur les noms de domaines disponibles (.bbs, .free, .geek, .libre, .neo, .null, .pirate...).
- Il existe d'autres racines DNS alternatives comme New Nations (.ko, .ku, .te, .ti, .uu...).



- **Jini**

- Message à tous pour trouver le serveur.
- Enregistrement des services offerts par chaque objet avec un TTL.
- Requêtes pour découvrir les services appropriés.
- Appariement des requêtes basée sur la hiérarchie de types Java.

# Service Location Protocol (SLP)

- Message à tous pour chercher un service (avec certains attributs).
- Les serveurs SLP qui connaissent un tel service répondent.

## X.500

- Composant de OSI.
- Wikipedia cite: « The original X.500 plan is unlikely ever to come to fruition », mais LDAP s'en inspire.
- DIT (Directory Information Tree): hiérarchie de noms répartie sur plusieurs serveurs.
- DIB (Directory Information Base): noms et ensembles d'attributs pour chaque nom.
- Agent usager: accédé par les applications.
- Agent serveur: fournit les réponses, possiblement en faisant des requêtes à d'autres serveurs, ou en redirigeant le client vers un autre serveur.
- Les types des attributs sont définis avec ASN.1 (Abstract Syntax Notation). Un des attributs est le nom.
- Opérations: lire (chemin et liste des attributs désirés), chercher (préfixe de chemin, et expression booléenne de tests sur les valeurs des attributs).
- La mise à jour se fait avec une interface d'administration qui inclut des opérations additionnelles.

# LDAP

- Utilisé dans les grosses entreprises à la place de NIS
- Version allégée de X500 basée sur TCP/IP plutôt que OSI.
- Utilise ASN.1 et BER.
- Connexion TCP port 389.
- Arbre de répertoires contenant des entrées, chaque entrée constituée d'attributs pouvant contenir plusieurs valeurs.
- Requêtes et réponses asynchrones (plusieurs requêtes de suite, réponses non ordonnancées).

# LDAP, opérations

- Start TLS: passer en mode encrypté.
- Bind: s'authentifier et spécifier la version du protocole.
- Search: effectuer une recherche dans le répertoire.
- Compare: vérifier si une entrée a une certaine valeur comme attribut.
- Add: ajouter une nouvelle entrée.
- Delete: effacer une entrée.
- Modify: modifier une entrée.
- Modify Distinguished Name (DN): renommer ou déplacer une entrée.
- Abandon: annuler une requête envoyée.
- Extended Operation: mécanisme pour extension.
- Unbind: fermer la connexion.

# LDAP, recherche

- baseObject: chemin absolu de l'entrée à laquelle commencer la recherche.
- scope: entrée, répertoire ou sous-arbre à chercher.
- filter: critères de recherche, combinaisons (et ou non) sur des relations (égal, commence par...) sur les valeurs des attributs.
- derefAliases: suivre ou non les alias.
- attributes: quels attributs retourner dans les résultats.
- sizeLimit, timeLimit: temps maximum et taille maximum des résultats à retourner.
- typesOnly: seulement retourner le type des attributs et non leur valeur.

# Discussion

- Le service DNS demeure le point d'entrée sur l'Internet. C'est un service facile à offrir mais essentiel. Il ne sert pratiquement que pour résoudre les adresses IP.
- Les autres services de répertoires (LDAP, Active Directory ou NIS) sont internes à une organisation et contiennent principalement la base de données des usagers (avec leur mot de passe, localisation du répertoire de fichiers, quotas...).
- Les requêtes externes passent souvent par une interface Web ou des Web Services (e.g. bottin du personnel de Polytechnique).
- Les données qui alimentent ces services peuvent souvent être stockées dans une base de donnée conventionnelle sous-jacente.