**Penses-bêtes:**

**CSV** = Command Separated Value = , et ; séparent les champs des fichiers générés par tableurs ou database.

**IHM =** Interfaces Hommes-Machines

**CLI =** Command Line Interface

**GUI** = Graphical User Interface

Fichier = Unité de stockage

Dossier = Organisation de fichier

Taille FileSystem = Taille de partitionnement

**FAT** = File Allocation System

**NTFS =** New Technology File System (Remplace le FAT)

**ACL** = Access Control List

**OS** = Operating System (Système d’exploitation) Ensemble de programme qui dirige les ressources de l’ordinateur à l’aide de logiciels applicatif. Gère processus CPU, mémoire,stockage, utilisateurs, périphérique et GUC.

**UID** = User IDentity. Identifiant unique d’utilisateur

**SID** ou **UID(**Windows) = Security IDentity

**ACL =** Access Control List

**IAM =** Identities Access Manager. Gestion des ID et accès

**SAM** = Security Account Manager. Gestionnaire de compte de sécurité

**MAC** = Medium Access Protocol

**LLC** = Logical Link Control

**NAS =** Network Attached Storage, appareil de stockage autonome qui peut se connecter à votre réseau privé ou professionnel via Internet.

**SMB** = *Server Message Block*, protocole qui permet aux ordinateurs d'un réseau de partager des fichiers, des imprimantes et d'autres ressources.

**RTC** = Réseau Téléphonique Commuté

**PABX** = Private Automatic Branch EXchange: Premier commutateurs automatique

**IPBX=** Internet Protocol Branch EXchange: Permet d’utiliser des réseaux informatiques sur IP pour faire transiter des communications téléphoniques.

**RNIS =** Réseau Numérique à Intégration de Services: Permet de numériser le signal analogique de la voix dans les transmissions téléphoniques

**PDU** = encapsulation protocole + payload

**PDU** = La **Protocol Data Unit** ou *Unité de données de protocole* (**PDU**) est l'unité de mesure des informations échangées dans un [réseau informatique](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique). Payload + Protocol = PDU

PDU et couche OSI <https://fr.wikipedia.org/wiki/Protocol_Data_Unit>

**Payload =** Charge de données dans une trame

**Disques IDE** : /dev/hda; Partitions : /dev/hda1 (a peut-être b ou… 1 peut être 2ou3..)

**Disques SATA** : /dev/sda; Partitions : /dev/sda1 (a peut-être b ou… 1 peut être 2ou3..)

**Disques nvme** : /dev/nvme0n1; Partitions : /dev/nvme0n1p1( 0 peut être 1,2….; 1 peut être 2,3…)

**HMAC =**  *Keyed-hash Message Authentication Code:* Code d’authentification de message.

**LDAP =** Lightweight Directory Access Protocol. Norme de système d'annuaire.

**LDIF =** LDIF permet des importations, exportations et modifications d’AD par fichiers de textes. Permet de charger AD à partir d’une BDD externe ou inversement : ex.: gestions des comptes utilisateurs à partir de la BDD RH

**SNTP =** (*Simple Network Time Protocol)* Permet la synchronisation des horloges des systèmes (stockage de l’heure UTC, affichée en tenant compte du fuseau horaire)

Impératif pour le protocole d’authentification de Windows (Kerberos)

Une mauvaise synchronisation du temps amène des problèmes : D’authentification Kerberos, De réplication, D’échecs de connexion aux ressources, D’échecs de communication sécurisée (certificats), De journalisation et d’audit.

**Keberos =** Protocole d’authentification central par défaut depuis Windows 2000 (remplace LM/NTLM utilisé jusqu’à NT4), Compatible Kerberos V5, Authentification mutuelle du client et du serveur, Adresse du serveur Kerberos utilisé pour l’ouverture de session extraite du DNS.

**FSMO =** *(Flexible Single Master Operation)*

*Maître de schéma:* Gère la structure du schéma, seul à pouvoir initier des changement dans le LDAP. 1 seul par forêt. Rôle sur le serveur principal.

*Maître d’attribution de nom de domaine:* Distribue les noms de domaine aux DC, un seul par forêt.

*Maître RID:* Attribue le pool de RID au DC qui attribue le RID des SID des objet AD. Un seul par domaine. Rôle sur le serveur principal.

*Maître d’infrastructure:* Gère les références entre plusieurs objets, assure la réplication des informations d’objets sur tous les DC du domaine, même entre 2 domaines différents. Un seul par domaine.

*Emulateur PDC:* Primary Domain Controller (Unique dans le domaine) a 5 missions:

* Modification des stratégies de groupes du domaine
* Synchroniser les horloges sur tous les DC
* Gérer le verrouillage des comptes
* Changer les mots de passe
* Assurer la compatibilité avec les DC WindowsNT

**AD CS** = (*Active Directory Certificate Service*).Gestion et création des clés ainsi que des certificats

**AD FS** = (*Active Directory Federation Services*) - depuis Serv.2008 Via un portail gestion d’un SSO (Single Sign-On) pour les applications

**AD RMS** = (*Active Directory Rights Management Services*) - depuis Serv.2008 R2 Gestion des autorisations fine sur les fichiers (uniquement sur applications compatibles, comme Office)

**AD LDS =** (*Active Directory Lightweight Directory Services*). Service d’annuaire light, pas de domaine (pas de contrôle d’accès).

**Active directory:**

*- Catalogue Global* : le conteneur de tous les objets AD DS. Si tu as besoin de trouver le nom d’un utilisateur, ce nom est stocké dans le catalogue global.

**-** *Lightweight Directory Access Protocol* (LDAP) : protocole qui permet à AD de communiquer avec d’autres services d’annuaire sur d’autres plates-formes.

**-** *Lightweight Directory Services* : Prend en charge LDAP pour des services de domaine multiplateformes, par exemple l’ensemble des ordinateurs Linux présents sur

ton réseau.

- *Les contrôleur de domaine* (CD) ou en anglais *DC* pour *Domain Controller*, sont les serveurs de ton réseau qui hébergent AD DS.

*- KDC (Kerberos Key Distribution Center)* : Le KDC vérifie et chiffre les tickets Kerberos utilisés par AD DS pour l'authentification

- *IsmServ (Intersite Messaging)* : Intersite Messagin permert aux CD de communiquer les uns avec les autres pour la réplication et le routage inter-sites.

- *Organization Unit* sont des conteneurs administratifs. Elles contiennent des objets ayant les mêmes besoins administratifs.

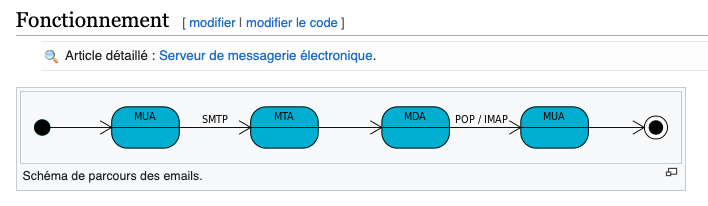
- *Une structure d'un Active Directory est donc composée de* :

1- La forêt : structure hiérarchique d'un ou plusieurs domaines indépendants (ensemble de tous les sous domaines Active Directory).

2- L'arborescence : domaine de toutes les ramifications. Par exemple, dans l'arbre wilders.lan, data.wilders.lan et dev.wilders.lan sont des sous-domaines de wilders.lan

3- Le domaine : constitue les feuilles de l'arborescence. dev.wilders.lan peut-être un domaine au même titre que wilders.lan

**Messagerie:**



**MUA** (*Mail User Agent*) : client de messagerie (logiciel client)Application permettant aux utilisateurs de créer, d'afficher, d'envoyer et de recevoir du courrier électronique. L'application MUA réside sur un système client, tel qu'un poste de travail ou un PC.

**MSA** (*Mail Submission Agent*) : composant qui accepte les e-mails du MUA et les transmets au MTA pour livraison.

**MTA** (*Mail Transfert Agent*) : élément principal d'un serveur SMTP qui transmet les e-mails d’un serveur à un autre. Les e-mails transitent de MTA en MTA.

**MDA** (*Mail Delivery Agent*) : service de remise des e-mails dans les BAL

**WIFI:**

**SIFS (**Short InterFrame Space) Intervalle inter trame court: temps (ms) nécessaire à une interface sans-fil, de traiter une trame et répondre avec une trame de réponse.

**DIFS (**DCF InterFrame Space) intervalle inter-trame utilisé par les réseaux WLAN IEEE 802.11. Une station ayant activé le DCF doit sonder le médium pendant une durée d’un DIFS. La station autorise la transmission si le trafic est libre, sinon la transmission est reportée.

**RADIUS (**Remote Authentication Dial-in User Service) protocole client-serveur permettant de centraliser des données d'authentification.

**A connaître par-coeur:**

- Modèle osi & TCP/IP

- Le format des @ mac

- Schéma de trame ethernet

- Données transportées (Payload)

- Glossaire cour notion réseau

- Lien physique et logique

**Ports TCP et protocoles:**

**TCP (*Couche Transport)*=** Transmission Control Protocol (littéralement, « protocole de contrôle de transmissions »), [abrégé](https://fr.wikipedia.org/wiki/Abr%C3%A9viation) TCP, est un protocole de transport fiable, en [mode connecté](https://fr.wikipedia.org/wiki/Mode_connect%C3%A9), documenté dans la RFC 9293[2](https://fr.wikipedia.org/wiki/Transmission_Control_Protocol#cite_note-RFC-9293-t-d-2) de l’[IETF](https://fr.wikipedia.org/wiki/Internet_Engineering_Task_Force).

Dans le [modèle Internet](https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet), aussi appelé modèle TCP/IP, TCP est situé au-dessus de IP. Dans le modèle [OSI](https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI), il correspond à la [couche transport](https://fr.wikipedia.org/wiki/Couche_transport), intermédiaire de la [couche réseau](https://fr.wikipedia.org/wiki/Couche_r%C3%A9seau) et de la [couche session](https://fr.wikipedia.org/wiki/Couche_session). Les applications transmettent des flux de données sur une connexion réseau. TCP découpe le flux d’[octets](https://fr.wikipedia.org/wiki/Octet) en *segments* dont la taille dépend de la [MTU](https://fr.wikipedia.org/wiki/Maximum_Transmission_Unit) du réseau sous-jacen

**Port 21 = FTP :** sert pour le transfert de fichiers

**port 22= SSH**: sert pour un accès à distance sécurisé

**port 25 = SMTP (*Couche Application)***: sert pour le transfert des courriels des serveurs de messagerie. *Port* ***465/587*** *en chiffrement*

**port 53=DNS (*Couche Application)***: sert à la traduction des noms de domain

**port 67 serveur et 68 client =DHCP**: assure la configuration automatique des paramètres IP d’une [station](https://fr.wikipedia.org/wiki/Station_de_travail) ou d'une machine, notamment en lui attribuant automatiquement une [adresse IP](https://fr.wikipedia.org/wiki/Adresse_IP) et un [masque de sous-réseau](https://fr.wikipedia.org/wiki/Masque_de_sous-r%C3%A9seau). DHCP peut aussi configurer l’adresse de la [passerelle](https://fr.wikipedia.org/wiki/Passerelle_(informatique)) par défaut et [DNS](https://fr.wikipedia.org/wiki/Domain_Name_System).

**port 80=HTTP** **(*Couche Application)***: sert pour le transfert de données entre un navigateur web et un serveur web.

**port 110= POP3:** Permet de relever le courrier d’un serveur pop qui établit le dialogue entre l’hôte et la BAL sur le serveur mail. Télécharge les mail en local.

**port 143= IMAP:** protocol d lecture de mail. Permet de lire les objets de mails ou les effacer sans les lire par exemple. Laisse les mails sur le serveur.

**port 389= LDAP:** Protocol d’authentification

**port 636= LDAP + TLS**

**port 853 = DNS over TLS (***Transport Layer Security)* « Sécurité de la couche de transport » chiffrement et encapsulation des requêtes et des réponses [DNS](https://fr.wikipedia.org/wiki/Domain_Name_System) via le protocole [TLS](https://fr.wikipedia.org/wiki/Transport_Layer_Security).

**port 443= HTTPS:** (*HyperText Transfer Protocol Secure* ) combinaison du [HTTP](https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol) avec une couche de [chiffrement](https://fr.wikipedia.org/wiki/Chiffrement) [TLS](https://fr.wikipedia.org/wiki/Transport_Layer_Security)

**Port 520 = Routage RIP** (Routing Information Protocol) permet à chaque [routeur](https://fr.wikipedia.org/wiki/Routeur) de communiquer avec les routeurs voisins. La [métrique](https://fr.wikipedia.org/wiki/M%C3%A9trique_(routage)) utilisée est la distance qui sépare un routeur d'un réseau IP déterminé quant au nombre de sauts (ou « *hops* » en anglais).

**Port 88 = Routage EIGRP** (Enhanced Interior Gateway Routing Protocol) **RIP de CISCO**

**Port 89 = Routage OSPF (*Couche Application)*** (Open Shortest Path First) chaque [routeur](https://fr.wikipedia.org/wiki/Routeur) établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages *hello* à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages *Link-state advertisements* ([LSA](https://en.wikipedia.org/wiki/Link-state_advertisement)) propagés de proche en proche à tous les routeurs du réseau.

**Port 179 = Routage BGP** (Border Gateway Protocol) échange les informations de routage et d'accessibilité de réseaux.

**port 1812 (Authentification) & 1813 (Traçabilité): RADIUS**: Centralise des données d'authentification.

**Port 5060=SIP** (Session Initiation Protocol) protocol de communication qui établit, modifie et termine des sessions multimédia.

**Port 5061=SIPS**

**Type de blindage RJ45**

Définition des blindages:

* **U** = Unfoiled (non blindé)
* **F** = Foiled (blindage par feuillard aluminium)
* **S** = Shielded (blindage par tresse d'aluminium)
* **TP** = Twisted Pairs (blindage par paires torsadées)

Ce qui donne les type de câble suivant par niveau de blindage :

* **U/UTP** = non blindé
* **F/UTP** = Blindage général, le câble est globalement blindé sous la gaine
* **U/FTP** = Blindé par paire, les conducteurs sont isolés et blindés
* **F/FTP** = Blindage général et un blindage sur chaque paire
* **S/FTP** = Blindage général en tresse de cuivre étamé et un blindage sur chaque paire

**Site de recherche:**

**- Chercher avec google dork** <https://www.exploit-db.com/google-hacking-database>

- Neptune.

- IT-Connect (Windows)

- Chaine cookies connect

- Docs officiels

- command+f = recherche dans la page

**Installation sur Github:**

* Bitwarden
* Serveur Core DC + intégration AD
* GLPI + agent
* PFSense
* RAID1 Windows graphique
* Mise en place dossier partagés réseau
* Restrictions horaire utilisateurs AD
* Windows Server Backup
* Restauration Server Backup
* Zabbix
* LAPS
* Zimbra
* Windows Server Update
* PRTG
* Freepbx
* IredMail
* RAID1 Debian sur système
* RAID1 Serveur Core
* Répartition rôles FSMO