

DOMAINES MICROSOFT & ADMINISTRATION SERVEUR

Agnès BENEZET

agnes.benezet@umontpellier.fr

<https://sites.google.com/site/agnesbenezet>

PLAN DU MODULE

Introduction + Domaines Microsoft: Généralités.

Active Directory: Comptes / groupes.

Active directory: GPO sécurités partages.

Rôles et fonctionnalités serveurs Microsoft

Sécurité réseaux d' entreprises et environnements
Microsoft

TP /TD

TD/TP1 Installation prise en main des machines.

TD/TP2 les comptes & groupes

TD/TP3 Création de GPO.

TD/TP4 Installations de rôles.

TD/TP5 Sécurité

SERVEUR

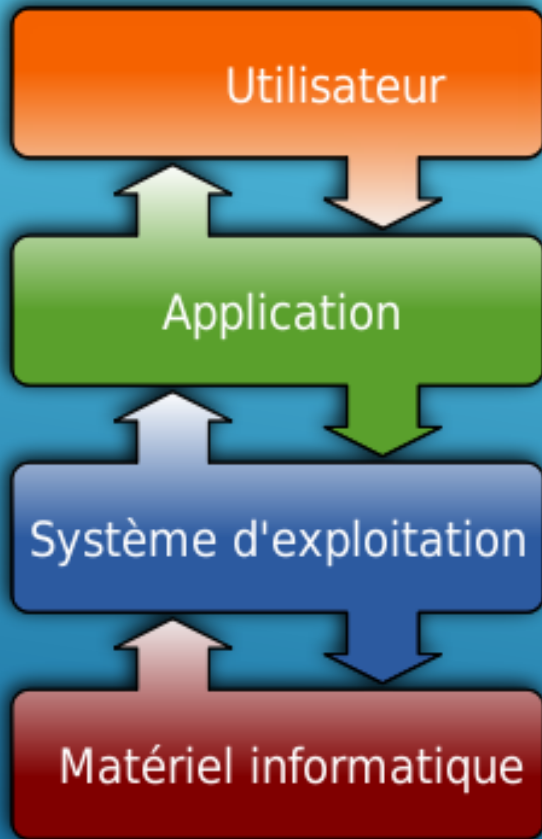
Dispositif informatique
matériel et/ou logiciel
délivrant divers services,
à différents clients.

CLIENT

Est client le poste de travail qui accède à un service.

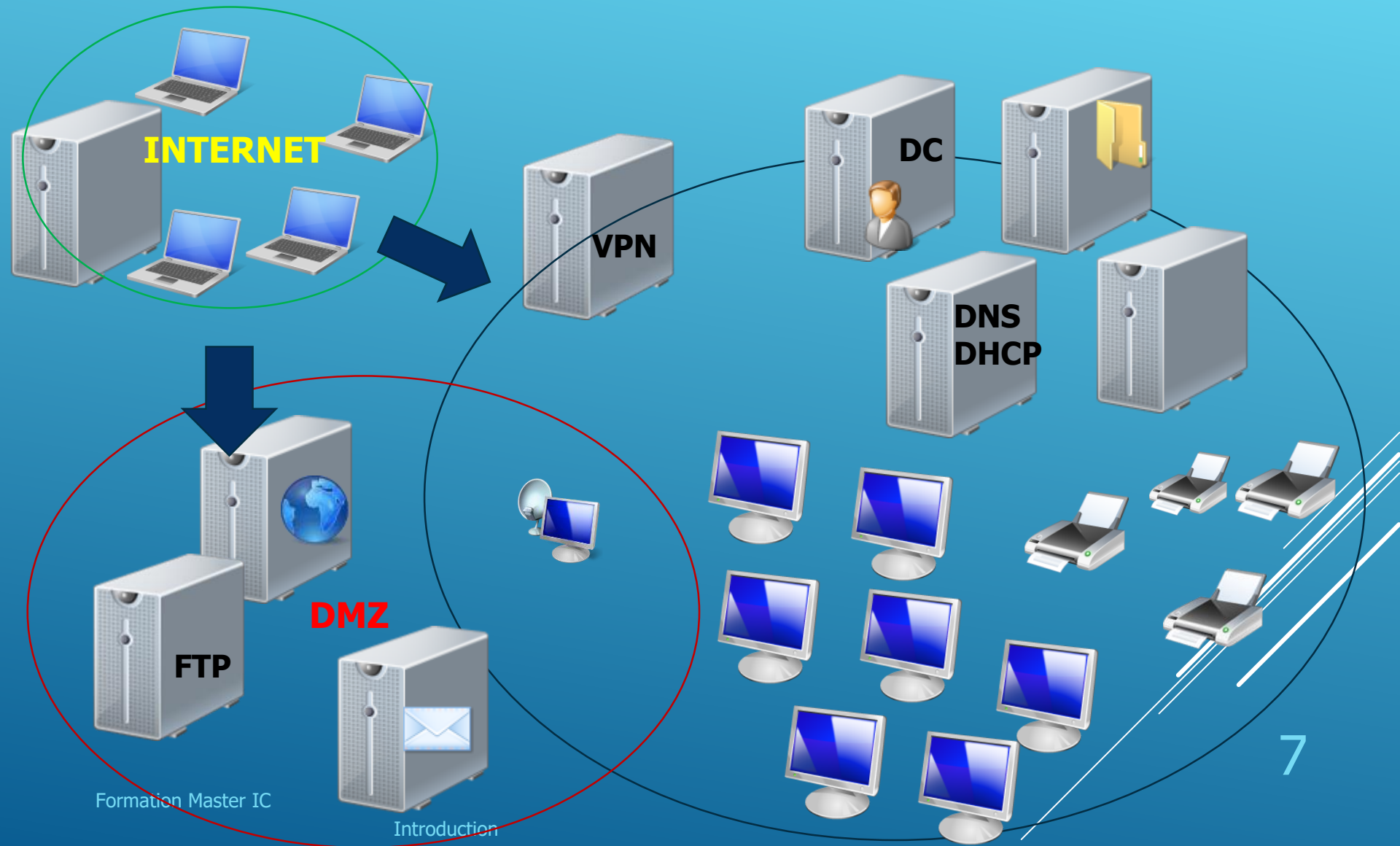
Est client l'utilisateur ou le logiciel qui réalise cet accès.

SYSTÈME D'EXPLOITATION



- ▶ Contrôle d'accès.
- ▶ Interface utilisateur.
- ▶ API Interface de programmation.
- ▶ Gestion de la mémoire.
- ▶ Gestion des entrées/sortie
- ▶ Pilotes.
- ▶ Système de fichiers.
- ▶ Réseau.
- ▶ HAL Couche d'abstraction matérielle

RÉSEAU D'ENTREPRISE WINDOWS



DHCP

Dynamic Host Configuration Protocol.

Assurer la distribution et la configuration automatique des paramètres IP d'une station:

- ▶ Adresse IP
- ▶ Masque de sous-réseau.
- ▶ Passerelle par défaut
- ▶ Serveurs de noms (DNS)
- ▶ Serveurs WINS.

CONFIGURATION DU SERVEUR DHCP

- ▶ Configuration des plages d'adresses.
=> Adresses non affectées ou exclues d'une plage disponible pour l'adressage fixe.
- ▶ Durée d'attribution des adresses limitées (Bail DHCP).
- ▶ DHCP relay pour acheminer les « adresses » a travers un routeur.

DNS : Domain Name System

Structure hiérarchique mondiale, permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

Avantages:

Système pratique, cohérent, simple.

- ▶ Les noms sont facilement mémorisables
- ▶ Indépendance des noms des serveurs / aux IP

L'ESPACE DE NOMS

Structure arborescente, chaque niveau est séparé du suivant par un point.

PC.polytech.umontpellier.fr

PC

Nom d'Hôte

.Polytech

Sous domaine

.umontpellier

Domaine de premier niveau

.fr

TLD (Top Level Domains)

LES SERVEURS DE NOM

- ▶ Communiquent entre eux de façon hiérarchique.
- ▶ Les serveurs de noms racine répondent aux requêtes de premier niveau (.com., .net, .fr...)
- ▶ Chaque serveur est déclaré au serveur de niveau immédiatement supérieur.
- ▶ Un serveur de noms définit une zone, c'est-à-dire un ensemble de domaines sur lequel le serveur a autorité.

REQUÊTES DNS

- ▶ Les hôtes s'adressent à un ou plusieurs serveurs de noms dits récurifs.
- ▶ Parcours de la hiérarchie DNS jusqu'à obtention d'une réponse.
- ▶ Les serveurs DNS récurifs font office de cache DNS, afin de ne pas effectuer ce processus à nouveau.

SÉCURITÉ DU DNS

Le protocole DNS a été conçu avec un souci minimum de la sécurité.

- Interception des paquets transmis possible.
- Fabrication de faux paquets en réponse.
- Empoisonnement du cache DNS, rendant vulnérable tous les utilisateurs du serveur.
- Dénis de service incapacité du serveur à répondre aux requêtes de ses clients.

DNSSEC

Protocole standardisé qui permet de résoudre certains problèmes de sécurité liés au protocole DNS.

- ▶ sécurisation des transactions DNS ;
- ▶ sécurisation des informations contenues dans les messages
- ▶ stockage et distribution des clés nécessaires au bon fonctionnement des deux premiers services cités ci-dessus.

Accès distant sécurisé

- ▶ Permet l'interconnexion de réseaux locaux
- ▶ Ou bien la connexion d'un poste client a un réseau,
- ▶ via une technique de « tunnel » sécurisant les échanges.
- ▶ Les données sont chiffrées et encapsulées en entrée, déchiffrées en sortie.

Protocoles

Niveau 2:

GRE, L2TP, PPTP

Niveau 3

Ipsec, SSL/TLS, SSH

WINS & NETBIOS

- ▶ **WINS** (*Windows Internet Naming Service*) est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.

Netbios:

- ▶ Protocole de transfert de fichiers utilisé principalement par Microsoft.
- ▶ Permet d'établir des sessions entre différents ordinateurs d'un réseau.
- ▶ Facilite les accès aux partages et imprimantes.

REMOTE DESKTOP PROTOCOL

- ▶ Permet à un utilisateur de se connecter sur un terminal serveur Microsoft.

Clients pour Windows, Linux, Mac...webphones et autres OS.

- ▶ Port d'écoute par défaut port TCP 3389.

FTP FILE TRANSFER PROTOCOL

Protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.

Deux types de connexions TCP :

- ▶ Une connexion de contrôle du client, vers le serveur (port 21), transmission des commandes de fichiers.
- ▶ Une connexion de données initialisée par le client ou le serveur pour le Transfer des données requises (port 20).

COMMANDES RÉSEAU

- ▶ **Hostname:** affiche le nom de la machine.
- ▶ **IPCONFIG:** Affiche ou rafraîchit la configuration réseau du poste.

`ipconfig /all /release /renew /flushdns`

- ▶ **NetSh:** configure le réseau sous Windows.
- ▶ **NETSTAT :** Affiche l'état TCP/IP sur la machine locale

`netstat-a` affiche toutes les connexions.

COMMANDES RÉSEAU

- ▶ **PING** : Teste la connexion réseau d'une adresse IP distante.

Ping -t ping continu.

- ▶ **TRACERT** : Affiche les adresses IP par lesquelles passe un paquet entre la machine locale et l'adresse IP spécifiée.

- ▶ **ARP** : Résolution des adresses IP en adresses MAC.

-a Affiche les entrées ARP actives.

COMMANDES RÉSEAU

- ▶ **NBTSTAT** : Affiche les statistiques du protocole et les connexions TCP/IP actuelles utilisant NBTMise à jour du cache du fichier Lmhosts.
nbtstat -A
- ▶ **NsLookUp**: envoie des requêtes DNS sur un serveur DNS au choix permet de trouver le nom relatif a une IP
- ▶ **TELNET** : permet d'accéder en mode Terminal à un host distant. Permet de vérifier si un service quelconque TCP tourne sur un serveur distant.

COMMANDES POUR OS WINDOWS

- ▶ **CHKDSK**: Vérifie un disque et affiche un relevé d'état.
- ▶ **PATH**: Affiche ou définit le chemin de recherche des fichiers exécutables.
- ▶ **SET**: Affiche, définit ou supprime des variables d'environnement.
- ▶ **SYSTEMINFO**: Permet à l'administrateur d'afficher les informations de base de la configuration système.
- ▶ **TIME**: Affiche ou définit l'heure de l'horloge interne du système
- ▶ **VER**: Affiche le numéro de version de Windows