**Fiche Révisions**

**Ping**

**C'est quoi ?**  
➡ Commande qui teste la connectivité réseau entre deux machines.

**Comment ça marche ?**

1. Envoie une requête ICMP Echo Request à une IP.
2. Attend une réponse Echo Reply.
3. Affiche le temps de réponse et la perte de paquets.

📌 **Exemple** : ping 8.8.8.8 teste la connexion avec Google DNS.

**Trunk en réseau (routeur on a stick)**

**C'est quoi ?**  
➡ Lien entre équipements réseau (switchs, routeurs) permettant de transporter plusieurs VLANs sur un même port.

**Comment ça fonctionne ?**  
🔹 Utilise le protocole **802.1Q** pour taguer les VLANs dans les trames Ethernet.

**Différence entre TCP et UDP**

* **TCP (Transmission Control Protocol)** : Connexion fiable, vérification des erreurs, retransmission des paquets perdus. (Ex : HTTP, FTP)
* **UDP (User Datagram Protocol)** : Plus rapide mais sans contrôle d’erreur, utilisé pour le streaming et la VoIP. (Ex : DNS, vidéo en direct)

**Différence entre Switch et Hub**

* **Hub** : Diffuse toutes les données à tous les ports (pas intelligent, pas de gestion des collisions).
* **Switch** : Envoie les données uniquement au destinataire grâce aux adresses MAC (plus performant).

**Routage**

➡ Oriente les paquets réseau vers la bonne destination.

📌 **Types de routage** :  
🔹 **Statique** → Route définie manuellement.  
🔹 **Dynamique** → Utilise des protocoles comme RIP, OSPF, BGP.

📌 **Rôle des routeurs** :  
🔹 Séparer et interconnecter des réseaux.  
🔹 Optimiser le chemin des paquets.  
🔹 Appliquer des règles de sécurité (ACL, NAT).

**Wireshark : À quoi ça sert ?**

➡ Analyseur de paquets réseau permettant d'inspecter le trafic en temps réel et de diagnostiquer des problèmes réseau.

**⚡ Payload (Charge Utile) dans une Trame Ethernet**

➡ Partie contenant les données utiles transmises sur le réseau.

📌 **À quoi ça sert ?**  
🔹 Transporte les informations échangées entre applications (ex: page web, email, fichier).  
🔹 Contenu encapsulé dans différents protocoles selon le modèle OSI.  
🔹 Taille généralement comprise entre **46 et 1500 octets** dans une trame Ethernet standard.

**📌 Structure d'une trame Ethernet**

Une trame Ethernet est composée de plusieurs parties :

🔹 **Préambule** (7 octets) + **SFD** (1 octet) → Synchronisation.  
🔹 **Adresse MAC Destination** (6 octets) → Identifie le récepteur.  
🔹 **Adresse MAC Source** (6 octets) → Identifie l’émetteur.  
🔹 **Type/Ethertype** (2 octets) → Indique le protocole de la couche supérieure (ex: IPv4, IPv6).  
🔹 **Payload (Données utiles)** (46 à 1500 octets) → Contenu transporté.  
🔹 **FCS (Frame Check Sequence)** (4 octets) → Vérification d'erreur.

**📌 Encapsulation des protocoles dans le Payload**

Le Payload contient généralement un paquet de couche supérieure :

🔹 **Paquet IP** → Contient des informations sur l’expéditeur/destinataire (adresse IP).  
🔹 **Segment TCP/UDP** → Gère le transport des données (ex : HTTP, DNS, SSH).  
🔹 **Données de l’application** → Contenu final échangé (ex : fichier, message).

Exemple :  
📌 Une requête web suit cette structure :  
🔹 Trame Ethernet → **Paquet IP** → **Segment TCP** → **Requête HTTP**.

**📌 Taille et fragmentation du Payload**

Pourquoi la taille du Payload est limitée ?  
🔹 **MTU (Maximum Transmission Unit)** → Définit la taille max des données pouvant être envoyées sans fragmentation (1500 octets pour Ethernet).  
🔹 Si les données dépassent le MTU → **Fragmentation** du paquet en plusieurs trames Ethernet.

**🚀 Points Clés à Retenir**

✅ **Le Payload est la partie utile d’une trame Ethernet**.  
✅ **Encapsule les protocoles des couches supérieures (IP, TCP/UDP, application)**.  
✅ **Ne dépasse pas 1500 octets pour éviter la fragmentation**.  
✅ **Protégé par des mécanismes d’intégrité comme le FCS (CRC-32)**.

**CSMA/CD**

C’est un mécanisme de gestion de partage. Gère les collisions en filaire.

**🖧 VLAN (Virtual Local Area Network)**

**➡** Segmentation logique d’un réseau pour améliorer la sécurité et les performances.

**➡** Un VLAN permet de segmenter un réseau physique en plusieurs réseaux logiques distincts au sein d’un même switch.

**📌 À quoi ça sert ?  
🔹 Isolation :** Sépare les flux pour renforcer la sécurité.  
**🔹 Optimisation :** Réduit les domaines de broadcast.  
**🔹 Flexibilité :** Organisation du réseau sans changer le câblage physique.

**📌 Fonctionnement**

**🔹** Les VLANs sont identifiés par un ID (1 à 4096).  
🔹 Ports en mode Access → Un seul VLAN attribué.  
🔹 Ports en mode Trunk → Transporte plusieurs VLANs via 802.1Q.

**📌 Avantages :**🔹 Isolation du trafic → Moins de collisions, plus de sécurité.  
🔹 Meilleure gestion du réseau → Ex : VLAN pour RH, VLAN pour IT.  
🔹 Réduction du broadcast → Moins de charge réseau.

**VPN (Virtual Private Network)**

**À quoi ça sert ?**  
➡ Sécurise une connexion à distance en créant un tunnel chiffré entre l’utilisateur et le réseau de l’entreprise.

📌 **Types de VPN** :

* **VPN Site-to-Site** : Connecte deux réseaux distants.
* **VPN Client-to-Site** : Permet à un utilisateur distant d’accéder au réseau interne.

**NAT (Network Address Translation) :**

* Permet de traduire des adresses IP privées en IP publique pour accéder à Internet.
* Types :
  + **NAT dynamique** : plusieurs IP privées partagent une IP publique.
  + **PAT (Port Address Translation)** : associe plusieurs connexions à une même IP publique via les ports.

**ACL (Access Control List)**

**À quoi ça sert ?**  
➡ Définit les permissions d’accès aux fichiers/dossiers sur un système.

📌 **Types de permissions** :

* **Lecture (Read)** : Voir le contenu.
* **Écriture (Write)** : Modifier le contenu.
* **Exécution (Execute)** : Lancer un programme/script.
* **Contrôle total (Full Control)** : Tous les droits.

**Les ports réseaux importants**

📌 **Quelques ports TCP/UDP à connaître** :

* **21** → FTP (Transfert de fichiers)
* **22** → SSH (Connexion sécurisée)
* **25** → SMTP (Envoi d’e-mails)
* **53** → DNS (Résolution de noms)
* **80** → HTTP (Navigation web)
* **443** → HTTPS (Navigation web sécurisée)
* **3389** → RDP (Bureau à distance)

**SNMP (Simple Network Management Protocol)**

**À quoi ça sert ?**  
➡ Permet de surveiller et gérer les équipements réseau à distance (switch, routeur, serveur).

📌 **Principaux composants** :

* **Agent** : Collecte et envoie les infos sur un périphérique.
* **Manager** : Centralise et analyse les infos envoyées par les agents.
* **OID (Object Identifier)** : Identifie une info spécifique (ex : utilisation CPU).

**DHCP (Dynamic Host Configuration Protocol) :**

* Attribue automatiquement une adresse IP, un masque, une passerelle et un DNS aux clients du réseau.
* Fonctionne avec un bail (temps d’attribution limité).

📌 **Étapes du DHCP** (DORA) :

* **Discover** : Le client cherche un serveur DHCP.
* **Offer** : Le serveur propose une IP.
* **Request** : Le client accepte l’offre.
* **Acknowledge** : Le serveur confirme l’attribution.

**DNS (Domain Name System) :**

* Résout les noms de domaine en adresses IP.
* Types d’enregistrements :
  + **A** (adresse IPv4), **AAAA** (IPv6)
  + **MX** (serveur mail), **CNAME** (alias), **PTR** (résolution inverse).

**Les niveaux RAID :**

* **RAID 0** : performance, pas de redondance.
* **RAID 1** : miroir, tolérance de panne.
* **RAID 5** : striping + parité, tolérance 1 disque.
* **RAID 10** : combinaison RAID 1 + 0 (mirroring + striping).

**Différence entre Hyper-V, VMware et Proxmox**

📌 **Solutions de virtualisation** :

* **Hyper-V** : Solution Microsoft intégrée à Windows Server.
* **VMware ESXi** : Solution performante mais propriétaire.
* **Proxmox** : Open-source, basé sur KVM avec gestion des conteneurs (LXC).

**Hyperviseurs Type 1 et Type 2**

📌 **Hyperviseur Type 1 ("Bare Metal")**  
➡ Fonctionne directement sur le matériel sans OS intermédiaire.  
**Exemples** :  
✅ **VMware ESXi**  
✅ **Microsoft Hyper-V** (en mode serveur)

📌 **Hyperviseur Type 2 ("Hosted")**  
➡ Fonctionne sur un OS existant (Windows, Linux, macOS).  
**Exemples** :  
✅ **Oracle VirtualBox**  
✅ **VMware Workstation**

**Les types de sauvegarde**

📌 **Méthodes principales** :

* **Complète** : Sauvegarde tout le système.
* **Incrémentale** : Sauvegarde uniquement les fichiers modifiés depuis la dernière sauvegarde (plus rapide).
* **Différentielle** : Sauvegarde les fichiers modifiés depuis la dernière sauvegarde complète.

**Exploiter des serveurs Linux**

**Gestion des utilisateurs et permissions**

➡ Sécurise l’accès aux fichiers et dossiers.

📌 **Commandes utiles** :  
🔹 adduser user1 → Ajouter un utilisateur.  
🔹 passwd user1 → Modifier le mot de passe.  
🔹 chmod 755 fichier → Modifier les permissions.  
🔹 chown user1:group1 fichier → Changer le propriétaire.

**Système de fichiers sous Linux**

📌 **Répertoires clés** :  
📂 /etc → Fichiers de configuration.  
📂 /var/log → Fichiers logs du système.  
📂 /home → Dossiers personnels des utilisateurs.  
📂 /usr/bin → Programmes exécutables installés.

**🔐 Permissions sur les fichiers et répertoires**

* Les **3 premiers caractères** (rwx) → droits du **propriétaire** (utilisateur ayant créé le fichier).
* Les **3 suivants** (rwx) → droits du **groupe** (groupe auquel appartient le fichier).
* Les **3 derniers** (rwx) → droits des **autres** (tous les autres utilisateurs).

📌 **Types de permissions (Unix/Linux)** :  
🔹 **Lecture (r)** → Permet de lire le contenu du fichier/répertoire.  
🔹 **Écriture (w)** → Permet de modifier ou supprimer le fichier/répertoire.  
🔹 **Exécution (x)** → Permet d'exécuter un fichier (pour les programmes et scripts).

📌 **Commandes utiles pour gérer les permissions** :  
🔹 chmod → Modifier les permissions d’un fichier ou d’un répertoire.  
🔹 chown → Changer le propriétaire d’un fichier ou répertoire.  
🔹 ls -l → Voir les permissions actuelles d’un fichier.

**Exemple : rwxr-xr--**

* **Propriétaire** (rwx) → a **tous** les droits (lecture, écriture, exécution).
* **Groupe** (r-x) → peut **lire et exécuter**, mais **pas écrire**.
* **Autres** (r--) → peuvent **seulement lire**.

📌 **Exemple de modification des permissions** :

chmod 755 fichier.txt

**Lettres/Chiffres :**

|  |  |  |
| --- | --- | --- |
| Propriétaire | Groupe | Les autres |
| R W X | R W X | R W X |
| 4 2 1 | 4 2 1 | 4 2 1 |

**Virtualisation**

➡ Technique permettant d’exécuter plusieurs systèmes d’exploitation sur un même matériel physique.

📌 **Types** :  
🔹 **Virtualisation de serveur** (ex : VMware ESXi, Hyper-V).  
🔹 **Virtualisation de poste de travail** (ex : VDI).

📌 **Avantages** :  
🔹 **Optimisation des ressources**.  
🔹 **Isolation des environnements**.  
🔹 **Facilité de sauvegarde et migration**.

**Hyperviseurs – Types et Différences**

**Hyperviseurs de Type 1 (Bare Metal)**

➡ Fonctionnent directement sur le matériel (sans OS hôte). Performants et adaptés aux environnements serveurs.  
**Exemples :**  
✅ VMware ESXi  
✅ Hyper-V  
✅ Proxmox  
✅ KVM

**Hyperviseurs de Type 2 (Hosted)**

➡ Installés sur un OS hôte, moins performants car dépendants de l’OS. Utilisés pour des tests ou des besoins ponctuels.  
**Exemples :**  
✅ VMware Workstation  
✅ VirtualBox

**Conteneurisation**

➡ Technique qui encapsule une application et ses dépendances dans un conteneur léger.

📌 **Exemples d’outils** :  
🔹 **Docker** → Exécution d’applications en conteneurs.  
🔹 **Kubernetes** → Orchestration de conteneurs.

📌 **Avantages** :  
🔹 **Portable et léger**.  
🔹 **Consomme moins de ressources qu’une VM**.  
🔹 **Facilité de déploiement et mise à l’échelle**.

**Wi-Fi (Wireless Fidelity)**

➡ Technologie permettant une connexion réseau sans fil via des ondes radio.

📌 **Normes Wi-Fi** :  
🔹 **802.11n** → Jusqu’à 600 Mbps.  
🔹 **802.11ac** → Jusqu’à 6.9 Gbps.  
🔹 **802.11ax (Wi-Fi 6)** → Meilleure efficacité et débit.

📌 **Glossaire** :

🔹 **AP** → Accès Point

🔹 **DS** → Système de Distribution

🔹 **SSID** → Service Set Identifier

🔹 B**SSID** → Identifiant MAC du Point d’Accès

📌 **Sécurisation** :  
🔹 **WPA2/WPA3** → Protocoles de chiffrement.  
🔹 **Filtrage MAC** → Limite l’accès aux appareils autorisés.

📌 **Priorisation** :

Hybrid Coordination Function - HCF

Ajoute une gestion de priorité de trafic pour

* La voix
* La vidéo
* Le trafic *best effort* classique
* Le trafic de fond (*background*) qui peut attendre les moments de faible charge

📌 **Topologies** :

Une image contenant cercle, croquis, dessin, conception

Le contenu généré par l’IA peut être incorrect.🔹 **BSS Mode infrastructure**

* 1 cellule = 1 BSS
* Stations partagent le canal de communication et donc le débit
* Les communications passent toutes par le point d'accès

Une image contenant cercle, diagramme, ligne, conception

Le contenu généré par l’IA peut être incorrect.🔹 **ESS Infrastructure étendue**

* Plusieurs points d'accès (AP) :
  + Connectés entre eux via un système de distribution (DS)
  + La communication passe par les AP et le DS (le cas échéant)
* DS : en général Ethernet

**Une image contenant cercle, diagramme, croquis, conception

Le contenu généré par l’IA peut être incorrect.**🔹 **Réseau mesh**

Le mode réseau maillé (mesh) permet les avantages de l'ESS sans le besoin d'un système de distribution (DS)

Le point d'accès primaire est relié aux autres réseaux

* Peut disposer d'un *failover*

Tous les AP doivent relayer le trafic :

* Nécessite un protocole de routage dynamique

**⚡ RADIUS, c'est quoi ?**

➡ **Remote Authentication Dial-In User Service** (RADIUS) est un protocole permettant **l’authentification, l’autorisation et la gestion des accès** aux réseaux.

📌 **À quoi ça sert ?**  
🔹 Authentifie les utilisateurs avant d’accéder à un réseau (Wi-Fi, VPN…).  
🔹 Centralise la gestion des accès sur un serveur.  
🔹 Applique des politiques de sécurité (droits d’accès, restrictions).

**📌 Fonctionnement**

🔹 Le client (ex : borne Wi-Fi) envoie une demande d’authentification.  
🔹 Le serveur RADIUS vérifie les identifiants (via base locale, LDAP, AD…).  
🔹 Il accorde ou refuse l’accès selon les règles définies.

**📌 Composants clés**

🔹 **Client RADIUS** → L’équipement qui envoie la requête (routeur, borne Wi-Fi, switch).  
🔹 **Serveur RADIUS** → Vérifie les identifiants et applique les autorisations.  
🔹 **Base d’identification** → Stocke les comptes utilisateurs (LDAP, AD, base SQL…).

**📌 Exemples d’implémentation**

🔹 **FreeRADIUS** → Serveur RADIUS open-source populaire.  
🔹 **Microsoft NPS (Network Policy Server)** → Intégré à Windows Server.

✅ **Points clés** : Sécurise l’accès aux réseaux, centralise l’authentification, compatible avec LDAP/AD. 🚀

**Stockage**

➡ Stocker, organiser et sécuriser les données.

📌 **Types de stockage** :  
🔹 **DAS (Direct Attached Storage)** → Disque dur local, USB.  
🔹 **NAS (Network Attached Storage)** → Serveur de fichiers en réseau.  
🔹 **SAN (Storage Area Network)** → Réseau dédié au stockage haute performance.

📌 **Systèmes de fichiers** :  
🔹 **NTFS** (Windows) → Sécurité avancée.  
🔹 **EXT4** (Linux) → Rapide et fiable.  
🔹 **ZFS** → Tolérance aux pannes, snapshots.

**SSH (Secure Shell)**

➡ Protocole permettant une connexion sécurisée à distance.

📌 **Commande de connexion** :

ssh user@adresse\_ip

📌 **Avantages** :  
🔹 **Chiffrement des échanges**.  
🔹 **Accès sécurisé aux serveurs**.  
🔹 **Tunnelisation pour sécuriser d’autres protocoles**.

**🔑 Clés de chiffrement**

➡ Utilisées pour sécuriser les données et les communications.

📌 **Types de chiffrement** :  
🔹 **Symétrique** (ex : AES, DES) → Une seule clé pour chiffrer et déchiffrer.  
🔹 **Asymétrique** (ex : RSA, ECC) → Une clé publique pour chiffrer, une clé privée pour déchiffrer.  
🔹 **Hachage** (ex : SHA-256, MD5) → Transforme les données en empreinte unique (non réversible).

📌 **Cas d’utilisation** :  
🔹 **HTTPS (TLS/SSL)** → Sécurisation des sites web.  
🔹 **VPN (IPSec, OpenVPN)** → Sécurisation des connexions.  
🔹 **Stockage de mots de passe** → Hashing pour éviter le stockage en clair.

**📑 Journaux (Logs)**

➡ Fichiers qui enregistrent les événements et actions du système.

📌 **Types de journaux** :  
🔹 **Logs système** → Informations sur le système d'exploitation (ex : /var/log/syslog sous Linux).  
🔹 **Logs applicatifs** → Informations sur les applications installées.  
🔹 **Logs de sécurité** → Événements de connexion, tentatives d'accès non autorisées.

📌 **Commandes utiles** :  
🔹 **Linux** : journalctl pour lire les logs, dmesg pour voir les messages du noyau.  
🔹 **Windows** : Utilisation du **Visualiseur d'événements** (eventvwr.msc) pour analyser les journaux système.

**☁️ Cloud Computing**

➡ Utilisation de ressources informatiques (serveurs, stockage, bases de données, réseaux) via Internet plutôt que sur des serveurs physiques locaux.

📌 **Principaux avantages** :  
🔹 **Évolutivité** → Ajout ou réduction rapide des ressources selon les besoins.  
🔹 **Flexibilité** → Accès aux ressources depuis n'importe quel appareil connecté à Internet.  
🔹 **Réduction des coûts** → Pas besoin d'investir dans des infrastructures matérielles coûteuses.  
🔹 **Disponibilité** → Accès continu aux services et applications, souvent avec un SLA (Service Level Agreement).

📌 **Types de Cloud** :  
🔹 **Cloud public** → Ressources partagées, hébergées par un fournisseur externe (ex : AWS, Microsoft Azure).  
🔹 **Cloud privé** → Infrastructure dédiée à une organisation, hébergée en interne ou par un fournisseur externe.  
🔹 **Cloud hybride** → Combinaison des deux, avec certaines ressources dans le cloud public et d'autres dans le cloud privé.

📌 **Modèles de services Cloud** :  
🔹 **IaaS (Infrastructure as a Service)** → Fourniture de ressources matérielles virtualisées (serveurs, stockage, réseaux). Exemple : AWS EC2, Microsoft Azure.  
🔹 **PaaS (Platform as a Service)** → Fourniture d’une plateforme permettant de développer, tester et déployer des applications sans gérer l'infrastructure sous-jacente. Exemple : Google App Engine, Microsoft Azure App Service.  
🔹 **SaaS (Software as a Service)** → Applications prêtes à l’emploi accessibles via un navigateur web. Exemple : Office 365, Gmail, Salesforce.

**⚡ Solutions de Haute Disponibilité (High Availability - HA)**

➡ Garantir la disponibilité continue des services et minimiser les interruptions en cas de panne matérielle, logicielle ou réseau.

📌 **Pourquoi la Haute Disponibilité ?**  
🔹 **Réduction des interruptions de service** → Minimise les temps d'arrêt pour les utilisateurs et applications critiques.  
🔹 **Amélioration de la fiabilité** → Permet aux services de fonctionner même en cas de défaillance matérielle.  
🔹 **Optimisation des performances** → Répartition intelligente des charges pour éviter les surcharges d’un seul serveur.  
🔹 **Sécurité et continuité des opérations** → Protection contre les défaillances imprévues et les attaques.

**🛠️ Principaux mécanismes de HA**

📌 **Load Balancing (Équilibrage de charge)** → Répartition du trafic entre plusieurs serveurs pour éviter la surcharge.

📌 **Redondance des composants** → Multiplication des équipements pour éviter un point de défaillance unique.  
🔹 **Alimentation redondante** → Deux blocs d’alimentation pour éviter une coupure en cas de panne électrique.  
🔹 **Stockage redondant** → RAID (ex : RAID 1, RAID 5, RAID 10).  
🔹 **Réseaux redondants** → Liens doubles avec agrégation de liens (LACP) et routage dynamique.

📌 **Data Replication (Réplication des données)** → Synchronisation des données sur plusieurs serveurs pour assurer la continuité.

**📂 Système de fichiers (File System)**

➡ Organisation et gestion des données sur un disque dur ou un support de stockage.

📌 **Rôle principal** :  
🔹 Permet de stocker, organiser et retrouver les données.  
🔹 Définit la manière dont les fichiers sont nommés, stockés et récupérés.

📌 **Types de systèmes de fichiers** :  
🔹 **FAT32** → Compatible avec la plupart des systèmes, mais limité à 4 Go par fichier et 8 To par partition.  
🔹 **NTFS** → Système de fichiers principal sous Windows, avec gestion des autorisations et compression.  
🔹 **EXT4** → Système de fichiers couramment utilisé sur Linux, avec une bonne gestion des performances et de la sécurité.  
🔹 **APFS** → Système de fichiers moderne d'Apple, conçu pour macOS et les appareils iOS.

**📂 Différents types de partitions**

➡ Structure logique du disque permettant de séparer les différents espaces de stockage.

📌 **Types de partitions** :  
🔹 **Primaires** → Permettent d'installer un système d'exploitation (limitée à 4 partitions par disque).  
🔹 **Étendues** → Permettent de créer plusieurs partitions logiques (utilisées pour dépasser la limite de 4 partitions primaires).  
🔹 **Logiques** → Crées à l'intérieur d'une partition étendue, utilisées pour organiser davantage d'espace.

📌 **Commandes pour partitionner** :  
🔹 **Linux** : fdisk, parted, gparted pour gérer les partitions.  
🔹 **Windows** : Utilisation du gestionnaire de disque (diskmgmt.msc).

**📁 Points de montage**

➡ Permet d'attacher un périphérique de stockage (disque, clé USB) à un répertoire du système.

📌 **Principaux points de montage** :  
🔹 **Root (/) :** Le répertoire racine, contient tous les fichiers et répertoires du système.  
🔹 **/home :** Répertoire pour les données personnelles des utilisateurs.  
🔹 **/mnt et /media :** Répertoires utilisés pour monter des périphériques temporaires (disques durs externes, clés USB).

📌 **Commandes utiles** :  
🔹 **Linux** : mount pour monter un périphérique, umount pour le démonter.  
🔹 **Windows** : Utilisation de l'Explorateur de fichiers ou la commande diskpart pour gérer les partitions.

**Fonctionnement d’un Gestionnaire de Paquets**

Un gestionnaire de paquets est un outil automatisant le processus d’installation, désinstallation, mise à jour de logiciels installés sur un système Linux de manière organisée et cohérente, souvent à partir de dépôts.

Ce processus est un élément fondamental du système d'exploitation Linux pour la maintenance et la sécurité.

Il comprend également la gestion des dépendances.

* **Paquet :** archive contenant des fichiers binaires, des bibliothèques, des scripts et des métadonnées…
* **Dépendances :** Les paquets peuvent dépendre d'autres paquets pour fonctionner correctement
* **Centralisation des ressources :** Liés à des référentiels de logiciels (dépôts) qui fournissent des applications vérifiées et compatibles avec la distribution Linux choisie

📌 **Dépôts de paquets**  
🔹 Les logiciels sont stockés sur des serveurs appelés **repositories**.  
🔹 Ils contiennent les différentes versions des paquets et leurs mises à jour.

📌 **Installation et mise à jour**  
🔹 Télécharge et installe automatiquement les fichiers et leurs dépendances.  
🔹 Exemple : apt install apache2 (Debian/Ubuntu) ou dnf install httpd (RedHat/CentOS).

📌 **Vérification et intégrité**  
🔹 Utilise des **systèmes de signatures numériques** (clé GPG) pour assurer l’authenticité des paquets.  
🔹 Évite l’installation de logiciels corrompus ou malveillants.

📌 **Désinstallation et nettoyage**  
🔹 Supprime proprement les paquets et leurs dépendances inutilisées.  
🔹 Exemple : apt remove package-name && apt autoremove.

**Exemples de Gestionnaires de Paquets**

📌 **Sur Linux**  
🔹 **APT (Debian/Ubuntu)** → apt install, apt update, apt remove.

apt update : met à jour la liste des paquets disponibles (sinforme de quelles mises à jour sont dispos).

apt upgrade : met à jour les paquets installés vers leur dernière version (installe les dernières mises à jour).  
🔹 **DNF/YUM (RedHat/Fedora/CentOS)** → dnf install, yum update.  
🔹 **Pacman (Arch Linux)** → pacman -S, pacman -R.

📌 **Sur Windows**  
🔹 **Chocolatey** → choco install package-name.  
🔹 **Winget** → winget install package-name.

📌 **Sur macOS**  
🔹 **Homebrew** → brew install package-name.

**🚀 Points Clés à Retenir**

✅ **Simplifie l’installation et la gestion des logiciels**.  
✅ **Gère les dépendances automatiquement**.  
✅ **Assure l’intégrité et la sécurité des paquets**.  
✅ **Facilite la mise à jour et la maintenance du système**.

📌 **Téléphonie via IP**

**À quoi ça sert ?**  
🔹 Réduit les coûts téléphoniques.  
🔹 Offre des fonctionnalités avancées (visioconférence, transferts, messagerie).  
🔹 Utilise une connexion Internet pour transmettre la voix sous forme de paquets.

**⚡VoIP/ToIP**

**VoIP = un protocole**.

La VoIP désigne la technologie utilisée (les protocoles) pour transmettre un flux voix (des appels) sur un réseau IP (en général internet).

**ToIP = une infrastructure**.

La ToIP est un ensemble de techniques.

Elles permettent la mise en place de la téléphonie et de services associés sur un réseau IP d’entreprise.

Un réseau d’infrastructure ToIP s’appuie sur de la VoIP pour fonctionner.

**Les éléments de la ToIP :**

Les équipements :

* Terminaux IP (téléphones ip, smartphones, ordinateurs), adaptateur ATA (connecte un tel classique à un réseau IP), softphone (par logiciel sur tel, tablettes, ordi)
* Commutateur, PABX (réseau RTC), IPBX (réseau IP)
* Passerelle VoIP (convertit le trafic téléphonique en données)

Les protocoles :

* H.323
* **SIP** : protocole de communication ouvert, utilisable par tout le monde, sans restriction. Le SIP est un protocole de signalisation, pour établir et contrôler des sessions multimédias (plusieurs médias pendant un appel).

⇒ Incontournable dans la ToIP.

🔹 Ports 5060/5061

🔹Couche 5 OSI

🔹 Un **User Agent** ou **UA** est un logiciel client qui sert à la transmission des messages SIP.

On les trouve dans les terminaux IP et dans les softphone.

On distingue :

* Les **UAC** : Agent Utilisateur Client ⇒ entité logique qui envoie une requête SIP et reçoit une réponse SIP
* Les **UAS** : Agent Utilisateur Serveur ⇒ entité logique qui génère une réponse SIP à une requête SIP

🔹 **Registrar** : 2 UA peuvent communiquer directement entre-eux avec leur @IP.

Pour éviter les problèmes d’@IP, on utilise un **Registrar**. Il va gérer les requêtes de type REGISTER en provenance des UA.

Une image contenant texte, capture d’écran, Police, conception

Le contenu généré par l’IA peut être incorrect.

🔹 Un **proxy SIP** se place entre 2 UA qui ne connaissent pas leur @IP, il va gérer le routage des messages SIP.

Il va chercher dans la BDD du Registrar le couple **URI/@IP** et va pouvoir diriger les messages SIP vers le bon UA.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

🔹 **Glossaire SIP :**

**Transaction SIP** :

Un échange de demandes/réponses finalisé et complet.

**Dialogue SIP** :

Une série de transaction entre 2 éléments.

**Session média** :

Flux média (audio et/ou vidéo) circulant entre 2 éléments.

Des transactions et des dialogues sont nécessaires pour obtenir une session média.

**Les évolutions réseaux :**

* Le **Trunk SIP** est un protocole utilisé pour acheminer les communications téléphoniques sur un réseau Internet en utilisant la voix sur IP (VoIP/ToIP).

Il permet à un IPBX de gérer les communications via les équipements fournis par un opérateur de téléphonie IP.

On doit souscrire à une **offre de service** auprès d'un opérateur pour en bénéficier. Cela permet à un IPBX de passer des appels simultanément sur Internet.

On peut connecter autant de canaux que l’on souhaite, il n’y a plus les limitations T0 et T2 du RNIS.

Une image contenant texte, diagramme, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, diagramme, Police, carte

Le contenu généré par l’IA peut être incorrect.

* Le **Centrex IP** :

Une architecture **Centrex** déporte la téléphonie dans le cloud de manière mutualisée. L’opérateur centralise sur une plateforme unique les serveurs téléphoniques de l’ensemble des terminaux clients.

Solution pratique et peu coûteuse pour les petites entreprises ⇒ fonctionnelle, simple et sécurisée.

Souvent la solution comprend un package regroupant les équipements.

Une image contenant texte, diagramme, Police, clipart

Le contenu généré par l’IA peut être incorrect.

**📌 Fiches de révision TSSR – Active Directory (AD)**

**À quoi ça sert ?**  
➡ Base de données centralisée qui gère les utilisateurs, groupes, ordinateurs et ressources d’un domaine Windows.

📌 **Principaux composants** :

* **OU (Unité d’Organisation)** : Conteneur pour organiser les objets AD.
* **GPO (Group Policy Object)** : Règles appliquées aux utilisateurs/ordinateurs (ex : restrictions, configurations réseau).
* **LDAP (Lightweight Directory Access Protocol)** : Protocole utilisé pour interroger AD.

**Les niveaux fonctionnels d’AD**

**Pourquoi c’est important ?**  
➡ Définissent les fonctionnalités disponibles en fonction des versions Windows Server utilisées.

📌 **Exemples** :

* **Windows Server 2008** : Prend en charge la corbeille AD.
* **Windows Server 2016** : Amélioration de la réplication et authentification.

**DC (Domain Controller) dans un domaine**

**À quoi ça sert ?**  
➡ Authentifie les utilisateurs et gère les ressources d'un domaine Active Directory.  
➡ Stocke la base de données des identifiants et droits d’accès (AD DS).

**Les rôles FSMO (Flexible Single Master Operations)**

➡ Gèrent certaines tâches critiques d’Active Directory.

📌 **Les 5 rôles FSMO** :  
**Schema Master** → Modifie le schéma AD.  
**Domain Naming Master** → Gère les noms de domaine.  
**RID Master** → Attribue les identifiants aux objets AD.  
**PDC Emulator** → Synchronise les mots de passe et gère les GPOs.  
**Infrastructure Master** → Assure la cohérence entre les domaines.

**🔧 GPO (Group Policy Object)**

➡ Permet d’appliquer des configurations et restrictions sur un parc informatique via Active Directory.

📌 **Exemples d’application** :  
🔹 **Sécuriser les postes utilisateurs** (désactiver l’accès au panneau de configuration).  
🔹 **Déployer des logiciels automatiquement**.  
🔹 **Configurer les stratégies de mots de passe** (longueur, expiration).

📌 **Commandes utiles** :  
🔹 gpedit.msc → Modifier une GPO localement.  
🔹 gpupdate /force → Appliquer immédiatement les GPO.  
🔹 gpresult /r → Vérifier les GPO appliquées.

**📌 Fiches de révision TSSR – Différents Services/Serveurs**

**Bareos (Backup Archiving Recovery Open Sourced)**

➡ Logiciel open-source de sauvegarde et restauration des données.

📌 **Fonctionnalités principales** :  
🔹 **Sauvegarde complète, différentielle, incrémentale**.  
🔹 **Chiffrement et compression des sauvegardes**.  
🔹 **Planification et automatisation** des sauvegardes.

**⚡ GLPI, c'est quoi ?**

➡ Outil open-source de gestion de parc informatique et de helpdesk.

📌 **À quoi ça sert ?**  
🔹 **Inventaire** : Suivi des matériels, logiciels et licences.  
🔹 **Helpdesk** : Gestion des tickets d’assistance.  
🔹 **Gestion financière** : Suivi des contrats et coûts.

**📌 Principales fonctionnalités**

✅ **Gestion des actifs** : Matériel, logiciels, périphériques.  
📌 **Gestion des interventions** : Création et suivi des tickets.  
🔄 **Base de connaissances** : Documentation interne pour les techniciens.  
📊 **Rapports et statistiques** : Analyse du parc et des incidents.

✅ **Points clés** : Optimise la gestion IT, facilite le support utilisateur et centralise les informations.

**WDS (Windows Deployment Services)**

➡ Permet le déploiement d’images Windows sur des machines en réseau.

📌 **Avantages** :  
🔹 **Installation sans support physique (PXE boot)**.  
🔹 **Gain de temps pour le déploiement en masse**.  
🔹 **Compatibilité avec MDT pour des installations automatisées**.

**WSUS (Windows Server Update Services)**

**À quoi ça sert ?**  
➡ Permet de gérer et déployer les mises à jour Windows sur un réseau d'entreprise.

**Différents statuts des mises à jour :**  
✅ **Approuvée** : Prête à être installée sur les postes.  
❌ **Refusée** : Ne sera pas installée.  
🔄 **En attente** : Téléchargement ou installation en cours.  
📥 **Non approuvée** : Pas encore validée par l’administrateur.

**🔄 Mise à jour régulière des systèmes et logiciels**

➡ Garantit la sécurité, la stabilité et les performances des infrastructures informatiques.

📌 **Enjeux principaux** :  
🔹 **Sécurité** → Corrige les failles exploitées par les hackers 🡪 Elimine les vulnérabilités de sécurité  
🔹 **Stabilité** → Améliore la compatibilité et réduit les bugs   
🔹 **Performance** → Optimise la rapidité et l’efficacité du système.  
🔹 **Conformité** → Respecte les normes de cybersécurité et réglementations (ex : RGPD).

📌 **Types de mises à jour** :  
🔹 **Correctives** → Corrigent des bugs et failles de sécurité.  
🔹 **Évolutives** → Apportent de nouvelles fonctionnalités.  
🔹 **Préventives** → Améliorent la compatibilité et la stabilité.

📌 **Bonnes pratiques** :  
✅ Tester les mises à jour sur un environnement de préproduction.  
✅ Automatiser les mises à jour critiques avec WSUS (Windows) ou apt/yum (Linux).  
✅ Planifier les mises à jour pour éviter les interruptions de service.

📌 **Absences de mises à jour** :  
🔹 **Vulnérabilités** → Atteinte à l’intégrité du système, fonctionnement normal, fonctionnalités, intégrité des données. Ex : Vulnérabilités de type « zero-day », OU d’utilisation du code à distance (RCE)  
🔹 **Conséquences sur la performance** → Détérioration de la performance, risques d’incompatibilité et défaillance système (OS, pilotes, domaine,…).  
🔹 **Impact sur la conformité et la réputation**.

**Supervision**

➡ Surveille en temps réel l’état des équipements et services d’un réseau.

📌 **Outils courants** :  
🔹 **Nagios** → Surveillance des infrastructures IT.  
🔹 **Zabbix** → Monitoring des performances.  
🔹 **Centreon** → Supervision complète avec alertes.

📌 **Indicateurs surveillés** :  
🔹 **CPU, RAM, stockage**.  
🔹 **Disponibilité des serveurs**.  
🔹 **Utilisation de la bande passante**.

**⚡ Le Web, c'est quoi ?**

➡ Le Web (World Wide Web) est un **système de consultation et d’échange de documents** via Internet, basé sur le protocole HTTP/HTTPS.

📌 **À quoi ça sert ?**  
🔹 Permet d’afficher des pages web via un navigateur (Chrome, Firefox, Edge…).  
🔹 Fonctionne grâce à un modèle **client-serveur** (le client demande une page, le serveur la fournit).  
🔹 Utilise des langages comme **HTML, CSS, JavaScript** pour l’affichage des pages.

**📌 Qu'est-ce qu'un Serveur Web ?**

➡ Un serveur web est un logiciel qui stocke, traite et sert les pages web aux clients via HTTP/HTTPS.

📌 **À quoi ça sert ?**  
🔹 Héberge des sites web et des applications accessibles via un navigateur.  
🔹 Répond aux requêtes des clients en fournissant du contenu (HTML, images, vidéos…).  
🔹 Gère la sécurité avec HTTPS et l’authentification des utilisateurs.

**⚡ Proxy, c'est quoi ?**

➡ Un serveur intermédiaire entre un client et Internet, servant à filtrer, sécuriser ou optimiser les connexions.

📌 **À quoi ça sert ?**  
🔹 **Cache** : Accélère l’accès aux sites web.  
🔹 **Sécurité** : Filtrage des contenus et anonymisation.  
🔹 **Contrôle** : Restriction et journalisation des accès.

✅ **Exemples** : Squid, Nginx, Microsoft Proxy 🚀

**⚡ IDS & IPS, c'est quoi ?**

➡ Des systèmes de sécurité réseau qui détectent et réagissent aux menaces.

📌 **À quoi ça sert ?**  
🔹 **IDS (Intrusion Detection System)** : Détecte les attaques et alerte l’administrateur.  
🔹 **IPS (Intrusion Prevention System)** : Bloque automatiquement les attaques en plus de les détecter.

**📌 Différences clés**

✅ **IDS** : Surveillance passive, analyse du trafic, alerte en cas d’intrusion.  
🚫 **IPS** : Surveillance active, bloque les menaces en temps réel.

**📌 Exemples d’outils**

🔹 **Snort** (IDS/IPS open-source).

✅ **Points clés** : Protège le réseau contre les attaques en détectant (IDS) ou en bloquant (IPS) les menaces. 🚀

**⚡ TCP/IP, c'est quoi ?**

➡ Suite de protocoles permettant la communication sur les réseaux, notamment Internet.

📌 **À quoi ça sert ?**  
🔹 **TCP (Transmission Control Protocol)** : Assure une transmission fiable des données (connexion, contrôle d’erreur).  
🔹 **IP (Internet Protocol)** : Identifie et achemine les paquets à travers le réseau.

**📌 Modèle TCP/IP (4 couches)**

1️ **Accès réseau** : Interface avec le matériel (Ethernet, Wi-Fi).  
2️ **Internet** : Routage des paquets (IP, ICMP).  
3️ **Transport** : Gestion de la connexion (TCP, UDP).  
4️ **Application** : Services réseau (HTTP, FTP, SMTP).

**⚡ ACL, c'est quoi ?**

➡ Liste de règles définissant **qui peut accéder à quoi** sur un réseau ou un système.

📌 **À quoi ça sert ?**  
🔹 **Filtrer le trafic** sur un routeur ou firewall.  
🔹 **Restreindre l’accès aux ressources** sur un switch ou un serveur.  
🔹 **Appliquer des règles spécifiques** selon l’adresse IP, le protocole, ou le port.

**📌 Types d’ACL**

✅ **ACL Standard** : Filtre le trafic selon l’IP source.  
✅ **ACL Étendue** : Filtre selon l’IP source/destination, protocole et port

**📌 Exemples d’utilisation**

🔹 **Bloquer un accès** à un réseau (deny 192.168.1.100 any).  
🔹 **Autoriser uniquement un service** (permit tcp any any eq 22 pour SSH).

✅ **Points clés** : Sécurise le réseau en contrôlant les accès et le trafic. 🚀

**📌 Bareos**

**Bareos-dir (Director):** Composant central qui gère la configuration, la planification des travaux de sauvegarde

**Bareos-sd (Storage Daemon):** Responsable du stockage physique des données de sauvegarde sur les supports de stockage qu'il reçoit des clients.

**Bareos-fd (File Daemon):** C'est l'agent installé sur chaque client qui permet à Bareos-dir de gérer les sauvegardes.