Les réseaux et la sécurité

1) Paramétrer un réseau informatique : complément au chapitre 9 du livre
2) Travailler avec des réseaux et des données sécurisés : complément au chapitre 10 du livre

Activité	
7.2 7.2.2	Gérer les informations de l'organisation Maintien de la fiabilité et de la sécurité des informations
Compétences	Identifier les ressources, leur localisation et leurs rôle au sein du SI, leurs droits d'accès et les services de sécurité

Prérequis : le SI

1. Les composantes
2. Les fonctions

Composante technologique du SI

1. Le poste de travail
2. Les progiciels et logiciels
3. Le réseau
4. La sécurité

1- Le réseau local d'entreprise

- Ensemble d'ordinateurs et de périphériques connectés entre eux
- Permet le transfert de données à des vitesses élevées, sur des courtes distances et dans la limite d'une enceinte privée
- Travail en aut[illegible] aux serveurs
- Intérêts

du SI en réseau:

Possibilités offertes	Gains attendus
• Communiquer et partager des données • Mise en place de politiques d'accès aux données(profils et groupes d'utilisateurs)	• Rendre le travail plus efficace • Garantir la cohérence et l'unicité de données • Économiser du temps
• Partager des ressources (logiciels, périphériques, accès à Internet)	• Réduire les coûts • Faciliter la maintenance
• Centraliser la gestion de certaines ressources	• Réduire les coûts • Faciliter, sécuriser

2- Internet/Intranet/Extranet

- Internet = réseau qui interconnecte à l'échelle mondiale un ensemble de réseaux
- propose des services :
  - Publication d'informations (web)
  - Communication par messagerie électronique asynchrone ou synchrone ou par téléphone
  - Commerce électronique
  - Services en ligne
  - Partage de contenus
  - …

2- Intranet/Extranet/Internet

- **Intranet = réseau local interne à l'entreprise qui utilise les technologies et les protocoles de l'Internet**
  - Applications spécifiques à l'entreprise
  - Accès authentifié, sécurisé
- **Extranet = extension du réseau de l'entreprise et de son SI auprès des partenaires et/ou des clients.**
  - Accès réglementé depuis l'extérieur par des politiques de sécurité très strictes

3- Architecture réseau :

- 2 types :
  - Modèle client/serveur : serveur partage ses ressources, les ordinateurs qui utilisent les ressources partagées sont les clients
  - Modèle peer to peer (pair à pair): tous les ordinateurs connectés au réseau sont égaux partagent leurs ressources et chacun y a accès
- Le modèle client/serveur est le plus utilisé car :
  - Centralisation des ressources (unicité, cohérence, maintenance, sécurité centralisée,…)
  - Accès décentralisé multiple aux ressources
- Différents types de serveurs (p.120)
- Les logiciels associés au réseau :
  - Les systèmes d'exploitation pour serveurs
  - Les logiciels collaboratifs …

4- Configuration physique (les composantes physiques p.119)

- **Point de connexion = carte réseau**
  - Adresse physique : MAC
  - Adresse logique : IP
- **Support de communication :**
  - **Filaires : types de câbles p.87**
  - **Non filaires : wifi p.86**
- **Étendue géographique selon la portée, l'échelle :**
  - LAN = réseau interne d'une entreprise
  - WLAN = LAN sans fil
  - MAN = relie plusieurs LAN géographiquement proches
  - WAN = relie plusieurs LAN sur de grandes distances
  - Internet

4- Configuration physique : matériel d'interconnexion (p.119)

- Dans un même réseau : commutateur

- Pour communiquer avec d'autres réseaux (adresses IP de réseau différentes)

Routeur 	Doté de plusieurs cartes réseau dont chacune possède une adresse IP appartenant à un des réseaux interconnectés. Assure le routage = recherche d'un chemin pour acheminer les données jusqu'à son destinataire Voir le routage p.103	**Proxy** 	Logiciel intermédiaire entre 2 réseaux : • Accélération navigation(mémoire cache, filtrage pub,…) • Journalisation(logs) • Sécurisation(point d'entrée-sortie) • Filtrage(avec parefeu) • Anonymat(masquer adresse réseau)
Pare-feu 	Défend un ordinateur local contre les virus, vers, chevaux de Troie et attaques de piratage par force brute. Composant logiciel ou matériel. Analyse le trafic réseau entrant afin de vérifier qu'il ne contient pas de données répertoriées sur liste noire. Souvent couplé à un routeur.		

5- Configuration logique : Les protocoles (p.121)

- **Assurent la communication entre les équipements**
- **Langage informatique qui permet de faire « dialoguer » les ordinateurs à travers des réseaux qui peuvent être de natures différentes**
- **Exemples pour l'usage d'un réseau :**
  - Intranet et Internet utilisent les protocoles
    - TCP : pour garantir la transmission des données
    - IP : pour l'acheminement des paquets de données
  - HTTP / HTTPS : permet la gestion des liens hypertextes
  - DNS : gestion les noms de domaine
  - DHCP : gestion de l'attribution dynamique des adresses IP
  - FTP : transfert de fichiers

5- Configuration logique : Les protocoles

- **Exemples pour l'usage de la messagerie électronique :**
  - Réception de courrier : POP(messages téléchargés), IMAP
  - Envoi : SMTP

6- Configuration logique d'un réseau : l'acheminement des données avec le protocole TCP-IP(p.121)

- Protocole de communication
- TCP/IP
  - Découpage en paquets
  - Contrôle de la transmission

7- Configuration logique : Adressage des machines (p.122 à 125), l'adresse IP

- Adresse IP : Internet Protocol
- Adresse unique pour chaque poste connecté à un réseau
- Version 4 ou 6
- Adresse statique/dynamique
- Rôle du masque de réseau
  - Partie réseau (NetId) et partie hôte(HostId) d'une adresse
  - Taille du réseau
- 2 adresses réservées : Adresse du réseau et adresse de diffusion

7- Adressage des machines (p.101) : adresse IP

- **En IPV4 : 3 classes selon le nombre de postes en réseau local à identifier**
  - Classe A : réseau d'adresse 10.0.0.0 et 16 millions ~ d'adresses disponibles
  - Classe B : réseau d'adresse 172.16.0.0 à 172.31.0.0 et 65 000~ adresses disponibles par réseau
  - Classe C : réseau d'adresse 192.168.0.0 à 192.168.255.0 et 255 adresses disponibles par réseau
- **Masque de réseau : permet de distinguer l'adresse réseau dans l'adresse IP d'un élément du réseau**
  - Classe A : masque 255.0.0.0 ou /8
  - Classe B : masque 255.255.0.0 ou /16
  - Classe C : masque 255.255.255.0 ou /24

Exercices :

1. Tableaux à compléter
2. Serveur DHCP
3. Pharmacie DECURY
4. Palais Ocean
5. Livre p.126 à 128

8. Sécurité du SI (p.136)

- Identifier les risques pour apporter des solutions préventives, palliatives (faire fonctionner le SI pendant le problème) et curatives :

Type de risques	Exemples de solutions
Physiques	Sécuriser les accès aux locaux, anti-incendie, redondance des équipements,…
Des accès logiques	Authentification, autorisations d'accès aux applications et aux données… (p.139)
Des échanges	Pare-feu, proxy, sensibilisation hameçonnage…
Des données	Antivirus, sauvegardes, chiffrement,…

8- Sécurité du SI

- Les services (p.138)
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Authentification
  - Traçabilité
  - Non répudiation
- La démarche
  1. Aspects technologiques, organisationnels et humains
  2. Charte d'usage du SI, gouvernance d'Internet, RFC, « neutralité » d'Internet…

8- Sécurité du SI

- Les moyens, quelques exemples :
  - Pare-feu
  - Proxy
  - VPN
  - VLAN
  - chiffrement