



Télécommunications et Réseaux

Chapitre 1 : Introduction et généralités

Cours de M. Petein Thomas

Email : thomas.petein@heh.be



Présentation

Une présentation s'impose :

Nom : Petein

Prénom : Thomas

Parcours scolaire :

- sorti en 2002 de l'athénée Royal René Magritte de Lessines
- entame une 1^{ère} année à la faculté polytechnique de Mons (ratée...)
- recommence une 1^{ère} année à la faculté polytechnique de Mons (ratée encore...)
- entame en 2004 une 1^{ère} année à l'ISIMs (devenu maintenant le Département des Sciences et technologies de la HEH)
- obtient (en 2009) son Master en sciences de l'ingénieur industriel finalité informatique à l'ISIMs (ancien nom du Département des Sciences et technologies)
- obtient (en 2014) son Master en sciences de gestion à la Louvain School of Management (anciennement les FUCAM)



Avant de commencer

Bienvenue dans les études supérieures !

Si vous avez choisi d'entreprendre des études supérieures, je suppose que vous êtes motivé et je vous en félicite déjà. Maintenant, la motivation est une chose importante mais elle ne fait pas tout...

Etant donné que les études supérieures sont, pour beaucoup d'entre vous, une étape complètement nouvelle, je vais essayer de vous donner quelques infos et quelques conseils pour mettre un maximum de chances de votre côté.

Tout d'abord, parmi les croyances tenaces à propos des études supérieures, il y a celles qui concernent la présence aux cours. On entend souvent dire : « *la présence aux cours n'est pas obligatoire, chacun est libre d'assister au cours comme bon lui semble (ou non). En plus, si le syllabus est bien fait, on peut franchement se contenter d'un bon travail à domicile.* »

Ceci est vrai... et faux à la fois !



Quand je dis que c'est *vrai*, cela implique qu'il est tout à fait possible de réussir son année académique sans assister aux cours théoriques. Seulement pour 90% des personnes qui tenteront cette approche, cela se traduira par un échec cuisant en fin d'année... Pour les 10% restant, soit ils possèdent des facultés particulières et tant mieux pour eux, soit ils ont eu de la chance et la prochaine fois qu'ils réitéreront l'expérience, cela ne se passera pas aussi bien.

Donc quand je dis que c'est faux, vous l'aurez compris, c'est que pour avoir un diplôme (quel qu'il soit) il faudra travailler. Seulement travailler, même parfois beaucoup, ne suffit souvent pas !!!

C'est pourquoi, je vais donc vous donner certains conseils afin de vous aider à réussir votre année (afin de profiter de vacances en juillet et en août !)

Et mon **premier conseil** est évident : **assister aux cours théoriques.**

Pourquoi ?

Car aller au cours, cela permet d'emmagasiner une première fois des connaissances.

C'est également une aide précieuse, pour les révisions : si on a écouté attentivement le professeur, on aura retenu déjà une bonne partie de ce que l'on doit savoir pour l'examen.

En plus de cela, à la fin des cours, si vous n'avez pas compris une notion, n'hésitez pas à aller demander des explications.



Introduction et généralités

Mon **deuxième conseil** pour réussir des études supérieures est qu'il faut **être organisé**.

Et pour cela, il faut se rendre aux cours, le suivre, et prendre des notes de manière régulière.

La méthode est assez simple, il vous faudra juste un bic, du papier et une farde (pour ranger et trier chaque cours). Grâce à vos notes, vous serez en mesure d'ajouter des compléments d'informations au syllabus et également d'effectuer des **fiches pour réviser** par la suite.

Mon **troisième conseil** est d'**assister aux laboratoires** qui, eux, sont obligatoires.

Plusieurs absences sont susceptibles de vous interdire l'accès aux examens si elles ne sont pas justifiées...

Lors de ces laboratoires, organisés en groupes, il est important de participer car c'est en participant que vous verrez si vous avez réellement compris la matière ou si quelque chose vous échappe.

Cette organisation est d'ailleurs faite pour que les étudiants puissent se retrouver en petit nombre face au professeur de laboratoire. En participant sérieusement à ces séances, vous ne pourrez ainsi que consolider vos acquis.

Introduction et généralités

Mon **quatrième conseil** est de **travailler de manière régulière**.

En effet, les enseignants des écoles supérieures et des universités considèrent les étudiants comme des *adultes*, et les responsabilisent un maximum. Dès lors, si l'on vous demande de faire un travail, de lire ou de revoir quelque chose, on ne perdra pas de temps à vous faire la morale si vous ne le faites pas...

Il est donc primordial d'organiser votre emploi du temps chaque semaine ! Un travail régulier vous permettra d'éviter de tout réviser à la dernière minute, à quelques heures du début des examens.

Travailler en petits groupes peut également être intéressant tant sur le plan de la motivation que sur le plan de la compréhension. Pensez aussi à mettre à profit votre temps perdu dans les transports en commun.

Finalement, mon **cinquième conseil** est de bien **préparer sa session d'examen en faisant** notamment **des résumés à l'avance** !

Alors qu'auparavant, des contrôles étaient organisés chaque semaines, maintenant ceux-ci seront quasi inexistantes et il n'y aura bien souvent que des examens en fin de semestre (voire en fin d'année).

→ Pour éviter d'avoir à se retrouver avec une pile gigantesque de cours à assimiler, mieux vaut apprendre un peu toutes les semaines. Car une fois que la session d'examens a débuté, il ne vous restera que quelques jours pour revoir...

Introduction et généralités

Bien entendu, parmi ces cinq conseils, seul le premier concerne mon cours de télécommunications et réseaux 1. Je vais donc insister encore un peu en vous donnant 7 arguments qui, je l'espère, vous convaincront.

Etre présent et participer au cours c'est :

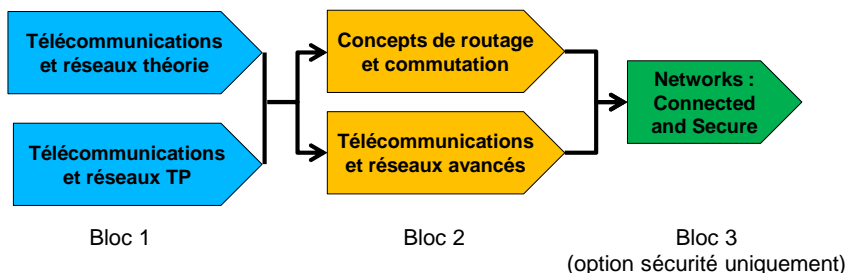
- s'approprier une première fois la matière. Cette appropriation est renforcée par la prise de notes et va bien évidemment faciliter l'apprentissage ultérieur.
- soutenir sa motivation en percevant le fil conducteur du cours. Il est bien plus difficile de faire des liens entre différents points de la matière si l'on est absent aux cours magistraux.
- favoriser la mise au travail et la persévérance par le soutien reçu des autres étudiants et des enseignants.
- prendre conscience de ce qui va être difficile à apprendre et sur quoi il va donc falloir insister lors de votre étude.
- repérer les tuyaux et les points sur lesquels le professeur insiste.
- noter de nouveaux exemples, de nouveaux exercices ou des explications supplémentaires qui ne feront que vous aider à réussir.
- le meilleur moyen d'être informé sur les interrogations et les examens à venir.

Introduction et généralités

But du cours

Le but de ce cours est de vous apprendre les bases des réseaux informatiques. Lorsque plus tard vous allez vous trouver devant du matériel informatique, il est important que vous puissiez distinguer les différents éléments se trouvant devant vous mais aussi que vous compreniez leurs fonctionnements.

Articulation du cursus de télécommunications & réseaux



Introduction et généralités

Cisco Systems

Entreprise informatique américaine, fondée en 1984, et spécialisée dans des domaines tels que :

- les commutateurs (switchs) et les routeurs
- les technologies sans fils
- la voix sur IP (VoIP)
- les solutions de sécurité
- les solutions de stockage en réseau
- ...



Mais Cisco c'est aussi une entreprise qui :

- Emploie plus de 72 000 personnes dans le monde (2017),
- A des bureaux dans 75 pays
- A réalisé 48 milliards \$ de revenus en 2017,
- Possède des « Cisco Networking Academies » dans 180 pays afin de former des professionnels à l'installation et au maintien de réseaux informatiques.

Introduction et généralités

Cisco Systems Formations

Track =	Enterprise	Service Provider	Data Center	Security	Collaboration	DevNet
Expert (CCIE)	300-401 ENCOR +1 Lab	300-501 SPCOR +1 Lab	300-601 DCCOR +1 Lab	300-701 SCOR +1 Lab	300-801 CLCOR +1 Lab	
Professional (CCNP)	300-401 ENCOR +1 exam	300-501 SPCOR +1 exam	300-601 DCCOR +1 exam	300-701 SCOR +1 exam	300-801 CLCOR +1 exam	300-901 DEVCOR +1 exam
Specialist	N'importe quel examen CORE					
Associate (CCNA)	CCNA 200-301					200-901 DEVASC

Cisco Systems

Pour pouvoir étudier et se former aux différentes certifications tel que la formation « CCNA », Cisco met à disposition des cours (dans différentes langues), mais également des exercices, des études de cas et des résolutions de problèmes.

En plus de cela, Cisco a développé un logiciel de simulation de réseaux, nommé « Cisco Packet Tracer ». Ce logiciel permet de créer et de simuler des réseaux à l'aide de différents équipements à configurer.

C'est ce logiciel que nous allons utiliser en partie durant nos séances de laboratoire.



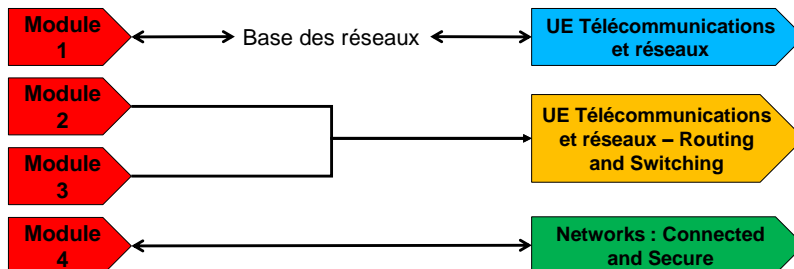
Cisco Systems formations

Certification Cisco CCNA (Cisco Certified Network Associate)
 → formation certificative décomposée en 4 modules (avec examen après chaque module) + examen final sur l'ensemble.



Cisco CCNA Routing & Switching

Département des Sciences et technologies



Introduction et généralités

Grille de cours : Bachelier bloc 1 (2023-2024)

Bloc 1 :

Unités d'enseignement du 1 ^{er} Quadrimestre	Unités d'enseignement du 2 ^e Quadrimestre
Electricité (6ects)  <ul style="list-style-type: none"> Electricité - théorie Electricité - travaux pratiques Etude de projet 	Développement web (4ects)  <ul style="list-style-type: none"> Développement web - théorie Développement web - travaux pratiques
Fonctionnement des systèmes (7ects)  <ul style="list-style-type: none"> Architecture des systèmes - théorie Internet of Everything Techniques numériques - travaux pratiques 	Mathématiques appliquées 2 (4ects)  <ul style="list-style-type: none"> Mathématique appliquée 2
Mathématiques appliquées 1 (1ects)  <ul style="list-style-type: none"> Mathématiques appliquées 1 	Programmation - Concepts avancés (8ects)  <ul style="list-style-type: none"> Algorithmique Programmation avancée - théorie Programmation avancée - travaux pratiques
Programmation - Concepts fondamentaux (7ects)  <ul style="list-style-type: none"> Bases de programmation - théorie Bases de Programmation - travaux pratiques 	Projet informatique (4ects)  <ul style="list-style-type: none"> Hackathon Méthodologie de projet
	Techniques d'interfaceage (6ects)  <ul style="list-style-type: none"> Eléments d'électronique pour l'interface informatique - théorie Eléments d'électronique pour l'interface informatique - travaux pratiques Projet d'interfaceage informatique
	Techniques numériques (2ects)  <ul style="list-style-type: none"> Techniques numériques - travaux pratiques avancés
Unités d'enseignement de l'année	
Télécommunications et réseaux (9ects)  <ul style="list-style-type: none"> Télécommunications et réseaux - théorie 1 Télécommunications et réseaux - théorie 2 Télécommunications et réseaux - Travaux pratiques 1 Télécommunications et réseaux - Travaux pratiques 2 	

Introduction et généralités

Organisation du cours en bloc 1

Activités d'Apprentissages

**Télécommunications
et réseaux théorie**

Activités d'Apprentissages

**Télécommunications
et réseaux TP**

→ Unité d'enseignement

Evaluation

Fiche ECTS disponible sur le site de la HEH

- Examen théorique (sur papier ou sur ordinateur) : 60%
- Examen de laboratoire : 40% (sur ordinateur)

L'étudiant doit absolument présenter chaque partie de l'examen sinon il se verra attribuer une absence pour l'unité d'enseignement.

Introduction et généralités

L'épreuve écrite peut être composée de questions à choix multiples ainsi que des questions ouvertes. Les questions de cette partie écrite peuvent porter à la fois sur des connaissances théoriques pures comme sur des questions de réflexion ou des petits exercices.

Il est également intéressant de noter que, parmi l'ensemble des questions, il est possible que certaines de celles-ci soient des questions à cotation négative (+1/-1).

L'épreuve de laboratoire porte sur des connaissances plus « pratiques » comme la configuration de matériel, la sécurisation et l'adressage IP. La durée de l'épreuve de laboratoire est de 1h30 maximum.

*Un team building est organisé pour les étudiants du bloc 1 et il est **obligatoire** !*

Introduction et généralités

Généralités : les unités de mesures

Faire une mesure, c'est comparer une grandeur physique (ou chimique) inconnue avec une grandeur de même nature prise comme référence à l'aide d'un instrument. Qui dit mesure, dit référentiel, donc **unité**.

Dans un passé (pas si lointain que ça), coexistaient de nombreuses unités qui n'avaient souvent que peu de rapports les unes avec les autres. Il a fallu attendre la révolution française pour qu'un premier système d'unités cohérent voit le jour : le système métrique.

Dans l'introduction de ce cours, nous allons donc commencer par (re)voir les principales unités qui pourraient vous servir dans un avenir proche car un bon petit rappel ne fait jamais de tort !

Généralités : les unités de mesures

En 1960, lors de la onzième Conférence générale des poids et mesures apparaît le **Système International d'unités**, noté couramment le « *SI* ».

Pour la longueur, l'unité utilisée est : le mètre (**m**)
 Pour la masse, l'unité utilisée est : le kilogramme (**kg**)
 Pour la intensité de courant, l'unité utilisée est : l'ampère (**A**)
 Pour le temps, l'unité utilisée est : la seconde (**s**)
 Pour la température, l'unité utilisée est : le kelvin (**K**)

En plus de ces unités de bases du SI, il existe ce qu'on appelle des unités dérivées de celles-ci. Elles peuvent avoir des noms spéciaux (hertz, pascal, becquerel, ...) mais peuvent toujours être exprimées à partir des unités de base.

Généralités : les unités de mesures

Dérivé de l'unité de longueur, nous avons :

Pour la longueur d'onde, l'unité utilisée est : le mètre (**m**)
 Pour l'angle plan, l'unité utilisée est : le radian (**rad**)
 Pour la surface, l'unité utilisée est : le mètre carré (**m²**)

Dérivé de l'unité de masse, nous retrouvons :

Pour la volume, l'unité utilisée est : le mètre cube (**m³**)
 Pour la force, l'unité utilisée est : le newton (**N**)
 Pour la pression, l'unité utilisée est : le pascal (**Pa**)
 Pour le couple, l'unité utilisée est : le newton mètre (**Nm**)

Dérivé de l'intensité de courant, nous retrouvons :

Pour la tension (ou différence de potentiel), l'unité utilisée est : le volt (**V**)
 Pour la résistance électrique, l'unité utilisée est : l'ohm (**Ω**)
 Pour la puissance, l'unité utilisée est : le watt (**W**)
 Pour l'énergie, l'unité utilisée est : le joule (**J**)

Généralités : les unités de mesures

Dérivé de l'unité de temps, nous avons :

Pour la vitesse de rotation, l'unité utilisée est : le tour par minute (**tr/min**)

Pour la fréquence, l'unité utilisée est : l'hertz (**Hz**)

D'autres unités sont également couramment utilisées, notamment pour la température !

Pour la température, on utilise le degré Celsius (**°C**) dans la plupart des pays.

Du côté des Etats-Unis et de certains pays du Commonwealth, on peut retrouver également les degrés Fahrenheit (**°F**).

Conversion Kelvin – degré Celsius et inversement :

$$T(^{\circ}\text{C}) = K - 273,15$$

$$K = T(^{\circ}\text{C}) + 273,15$$

Conversion degré Celsius – degré Fahrenheit et inversement :

$$T(^{\circ}\text{C}) = (T(^{\circ}\text{F}) - 32)/1,8$$

$$T(^{\circ}\text{F}) = T(^{\circ}\text{C}) \times 1,8 + 32$$

Généralités : les unités de mesures

Une autre unité de volume, qui n'est pas reprise comme unité de base dans le « *Système International* » est le litre (**l**).

Pour passer du m³ au litre, il suffit de se souvenir qu'1 l équivaut à 1 dm³ ou que 1000 l équivalent à 1 m³.

Remarque : ne pas confondre « *capacité* » et « *volume* »

Dans un registre plus concret, la *capacité* désigne la quantité théorique maximum de matière, d'information, ou autre contenu, qu'une entité peut contenir.

La *capacité* fait donc référence à un contenu potentiel, alors que le volume est une grandeur qui fait référence au contenant ou au contenu réel.

Autres unités intéressantes hors du « *SI* » :

Au niveau des unités de surface (ou d'aire), il existe également l'are (**a**).

Cette unité est plutôt utilisée lors de la mesure de terrain.

$$1 \text{ hectare (ha)} = 100 \text{ a} = 10\,000 \text{ m}^2$$

$$1 \text{ are (a)} = 100 \text{ m}^2$$

$$1 \text{ centiare (ca)} = 0,01 \text{ a} = 1 \text{ m}^2$$

Introduction et généralités

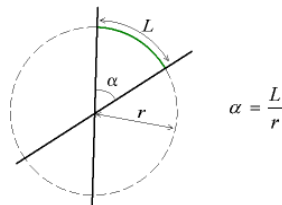
Généralités : les unités de mesures

Autres unités de mesures d'angles : le degré

Conversion degré-radian et inversement :

$$\theta_{\text{degré}} = \theta_{\text{radian}} \times (360/2\pi)$$

$$\theta_{\text{radian}} = \theta_{\text{degré}} \times (2\pi/360)$$



Et on a pas fini !

Que connaissez-vous comme autre unité de mesure pour la masse ?

La masse, qui s'utilise en kilogramme chez nous en Europe, peut être définie selon d'autres unités dans certains pays (comme les Etats-Unis ou au Royaume-Uni), on utilise la **livre (lb)**. Une livre valant très exactement 0,45359237 kg.

Cette livre peut se diviser en 16 onces. Chaque **once (oz)** vallant quant à elle 28,349 g.

Introduction et généralités

Généralités : les unités de mesures

Et pour la longueur ? Tout le monde utilise-t-il le mètre ?

Une autre unité de mesure pour la longueur, qui est notamment utilisée aux Etats-Unis ou au Royaume-Uni est le **pouce (po)**. En anglais, pouce se dit *inch* (*inches* au pluriel) et son abréviation est **in**, ou " (double prime). En plus du pouce, il existe également comme mesure le **pied (pi)**. En anglais, le pied se dit *foot* (*feet* au pluriel) et son abréviation est **ft**, ou ' (single prime).

Un pouce équivaut à 25,4 mm. Il y a douze pouces dans un pied.

Un pied vaut donc : $12 \times 2,54 = 304,8$ mm exactement.

Par exemple : 10' 6¼" signifie 10 pieds et 6,75 pouces, ce qui fait 126,75 pouces ou encore 3 219,45 mm.

Généralités : les unités de mesures

Quelqu'un ici, connaît-il la circonférence orbitale de la planète Neptune ?

Réponse :

Sa circonférence orbitale vaut 28295449561000 m

Quelqu'un ici, connaît-il maintenant la masse de la planète Neptune ?

Réponse :

Sa masse vaut 102430000000000000000000 kg !!!!!

Généralités : les préfixes

Chaque grandeur peut avoir à couvrir une vaste étendue de valeurs.

Pour éviter d'avoir à utiliser des facteurs multiplicatifs ou des valeurs avec un grand nombre de zéros, on a recourt à des préfixes.

Ces derniers vont permettre de couvrir une gamme allant de 10^{24} à 10^{-24} fois l'unité.

Généralités : les préfixes

Facteur	Préfixe	Symbole
10^{24}	yotta	Y
10^{21}	zetta	Z
10^{18}	exa	E
10^{15}	péta	P
10^{12}	téra	T
10^9	giga	G
10^6	méga	M
10^3	kilo	k
10^2	hecto	h
10^1	déca	da

Généralités : les préfixes

Facteur	Préfixe	Symbole
10^{-1}	déci	d
10^{-2}	centi	c
10^{-3}	milli	m
10^{-6}	micro	μ
10^{-9}	nano	n
10^{-12}	pico	p
10^{-15}	femto	f
10^{-18}	atto	a
10^{-21}	zepto	z
10^{-24}	yocto	y

Généralités : les préfixes et les notations

Si l'on revient donc à ma question concernant la circonférence orbitale de Neptune, et admettons que vous connaissez la réponse, vous m'auriez alors sans doute répondu une de ces trois réponses ci :

- Soit la circonférence orbitale vaut $2,8295449561 \times 10^{13}$ m \longrightarrow notation scientifique
 - Soit la circonférence orbitale vaut $28,295449561 \times 10^{12}$ m
 - Soit la circonférence orbitale vaut $28,295449561 \times 10^9$ km
- $\} \longrightarrow$ notation ingénieur

La **notation scientifique** est une représentation d'un nombre décimal. Elle consiste à exprimer le nombre sous la forme , $a \times 10^n$ avec a étant un nombre décimal appartenant à l'intervalle $[-9,9]$ et n est un entier.

La **notation ingénieur** est une notation scientifique dans laquelle l'exposant n ne peut qu'être un multiple de 3. La notation ingénieur est largement utilisée par les scientifiques en raison de l'utilisation du multiple de 3 obligatoire pour l'exposant qui va correspondre à des mesures scientifiques communément utilisées.

Généralités : les unités en informatique

En informatique, l'unité de base est le **bit (bit)**, venant de « *Binary digiT* ». C'est l'unité élémentaire d'information qui ne peut prendre qu'une des deux valeurs suivantes : 0 ou 1.

En général, les bits sont groupés par huit pour former un **octet (o)**, aussi appelé un « *byte* » (**B**). Il peut prendre 2^8 , soit 256, valeurs possibles.

1 Ko = 1000 octets

1 Mo = 1000 Ko

1 Go = 1000 Mo

1 To = 1000 Go

Au niveau des moniteurs d'affichage, vous avez déjà sûrement entendu parler d'une unité bien connue aussi, le **pixel (px)**. Pixel provient de l'anglais « *picture element* » et c'est l'unité minimale adressable par le contrôleur vidéo (appelé vulgairement la carte graphique). C'est aussi l'unité utilisée pour spécifier les définitions d'affichage.

La **définition d'écran** est le nombre de points ou pixels que peut afficher une carte graphique sur un écran. La définition est le produit du nombre de points selon l'horizontale par le nombre de points selon la verticale de l'affichage.

Toujours en rapport avec les écrans, une autre unité qui ne doit pas vous être inconnue et qui est (quasiment) toujours utilisée sous son nom anglais est le **frames per second (fps)**, qui correspond au nombre d'images affichées par seconde par votre moniteur.

Introduction et généralités

Au niveau des unités de débits en informatique, les mesures s'effectuent généralement en **bits par seconde (bit/s)**, notées parfois **bps** en anglais. Ces unités de mesure servent à mesurer un débit (maximal) d'information entre deux points d'un réseau informatique.

Remarque :

Dans certains cas, comme par exemple pour certains composants informatiques, il est possible d'observer d'autres unités de mesures dérivées du bit/s.

C'est le cas si vous analysez les débits de transfert en écriture et en lecture des cartes mémoires.

En général, le constructeur vous donnera alors des valeurs exprimées en Mo/s.



Introduction et généralités

Généralités : rôles de l'administrateur

L'administration d'un système d'exploitation et d'un réseau sont des tâches complexes. Dès lors, il est indispensable que les administrateurs respectent certaines règles et travaillent avec discipline et méthodologie.

Pouvez-vous me citer des tâches dont est responsable l'administrateur ?

L'administrateur doit notamment s'occuper de :

- La gestion des besoins, du budget et des priorités.
- La gestion des ordinateurs et des périphériques.
- La gestion des performances des systèmes.
- La gestion des utilisateurs.
- La gestion des fichiers et des disques.
- La gestion des services.
- La gestion des problèmes.
- La gestion des sauvegardes et du stockage des données.
- La gestion du réseau.
- La gestion de la sécurité.

▪ La gestion des besoins, du budget et des priorités

Les entreprises ont des besoins informatiques spécifiques qui sont fonction de leur domaine d'activité. Certaines de ces fonctions peuvent éventuellement être externalisée (serveur Web, serveur mail,...) mais ce n'est pas possible pour les applications stratégiques ni les applications « métiers ».

Les divers éléments du réseau (ordinateurs, serveurs, câbles, switches, ...) doivent donc permettre le fonctionnement de ces applications de manière optimale mais aussi permettre l'installation d'autres applications en fonction des évolutions.

L'administrateur doit donc établir un cahier des charges dans lequel sont renseignés les besoins en services, applications et matériels. Les budgets étant toujours insuffisants, il faut déterminer, au départ du cahier des charges, quels sont les achats prioritaires parmi les nombreux besoins : le système de câblage, les éléments d'interconnexions, les serveurs, les systèmes de sauvegardes, les logiciels métiers, les logiciels de supervision,...

Une fois les priorités établies, l'administrateur doit rédiger les appels d'offres et comparer les devis afin de réaliser un choix judicieux : la solution est-elle sécurisée ? Evolutive ? Tolérante aux pannes ?

▪ La gestion des ordinateurs et des périphériques

L'administrateur doit pouvoir gérer les machines (et leurs composants : disque dur, carte graphique,...) ainsi que leurs périphériques (scanner, imprimante, clavier, ...)

- Installer les systèmes d'exploitation, paramétrer le démarrage et l'arrêt.
- Gérer les disques (initialisation, partitionnement, remplacement,...).
- Ajouter ou enlever un périphérique.
- Planifier le vieillissement du matériel et son remplacement.
- Ajouter (ou supprimer) un pilote de périphérique ("driver") à un OS.

▪ La gestion des performances des systèmes

L'administrateur doit surveiller (voire améliorer) les performances des serveurs et des stations de travail, dont notamment :

- Paramétrer et répartir les ressources de manière à garder un système parfaitement fonctionnel.
- Surveiller les ressources (processeur, mémoire, bande passante, entrées/sorties et espace disque) afin de prévoir et donc réagir avant un éventuel manque de ressources.

▪ La gestion des utilisateurs

L'administrateur doit gérer les comptes des utilisateurs. Son rôle sera donc :

- De créer, modifier et supprimer les comptes utilisateurs sur les systèmes dont il a la charge.
- D'être capable de modifier l'environnement de travail des utilisateurs, changer leur mot de passe, gérer leurs droits d'accès,...
- D'informer et "éduquer" les utilisateurs pour qu'ils utilisent correctement les outils informatiques mis à leur disposition.

▪ La gestion des fichiers et des disques

L'administrateur doit gérer les fichiers et systèmes de fichiers présents sur les disques, ce qui comprend :

- Mettre en place et gérer les systèmes de fichiers (création, configuration des permissions d'accès, cryptage,...).
- Veiller à l'intégrité des systèmes de fichiers et donc des données.
Des données sont intègres lorsqu'elles n'ont subi aucune altération (volontaire ou involontaire) et sont toujours utilisable.
- Gérer l'arborescence des fichiers (organisation et contrôle des accès).
- Surveiller l'espace disque : contrôler le taux d'occupation des disques, mettre en place des quotas.

▪ La gestion des services

L'administrateur doit savoir configurer et utiliser les services adéquats pour répondre aux besoins de l'entreprise tels que les services de base fournis par le système Linux (gestion des tâches, service d'impression, ...) ou d'autres services spécifiques.

▪ La gestion des problèmes

L'administrateur doit connaître ses machines (partitionnement effectués, services actifs, ...) et son réseau (architectures, protocoles, ...) de manière à pouvoir intervenir rapidement et efficacement en cas de problème.

Cela nécessite la mise en place d'outils aidant au diagnostic des problèmes et générant des alarmes face aux pannes qui peuvent survenir.

Il peut être utile de préparer des fiches préformatées que les utilisateurs peuvent compléter, à l'attention du service informatique, avec le détail des problèmes qu'ils rencontrent.

▪ La gestion des sauvegardes et du stockage des données

L'organisation des sauvegardes est très importante, c'est un point crucial pour l'administrateur. Celui-ci doit absolument être capable de récupérer toutes les données importantes dans le délai le plus bref possible.

▪ La gestion du réseau

L'administrateur doit mettre en place des outils de surveillance afin de vérifier que les performances du réseau ne se dégradent pas, notamment suite à l'utilisation de nouvelles applications ou à des modifications de configuration.

En plus l'administrateur doit être capable de choisir, de mettre en place et de modifier l'architecture du réseau. Il doit donc :

- choisir la topologie du réseau.
- choisir les protocoles réseau.
- mettre en place la redondance.
- organiser le routage et le filtrage.

Introduction et généralités

Bien entendu, l'administrateur doit être capable de gérer les différents éléments constituant le réseau :

- Choisir, installer et paramétrer les éléments adéquats (stations de travail, switches, routeurs, points d'accès, antennes, câbles, ...).
- Paramétrer le démarrage et l'arrêt de tous les systèmes.
- Automatiser le processus de démarrage des nouveaux services et produits sur les machines clientes et serveurs.

Introduction et généralités

▪ La gestion de la sécurité

L'administrateur doit veiller à la sécurité, en prenant en compte trois axes :

- **Assurer la confidentialité** : garantir la confidentialité des données consiste à limiter l'accès aux données aux destinataires autorisés (individus, processus ou périphériques).
- **Garantir l'intégrité des données** : garantir l'intégrité des données consiste à veiller à ce que les informations ne soient pas modifiées lors de leur transmission de leur point d'origine à leur destination.
- **Assurer la disponibilité** : garantir la disponibilité consiste à veiller à ce que les utilisateurs autorisés puissent accéder en temps voulu et de façon fiable aux services de données.

Que pouvez-vous me citer comme types de menaces liées à la sécurité ?

- **Virus, vers, et chevaux de Troie** – logiciels malveillants et code arbitraire s'exécutant sur un périphérique utilisateur.
- **Logiciels espions et publicitaires** – logiciels installés sur un périphérique utilisateur qui collectent secrètement des informations sur l'utilisateur.
- **Attaques zero-day, également appelées attaques zero-hour** – attaques qui se produisent le jour où une vulnérabilité est détectée.
- **Attaques de pirates** – attaques lancées sur des périphériques utilisateur ou des ressources réseau par une personne qui possède de solides connaissances en informatique.
- **Attaques par déni de service** – attaques conçues pour ralentir ou bloquer les applications et les processus d'un périphérique réseau.
- **Interception et vol de données** – attaques visant à acquérir des informations confidentielles à partir du réseau d'une entreprise.
- **Usurpation d'identité** - attaques visant à recueillir les informations de connexion d'un utilisateur afin d'accéder à des données privées.

Quels sont à votre avis, pour une entreprise, les risques liés à un manque de sécurité ?

- des pannes du réseau qui empêchent les communications et les transactions, entraînant donc une perte d'activité (et donc une perte d'argent !).
 - le vol d'éléments de propriété intellectuelle (idées de recherche, brevets ou dessins de conception) ensuite utilisés par un concurrent .
 - la divulgation ou la compromission de données personnelles ou privées sans le consentement des utilisateurs.
 - la perte de données importantes, très difficiles à remplacer ou irremplaçables.
 - une mauvaise utilisation ou une perte de fonds personnels ou de l'entreprise.
- Pour éviter tout cela, deux aspects de la sécurité réseau doivent être pris en compte : la sécurité de l'infrastructure réseau et la protection des données.
- ✓ **Sécuriser l'infrastructure réseau** implique de sécuriser matériellement les périphériques qui assurent la connectivité réseau et d'empêcher tout accès non autorisé aux logiciels de gestion qu'ils hébergent.

Quels moyens mettriez-vous en place pour assurer la sécurité de l'infrastructure réseau ?

- toute salle contenant du matériel informatique doit être fermée à clé afin de limiter l'accès au matériel physique à un minimum de personnes et avoir un contrôle d'accès (via des badges par exemple) pour garder une trace des allées et venues.
- mettre en place un pare-feu pour bloquer les accès non autorisés au réseau.
- toute armoire (contenant des commutateurs, des routeurs ou des serveurs) doit également être fermée à clé. Ainsi dans le cas où une personne mal intentionnée réussirait à entrer dans la salle, il n'a toujours pas un accès physique au matériel.
- mettre en place des systèmes de vidéosurveillance.
- pour les accès à distance sur le matériel, mettre en place une bannière afin que toute personne qui tente de se connecter au matériel via le réseau (et qui n'y est pas autorisée) sache qu'elle risque des poursuites judiciaires et utiliser des réseaux privés virtuels (VPN) pour les accès à distance.
- mettre en place des mots de passes cryptés sur tous les périphériques.
- mettre en place des logs afin de savoir exactement quel utilisateur s'est connecté à quel moment sur le matériel.
- mettre en place une politique de sécurité et sensibiliser les utilisateurs afin qu'ils se rendent compte des risques engendrés par une faille dans cette politique de sécurité.

✓ **Sécuriser les données** consiste à protéger les informations contenues dans les paquets transmis sur le réseau, ainsi que les informations stockées sur des périphériques reliés au réseau.

Concernant la sécurité des données, quels moyens mettriez-vous en place ?

- mettre en place un système de backup des données indispensables afin d'avoir une sauvegarde de celles-ci en cas de problèmes. Au niveau des backups, plusieurs politiques sont utilisées dans le monde de l'entreprise. Ceux-ci peuvent être effectués de manière automatique et journalière pour les données très sensibles et peut être de manière hebdomadaire pour d'autres données. Au niveau du stockage de ceux-ci, certaines entreprises les stockent en interne, dans une pièce sécurisée, spécialement prévue à cet effet. D'autres les stockent à l'extérieur de l'entreprise et parfois des entreprises optent pour une sauvegarde interne et externe à la fois.
- mettre en place des logiciels antivirus ainsi que des logiciels anti-espion.
- mettre en place de la redondance (comme dans le cas de la tolérance aux pannes) permet d'éviter toute perte de données qui seraient en transit sur le réseau à ce moment là.

Généralités : méthodologie de l'administrateur

Nous venons de voir que la fonction d'administrateur système/réseau est à la fois complexe mais aussi variée. Dès lors, il est primordial que l'administrateur informatique travaille de manière rigoureuse et méthodique.

Voici donc quelques éléments de méthodologie lui permettant d'améliorer l'efficacité et la qualité de son travail.

▪ La documentation

L'administrateur doit suffisamment documenter ses actions car le fait de les consigner lui permet de connaître exactement l'état de ses machines et de son réseau. Cela facilitera la réalisation de son travail journalier, mais aussi ses différents dépannages. Il pourra, par exemple, faire le lien entre le jour où il a opéré une modification et le jour où tel service ne fonctionne plus correctement.

D'autre part, l'administrateur ne travaille pas toujours seul et doit donc laisser une trace de ses actes aux autres administrateurs afin que ceux-ci trouvent rapidement les informations dont ils ont besoins.

Ainsi, l'administrateur doit tenir un journal de bord. Il s'agit d'un document qui doit être daté et dans lequel sont consignées les opérations importantes d'exploitation telles que :

- l'installation du système (partitionnement, systèmes de fichiers,...)
- la configuration réseau du système
- l'ajout de périphériques
- l'installation de nouveaux logiciels ou services
- la mise à jour du système
- la sauvegarde complète du système et des données
- les événements anormaux (lenteur inhabituelle du système, messages d'erreurs, ...)
- les fichiers de configuration
- il peut également être utile de consigner les fichiers logs

L'administrateur doit aussi veiller à ce qu'une copie de la documentation du matériel (manuel d'installation, guide de l'utilisateur,...) soit accessible à proximité de celui-ci dans le réseau.

Enfin, il faut réaliser un repérage adéquat sur les appareils (étiquette, code couleur des câbles,...) afin de les repérer et les identifier facilement.

De manière générale il faut aussi documenter les programmes, scripts et fichiers de configuration en y insérant des lignes de commentaires.

Introduction et généralités

▪ Sauvegarder

Le fait de savoir qu'il faut sauvegarder ne suffit pas !!!

La gestion des sauvegardes comprend un ensemble d'éléments et de choix parmi lesquels on peut citer le choix des types de sauvegarde, du logiciel à utiliser, la fréquence des sauvegardes, le type de support de stockage, la liste des personnes chargées de réaliser les sauvegardes,...

Pour ne rien laisser au hasard, il faut mettre en place un plan de sauvegarde et même mieux, un plan de recouvrement après sinistre.

Un plan de recouvrement est un plan qui permet de traiter une crise (l'arrêt d'une production, ...) de manière organisée et ainsi, d'assurer le maintien des activités critiques de l'entreprise ou, tout du moins, de les reprendre le plus rapidement possible.

Une sauvegarde qui n'a pas été testée n'a que peu de valeur !

Dès lors, l'idéal est de disposer d'un système de test (identique au système en production) via lequel il est possible de tester les restaurations des sauvegardes effectuées. A défaut d'une machine spécifique dédiée aux tests, on se tournera vers un système de virtualisation.

Introduction et généralités

▪ Automatiser

L'automatisation des différentes tâches d'administration (à l'aide de scripts, par exemple) permet de gagner un temps précieux en « laissant » la machine travailler pour l'homme. En pratique, lorsqu'une procédure doit être utilisée plus d'une fois, il est souvent intéressant de l'automatiser.

Exemples de tâches que l'on peut automatiser :

- l'installation de systèmes d'exploitation
- l'installation de mises à jour
- les sauvegardes

De plus, l'automatisation réduit le risque d'erreurs encouru lors de la réalisation manuelle des tâches (faute de "frappe", oubli, ...)

Introduction et généralités

▪ Agir de manière réversible

Chaque fois que l'administrateur effectue une tâche d'administration (installation de périphérique, de logiciels, de drivers, modifications de configurations,...), un problème peut survenir.

Or, quel que soit le problème, l'activité doit continuer ou, au pire, reprendre dans les plus brefs délais.

Ainsi, il faudra, à chaque fois que cela est possible, agir de manière réversible afin de savoir revenir rapidement à un système fonctionnel. Dans ce contexte, on se rend compte de l'importance de la journalisation de ses opérations, ainsi que des sauvegardes.

▪ Etre proactif

L'administrateur doit agir de manière proactive, c'est-à-dire qu'il doit constamment anticiper les problèmes qui ne manqueront pas de survenir. Un exemple simple consiste à installer un anti-virus sur un ordinateur. Cette action permet d'éviter que le système ne soit infecté par de nombreux virus qui risquent de le rendre non opérationnel.

Autres exemples : Si l'administrateur tombe malade, qui peut le remplacer ? Si le switch qui interconnecte tous les utilisateurs tombe en panne, dispose-t-on d'un appareil de rechange ? Si l'ordinateur d'un directeur tombe en panne, a-t-on un ordinateur de rechange prêt directement ?

Introduction et généralités

▪ Autres qualités requises de l'administrateur

➤ **Savoir communiquer**

La communication est essentielle car un informaticien travaille rarement seul, il est en contact avec tous les acteurs de l'entreprise.

Exemples :

- il doit se montrer persuasif afin de disposer des budgets nécessaires à sa tâche.
- il doit discuter avec les fournisseurs de matériel, les prestataires de services,...
- il doit discuter avec les utilisateurs finaux afin de connaître leurs besoins.
- il doit comprendre les problèmes que leurs soumettent les utilisateurs.
- il doit former les utilisateurs à l'utilisation des outils informatiques et les informer des contraintes liées à ces outils.

➤ **Avoir une bonne connaissance du marché**

L'administrateur doit se tenir au courant de l'évolution du marché car celui-ci peut influencer sur les choix de gestion et d'évolution d'un parc informatique. Il est difficile de réaliser des choix judicieux ou mettre en place des solutions si l'administrateur n'est pas au courant que ces solutions existent.

▪ Autres qualités requises de l'administrateur

➤ **Connaître ses limites**

Pour de petites entreprises, il est possible que l'administrateur s'occupe de « tout ».

Cependant, lorsque le système devient plus complexe ou plus important, il sera nécessaire de répartir l'administration entre plusieurs personnes.

Il peut s'agir d'une aide ponctuelle de quelques employés, ou bien d'une charge de travail nécessitant plusieurs administrateurs.

Dans tous les cas, il faut être conscient de ses limites. D'une part, personne ne peut tout connaître sur tout, d'autre part, personne ne peut réaliser un travail de quatre heures en une heure.

Les bases

Parmi toutes les bases de calcul existantes, comme en informatique chaque signal ne possède que deux états possibles (0 et 1), les bases que nous allons être amené à utiliser pour coder des signaux seront des multiples de cette base binaire :

- **la base 2**, ou base binaire. Elle est la base de la logique booléenne ou algèbre de Boole.

→ valeurs possibles : 0 ou 1

- **la base 8**, ou base octale. Utilisée il y a un certain temps en informatique lorsque les machines utilisées étaient peu gourmandes en puissance de bus.

→ valeurs possibles : 0, 1, 2, 3, 4, 5, 6 ou 7

- **la base 10**, ou base décimale. Elle est considérée comme la base universelle.

→ valeurs possibles : 0, 1, 2, 3, 4, 5, 6, 7, 8 ou 9

- **la base 16**, ou base hexadécimale. Cette base est très utilisée dans le monde de la micro-informatique et des automates. Elle permet de coder un mot (16 bits) sur 4 variables hexadécimales. Cette base fait intervenir tous les chiffres de la base 10 complétée par les 6 premières lettres de l'alphabet.

→ valeurs possibles : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E ou F

Les conversions de bases

→ Un nombre peut toujours être écrit ou représenté de manières différentes suivant la base dans laquelle nous allons travailler.

Exemple :

le nombre 413_{10} en décimal s'écrit également 110011101_2 en binaire, 635_8 en octal ou encore $19D_{16}$ en hexadécimal.

Comment passer d'une base à l'autre ?

Comment connaître la valeur d'un nombre écrit en base X dans une autre base Y ?

Les conversions de bases

Conversion base 10 en base 2

Un nombre décimal peut facilement être converti en nombre binaire si l'on connaît un tableau assez simple qui est celui des valeurs de 2^x

2^x	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
valeur	1024	512	256	128	64	32	16	8	4	2	1

Reprenons notre nombre 413_{10} en décimal, **quel est sa valeur en binaire ?**

Il suffit juste de regarder, par rapport au tableau ci-dessus, et pour chaque élément en partant de la gauche s'il apparaît au moins une fois dans le nombre.

Deux possibilités s'offrent à vous :

- Soit votre nombre à convertir (413_{10}) est inférieur à la valeur décimale représentant le 2^x
 → on note un « 0 » en dessous du tableau.
- Soit il est supérieur à la valeur décimale représentant le 2^x , alors on notera un « 1 » en dessous du tableau et on soustraira cette valeur à notre nombre à convertir, puis on passera à la case suivante.

Les conversions de bases**Conversion base 10 en base 2**

Si on applique ce que l'on vient de voir, cela nous donne ceci :

2^x	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Base 10	1024	512	256	128	64	32	16	8	4	2	1
Base 2	0	0	1	1	0	0	1	1	1	0	1

réponse : $413_d = 110011101_b$

Comment est-on sûr que c'est bien cette valeur là ?

En vérifiant bien entendu !

$$1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 + 1 \times 2^4 + 0 \times 2^5 + 0 \times 2^6 + 1 \times 2^7 + 1 \times 2^8 = ?$$

$$1 + 0 + 4 + 8 + 16 + 0 + 0 + 128 + 256 = 413$$

Les conversions de bases**Conversion base 2 en base 10**

Et dans l'autre sens c'est encore plus simple !

Si l'on vous demande que vaut 1010101_b en nombre décimal ?

2^x	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Base 2	0	0	0	0	1	0	1	0	1	0	1
Base 10	1024	512	256	128	64	32	16	8	4	2	1

Soit vous refaites votre tableau comme précédemment, soit vous faites directement l'addition :

$$1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 0 \times 2^3 + 1 \times 2^4 + 0 \times 2^5 + 1 \times 2^6 = ?$$

$$1 + 0 + 4 + 0 + 16 + 0 + 64 = 85_d$$

Les conversions de bases

Conversion base 2 en base 8

Dans ce cas ci on va fonctionner de manière un peu différente.

Il faut vous souvenir d'une chose importante, une base binaire utilise 1 bit pour stocker une valeur puisqu'elle ne possède que deux types de valeurs : **0** ou **1**.

En réfléchissant comme cela, et sachant qu'une base octale peut prendre 8 valeurs différentes (0, 1, 2, 3, 4, 5, 6, 7), combien de bits faudra-t-il utiliser pour stocker ces possibilités ?

→ Il faudra un groupe de **3 bits**.

Dès lors si je vous demande de convertir 1010101_b en nombre octal ?

Il suffira, en partant de la droite, de regrouper les bits par 3, et de regarder leur valeur identiquement comme on l'a fait juste avant !

$$\begin{aligned}
 1010101_b &= (00)1 \ 010 \ 101_b = 125_o \\
 &\quad \rightarrow 101_b = 1x2^2 + 0x2^1 + 1x2^0 \\
 &\quad \rightarrow 010_b = 0x2^2 + 1x2^1 + 0x2^0 \\
 &\quad \rightarrow 001_b = 0x2^2 + 0x2^1 + 1x2^0
 \end{aligned}$$

Les conversions de bases

Conversion base 2 en base 16

Maintenant que l'on a vu la conversion binaire → octale, vous allez voir que la conversion binaire → hexadécimale est assez simple puisqu'il s'agit exactement du même raisonnement !

En réfléchissant comme cela, et sachant qu'une base hexadécimale peut prendre 16 valeurs différentes (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F), combien de bits faudra-t-il utiliser pour stocker ces possibilités ?

→ Il faudra un groupe de **4 bits**.

Dès lors si je vous demande de convertir 11010101_b en nombre hexadécimal ?

Il suffira, en partant de la droite, de regrouper les bits par 4, et de regarder leur valeur identiquement comme on l'a fait juste avant !

$$\begin{aligned}
 11010101_b &= 1101 \ 0101_b = D5_h \\
 &\quad \rightarrow 0101_b = 0x2^3 + 1x2^2 + 0x2^1 + 1x2^0 = 5_h \\
 &\quad \rightarrow 1101_b = 1x2^3 + 1x2^2 + 0x2^1 + 1x2^0 = D_h
 \end{aligned}$$

Les conversions de bases

Conversion base 8 en base 2

Dans le sens inverse c'est assez simple : il suffit, lorsqu'on vous donne un nombre octal, de prendre un par un, en partant par la droite toujours, les chiffres en octal et de convertir ceux-ci en binaire sur 3 bits (avec le tableau vu tout au début).

Exemple : $63_o = 110011_b$

$$\begin{aligned} &\rightarrow 3_o = 0x2^2 + 1x2^1 + 1x2^0 \\ &\rightarrow 6_o = 1x2^2 + 1x2^1 + 0x2^0 \end{aligned}$$

Conversion base 16 en base 2

Dans le sens inverse c'est assez simple : il suffit, lorsqu'on vous donne un nombre octal, de prendre un par un, en partant par la droite toujours, les chiffres en octal et de convertir ceux-ci en binaire mais cette fois-ci sur 4 bits.

Exemple : $63_h = 01100011_b$

$$\begin{aligned} &\rightarrow 3_h = 0x2^3 + 0x2^2 + 1x2^1 + 1x2^0 \\ &\rightarrow 6_h = 0x2^3 + 1x2^2 + 1x2^1 + 0x2^0 \end{aligned}$$

Les conversions de bases

Conversion base 10 en base 8 (ou en base 16) et inversement

Pour convertir un nombre donné en base décimale en une base octale (ou hexadécimale), aux vues de ce que l'on vient de voir précédemment, le plus simple est de repasser tout d'abord par la base binaire (qui est la plus simple) et puis d'ensuite reconvertir, depuis cette base binaire, en une base octale (ou hexadécimale).

Principe : base décimale \rightarrow base binaire \rightarrow base octale (ou hexadécimale)

Exemples :

$$413_d = 110011101_b = 635_o \text{ (ou } 19D_h)$$

$$F5_h = 11110101_b = 128 + 64 + 32 + 16 + 4 + 1 = 245_d$$

$$44_o = 100100_b = 24_h$$

Un conseil : pour toutes les conversions de bases, passez automatiquement par la base binaire pour éviter de vous tromper et vérifiez à chaque fois vos calculs !!!

Les conversions de bases

Exercices :

1) Que valent ces chiffres hexadécimaux en binaire :

29_h $E5_h$ AB_h $C1_h$ $F1_h$ 40_h

2) Coder ces chiffres en hexadécimal :

10101101_b 01110010_b 10110011_b 01101100_b 10001001_b

3) Coder ces chiffres décimaux en base octale :

23_d 152_d 191_d 64_d 490_d

4) Faites la conversion octale en hexadécimale :

113_o 71_o 256_o 22_o 365_o

5) Faire la conversion binaire/décimal/octal de :

$1F_h$ 20_h 57_h $A5_h$ $C7_h$ FF_h $3A_h$

Les conversions de bases

Exercices (suite) :

binaire	octale	décimale	hexadécimale
01101011_b			
	73_o		
			$B2C_h$
		2561_d	
11010110_b			
	306_o		
			$FADE_h$
		432_d	
			$2B3_h$
	610_o		

La communication et les réseaux d'aujourd'hui

Depuis toujours, le besoin de communiquer a toujours été d'une importance capitale pour l'homme. D'ailleurs, les méthodes que nous utilisons pour communiquer changent et évoluent constamment.

Si par le passé les interactions étaient limitées au face à face, de nos jours les innovations technologiques ont considérablement augmenté la portée de nos communications.

Des peintures rupestres à la radio et la télévision, en passant par la presse écrite, chaque innovation a développé et amélioré nos possibilités de connexion et de communication avec les autres.

La création et l'interconnexion de réseaux de données fiables ont eu un impact important sur la communication et ces réseaux sont aujourd'hui une nouvelle plate-forme sur laquelle les communications modernes s'effectuent.

Aujourd'hui, grâce à ces réseaux de données fiables, nous sommes plus connectés que jamais ! Les événements et les découvertes font le tour du monde en quelques secondes seulement.

Grâce aux réseaux et plus particulièrement à l'Internet, nous pouvons faire un tas de choses qu'il nous aurait été impossible de faire si ces avancées n'existaient pas.

Pouvez-vous me citer des exemples d'aide que les ressources disponibles sur Internet vous apporte dans votre quotidien ?

- Jouer
- acheter des objets
- parler
- apprendre
- ...

Introduction et généralités

La communication et les réseaux d'aujourd'hui

Les réseaux et Internet ont fait évoluer notre quotidien : notre façon d'apprendre, notre façon de communiquer, notre façon de travailler et même notre façon de nous divertir.

Auparavant les méthodes d'apprentissage étaient limitées à deux sources principales de connaissances :

- les livres, les manuels,...
- les instructeurs, les enseignants,...

Aujourd'hui, Internet nous permet d'améliorer notre façon d'apprendre et d'enrichir l'expérience didactique aux étudiants : classes virtuelles, forum, e-learning, VoD,...



Introduction et généralités

Internet a également révolutionner nos moyens de communications, tant au niveau privé que professionnel, créant de nouvelles formes de communications ou de nouveaux moyens d'échanger des informations pouvant être consultées par un grand nombre de personnes.

Exemples :

• **Messagerie instantanée/messages texte** – la messagerie instantanée et les messages texte facilitent la communication en temps réel entre deux (ou plusieurs) personnes. De nombreuses applications de messagerie instantanée et de messages texte intègrent des fonctionnalités telles que le transfert de fichiers, la communication vocale et vidéo.



Introduction et généralités

• **Réseaux sociaux** – où les personnes et communautés créent et partagent du contenu avec leurs amis, leur famille, leurs homologues et parfois même des inconnus provenant du monde entier.



• **Outils collaboratifs** – les outils de collaboration donnent aux utilisateurs la possibilité de travailler ensemble sur des documents partagés. Sans contraintes d'emplacement ou de fuseau horaire, les personnes connectées à un système partagé peuvent communiquer entre eux, souvent grâce à la vidéo interactive en temps réel. Sur tout le réseau, elles peuvent partager du texte et des images, puis modifier les documents ensemble.



Dropbox



Microsoft Teams



Introduction et généralités

• **Blogs** – les blogs sont des pages Web qui sont faciles à mettre à jour et à modifier. Contrairement aux sites Web commerciaux qui sont créés par des experts en communication professionnelle, les blogs permettent à n'importe qui de partager des pensées avec un public international sans avoir besoin de posséder des connaissances techniques en matière de conception Web. Il existe des blogs sur pratiquement tous les sujets possibles et imaginables et des communautés se forment souvent autour d'auteurs de blogs populaires.



progresser en informatique

<https://progresser-en-informatique.com/blog/>

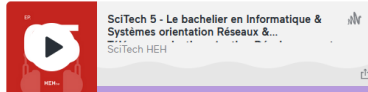
• **Wikis** – les wikis sont des pages Web que des groupes de personnes peuvent modifier et consulter ensemble. Alors qu'un blog est généralement l'œuvre d'une seule personne et s'apparente à un journal, un wiki est une création collective. De ce fait, il peut être soumis à des relectures et modifications plus poussées. Comme les blogs, les wikis peuvent être créés en plusieurs phases, par n'importe qui, sans le parrainage d'une grande entreprise commerciale.



WIKIPÉDIA
L'encyclopédie libre



- **Podcasts** - les podcasts sont des supports audio qui permettaient initialement d'enregistrer des données audio et de les convertir. Ces fichiers audio sont placés sur un site Web (ou sur un blog ou un wiki) sur lequel des tiers peuvent les écouter ou les télécharger pour les lire sur leurs ordinateurs de bureau, ordinateurs portables et autres appareils mobiles.



- **Partage de fichiers en peer-to-peer (P2P)** – le partage en peer-to-peer permet de partager des fichiers sans avoir à les stocker et à les télécharger depuis un serveur central. L'utilisateur se connecte au réseau P2P en installant un logiciel P2P. Cela lui permet de localiser et de partager des fichiers avec d'autres utilisateurs sur le réseau P2P. La numérisation généralisée des fichiers multimédias, tels que la musique et les fichiers vidéo, a amélioré l'intérêt pour le partage de fichiers en peer-to-peer.



La communication et les réseaux d'aujourd'hui

Les réseaux d'aujourd'hui ont également permis à de nombreuses entreprises de changer leur façon de travailler.

Au départ, les entreprises exploitaient les réseaux de données pour enregistrer et gérer en interne des informations financières, des renseignements sur les clients et des systèmes de paie des employés,...

A présent, ces réseaux d'entreprise ont évolué pour permettre la transmission de nombreux types de service d'informations, parmi lesquels les e-mails, la vidéo, les messageries et la téléphonie (VoIP), et ce de façon sûre et productive.

Ces entreprises exploitent les réseaux en tant que moyen efficace et rentable de former les employés, grâce par exemple à des formations en ligne. Celles-ci permettent de réduire des déplacements coûteux en termes de temps et d'argent tout en s'assurant que tous les employés sont correctement formés pour accomplir leurs tâches, et ce de façon sûre et productive.



Introduction et généralités

Finalement, la dernière chose (et non la moindre) qu'a modifié l'évolution des réseaux est la manière dont nous nous divertissons aujourd'hui.

L'utilisation généralisée d'Internet par l'industrie du loisir et des voyages nous offre le moyen de profiter de nombreuses formes de distraction (jouer, acheter/vendre, écouter de la musique, regarder des films, lire des livres, réserver des vacances,...)



FORTNITE

amazon

NETFLIX



Introduction et généralités

Les réseaux

Depuis tantôt nous parlons de « réseaux », mais comment définiriez-vous ce terme ?

Existe-t-il différents types réseaux ?

Si oui, selon quels critères peut-on les différencier ?

On peut dire, d'une manière générale, qu'un réseau est un ensemble d'équipements et de logiciels qui permettent d'acheminer de l'information d'un émetteur jusqu'à un ou plusieurs récepteurs.

Exemples de réseaux :

Réseaux de télécommunications
 ● Téléphonie fixe et mobile

Réseaux des câblo-opérateurs
 ● Télédistribution (TV)

Réseaux informatiques
 ● Internet



Introduction et généralités

Les réseaux

Les réseaux peuvent être classés selon 2 critères :

- L'étendue du réseau
- La technologie de transmission

A. L'étendue du réseau

Les réseaux peuvent être de différentes tailles. Il existe des réseaux élémentaires, constitués de deux ordinateurs, mais également des réseaux extrêmement complexes, capables de connecter des millions de périphériques.

Dès lors on peut décomposer ceux-ci en 4 catégories de réseaux :

- **PAN** (Personal Area Network) => réseaux personnels
- **LAN** (Local Area Network) => réseaux locaux
- **MAN** (Metropolitan Area Network) => réseaux métropolitains
- **WAN** (Wide Area Network) => réseaux longues distances

Introduction et généralités

Réseau PAN

Il s'agit des réseaux les plus simples permettent de partager des ressources, telles que des imprimantes, des documents, des images et de la musique, entre quelques ordinateurs locaux ou entre des téléphones portables par exemple.

Caractéristiques :

Taille : 1 m à 10 m.

Étendue : équipements proches.

Technologies associées : Bluetooth.

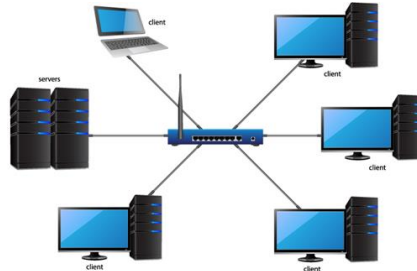
Exemple : réseau entre GSM, kit mains libres,...



Introduction et généralités

Réseau LAN

Les **réseaux locaux** sont souvent des réseaux configurés par des personnes qui travaillent dans les locaux de l'entreprise et/ou à domicile (à distance) et qui doivent se connecter à un réseau d'entreprise ou à d'autres ressources centralisées.



Caractéristiques :

Taille : 10 m à 1 km.

Étendue : bâtiment ou campus.

Technologies associées : Ethernet, Token Ring et FDDI.

Exemple : réseau de l'ISIMs.

Introduction et généralités

Réseau MAN

Un **réseau métropolitain** désigne un réseau composé d'ordinateurs habituellement utilisés dans les campus ou dans les villes. Le réseau utilise généralement des fibres optiques pour relier les bâtiments entre eux.

Par exemple, une université (comme l'UMons) peut avoir un MAN qui lie ensemble plusieurs réseaux locaux situés dans un espace de quelques km². Puis, à partir des MAN des différentes universités implantées sur Mons, on pourrait avoir plusieurs réseaux étendus (WAN) les liant à d'autres universités en Belgique et à Internet.

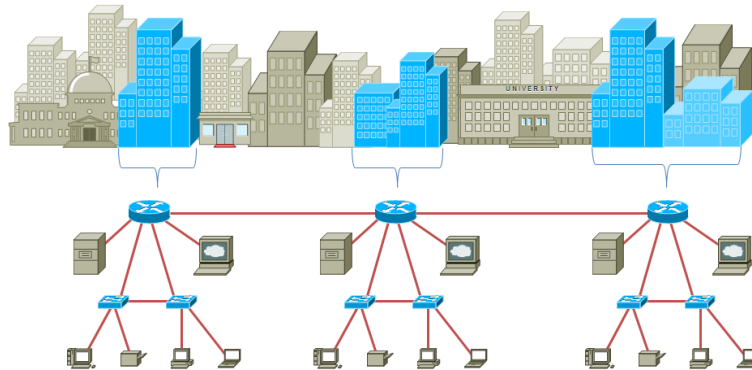
Caractéristiques :

Taille : 1 km à 100 km.

Étendue : villes

Technologies associées : FDDI, DQDB, MPLS.

Exemple : réseau FedMAN (Federal MAN) => ce réseau relie les bâtiments des administrations fédérales, dispersés dans Bruxelles, entre eux et à internet.

Réseau MAN

Réseau WAN

Le WAN est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière.

Le plus grand WAN est le réseau Internet.

Caractéristiques :

Taille : + de 100 km

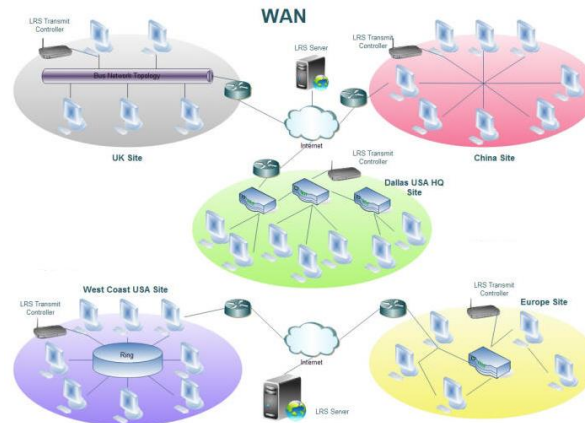
Étendue : Pays ou continent.

Technologies associées : ATM, Frame Relay, MPLS et Ethernet.

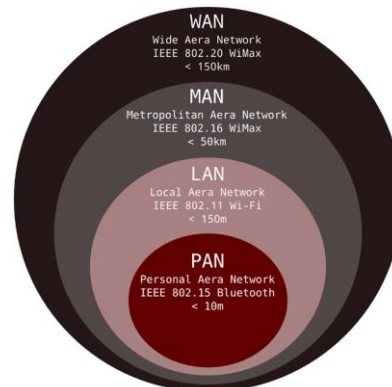
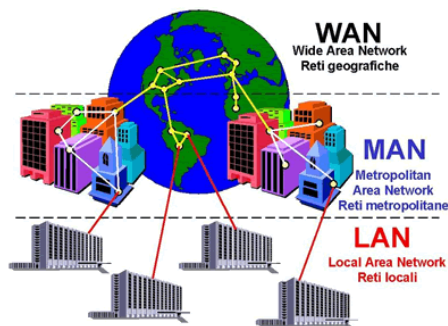
Exemple : réseau BELNET (réseau de la recherche) accessible aux universités, aux hautes écoles, aux centres de recherche et aux services publics.

Introduction et généralités

Réseau WAN



Introduction et généralités



B. Technologie de transmission

On distingue encore deux sous types :

- la diffusion
- le point-à-point

Un **réseau à diffusion** dispose d'un seul support de transmission qui est **partagé** par tous les équipements qui y sont connectés.

=> chaque message envoyé par un équipement sur le réseau est reçu par tous les autres mais seul le destinataire concerné le traitera.

Dans certains cas, le message peut être destiné à tous les équipements

=> transmission à diffusion générale (ou envoi **broadcast**).

Un **réseau point-à-point** dispose d'un seul support de transmission qui relie une paire d'équipements seulement. Quand deux équipements non connectés directement entre eux veulent communiquer, ils le font par le biais des autres équipements du réseau.

Une transmission point-à-point entre un expéditeur et un destinataire est appelée diffusion individuelle (ou envoi **unicast**).

La technologie de transmission utilisée par le réseau a un impact sur la topologie du réseau.

Attention, lorsqu'on parle de topologie de réseau, il ne faut pas confondre la topologie physique et la topologie logique !!!

Une **topologie physique** est en fait la structure physique de votre réseau. C'est donc la forme, l'apparence, l'arrangement spatial du réseau.

Une **topologie logique** est la manière dont les stations se partagent le support et dépend de la méthode d'accès au réseau.

En général, la topologie représente la disposition physique de l'ensemble des composants d'un réseau. La topologie d'un réseau est aussi appelée **schéma** ou **architecture** ou encore **plan** du réseau.

La topologie d'un réseau peut avoir une extrême importance sur l'évolution du réseau, sur son administration, et sur les compétences des personnels qui seront amenés à s'en servir.

Introduction et généralités

Au niveau des différentes topologies physiques, on retrouve :

Réseaux en mode de diffusion



Topologie en bus



Topologie en anneau

Réseaux en mode point-à-point



Topologie point-à-point



Topologie en étoile



Topologie maillée

Introduction et généralités

Au niveau des différentes topologies logiques, on retrouve :

Ethernet

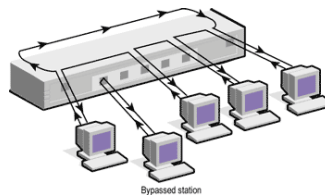
Ethernet est aujourd'hui l'un des réseaux les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul support de transmission.

Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole d'accès au média appelé CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Ce protocole (que l'on étudiera plus tard dans ce cours) gère la manière dont les données seront transmises sur le réseau.

Token Ring

Token Ring repose sur une topologie en anneau (*ring*) et utilise la méthode d'accès par jeton (appelé *token*). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre sur le réseau.

Si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton. Dans un réseau Token Ring, chaque nœud du réseau est relié à un MAU (*Media Access Unit* ou *Multistation Access Unit*) qui peut recevoir les connexions des postes.



Introduction et généralités

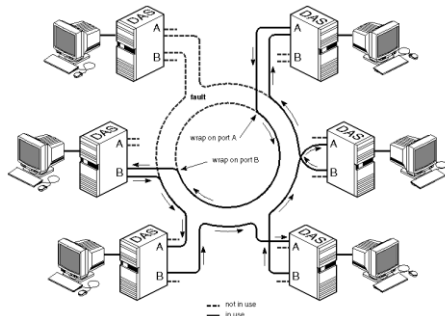
FDDI

La technologie LAN FDDI (*Fiber Distributed Data Interface*) est une technologie d'accès réseau utilisant des câbles fibres optiques.

Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire.

L'anneau secondaire sert à rattraper les erreurs en cas de problème avec l'anneau primaire.

Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.



DAS : Dual Attachment Station

Introduction et généralités

Les réseaux : mode de fonctionnement

Tous les ordinateurs connectés à un réseau et qui participent directement aux communications réseau s'appellent des hôtes ou des périphériques finaux. Ces hôtes peuvent envoyer et recevoir des messages sur le réseau.

Dans les réseaux actuels, les périphériques finaux peuvent jouer le rôle de client, de serveur, ou les deux. Les logiciels installés sur l'ordinateur déterminent le rôle qu'il tient au sein du réseau.

D'une part on a les **serveurs**, qui sont des hôtes équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages Web, à des clients. Attention, chaque service nécessite un logiciel serveur distinct.

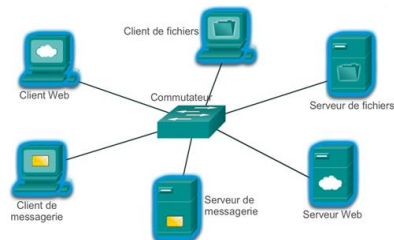
D'autre part on a les **clients** sont des ordinateurs hôtes équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher.

Les réseaux : mode de fonctionnement

Ce type de réseau fonctionne selon un modèle que l'on appelle le **modèle client-serveur**.

Exemple :

Le serveur de messagerie exécute le logiciel du serveur et les clients utilisent le logiciel du client de messagerie, tel Microsoft Outlook, pour accéder à la messagerie sur le serveur.



Remarque :

Il peut arriver, par nécessité, qu'un ordinateur fasse office à la fois de serveur de fichiers, de serveur Web et de serveur de messagerie.

Un seul ordinateur peut également exécuter différents types de logiciel client en même temps.

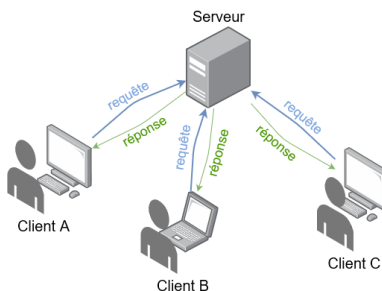
Caractéristiques du **modèle client-serveur** :

Dans ce modèle, le client est un consommateur de services. C'est lui qui effectuera ce qu'on appelle une requête auprès du serveur afin de recevoir des informations. Il est donc toujours actif en premier.

Une fois la requête envoyée, il attend une réponse de la part du serveur.

Au niveau du serveur, celui-ci est dit passif. C'est un fournisseur de service qui est constamment à l'écoute, grâce à ce qu'on appelle un démon, prêt à répondre aux différentes requêtes des clients.

Dès qu'il reçoit une requête, il la traite et envoie une réponse.



Introduction et généralités

Dans certains cas (réseaux de particuliers et de petites entreprises), les ordinateurs peuvent opérer en tant que clients **ou** en tant que serveurs des autres PC du réseau simultanément, contrairement aux systèmes de type client-serveur.

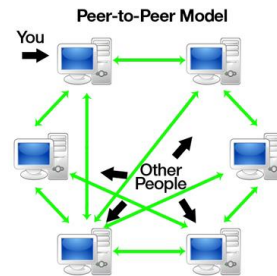
Ce type de réseau utilise un **modèle Peer to peer (P2P)**.

Avantages du réseau P2P :

- > Facile à configurer
- > Moins complexe
- > Coût plus faible
- > Pratique pour les tâches simples et les réseaux de petite envergure

Inconvénients du réseau P2P :

- > Pas d'administration centralisée
- > Peu sécurisé
- > Non évolutif
- > Risques de ralentissement sur le réseau car tout les périphériques peuvent servir à la fois de client et de serveur, ce qui peut ralentir les performances



Introduction et généralités

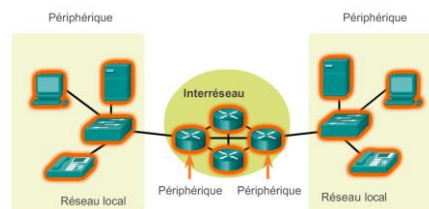
Les réseaux : les composants

Peu importe le chemin emprunté par un message entre sa source et sa destination, dans chaque cas, l'infrastructure réseau sera toujours composée de 3 catégories de composants.

1. La première est évidente, il s'agit des **périphériques**.

Au niveau de ces périphériques, on peut décomposer ceux-ci en deux groupes distincts :

• **les périphériques finaux** ou **hôtes**. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent.



• **les périphériques intermédiaires**. Ceux-ci relient des périphériques finaux. Ils offrent une connectivité et opèrent en arrière-plan pour s'assurer que les données sont transmises sur le réseau

Introduction et généralités

2. La seconde catégorie de composants sont bien évidemment les **supports de transmission** ou médium de transmission.

Le support de transmission fournit le canal via lequel le message se déplace de la source à la destination.

Les réseaux modernes utilisent principalement 3 types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises :

- le câblage en cuivre
- la fibre optique
- les transmissions sans fil

Selon le type de support utilisé, le codage du signal qui doit se produire afin de transmettre le message va différer :

Sur des fils de cuivre, les données sont codées en impulsions électriques.

Les transmissions par fibre optique s'effectuent via des impulsions de lumière.

Concernant les transmissions sans fil, on utilisera des ondes électromagnétiques.

Introduction et généralités

Si on utilise autant de types de supports différents, c'est bien entendu parce que chacun d'entre eux possède ses avantages et ses fonctionnalités.

Tous les supports réseau ne possèdent pas les mêmes caractéristiques et ne conviennent pas pour les mêmes objectifs ou dans les mêmes situations !



le câble en cuivre



la fibre optique



le sans fil

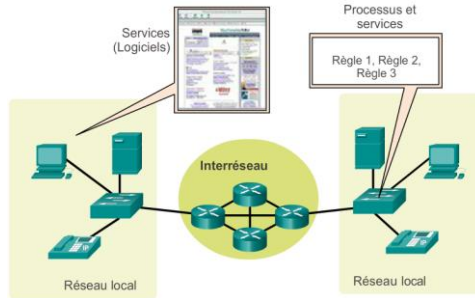
Introduction et généralités

3. La troisième catégorie de composants sont **les services et les processus**.

Les services et les processus sont les programmes de communication qui sont exécutés sur les périphériques réseau.

Un service réseau fournit des informations en réponse à une demande. Exemple : les services d'hébergement de messagerie et les services d'hébergement Web.

Les processus fournissent les fonctionnalités qui dirigent et déplacent les messages à travers le réseau.



Introduction et généralités

Les réseaux : les symboles

Pour pouvoir comprendre le fonctionnement des réseaux, il est important d'utiliser des représentations visuelles.

Dès lors, un schéma constitue un moyen facile de comprendre comment les périphériques d'un grand réseau sont connectés.

Mais pour que tout le monde puisse lire et distinguer exactement tous les éléments présents sur ce schéma, il faut impérativement que celui-ci utilise des symboles connus de tous afin de représenter les différents composants du réseau (les périphériques, les connexions).

Un schéma de réseau est aussi appelé un **diagramme de topologie**.

Introduction et généralités

Symboles utilisés dans ces diagrammes de topologies :

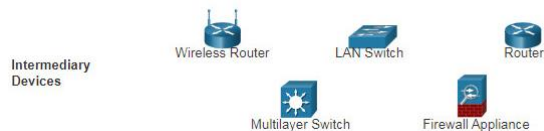


Les différents symboles ci-dessus représentent différentes sortes de **terminaux** (ou de périphériques finaux c'est la même chose).

Un périphérique final constitue soit la source soit la destination d'un message transmis à travers le réseau et on peut les identifier (et donc les distinguer les uns des autres) grâce à des adresses.

Introduction et généralités

En plus de ces périphériques finaux, nous avons vu qu'un réseau était également composé de périphériques intermédiaires. Ces périphériques fournissent la connectivité et s'assurent que les données sont transmises sur le réseau.



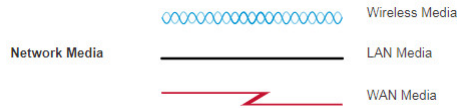
Ils vont donc pouvoir (en partie ou totalement selon le périphérique) :

- régénérer et retransmettre les signaux de communication
- gérer les informations concernant les chemins existant à travers le réseau
- prévenir les autres périphériques du réseau en cas d'erreurs ou d'échecs de transmission
- classer et diriger des messages en fonction de priorités
- gérer des flux de données, selon des paramètres de sécurité

Remarque : un ancien type de périphérique intermédiaire portant le nom de concentrateur (« hub » en anglais) n'est plus représenté ici mais on l'abordera tout de même plus loin dans le cours.

Introduction et généralités

Il nous reste à savoir représenter les supports de transmission :



Introduction et généralités

En plus de ces représentations, une terminologie spécialisée est utilisée pour étudier la manière dont ces périphériques et supports se connectent entre eux. Les termes importants dont il faut se souvenir sont les suivants :

Carte réseau (NIC en anglais) – une carte réseau fournit la connexion physique au réseau à partir de l'ordinateur ou d'un autre périphérique hôte. Les supports qui relient l'ordinateur au périphérique réseau se branchent directement à la carte réseau.

Port physique – connecteur ou prise sur un périphérique réseau par lequel/laquelle le support est connecté à un hôte ou à un autre périphérique réseau.



Interface – ports spécifiques d'un périphérique interréseau qui se connectent à des réseaux individuels. Puisque les routeurs sont utilisés pour interconnecter des réseaux, les ports sur un routeur sont appelés interfaces réseau.

Introduction et généralités

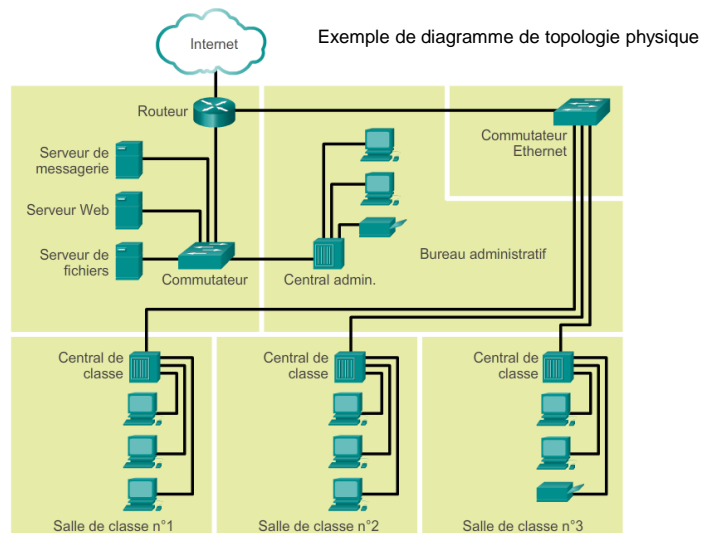
A partir de ces symboles, il est indispensable pour toute personne travaillant sur un réseau de concevoir des diagrammes de topologie !

Cependant, il existe deux types de diagrammes de topologie différents et complémentaires :

Des diagrammes de topologie physique – sur lesquels on va indiquer l'emplacement physique des périphériques intermédiaires, des ports configurés et des câbles.

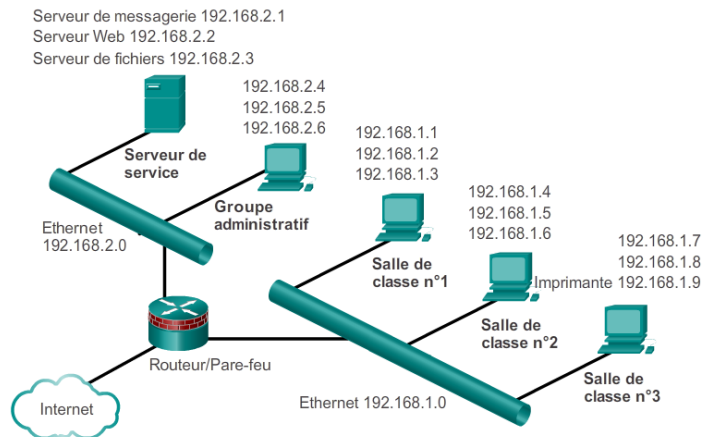
Des diagrammes de topologie logique – sur lesquels on retrouvera les périphériques, les ports, et le schéma d'adressage IP.

Introduction et généralités



Introduction et généralités

Exemple de diagramme de topologie logique



Introduction et généralités

Les réseaux : Internet le seul, le vrai !

Nous avons vu précédemment qu'il existait différents types de réseaux (LAN, WAN,...) qui sont utilisés par des personnes qui doivent communiquer entre elles sur un réseau d'étendue plus ou moins grande.

Mais comment est-ce que l'ensemble de ces réseaux parviennent-ils à communiquer entre eux ?

La réponse est on ne peut plus simple : via *Internet*.

Internet est un ensemble mondial de réseaux interconnectés qui coopèrent pour échanger des informations en utilisant des normes cohérentes et communément reconnues.

Qui dit mondial, dit que cela implique de nombreux organismes gouvernementaux et qui dit normes cohérentes et reconnues, dit qu'il a fallu mettre au point des règles identiques pour tous.

→ Il a fallu créer des organismes pour gérer la structure et la normalisation des protocoles et des processus Internet. Parmi ceux-ci on retrouve l'*Internet Engineering Task Force* (IETF), l'*Internet Corporation for Assigned Names and Numbers* (ICANN) ou encore l'*Internet Architecture Board* (IAB).

Introduction et généralités

Internet, intranet, extranet ?!? Qu'est-ce que c'est que tout ça encore ?

Le terme **intranet** est souvent utilisé pour faire référence à un réseau LAN privé qui appartient à une entreprise (ou une administration) et auquel peuvent accéder uniquement ses membres, ses employés.

Il n'est généralement accessible que depuis le site d'une entreprise.

Sur l'intranet d'une entreprise on peut retrouver des pages Web sur les événements internes, des documents liés à la politique de santé et de sécurité, des lettres d'information destinées au personnel, un répertoire téléphonique du personnel,...

L'intérêt de l'intranet c'est qu'il permet généralement d'éliminer certains documents papier et d'accélérer le flux de travail du personnel.

Un intranet peut être utilisé par le personnel travaillant en dehors du site de l'entreprise grâce à des connexions sécurisées au réseau interne.

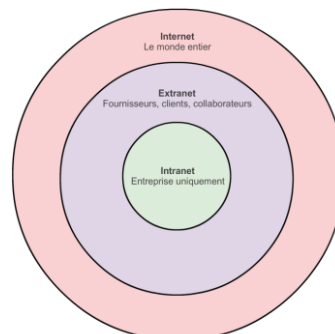
Introduction et généralités

Le terme **extranet** est quant à lui utilisé lorsqu'une entreprise fournit un accès sécurisé aux personnes qui travaillent pour d'autres entreprises, mais qui ont besoin des données de l'entreprise en question.

C'est par exemple le cas si vous possédez une société et qu'elle fournit un accès à des fournisseurs/sous-traitants externes.

Voici quelques exemples d'extranets :

- Une entreprise qui donne accès aux fournisseurs et entrepreneurs extérieurs.
- Un hôpital qui fournit un système de réservation aux médecins afin qu'ils puissent prendre des rendez-vous pour leurs patients.
- Un bureau local de l'éducation qui fournit des informations sur le budget et le personnel aux écoles de son district



Introduction et généralités

Bref, Internet est le plus grand des inter-réseaux et nous sommes donc tous obligé de passer par lui si l'on veut communiquer dans le monde entier.

Mais alors, savez-vous par quels moyens nous nous connectons à celui-ci ?

Pour un particulier comme vous et moi ou une petite entreprise, il existe différentes manières d'accéder à Internet, même si généralement nous devons passer par ce que l'on appelle un fournisseur d'accès internet (FAI).



Manières d'accéder à Internet pour les particuliers :

- **par câble** – Généralement proposé par les fournisseurs de services de télévision par câble, le signal de données Internet est transmis grâce au câble coaxial utilisé pour la télévision par câble. Il offre une connexion permanente à Internet haut débit. Un modem câble spécial sépare le signal Internet des autres signaux transmis sur le câble et fournit une connexion Ethernet à un ordinateur hôte ou à un LAN.

Introduction et généralités

- **par xDSL (Digital Subscriber Line)** – La ligne DSL utilise un modem spécifique haut débit, qui sépare le signal DSL du signal téléphonique et fournit une connexion Ethernet à un ordinateur hôte ou à un LAN.

La DSL fonctionne sur une ligne téléphonique divisée en trois canaux :

- Un canal est utilisé pour les appels téléphoniques.
- Un deuxième canal de téléchargement, plus rapide, est utilisé pour recevoir des informations depuis Internet (*download*).
- Un troisième canal (généralement légèrement moins performant) est utilisé pour envoyer des informations (*upload*).

La qualité et la vitesse de la connexion DSL dépendent essentiellement de la qualité de la ligne téléphonique et de la distance du central de la compagnie de téléphone.

- L'**ADSL (Asymmetric Digital Subscriber Line)** : Son principe consiste à exploiter une autre bande de fréquence, située au-dessus de celle utilisée pour la téléphonie, pour échanger des données numériques en parallèle avec une conversation téléphonique.
- Le **VDSL (Very-high-bit-rate DSL)** permet d'atteindre des débits de 13 à 55 Mb/s dans un sens et de 1,5 à 8 Mb/s dans l'autre ou, si l'on veut en faire une connexion symétrique, un débit de 34 Mb/s.
- Le **VDSL2 (Very high speed Digital Subscriber Line 2)**, successeur du VDSL permet une vitesse maximale théorique de 100 Mbit/s en full-duplex.

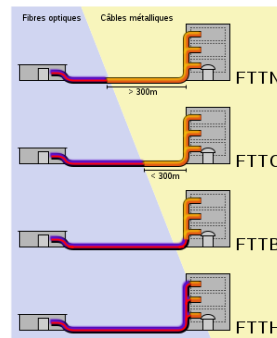
Introduction et généralités

• **par fibre** (FTTx pour *Fiber To The ...*) – consiste à amener la fibre optique au plus près de l'utilisateur, afin d'augmenter la qualité de service (en particulier le débit) dont celui-ci pourra bénéficier.

Le débit fourni via une fibre optique est indépendant de la distance, alors que le débit fourni via les derniers mètres (via des câbles de cuivre) dépend de la longueur de la paire de cuivre (à cause de l'affaiblissement du signal).

Il existe d'ailleurs différents types de réalisations possibles (en fonction du prix bien souvent) et on retrouve donc plusieurs appellations possibles :

- FTTN : *Fiber To The Neighbourhood*
- FTTC : *Fiber To The Curb* (Fibre jusqu'au trottoir)
- FTTB : *Fiber To The Building*
- FTTH : *Fiber To The Home*



Introduction et généralités

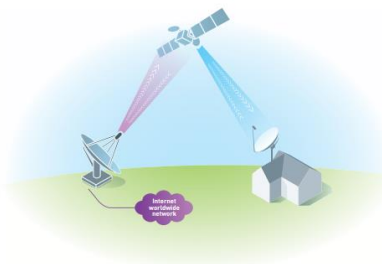
• **par satellite** – Le service par satellite est l'option idéale pour les maisons ou les bureaux qui n'ont pas accès à la DSL ou au câble.

Les paraboles nécessitent une visibilité directe sur le satellite et peuvent ne pas fonctionner convenablement dans des zones boisées ou des emplacements entourés d'éléments faisant obstacle aux transmissions.

Les débits dépendent du contrat choisi, mais sont en général élevés. Les frais liés au matériel et à l'installation peuvent être élevés (même si les fournisseurs peuvent proposer des promotions), et un forfait mensuel est ensuite mis en place.

La disponibilité de l'accès Internet par satellite constitue un réel avantage dans les régions qui n'ont aucune autre possibilité d'accéder à Internet.

La principale force du satellite réside dans le fait que le déploiement au sol est immédiat. En effet, contrairement à l'ADSL ou au câble, l'Internet par satellite ne nécessite aucun réseau terrestre.



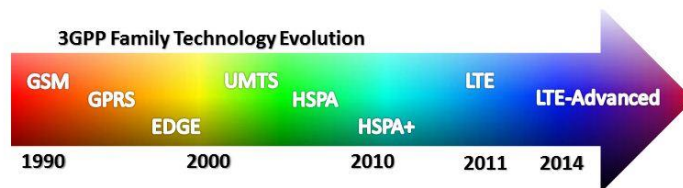
Introduction et généralités

• **par cellulaire** – Cette solution, vous la possédez tous déjà (ou presque) puisque l'accès Internet cellulaire utilise un réseau de téléphonie mobile.

Donc partout où vous captez un signal cellulaire, vous pouvez accéder à Internet.

Les performances sont cependant limitées par les fonctionnalités du téléphone et de la station de base à laquelle l'appareil est connecté.

La disponibilité de l'accès Internet cellulaire constitue un réel avantage dans les régions qui n'ont aucune autre possibilité d'accéder à Internet ou pour les utilisateurs constamment en déplacement.



Introduction et généralités

3GPP (*3rd Generation Partnership Project*) est une coopération entre organismes de standardisation régionaux en télécommunications tels que : l'UIT, l'ETSI (Europe), l'ARIB/TTT (Japon), le CCSA (Chine), l'ATIS (Amérique du Nord) et le TTA (Corée du Sud), visant à produire des spécifications techniques pour les réseaux mobiles de 3^e (3G), 4^e (4G) et maintenant 5^e génération.

3GPP assure par ailleurs la maintenance et le développement de spécifications techniques pour les normes mobiles GSM, notamment pour le GPRS, l'EDGE, l'UMTS et le LTE.

Introduction et généralités

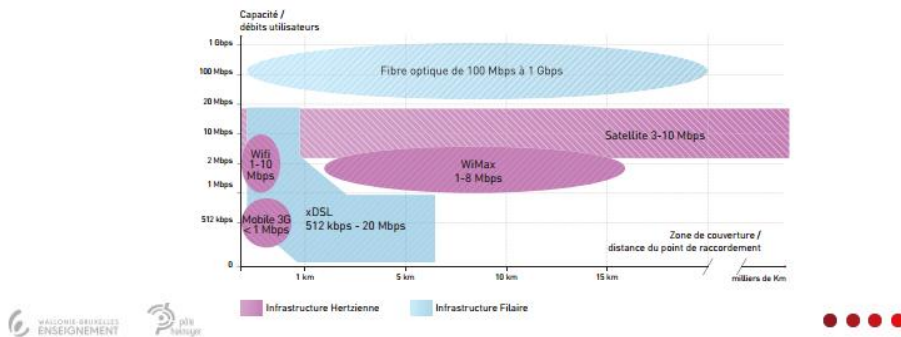
• **par ligne commutée** – Vous ne l'avez sans doute pas connu mais ceci est l'ancêtre de l'ADSL.

L'internet par ligne commutée nécessitait une ligne téléphonique et un modem.

Pour se connecter au FAI, l'utilisateur appelle le numéro de téléphone d'accès du FAI.

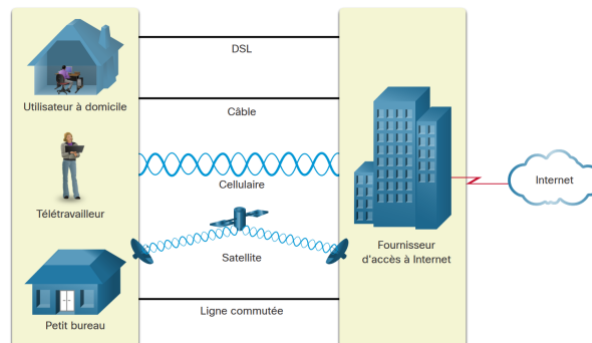
La faible bande passante des connexions par ligne commutée n'est généralement pas suffisante pour les transferts de données importants. Il ne faut opter pour une connexion par ligne commutée que lorsque les autres options de connexion haut débit ne sont pas disponibles.

Panorama des solutions technologiques



Introduction et généralités

En résumé :



Introduction et généralités

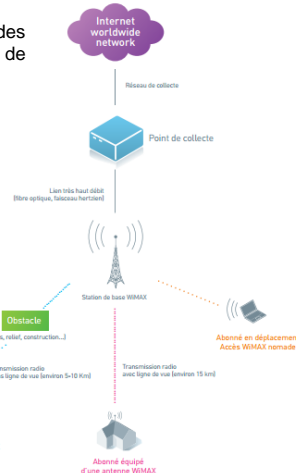
Le WiMax (Worldwide Interoperability for Microwave Access)

Le WiMAX est une technologie de transmission haut débit par ondes radio conçue pour couvrir des surfaces importantes (rayon de plusieurs kilomètres de couverture autour de l'émetteur).

Son utilisation permet de mettre en place des liaisons point-multipoint afin de relier l'utilisateur et un point de collecte, connecté au réseau Internet.

Le débit maximum est de quelques dizaines de Mbps, partagés entre tous les utilisateurs raccordés à une même station.

Par ailleurs, le débit réel de l'utilisateur dépend de nombreux facteurs, tels que la distance entre l'utilisateur et la station, ou la topographie des lieux, et le nombre d'utilisateurs sur le réseau.



Introduction et généralités

Ce standard de réseau sans fil métropolitain créé par les sociétés Intel et Alvarion en 2002 et ratifié par l'IEEE (*Institute of Electrical and Electronics Engineer*) sous le nom IEEE-802.16

En théorie, le WiMax permet d'obtenir des débits montants et descendants de 70 Mbit/s avec une portée de 50 kilomètres.

Dans la réalité, le WiMAX ne permet de franchir que de petits obstacles tels que des arbres ou une maison mais ne peut en aucun cas traverser les collines ou les immeubles.

Dès lors, le débit réel lors de la présence d'obstacles ne pourra ainsi excéder 20 Mbit/s.

La technologie WiMax est bien adaptée à deux types d'usage :

- Zone rurale peu dense : il permet de réaliser la couverture haut débit de superficies relativement importantes sans avoir à réaliser des travaux de génie civil, et en s'affranchissant des contraintes du réseau téléphonique qui limitent les zones d'éligibilité ADSL.
- Zone urbaine dense : il permet d'offrir du haut débit nomade (avec la possibilité de se connecter avec un même abonnement depuis différents endroits, mais sans déplacement pendant la connexion), comme avec les hotspots WiFi, mais à une échelle plus étendue.

Introduction et généralités

Manières d'accéder à Internet pour les grandes entreprises :

- **par xDSL** – Et oui, comme nous l'avons vu, la DSL est disponible dans divers formats dont la SDSL (*Symmetric Digital Subscriber Line*) qui est largement utilisée. La SDSL est similaire à une ligne ADSL (*Asymmetric Digital Subscriber Line*), mais présente les mêmes débits ascendant (upload) et descendant (download) alors que l'ADSL est conçue pour fournir une bande passante dont les débits ascendant et descendant sont différents.

- **par ligne louée spécialisée** – Il s'agit d'une connexion dédiée du fournisseur de services sur le site du client. Les lignes louées sont des circuits dédiés qui relient des bureaux distincts pour la transmission de données et/ou de communications vocales privées. Les circuits sont généralement loués sur une base mensuelle ou annuelle, ce qui rend cette solution onéreuse.

En Europe on retrouve des lignes :

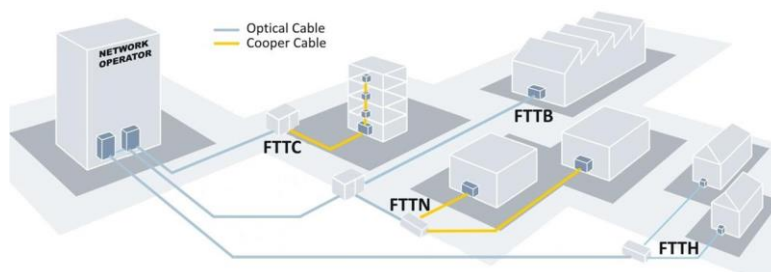
E0 (64Kbps),
 E1 = 32 lignes E0 (2Mbps),
 E2 = 128 lignes E0 (8Mbps),
 E3 = 16 lignes E1 (34Mbps),
 E4 = 64 lignes E1 (140Mbps)

Aux Etats-Unis la notation est la suivante :

T1 (1.544 Mbps)
 T2 = 4 lignes T1 (6 Mbps),
 T3 = 28 lignes T1 (45 Mbps),
 T4 = 168 lignes T1 (275 Mbps).

Introduction et généralités

- **par fibre (FTTx)** – Le service Ethernet sur fibre optique assure les connexions les plus rapides à un prix réduit par mégabit. Même si celui-ci se répand peu à peu, il reste encore beaucoup de zones (rurales) où ce service n'est pas disponible.



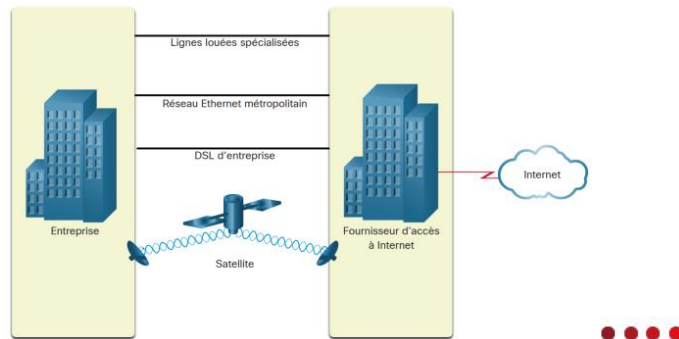
Introduction et généralités

• **par satellite** – Le service par satellite est souvent utilisé lorsqu'aucune solution par câble n'est disponible.

Tout comme pour les particuliers, les paraboles nécessitent une visibilité directe sur le satellite. Les frais liés au matériel et à l'installation peuvent être élevés, et un forfait mensuel est ensuite mis en place.

Ces connexions ont tendance à être plus lentes et moins fiables que les connexions terrestres, ce qui les rend moins intéressantes que les autres solutions, surtout pour le monde de l'entreprise !

En résumé :



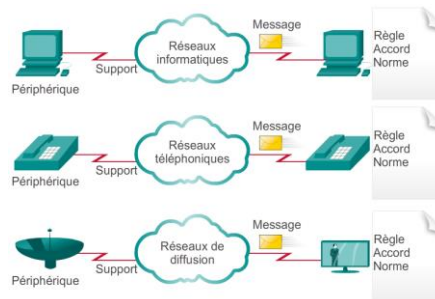
Introduction et généralités

Les réseaux d'hier et d'aujourd'hui

Auparavant, chacun de ces services nécessitait un réseau dédié, avec des canaux de communication différents et des technologies différentes pour transmettre un signal de communication particulier.

Chaque service avait son propre ensemble de règles et de normes, destiné à garantir les communications.

→ Il était donc impossible de faire communiquer des réseaux distincts entre eux !



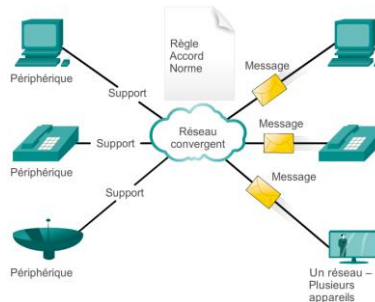
Introduction et généralités

Aujourd'hui, grâce aux évolutions technologiques, nous pouvons regrouper ces différents types de réseau sur une même plate-forme afin d'obtenir ce qu'on appelle un **réseau convergent**.

Contrairement aux réseaux spécialisés, les réseaux convergents peuvent transmettre des sons, des flux vidéo, du texte et des images entre différents types d'appareil, par le biais d'un même canal de communication et d'une même structure réseau.

Cette infrastructure réseau utilise le même ensemble de règles, de contrats et de normes de mise en œuvre.

Les réseaux de données convergents exécutent plusieurs services sur un même réseau.



Introduction et généralités

En pratique comment cela se passe-t-il lorsqu'il y a plusieurs communications qui veulent traverser un même réseau en même temps ?

Grâce à deux éléments essentiels :

- La segmentation
- Le multiplexage

La **segmentation** consiste en fait à découper les données à envoyer en parties de taille moins importante.

But :

L'envoi de parties de plus petite taille, depuis une source vers une destination, permet d'entremêler plusieurs conversations différentes. Ce processus porte le nom de **multiplexage**.

Cela permet également d'augmenter la fiabilité du réseau puisque les différentes parties de chaque message n'ont pas besoin de parcourir le même chemin sur le réseau pour aller de la source à la destination.

Introduction et généralités

De plus, si une communication (par exemple une vidéo) était envoyée dans son intégralité, alors pendant cette communication, aucun autre périphérique ne serait en mesure de communiquer quoi que ce soit pendant ce laps de temps.

De plus si une erreur se produisait lors du transfert en continu, il faudrait renvoyer la totalité de la vidéo !!!

Inconvénient :

L'utilisation de ces deux techniques rend néanmoins les communications un peu plus complexe puisqu'il va falloir étiqueter toutes les parties des différents messages à transmettre afin de pouvoir les diriger sur le réseau et les réassembler dans l'ordre lorsqu'elle seront arrivées au destinataire.

Introduction et généralités

De nos jours, les réseaux doivent prendre en charge une large gamme d'applications et de services, et fonctionner sur de nombreux types de câble et de périphérique, qui constituent l'infrastructure physique.

Dans le contexte actuel, l'expression « *architecture réseau* » désigne aussi bien les technologies prenant en charge l'infrastructure que les services programmés et les règles, ou protocoles, qui font transiter les messages sur le réseau.

Avec l'évolution des réseaux en général, et en particulier celle d'Internet, on essaie de concevoir des architectures réseaux afin d'arriver à une règle que l'on appelle la règle des 5 neufs (c-à-d 99,999% de disponibilité du réseau → ce qui représente 5,26 minutes d'indisponibilité par an)

Ce qui fait que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs :

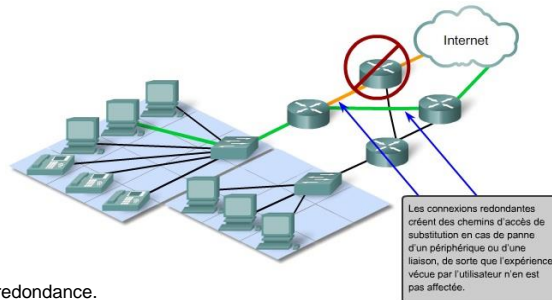
- > la tolérance aux pannes
- > l'évolutivité
- > la qualité de service (QoS)
- > la sécurité

Introduction et généralités

1. La tolérance aux pannes

Lorsqu'on prend un utilisateur connecté à internet, il s'attend à ce que ce réseau soit constamment disponible.

→ Il faut que le réseau limite l'impact des pannes (matérielles ou logicielles)



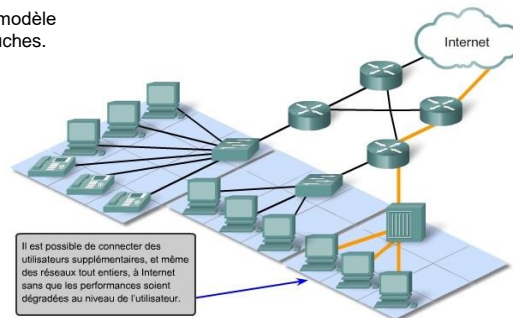
Solution : la redondance.

Introduction et généralités

2. L'évolutivité

Lorsqu'on a un certain nombre de personnes connectées à un réseau, il faut que les performances de celui-ci restent inchangées pour les utilisateurs déjà présents et cela même si de nouveaux utilisateurs viennent s'ajouter au réseau.

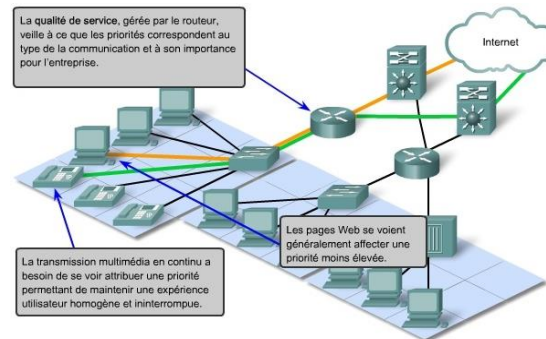
Solution : l'utilisation d'un modèle hiérarchisé à plusieurs couches.



Introduction et généralités

3. La qualité de service (QoS)

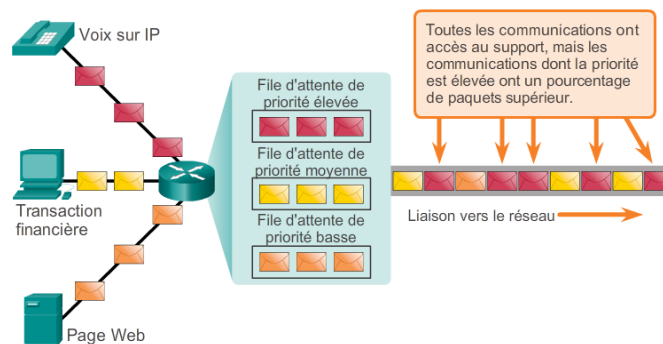
Lorsqu'un utilisateur utilise un réseau, il exige un niveau de qualité et un service ininterrompu.



Solution : l'utilisation de niveaux de priorité.

Introduction et généralités

L'utilisation de niveaux de priorité :



Vu qu'il y a différents types de trafic qui circule (voix, vidéo, données) on doit classer les communications selon leur importance.

Ensuite toutes les données appartenant à la même classe seront traitées de la même manière.

Introduction et généralités

Dans une entreprise par exemple, les décisions en matière de priorités peuvent par exemple porter sur :

- Les communications pour lesquelles la vitesse de livraison sera important (téléphonie, vidéo)
- Les communications pour lesquelles la vitesse de livraison n'est pas importante (pages web, courriels)
- Les communications qui ont une grande importance pour l'entreprise (transactions financières)
- Les communications indésirables (réduire voire bloquer certaines activités)

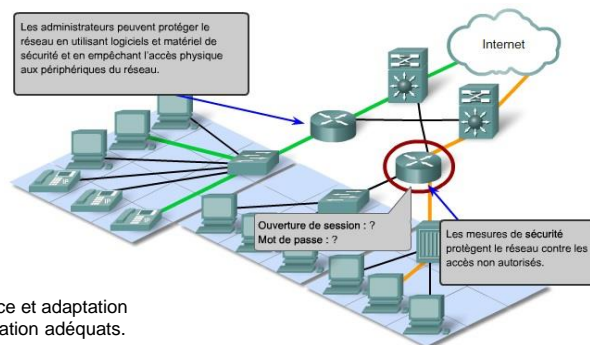
La disponibilité est aujourd'hui un enjeu important des infrastructures informatiques. Une étude de 2010, d'Emerson Network Power, estime que la non-disponibilité des services informatiques d'une entreprise peut lui coûter **5000\$ par minute** ! Alors imaginez cela à l'échelle d'un pays...

Bien entendu, l'indisponibilité des services informatiques peut avoir des conséquences bien différentes en fonction de l'entreprise touchée et du domaine dans lequel elle travaille, mais dans tout les cas, une chose est sûre, votre patron préférera que cela ne se produise pas.

Introduction et généralités

4. La sécurité

Avec l'évolution d'internet comme moyen de transmission de communications professionnelles et personnelles largement accessible, les exigences en matière de sécurité ont évolué.



Solution : mise en place et adaptation de moyens de sécurisation adéquats.

Les réseaux : nouvelles tendances

Comme de nouvelles technologies et de nouveaux périphériques apparaissent jours après jours sur le marché, les entreprises et les consommateurs doivent continuer à s'adapter à cet environnement en constante évolution.

Les réseaux doivent donc être transformés pour permettre aux personnes et aux périphériques d'échanger des informations.

Nous allons aborder quelques nouvelles tendances relatives au réseau, qui affecteront les entreprises et les clients.

a) Le BYOD

Le BYOD ? Qu'est-ce que c'est encore que ça ?

Le **BYOD** c'est le concept de « Bring Your Own Device ».

Le BYOD consiste à offrir aux utilisateurs finaux la liberté d'utiliser leurs propres outils pour accéder aux informations et communiquer au sein d'une entreprise ou d'un réseau de campus.

Avec la croissance des appareils personnels et la réduction de leur coût, les employés peuvent disposer des meilleurs outils informatiques et de réseau pour leur usage personnel.

Ces outils personnels incluent notamment des ordinateurs portables, des netbooks, des tablettes, des smartphones,...

Le BYOD, c'est pour n'importe quel appareil, quel que soit son propriétaire, n'importe où.

Le BYOD est une tendance importante, qui concerne ou concernera tous les services informatiques.

b) La virtualisation

Qu'est-ce que la virtualisation ?

La **virtualisation** est un mécanisme informatique qui consiste à faire fonctionner plusieurs systèmes, serveurs ou applications, sur un même serveur physique.

Elle consiste à faire fonctionner un ou plusieurs systèmes d'exploitation/applications comme un simple logiciel, sur un serveur, au lieu de ne pouvoir en installer qu'un seul par machine.



Avantages de la virtualisation :

- consolidation et rationalisation d'un parc de serveurs en entreprise : les entreprises ne sont plus obligées d'acheter un serveur physique pour chaque application.
- rationalisation des coûts de matériels informatiques.
- portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre (lorsque celle-ci a, par exemple, besoin de davantage de ressources).
- administration simplifiée de l'ensemble des serveurs.
- réduction de la facture d'électricité, en diminuant le nombre de serveurs physiques.
- accélération des déploiements de systèmes et d'applications en entreprise.

Introduction et généralités

Inconvénients de la virtualisation :

- coût de mise en œuvre important : pour faire fonctionner convenablement une architecture virtualisée, l'entreprise doit investir dans un serveur physique disposant de plusieurs processeurs et de beaucoup de mémoire.
- pannes généralisées : si le serveur physique tombe en panne, les machines virtuelles tombent également en panne.
- vulnérabilité généralisée : si l'hyperviseur est exposé à une faille de sécurité, les machines virtuelles peuvent l'être également et ne sont donc plus protégées. De plus, la virtualisation, en augmentant les couches logicielles, a pour conséquence d'augmenter la surface d'attaque de l'entreprise.

Introduction et généralités

Il existe plusieurs manières de faire de la virtualisation :

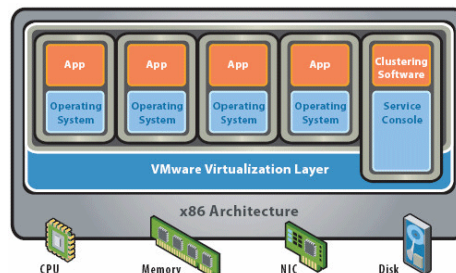
1. L'hyperviseur de type 1

L'hyperviseur de type 1 est un outil qui s'interpose entre la couche matérielle et logicielle. Celui-ci a accès aux composants de la machine et possède son propre noyau.

C'est donc par dessus ce noyau que les OS seront installés. Il pilote donc les OS à partir de la couche matérielle, il s'administre via une interface de gestion des machines virtuelles.

Exemples :

- Microsoft Hyper-V
- VmWare vSphere
- XEN



2. L'hyperviseur de type 2

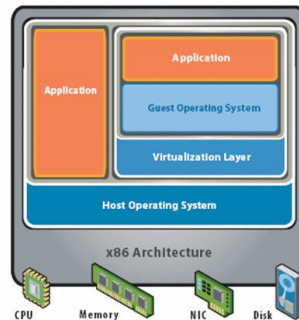
L'hyperviseur de type 2 (ou architecture hébergée) est une application installée sur un système d'exploitation, elle est donc dépendante de celui-ci.

Les performances sont réduites en comparaison des hyperviseurs de type 1 car l'accès au matériel (CPU, RAM...) se fait via une couche intermédiaire.

Néanmoins il propose une parfaite étanchéité entre les systèmes d'exploitations installés.

Exemples :

- VirtualBox
- VmWare Workstation



c) Le Cloud Computing

Qu'est-ce que le cloud computing ?

Le **cloud computing** consiste à utiliser des ressources informatiques (matérielles et logicielles) sous forme de service sur un réseau. Une société utilise le matériel et les logiciels dans le cloud moyennant des frais de service.

Les ordinateurs locaux n'ont plus à effectuer de tâches complexes lorsqu'il s'agit d'exécuter des applications réseau. Les ordinateurs en réseau qui constituent le cloud s'en chargent.

→ Le matériel et les logiciels requis par l'utilisateur sont donc réduits.

L'ordinateur de l'utilisateur doit interagir avec le cloud grâce à un logiciel, comme un navigateur Web, et le réseau du cloud se charge du reste.

Le cloud computing est également une tendance globale qui fait évoluer l'accès aux données et leur stockage.

Le cloud computing nous permet de stocker des fichiers personnels, voire de sauvegarder tout le contenu d'un disque dur sur des serveurs via Internet.

Introduction et généralités

Les opérations bancaires en ligne, les magasins en ligne et les sites de téléchargement de musique sont des exemples courants de cloud computing. Les utilisateurs accèdent aux applications du cloud via un navigateur Web.

→ Aucun logiciel supplémentaire n'est nécessaire sur leurs ordinateurs.

→ Cela permet à de nombreux types de périphérique d'accéder au Cloud.

Au niveau des types de cloud, on peut en distinguer 4 différents :

- Cloud personnalisé - Ce sont des clouds conçus pour répondre aux besoins d'un secteur spécifique, tels que la santé, les administrations ou les médias. Les clouds personnalisés peuvent être privés ou publics.

- Cloud public - Les applications et les services proposés par un cloud public sont accessibles par tous. Les services peuvent être gratuits ou payants en fonction de l'utilisation, par exemple en fonction de la quantité de stockage utilisée. Le cloud public utilise Internet pour fournir des services.



iCloud



Dropbox



Introduction et généralités

- Cloud privé - Les applications et les services proposés par un cloud privé sont destinés à une entreprise ou une entité spécifique, comme un gouvernement.

Un cloud privé peut être configuré via le réseau privé d'une entreprise. Cette fonctionnalité peut cependant être chère à mettre en place et à prendre en charge.

Un cloud privé peut également être géré par une entreprise externe par le biais d'une stratégie de sécurité d'accès très stricte.



Windows® Azure™



- Cloud hybride - Un cloud hybride comprend au moins deux clouds (par exemple, un cloud personnalisé et un cloud public).

Ces clouds restent indépendants, mais sont connectés au sein d'une architecture unique. Les utilisateurs d'un cloud hybride peuvent avoir différentes autorisations d'accès aux divers services, en fonction de droits d'accès utilisateur.



Avantages du cloud computing :

- **Flexibilité organisationnelle** – les utilisateurs peuvent accéder aux informations à tout moment et partout via un navigateur Web.
- **Réactivité et rapidité de déploiement** – le service informatique peut se concentrer sur la fourniture d'outils pour extraire, analyser et partager les informations provenant de bases de données, de fichiers, et de données utilisateur.
- **Coûts d'infrastructure réduits** – l'infrastructure technologique, précédemment sur site, est gérée par le fournisseur de services cloud : les coûts liés au matériel et aux applications sont nuls et cette économie réalisée peut être réaffectée à d'autres secteurs de l'entreprise.
- **Création de nouveaux business models** – les applications et les ressources sont facilement accessibles. Les entreprises peuvent donc réagir rapidement aux besoins des clients. Elles peuvent ainsi développer des stratégies pour promouvoir l'innovation tout en pénétrant de nouveaux marchés.

d) Le communication en ligne

Les utilisateurs individuels souhaitent se connecter au réseau pour accéder aux applications de données, mais aussi pour collaborer les uns avec les autres.

La collaboration est définie comme « le fait de travailler avec une ou plusieurs autres personnes sur un projet commun ».

Les outils de collaboration sont nombreux et ils donnent la possibilité aux employés, aux étudiants, aux enseignants, aux clients et aux partenaires un moyen de se connecter, d'interagir et d'atteindre leurs objectifs instantanément.



Introduction et généralités

e) Le CPL

Qu'est-ce que le CPL ?

La communication par **courants porteurs en ligne (CPL)** permet de construire un réseau informatique sur le réseau électrique d'une habitation ou d'un bureau.

Le concept « pas de nouveaux câbles » repose sur la possibilité de connecter un périphérique au réseau grâce à n'importe quelle prise électrique.

Cela permet d'éliminer les coûts d'installation de câbles de données, sans coûts supplémentaires sur la facture d'électricité.

Grâce au câblage électrique, le réseau sur courant électrique transmet des informations en envoyant les données sur des fréquences spécifiques, tout comme la technologie utilisée pour la DSL.

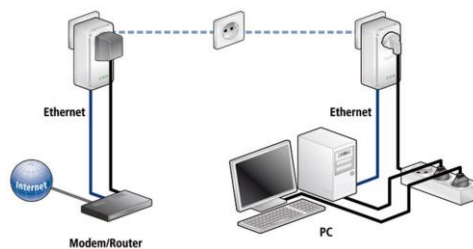


Introduction et généralités

Fonctionnement :

À l'aide d'un adaptateur HomePlug standard, les périphériques peuvent se connecter au LAN en utilisant n'importe quelle prise de courant.

Le réseau sur courant électrique est particulièrement utile lorsque les points d'accès sans fil ne peuvent pas être utilisés ou ne peuvent pas couvrir tous les périphériques d'un domicile.



Le réseau sur courant électrique n'est pas conçu pour remplacer les câblages dédiés aux réseaux de données. Cependant, c'est une alternative viable lorsque les câbles ou les communications sans fil du réseau de données ne sont pas utilisables.