



Support de cours TE1

SOMMAIRE

Définition d'un réseau	2
Les topologies	4
Les différents types de réseaux	7
L'architecture Client / Serveur	8
L'architecture poste à poste, d'égal à égal	10
VPN	11
Intranet et Extranet.....	14
Glossaire	16

1. Définition d'un réseau

« Répartition des éléments d'une organisation en différents points »

Un réseau est un **ensemble d'objets interconnectés les uns avec les autres**. Il permet de faire **circuler des éléments** entre chacun de ces objets selon **des règles bien définies**.

ENSEMBLE D'OBJETS
INTERCONNECTÉS
+
CIRCULATION D'ÉLÉMENTS
+
RÈGLES BIEN DÉFINIES

- **Réseau (Network) :** Ensemble des ordinateurs et périphériques connectés les uns aux autres. (Remarque : deux ordinateurs connectés constituent déjà un réseau).
- **Mise en réseau (Networking) :** Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources

Un réseau informatique est un **ensemble d'ordinateurs reliés entre eux** grâce à **des lignes physiques** et **échangeant des informations** sous forme de données numériques (=binaire).

Valeurs possible avec le **binaire** : 0 et 1 ; Valeurs possible avec un **signal analogique** : infinies.

1.1 Exemples concrets

- **Entreprise :** Serveur d'impression et PC d'une entreprise
Objets reliés entre eux : PC & Imprimante
Données : Binaires
Règles établies : Protocole TCP/IP
- **Télé-réseau :** Cablecom diffuse les chaînes à ses abonnés
Objets reliés entre eux : Télévisions
Données : Analogiques
Règles établies : Télé-réseau
- **Téléphonie :** Swisscom fournit à ses abonnés le réseau
Objets reliés entre eux : Téléphoness
Données : Analogique
Règles établies : GSM

1.2 Homogène – hétérogène

Ces considérations sont liées au matériel

- **Homogène :** Tous les ordinateurs reliés sont issus du **même** constructeur. Exemple : Protocole Apple-talk
- **Hétérogène :** Les ordinateurs reliés au réseau sont de constructeurs **divers**. Exemple : Protocole Ethernet.

Notez que plus le réseau est homogène plus il sera facile à installer et à maintenir aussi bien au niveau logiciel que matériel.

1.3 Intérêt d'un réseau

Un réseau permet

- Le **partage de fichiers, d'applications et de ressources**
- La **communication** entre **personnes**
courriers électroniques, messageries instantanées, ...
- La **communication** entre **processus**
machines industrielles
- La **garantie de l'unicité de l'information**; pour avoir les mêmes données partout
base de données
- Le **jeu à plusieurs**

Un réseau permet aussi de **standardiser les applications**, on appelle généralement cette pratique le *groupware*. Par exemple pour les mails ou les agendas de groupes (Microsoft Schedule +) qui permettent de communiquer plus efficacement et rapidement. Avantages :

- **Diminution des coûts**
partages des données et des périphériques ; exemple : une seule imprimante pour plusieurs personnes
- **Standardisation des applications**
même version
- **Accès aux données en temps utile**
- Communication et **organisation plus efficace**

L'organisation est effectivement plus efficace alors que pour la communication, elle n'est pas significativement améliorée. **Trop d'informations** arrivent généralement **pour le même utilisateur**. Par exemple pour le spam dans les mails, une personne va passer énormément de temps à trier et à lire les centaines de mail qu'elle peut recevoir par jour pour trier ceux qui sont utiles ou non.

1.4 Les similitudes des différents réseaux

Éléments constitutants :

- **Serveurs** : Ordinateurs qui **fournissent des ressources** partagées aux utilisateurs par un serveur de réseau
- **Clients** : Ordinateurs qui **accèdent aux ressources** partagées fournies par un serveur de réseau
- **Support de connexion** : Conditionne **la façon dont les ordinateurs sont reliés** entre eux.
Exemple : Câbles, modems, ...
- **Données partagées** : Fichiers accessibles sur les serveurs du réseau
- Imprimantes et autres périphérique partagés : autres ressources fournies par le serveur

1.5 Type de réseaux

- Réseaux **poste à poste** (Peer to peer / égal à égal) :
Il n'y a pas de serveur dédié, chaque ordinateur dans un tel réseau est un peu serveur et un peu client.
- Réseaux organisés **autour de serveur** (Architecture client serveur) :
Des machines clientes (faisant parties du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, ...)

Ces deux types de réseaux ont des capacités **différentes**. Le type de réseau à installer dépend des **critères** suivants :

- **Taille de l'entreprise**
- Niveau de **sécurité nécessaire**
- Type d'**activité**
- Niveau de **compétence d'administration possible**
Combien de personnes dédiées, Quid de leur formation ?
- **Volume du trafic** sur le réseau
- **Besoins des utilisateurs** du réseau
- **Budget alloué** au fonctionnement du réseau
Pas seulement à **l'achat** mais aussi à **l'entretien** et la **maintenance**

» Architectures P2P ou client/serveur voir page 8

2. Les topologies

2.1 Définition

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).

L'arrangement physique de ces éléments est appelé topologie physique. Il en existe trois

- La topologie **en bus**
- La topologie **en étoile**
- La topologie **en anneau**

On distingue la **topologie physique** (la **configuration spatiale (=visible) du réseau**) de la topologie logique. La topologie logique représente la **façon dont les données transitent dans les câbles**. Les topologies logiques les plus courantes sont **Ethernet, Token Ring et FDDI** (voir fin page 5 pour en savoir plus)

2.2 Topologies physiques

2.2.1 Topologies en bus

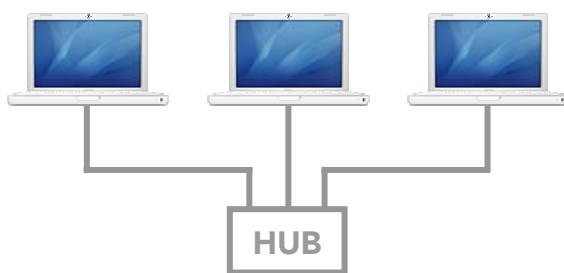
Une **topologie en bus** est l'**organisation la plus simple d'un réseau**. En effet, dans une topologie en bus, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble généralement coaxial. **Le mot « bus » désigne la ligne physique qui relie les machines du réseau**



Cette topologie a pour avantage **d'être facile à mettre en œuvre** et de fonctionner facilement, par contre, elle en est **extrêmement vulnérable** étant donné que **si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté**.

Aujourd'hui, on ne crée plus de réseau en topologie en bus

2.2.2 Topologie en étoile



Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un **système matériel appelé hub ou concentrateur**. Il s'agit d'une boîte contenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. **Celle-ci a pour rôle d'assurer la communication entre les différentes jonctions**.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont **beaucoup moins vulnérables car on peut aisément retirer une des connexions** en la débranchant du concentrateur **sans pour autant paralyser le reste du réseau**. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub)

Actuellement, c'est la **topologie la plus utilisée**. Elle est aussi **évolutive** car on peut **très rapidement ajouter un nouveau nœud au réseau**.

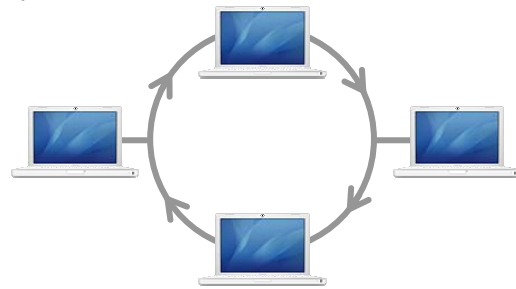
2.2.3 Topologie en anneau

Dans un réseau en **topologie en anneau**, les ordinateurs communiquent chacun à leur tour, on a donc **une boucle d'ordinateur sur laquelle chacun d'entre-eux va « avoir la parole » successivement.**

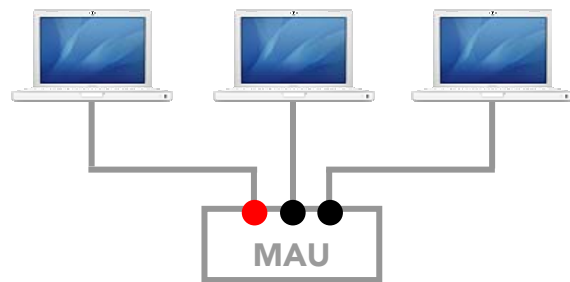
En réalité, les ordinateurs d'un réseau en topologie en anneau **ne sont pas reliés en boucle**, mais sont **reliés à un répartiteur** (appelé **MAU, Multistation Access Unit**) qui va gérer la communication entre les ordinateurs qui lui sont **reliés en impartissant à chacun d'entre-eux un temps de parole.**

Les deux principales topologies logiques utilisant cette topologie physique sont **Token Ring** (anneau à jeton) et **FDDI**.

Topologie logique



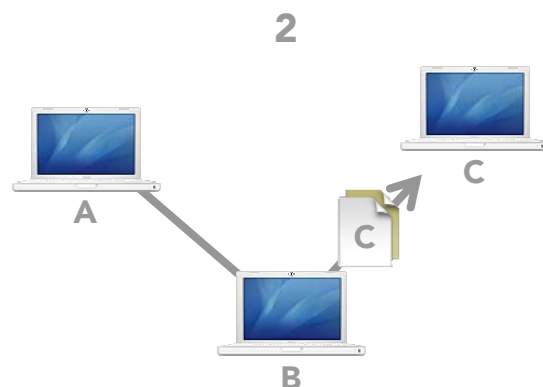
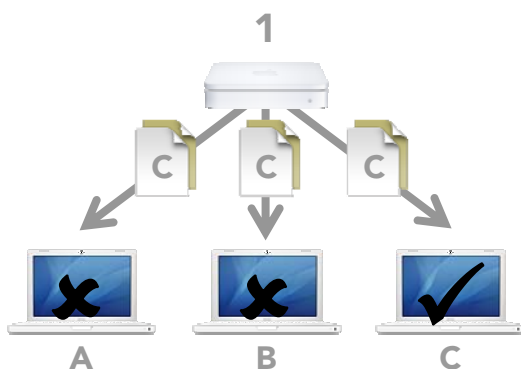
Topologie physique



2.2.4 Schéma des différentes topologies

» Se référer au support de cours page 7

1. Réseau en mode de diffusion Partage d'un même support de transmission. Chaque message envoyé sur le réseau est reçu par chacun des nœuds y étant connecté. L'adresse spécifique placée dans le message permettra à chaque récepteur de savoir si le message lui est adressé ou non
2. Mode point à point : Le support physique relie une paire d'équipement. Lorsque deux équipements non directement connectés veulent communiquer entre eux, ils le font par l'intermédiaire d'autres nœuds.



2.3 Topologie logiques

La façon de laquelle les données transitent dans les câbles (= code de la route)

2.3.1 Ethernet

Ethernet, aussi connu sous le nom de norme **IEEE 802.3**) est une technologie de réseau local basé sur le principe suivant :

« Toutes les machines du réseau Ethernet sont connectées à une même ligne de communication constituée de câble cylindriques »

Technologie	Type de câble	Vitesse	Portée
10Base-2	Câble coaxial de faible diamètre	10Mb/s	185m
10Base-5	Câble coaxial de gros diamètre (0,4 inch)	10Mb/s	500m
10Base-T	Double paire torsadée	10Mb/s	100m
100Base-TX	Double paire torsadée	100Mb/s	100m
1000Base-SX	Fibre optique	1000Mb/s	500m

Ethernet est une technologie de réseau très utilisée car le prix de revient d'un tel réseau n'est pas très élevé

2.3.1.1 Principe de transmission

Tous les ordinateurs d'un réseau Ethernet **sont reliés à une même ligne de transmission**, et la communication se fait à l'aide d'un **protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect)** ce qui signifie qu'il s'agit d'un protocole d'accès multiple avec surveillance de porteur (Carrier Sense) et détection de collision).

Avec ce protocole toute machine est autorisée à émettre sur la ligne à n'importe quel moment et sans notion de priorité entre les machines. Cette communication se fait de façon simple :

- **Chaque machine** vérifie qu'il n'y a **aucune communication sur la ligne** avant d'émettre
- **Si deux machines émettent simultanément**, alors il y a **collision** (c'est-à-dire que plusieurs trames de données se trouvent sur la ligne au même moment)
- **Les deux machines interrompent leur communication** et attendent un **délai aléatoire**, puis la première ayant passé ce délai peut alors réémettre

Ce principe est basé sur plusieurs **contraintes** :

- Les **paquets** de données **doivent** avoir une **taille maximale**
- Il doit y avoir un **temps d'attente entre deux transmissions**

Le temps d'attente varie selon la fréquence des collisions

- Après la **première** collision, une machine attend **une unité de temps**
- Après la **seconde** collision, la machine attend **deux unités de temps**
- Après la **troisième** collision, la machine attend **quatre unités de temps**

2.3.2 L'anneau à jeton / Token Ring

L'anneau à jeton (en anglais Token Ring) est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour, c'est-à-dire que chaque ordinateur du réseau a la possibilité de parler à son tour. C'est un jeton (un paquet de données), circulant en boucle d'un ordinateur à un autre qui détermine quel ordinateur aura le droit d'émettre des informations.

Lorsqu'un ordinateur est en possession du jeton, il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.

En réalité, les ordinateurs d'un réseau de type « anneau à jeton » ne sont pas disposés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va donner successivement « la parole » à chacun d'entre eux.

» Se référer à la page 5

2.3.3 La technologie LAN FDDI

La technologie **LAN FDDI (Fiber Distributed Data Interface)** est une technologie d'accès au réseau sur des lignes type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit « **primaire** », l'autre, permettant de rattraper les erreurs du premier, est dit « **secondaire** »). Le FDDI est un anneau à jeton **à détection et correction d'erreurs** (c'est là que l'anneau secondaire prend son importance).

Le jeton circule entre les machines à une vitesse **très élevée**. Si celui-ci **n'arrive pas au bout d'un certain délai**, la machine considère **qu'il y a eu une erreur sur le réseau**.

La topologie **FDDI ressemble de près à celle de Token Ring** à la différence près qu'un ordinateur faisant partie d'un réseau FDDI peut aussi être relié à un concentrateur MAU d'un second réseau. On parle alors de réseau **bi connecté**.

3. Les différents types de réseaux

Il y a plusieurs moyens de distinguer les différents types de réseaux et de les classer

On peut distinguer différents types de réseaux (privés) selon leur taille (en terme de nombre de machine), leur vitesse de transfert de données ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On fait généralement trois catégories de réseaux :

NOMBRE DE MACHINE
+
VITESSE DE TRANSFERT
(BANDE PASSANTE)
+
SURFACE GÉOGRAPHIQUE

- **LAN** (Local Area Network)
- **MAN** (Metropolitan Area Network)
- **WAN** (Wide Area Network)

Il existe trois autres types de réseaux :

- **TAN** (Tiny Area Network), identiques aux LAN mais en moins étendu (2-3 machines)
- **CAN** (Campus Area Network), identiques aux MAN (avec une bande passante maximale entre tous les LAN du réseau)
- **GAN** (Global Area Network), WAN sans restriction spatiale ou géographique (= Internet)

On peut se contenter de la taille physique pour les classer, ou mettre l'accent sur leur disposition au sein d'un ou des bâtiments d'une organisation humaine liée à son exploitation.

Il n'y a pas de normalisation au niveau de la classification de ces réseaux, de ce fait, plusieurs interprétations existent

Exemple de classification en fonction de la taille, on voit ici que la notion de réseau informatique dispose d'un sens élargi. Cette classification se fait généralement dans les hautes écoles supérieures et les polytechniques

3.1 LAN ≈ TAN

LAN signifie **Local Area Network** (en français **Réseau Local**). Il s'agit d'un **ensemble d'ordinateurs** appartenant à **une même organisation** et reliés entre eux dans une **petite aire géographique** par un réseau, souvent à l'aide **d'une même technologie** (la **plus répandue** étant **Ethernet**).

Un réseau local est donc un réseau sous sa forme **la plus simple**. La vitesse de transfert de donnée d'un réseau local peut s'échelonner **entre 10 Mbps** (pour un réseau **Ethernet** par exemple) **et 1 Gbps** (en **FDDI** ou **Gigabit Ethernet** par exemple). La taille d'un réseau local peut atteindre jusqu'à **100** voir **1000 utilisateurs**.

3.2 MAN ≈ CAN

Les **MAN (Metropolitan Area Network)** interconnectent **plusieurs LAN** de **façon transparente** et **géographiquement proches** (au maximum **quelques dizaines de km**) à des **débits importants**. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

Un MAN est **formé de commutateurs ou de routeurs interconnectés par des liens hauts débits** (en général **en fibre optique**).

Les MAN sont automatiquement des WAN, mais tous les WAN ne sont pas des MAN.

Exemple de MAN : les différentes sections du CPNV.

3.3 WAN \approx GAN

Un WAN (**Wide Area Network** ou **réseau étendu**) interconnecte plusieurs LANs à **travers de grandes distances géographiques**.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et **peuvent être faibles**.

Les **WAN fonctionnent grâce à des routeurs** qui permettent de « choisir » le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet, qui est également un GAN (Global Area Network)

4. L'architecture Client / Serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que **des machines clientes** (des machines faisant partie du réseau) contactent **un serveur**, une machine généralement **très puissante** en termes de capacités d'entrée-sortie, qui leur **fournit des services**. Ces **services sont des programmes** fournissant des données telles que l'heure, des fichiers, une connexion, etc.

Les **services sont exploités** par des programmes, appelés **programmes clients**, **s'exécutant sur les machines clientes**. On parle ainsi de **client FTP**, **client de messagerie**, ..., lorsqu'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP, il s'agit de fichier, tandis que pour le client messenger, il s'agit de courrier électronique).

Dans un environnement purement client/serveur, les ordinateurs du réseau (les clients) **ne peuvent voir que le serveur**, c'est l'un des **principaux atouts** de ce modèle.

4.1 Avantages de l'architecture client/serveur

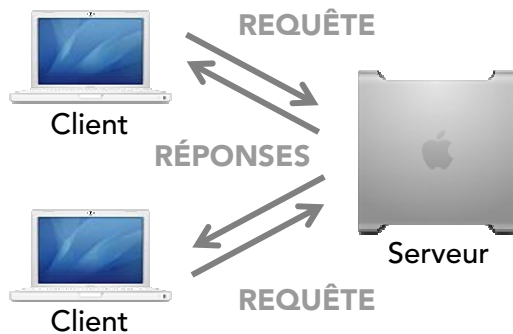
Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- Des ressources centralisés
étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de donnée centralisée, afin d'éviter les programmes de redondances et de contradiction
- Une meilleure sécurité
car le nombre de points d'entrée permettant l'accès aux données est moins important
- Une administration au niveau serveur
les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés
- Un réseau évolutif
grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures

4.2 Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- Un cout élevé
dû à la technicité du serveur (bien plus puissant qu'une machine de bureau)
- Un maillon faible
le serveur est le seul maillon faible du réseau client/serveur étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID)



4.3 Fonctionnement d'un système client serveur

- Le client émet une requête vers le serveur grâce à son adresse et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

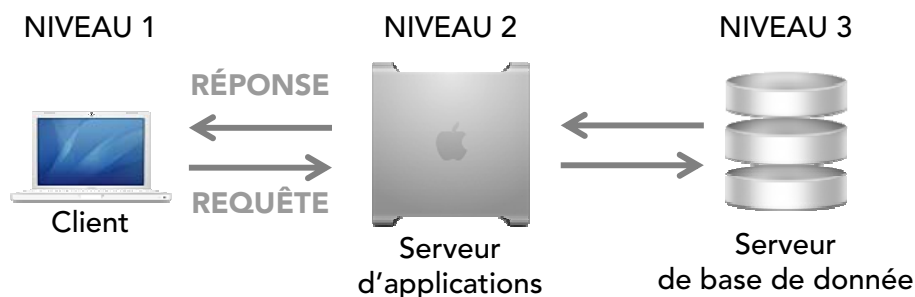
4.4 Architecture à deux niveaux

L'architecture à deux niveaux (aussi appelée *architecture 2-tiers*, tiers signifiant *tierce partie*) caractérise les **systèmes clients/serveurs** dans lesquels **le client demande une ressource** et le **serveur la lui fournit directement**. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir le service.

4.5 Architecture à trois niveaux

Dans l'architecture à trois niveaux (appelée *architecture 3-tiers*), il existe un **niveau intermédiaire**, c'est-à-dire que l'on a généralement une architecture partagée entre :

1. Le client : le demandeur de ressources
2. Le serveur **d'application** (appelé aussi **middleware**) : **le serveur chargé de fournir la ressource** (donc pas de changement à ce niveau là) mais **en faisant appel à un autre serveur**. Le serveur intermédiaire est donc déchargé par le(s) serveur(s) secondaires.
3. Le serveur secondaire (généralement un serveur de base de données), fournissant un service au premier serveur.



Attention : Étant donné l'emploi massif du terme d'architecture à 3 niveaux, celui-ci peut parfois désigner aussi les architectures suivantes :

- Partage d'application entre client, serveur intermédiaire, et serveur d'entreprise
- Partage d'application entre client, base de données intermédiaire, et base de données d'entreprise

4.6 Comparaison entre les deux types d'architecture

L'architecture à deux niveaux est donc une architecture client/serveur dans laquelle le serveur est polyvalent, c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client. Dans l'architecture à trois niveaux, par contre, les applications au niveau serveur sont délocalisées, c'est-à-dire que chaque serveur est spécialisée dans une tâche (serveur web, de base de données, de messagerie, etc.). Ainsi, l'architecture à trois niveaux permet :

- **Une plus grande flexibilité/souplesse**
- **Une plus grande sécurité** (la sécurité peut être définie pour chaque service)
- **De meilleures performances** (les tâches sont partagées) parce que les serveurs sont spécialement conçus pour des tâches bien spécifiques.

4.7 L'architecture multi-niveaux

Dans l'architecture à 3 niveaux, chaque serveur effectue une tâche (un service) spécialisée. Ainsi, un serveur peut utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service. Par conséquent, l'architecture à trois niveaux est potentiellement une architecture à N niveaux.

5. L'architecture poste à poste, d'égal à égal

Dans **une architecture d'égal à égal** (où dans sa dénomination anglaise peer to peer), contrairement à une architecture de réseau de type client/serveur, il n'y a **pas de serveur dédié**. Ainsi, chaque ordinateur dans un tel réseau **est un peu serveur et un peu client**. Cela signifie que **chacun des ordinateurs du réseau est libre de partager ses ressources**.

Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau

5.1 Inconvénients des réseaux d'égal à égal

Les réseaux d'égal à égal ont énormément d'inconvénients :

- Ce système **n'est pas du tout centralisé**, ce qui le **rend très difficile à administrer**
- La sécurité est très peu présente
- **Aucun maillon** du système **n'est fiable**

Ainsi, les réseaux d'égal à égal ne sont valables que pour **un petit nombre d'ordinateurs** (généralement une **dizaine**), et pour des applications **ne nécessitant pas une grande sécurité** (il est donc **déconseillé pour un réseau professionnel** avec des données sensibles).

5.2 Avantages de l'architecture d'égal à égal

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- Un **coût réduit** (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance)
- Une **simplicité** à toute épreuve

5.3 Mise en œuvre d'un réseau peer to peer

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés. On peut donc utiliser Windows NT Workstation, Windows pour Workgroups ou Windows 95 car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :

- Placer les ordinateurs sur le bureau des utilisateurs

- **Chaque utilisateur** est son propre **administrateur** et planifie lui-même sa sécurité (=sécurité médiocre)
- Pour les connexions, on utilise **un système de câblage simple et apparent**

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- **Moins de 10 utilisateurs**
- Tous les utilisateurs se situent dans la **même zone géographique**
- **La sécurité n'est pas un problème**
- **Ni l'entreprise, ni le réseau ne sont susceptibles d'évoluer** de manière significative dans un proche avenir

5.4 Administration d'un réseau poste à poste

Le réseau poste à poste répond aux besoins d'une petite entreprise mais peut s'avérer inadéquat dans certains environnements. Voici les questions à résoudre avant de choisir le type de réseau : On désigne par le terme « Administration » :

4. Gestion des utilisateurs et de la sécurité
5. Mise à disposition des ressources
6. Maintenance des applications et des données
7. Installation et mise à niveau des logiciels utilisateurs

Dans un réseau poste à poste typique, il n'y a pas d'administrateur, Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax, etc.)

5.4.1 Notions de sécurité

La politique de sécurité minimale consiste à mettre un mot de passe à une ressource. Les utilisateurs d'un réseau poste à poste définissent leur propre sécurité et comme tous les partages peuvent exister sur tous les ordinateurs, il est difficile de mettre en œuvre un contrôle centralisé. Ceci pose également un problème de sécurité globale du réseau car certains utilisateurs ne sécurisent pas du tout leurs ressources.

6. VPN

Les réseaux locaux d'entreprise (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. **Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipement d'interconnexion.** Il arrive ainsi souvent que **des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignés via Internet.**

Pour autant, **les données transmises sur Internet sont beaucoup plus vulnérables** que lorsqu'elles circulent sur un réseau interne à une organisation car **le chemin emprunté n'est pas défini à l'avance**, ce qui signifie que **les données empruntent une infrastructure réseau publique appartenant à différents opérateurs.** Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit **écouté** par un utilisateur indiscret ou même **détourné**. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise

La **première solution** pour répondre à ce besoin de **communication sécurisé** consiste à **relier les réseaux** distants à l'aide de **liaisons spécialisées**. Toutefois la plupart des entreprises ne peuvent pas se permettre financièrement de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire **d'utiliser Internet comme support de transmission.**

Un **bon compromis** consiste à **utiliser Internet** comme support de transmission **en utilisant un protocole d'« encapsulation »** (en anglais tunneling, d'où l'utilisation impropre parfois du terme

« tunnelisation »), c'est-à-dire en **encapsulant les données à transmettre de façon chiffrée**. On parle alors de **réseau privé virtuel** (noté **RPV** ou **VPN**, acronyme de **Virtual Private Network**) pour **désigner le réseau ainsi artificiellement créé**.

Ce réseau est **dit virtuel** car il **relie deux réseaux « physiques »** (réseaux locaux) **par une liaison non fiable** (Internet), et **privé** car seuls **les ordinateurs des réseaux locaux de part et d'autres du VPN peuvent « voir » les données**.

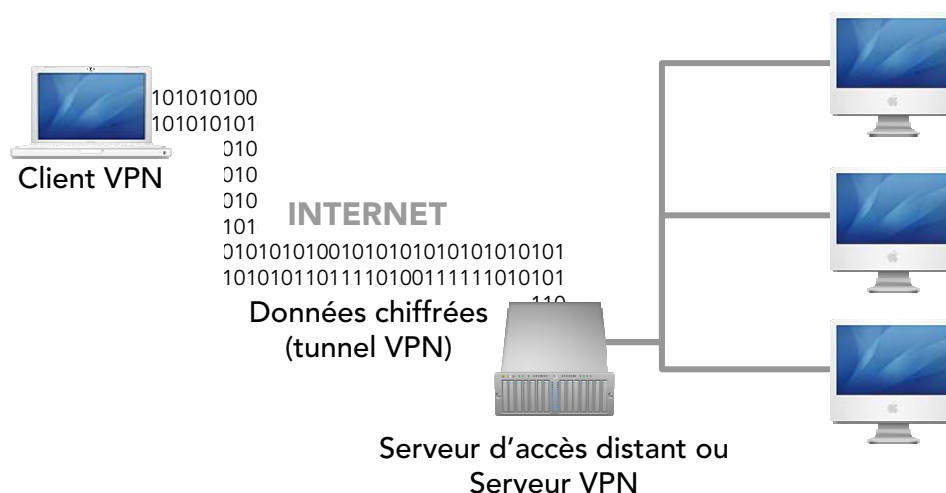
Le système de **VPN permet donc d'obtenir une liaison sécurisée à moindre coût**, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie, il **ne permet pas d'assurer une qualité de service comparable à une ligne louée** dans la mesure où le réseau physique est public et donc non garanti.

6.1 Équipement d'interconnexions

Liste des éléments matériels mis en place dans les réseaux locaux.

- Les répéteurs : permettant de **régénérer un signal**
- Les concentrateurs (hubs) : permettant de **connecter entre eux plusieurs hôtes**
- Les ponts (bridges) permettant de **relier des réseaux locaux de même type**
- Les commutateurs (switches) permettant de **relier divers éléments tout en segmentant le réseau**
- Les passerelles (gateways) : permettant de **relier des réseaux locaux de types différents**
- Les routeurs : permettant de **relier de nombreux réseaux locaux de telles façon à permettre la circulation de données d'un réseau à un autre de façon optimale**
- Les B-routeurs : **associant les fonctionnalités d'un routeur et d'un pont**

6.2 Fonctionnement d'un VPN



Un **réseau privé virtuel** repose sur un **protocole appelé protocole d'encapsulation (tunneling)**, c'est-à-dire un protocole **permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie**

Le **terme de « tunnel »** est utilisé **pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées** (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, **comme si les données passaient dans un tunnel**. Dans le cas d'un VPN établi entre deux machines, on appelle **client VPN** l'élément permettant de **chiffrer et de déchiffrer les données du côté utilisateur** (client) et **serveur VPN** (ou plus généralement serveur d'accès distant) l'élément **chiffrant et déchiffrant les données du côté de l'organisation**.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public¹, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. À réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur...

6.3 Les protocoles de tunnelisation

Les principaux protocoles de tunneling sont les suivant :

- **PPTP (Point-to-point Tunneling Protocol)** est un protocole de **niveau 2** développés par **Microsoft, 3Com, Ascend, US Robotics** et **ECI Telematics**.
- **L2F (Layer Two Forwarding)** est un protocole de **niveau 2** développés par **Cisco, Northern Telecom** et **Shiva**. Il est désormais **quasi-obsolète**
- **L2TP (Layer Two Tunneling Protocol)** est l'aboutissement des travaux de **l'IETF (RFC 2661)** pour faire **converger les fonctionnalités de PPTP et L2F**. Il s'agit ainsi d'un protocole de **niveau 2 s'appuyant sur PPP**.
- **IPSec** est un protocole de **niveau 3** issu des travaux de **l'IETF** permettant de transporter des données chiffrées pour les réseaux IP

6.4 Le protocole PPTP

Le principe du protocole **PPTP (Point-To-Point Tunneling Protocol)** est de créer des paquets sous le protocole PPP et des les encapsuler dans un datagramme IP.

Ainsi, dans ce mode de connexion, **les machines distantes des deux réseaux locaux sont connectés par une connexion point à point** comprenant un **système de chiffrement et d'authentification**, et le **paquet transite au sein d'un datagramme IP**.

De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP qui est lui-même encapsulé dans un message IP.



6.5 Le protocole IPSec

IPSec est un protocole défini par **l'IETF** permettant de **sécuriser les échanges au niveau de la couche réseau**. Il s'agit en fait d'un **protocole apportant des améliorations au niveau de la sécurité au protocole IP** afin de **garantir la confidentialité, l'intégrité et l'authentification des échanges**.

Le protocole IPSec est basé sur trois modules :

- *IP Authentication Header (AH)* concernant l'intégrité et la confidentialité des paquets à encapsuler
- *Encapsulating Security Payload (ESP)* définissant le chiffrement de paquets
- *Security Association (SA)* définissant l'échange des clés et des paramètres de sécurité

¹ Internet par exemple.

7. Intranet et Extranet

7.1 L'intranet

Un **intranet** est un **ensemble de services Internet** (par exemple un serveur web) **interne à un réseau local**, c'est-à-dire **accessible uniquement à partir des postes d'un réseau local** ou bien d'un ensemble de réseaux bien définis et **invisible de l'extérieur**. Il consiste à **utiliser les standards client-serveur de l'Internet** (en utilisant les protocoles TCP/IP), comme par exemple l'utilisation de navigateurs Internet (client basé sur le protocole http) et des serveurs web (protocoles http), **pour réaliser un système d'information interne à une organisation ou une entreprise**.

Un intranet **repose généralement** sur une **architecture à trois niveaux**, composée :

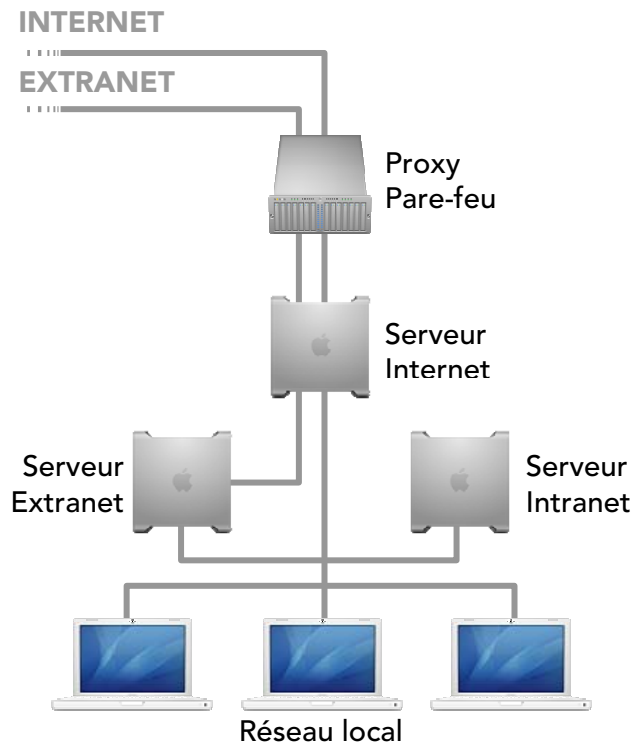
- De **clients** (navigateur Internet généralement)
- D'un ou plusieurs **serveurs d'application (middleware)** : un **serveur web** permettant d'interpréter des scripts CGI, PHP, ASP ou autres, et les traduire en requêtes SQL afin d'interroger une base de données
- D'un **serveur de bases de données**

De cette façon, les machines clientes gèrent l'interface graphique, tandis que le serveur manipule les données. Le réseau permet de véhiculer les requêtes et les réponses

Un intranet possède naturellement plusieurs clients (les ordinateurs du réseau local) et peut aussi être composé de plusieurs serveurs. Une grande entreprise peut par exemple posséder un serveur web pour chaque service afin de fournir un intranet composé d'un serveur web fédérateur liant les différents serveurs gérés par chaque service.

7.1.1 L'utilité d'un intranet

Un intranet dans une entreprise permet de mettre facilement à la disposition des employés des documents divers et variés ; cela permet d'avoir un accès centralisé et cohérent à la mémoire de l'entreprise, on parle ainsi de capitalisation de connaissances. De cette façon, il est généralement nécessaire de définir des droits d'accès pour les utilisateurs de l'intranet aux documents présent sur celui-ci, et par conséquent une authentification de ceux-ci afin de leur permettre un accès personnalisé à certains documents.



Des documents de tous types (textes, images, vidéos, sons, ...) peuvent être mis à disposition sur un intranet. De plus, un intranet peut réaliser une fonction de « groupware » très intéressante, c'est-à-dire permettre un travail coopératif. Voici quelques unes des fonctions qu'un intranet peut réaliser :

- Mise à disposition d'informations sur l'entreprise (panneau d'affichage)
- Mise à disposition de documents techniques
- Moteurs de recherche de documentations
- Un échange de données entre collaborateurs
- Un annuaire du personnel
- Gestion de projets, aide à la décision, agenda, ingénierie assistée par ordinateur
- Messagerie électronique
- Forum de discussion, listes de diffusions, chat en direct
- Visio conférence
- Portail vers Internet

De cette façon, un intranet favorise la communication au sein de l'entreprise et limite les erreurs dues à la mauvaise circulation d'une information. L'information disponible sur l'intranet doit être mise à jour en évitant les conflits de version.

7.1.2 Avantages d'un intranet

Un intranet permet de constituer un système d'information à faible coût (concrètement le coût d'un intranet peut très bien se réduire au coût du matériel, de son entretien et de sa mise à jour, avec des postes clients fonctionnant avec des navigateurs gratuits, un serveur fonctionnant sous *Linux* avec le serveur web *Apache* et le serveur de base de données *MySQL*).

D'autre part, étant donné la nature « universelle » des moyens mis en jeu, n'importe quel type de machine peut être connecté au réseau local, donc à l'intranet

7.1.3 Mise en place d'un intranet

Un intranet doit être conçu selon les besoins de l'entreprise ou de l'organisation (au niveau des services à mettre en place). Pour ce qui est de la mise en place matérielle, il suffit de mettre en place un serveur web (par exemple une machine fonctionnant sous *Linux* avec le serveur web *Apache* et le serveur de bases de données *MySQL* ou bien *Windows NT* et le serveur *Microsoft Internet Information Server*).

Il suffit ensuite de configurer un nom de domaine pour votre machine. Par exemple *intranet.votre_entreprise.com*, ainsi que d'installer TCP/IP sur toutes les machines clientes et de leur définir une adresse IP.

7.2 Extranet

Un **Extranet** est une **extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau**

L'accès à l'extranet doit être sécurisé dans la mesure où il **offre un accès au système d'information à des personnes situées en dehors de l'entreprise**. Il peut s'agir soit d'une **authentification simple** (authentification **par nom d'utilisateur et mot de passe**) ou d'une **authentification forte** (authentification **à l'aide d'un certificat**). Il est conseillé d'utiliser **HTTPS** pour toutes les pages web consultées depuis l'extérieur.

De cette façon, un **extranet n'est ni un intranet, ni un site Internet**, il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales, un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface web.

8. Glossaire

- Nœud	Élément (périphériques) d'un réseau. Exemples : scanner, imprimante, NAS)
- MAU	Multistation Access Unit, répartiteur dans la topologie en anneau (voir page 5)
- Hub (ou concentrateur)	Boîtier comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenances des ordinateurs du réseau. Il a pour rôle d'assurer la communication entre les différentes jonctions.
- NAS	Network Attached Storage
- Support physique	= Ligne physique
- Transceiver (=adaptateur)	Transforme les signaux du support physique en signaux logiques manipulable par la carte réseau
- Prise	Assure la jonction mécanique entre la carte réseau et le support physique
- IEEE	Institut of Electrical and Electronic Engineer
- FDDI	Fiber Distributed Data Interface
- MAU	Multistation Access Unit
- CSMA/CD	Carrier Sense Multiple Access with Collision Detect
- Routeurs	Dispositifs qui permet de « choisir » le chemin qu'un message va emprunter à travers le réseau
- LS	Lignes spécialisée, lignes « louées »
- Protocole	Méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règle et de procédure à respecter pour émettre et recevoir des données sur un réseau
- RFC	Request For Comments ; Ensemble de documents contenant les spécifications techniques sur divers point de TCP/IP (protocoles, services, ...)
- TAN	Tiny Area Network ; LAN avec 2-3 machines
- CAN	Campus Area Network ; MAN avec une plus grande bande passante
- GAN	Global Area Network ; WAN mais sans limite géographique
- IETF	Internet Engineering Task Force