

Notre magasinRue Albert 1er, 7
6810 Pin - Chiny**Route Arlon -
Florenville**

(/fax: 061/32.00.15

Le cours informatique HARDWARE 2 YBET: Serveurs,
réseaux et communicationsDe la plus petite
à la plus grande,
la gestion
commerciale
SAGE gère
votre entreprise**FORMATIONS**Formations à ChinyCOURS HARDWARE**Le MAGASIN YBET**Activités et présentationRayon d'action**PRODUITS et SERVICES**MATERIEL INFORMATIQUEFacturation, gestion de stock CIEL et
SAGEACCUEILDictionnaire réseauForum informatique
techniqueVente en ligne

2. Introduction aux réseaux informatiques



2.1. Introduction - **2.2. Modèle OSI** - **2.3. Modèle TCP/IP** - **2.4. Types d'ordinateurs connectés** - **2.5. Applications réseaux**
- **2.6. Types de serveurs** - **2.7. Caractéristique d'un réseau** - **2.8. Sécurité et administration**

2.1. Introduction

Avant de nous attaquer aux infrastructures réseaux, reprenons quelques notions de base sur les réseaux informatiques en général.

Un réseau permet de partager des ressources entre plusieurs ordinateurs: données ou périphériques (imprimante, sauvegarde sur bandes, modem, scanner, ...). La première partie de ce cours reprend toutes les informations permettant de connecter ces ordinateurs entre-eux. Comme cette formation informatique est **typiquement hardware**, je ne m'intéresserai principalement qu'à l'aspect matériel. Les autres parties d'un réseau sont repris dans les autres formations de technicien PC/ réseaux, notamment "Base réseau", "Initiation aux systèmes LINUX & UNIX", "Logiciels réseaux", ...

La transmission d'information entre 2 programmes informatiques sur 2 machines différentes passe par deux modèles: le modèle OSI ou le modèle TCP/IP. Ces deux normes permettent à chaque partie de la communication de dialoguer. Chaque modèle inclut plusieurs couches. Chaque couche doit envoyer (et recevoir pour l'autre PC) un message compréhensible par les deux parties, compatibilité des informations. Le chapitre suivant ([base de transmission réseau](#)) traitera de la communication dans ses détails.

2.2. Le modèle OSI

Les autres cours portant sur les réseaux informatiques vous ont parlé des différentes couches du modèle OSI (Open System Interconnection Model). Ce modèle théorique définit en 1977 régit la communication entre 2 systèmes informatiques selon 7 couches. A chaque couche, les 2 systèmes doivent communiquer "compatibles". Rassurez-vous, je ne suis pas un adepte de cette matière de procéder. S'ils sont mentionnés, ils ne font pas réellement partie de la formation "hardware réseau". En hardware nous n'utilisons que les couches inférieures. L'utilisation de Novell Netware, Microsoft Windows NT, Windows 2000, Linux ou tout autre gestionnaire de réseaux) n'intervient pas de manière significative sur l'hardware, à part pour les pilotes.

L'OSI est un modèle de base qui a été défini par l'International Standard Organisation. Cette organisation revient régulièrement pour normalisé différents concepts, tant en électronique qu'en informatique. Ce modèle définit 7 niveaux différents pour le transport de données. Ces niveaux sont également appelés couches.



	⇓	Couche Présentation	6	Couche Présentation	⇑	
	⇓	Couche Session	5	Couche Session	⇑	
Transport des données	⇓	Couche Transport	4	Couche Transport	⇑	
	⇓	Couche Réseau (Network)	3	Couche Réseau (Network)	⇑	Trame
	⇓	Couche liaison de données (Data Link)	2	Couche liaison de données (Data Link)	⇑	Paquet
	⇒	Couche Physique (Physical)	1	Couche Physique (Physical)	⇒	BIT
Support de communication						

Niveau 7: couche application, gère le transfert des informations entre programmes.

Niveau 6: couche présentation, s'occupe de la mise en forme des données, éventuellement de l'en cryptage et de la compression des données, par exemple mise en forme des textes, images et vidéo.

Niveau 5: la couche session, s'occupe de l'établissement, de la gestion et coordination des communications

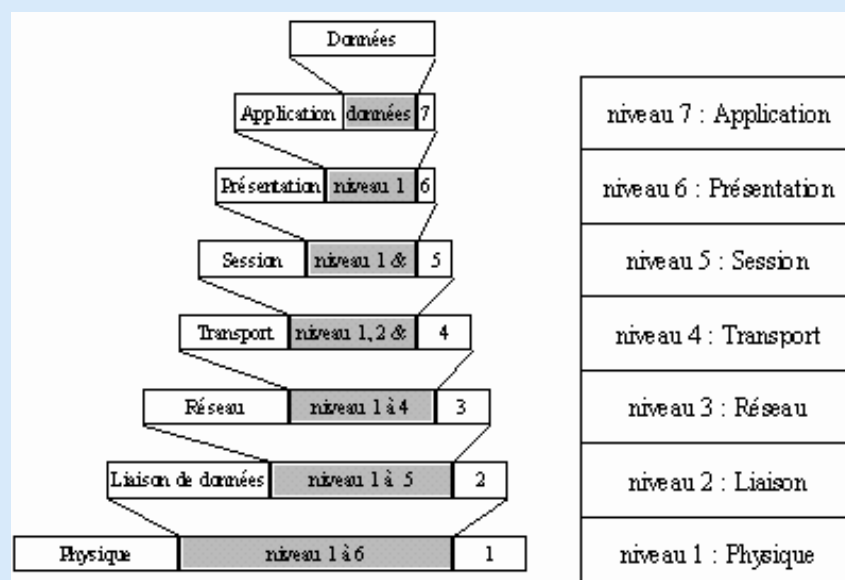
Niveau 4: la couche transport, gère la remise correcte des informations (gestion des erreurs), utilise notamment l'UDP et le TCP/IP

Niveau 3: la couche réseau, détermine les routes de transport et s'occupe du traitement et du transfert de messages: gère IP et ICMP

Niveau 2: la couche liaison de données, définit l'interface avec la carte réseau: hubs, switch, ...

Niveau 1: la couche physique, gère les connections matérielles, définit la façon dont les données sont converties en signaux numériques

A chacun de ces niveaux du modèle OSI, on encapsule un en-tête et une fin de [trame](#) (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole utilisé. Ce [protocole](#) est le langage de communication pour le transfert des données (TCP/IP, NetBui, IPX sont les principaux) sur le réseau informatique. Sur le schéma ci-dessous, la partie qui est rajoutée à chaque niveau est la partie sur fond blanc. La partie sur fond grisé est celle obtenue après encapsulation du niveau précédent. La dernière trame, celle qu'on obtient après avoir encapsulé la couche physique, est celle qui sera envoyée sur le réseau.



Le modèle OSI

En hardware, nous ne nous intéressons qu'aux trois premiers niveaux du modèle OSI (jusqu'aux routeurs et switch de haut de gamme), éventuellement au niveau 4 pour les firewall. Les couches supérieures sont réservées aux autres cours de la formations technicien PC/ Réseaux, notamment base réseau et protocole TCP/IP.

2.3. Le modèle TCP/IP

Le modèle TCP/IP est inspiré du modèle [OSI](#). Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre:

Protocoles utilisés	Modèle TCP/IP	Modèle OSI
	Couche application	Couche application
		Couche Présentation
		Couche session
TCP / UDP	Couche Transport	Couche transport
IP / ARP / ICMP / RARP / IGMP	Couche Internet (IP)	Couche réseau
	Couche Accès réseau	Couche Liaison de donnée
		Couche Physique

A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches:

- Le paquet de données est appelé **message** au niveau de la couche application
- Le message est ensuite encapsulé sous forme de **segment** dans la couche transport. Le message est donc découpé en morceau avant envoi.
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**
- Enfin, on parle de **trame** au niveau de la couche accès réseau

Les **couches TCP/IP** sont plus générales que dans le modèle OSI

2.3.1. Couche application

La **Couche Application** englobe les applications standards du réseau:

- **SMTP**: "Simple Mail Transport protocol", gestion des mails
- **TELNET**: protocole permettant de se connecter sur une machine distante (serveur) en tant qu'utilisateur
- **FTP**: "File Transfert Protocol", protocole permettant d'échanger des fichiers via Internet

et d'autres moins courants.

2.3.2. Couche transport

La **Couche transport** assure l'acheminement des données et les mécanismes permettant de connaître l'état de la transmission

Les protocoles des couches suivantes permettent d'envoyer des informations d'une machine à une autre. La couche transport permet d'identifier les applications qui communiquent. Pour faciliter la communication, on a défini non pas des noms d'applications, mais des **ports** de communication (numéro variant de 0 à 65535, 2¹⁶) spécifiques à chaque application.

La couche transport gère 2 protocoles de livraison des informations, indépendamment du type de réseau emprunté:

TCP assure le contrôle des données, orienté connexion (vérifie les envois de données par des signaux d'accusés de réception - acknowledge - du destinataire), il assure ainsi le contrôle des données

UDP, archaïque et non orienté connexion, n'assure aucun contrôle de transmission des données.

Ces 2 types (orienté connexion ou non) sont une notion utilisée pour les firewall. En effet, lorsque vous fermez un port en TCP, l'envoi d'un message ne renvoie pas de signal de retour (acknowledge), faisant croire que l'adresse IP n'est pas utilisée. Par contre, en UDP, le port fermé ne renvoyant pas d'informations fait croire que l'adresse IP est utilisée. En effet, l'UDP renvoie un message uniquement si le port est en erreur (ne répond pas)

2.3.3. Couche INTERNET

La **couche INTERNET** est chargée de fournir le paquet des données. Elle définit les [datagrammes](#) et gère la décomposition / recombinaison des segments.

La couche Internet contient 5 protocoles (les 3 premiers sont les plus importants):

1. Le **protocole IP**: gère les destinations des messages, adresse du destinataire
2. Le **protocole ARP** (Adresse Resolution Protocol): gère les adresses des cartes réseaux. Chaque carte a sa propre adresse d'identification codée sur 48 bits.
3. Le **protocole ICMP** (Internet Control Message Protocol) gère les informations relatives aux erreurs de transmission. ICMP ne corrige pas les erreurs, mais signale aux autres couches que le message contient des erreurs.
4. Le **protocole RARP** (Reverse Address Resolution Protocol) gère l'adresse IP pour les équipements qui ne peuvent s'en procurer une par lecture d'information dans un fichier de configuration. En effet, lorsqu'un PC démarre, la configuration réseau lit l'adresse IP qu'elle va utiliser. Ceci n'est pas possible dans certains équipements qui ne possèdent pas de disques durs (terminaux essentiellement)
5. Le protocole **IGMP** (Internet Group Management Protocol) permet d'envoyer le même message à des machines faisant partie d'un groupe. Ce protocole permet également à ces machines de s'abonner ou de se désabonner d'un groupe. Ceci est utilisé par exemple dans la vidéo conférence à plusieurs machines, envoi de vidéos, ... La principale application HARDWARE de l'IGMP se retrouve dans les SWITCH manageables. Ce protocole permet de regrouper des stations.

2.3.4. Couche Accès réseau

La **couche Accès réseau** spécifie la forme sous laquelle les données doivent être acheminées, quel que soit le type de réseau utilisé.

Elle prend en charge les notions suivantes:

- Acheminement des données sur la liaison
- Coordination de la transmission de données (synchronisation)
- Format des données
- Conversion des signaux (analogique/numérique) pour les modems [RTC](#)
- Contrôle des erreurs à l'arrivée

2.4. Les types d'ordinateurs connectés, types de réseaux

Un réseau permet de relier des ordinateurs quel que soit le type: PC, Mac, Main Frames (ordinateur central), ... entre-eux pour partager des ressources.

On détermine deux types d'ordinateurs connectés sur le réseau: les **serveurs** et les **clients**. Les serveurs réseaux partagent leurs ressources (fichiers, périphériques de stockage, périphériques d'impression, ...). Les clients utilisent ces ressources partagées.

On distingue trois types de réseaux:

1. les réseaux "**Peer to Peer**" ou **points à points**. Dans ces petits réseaux, les ordinateurs connectés sont à la fois clients et serveurs. Un réseau Peer to Peer courant est constitué de PC sous Windows 95 /98 mis en réseaux. Ce terme est également utilisé par extension pour le partage de musiques et fichiers divers entre PC connectés sur INTERNET, un cauchemar pour les administrateurs réseaux et une excellente faille de sécurité pour les hackers.
2. Les réseaux **dits lourds** utilisent un ordinateur central (appelé serveur) qui partage ses ressources. Dans ce cas, les niveaux d'accès des utilisateurs permettent de sécuriser les données. Les différents périphériques connectés sur ce serveur augmentent encore cette sécurité (backup, UPS, ...). La gestion se fait par un système d'exploitation spécifique de type "Serveur" comme par exemple Lynux, Windows NT serveur, Windows 2000 serveur ou Novell Netware.
3. Les réseaux **Wan** (World Area Network) sont des réseaux internationaux permettant d'interconnecter des réseaux de type lourds. Internet est un réseau de ce type. Un réseau Wan n'est pas lié à la distance, mais bien au type d'interconnexion entre deux réseaux.

Les applications, les coûts et les difficultés de mise en oeuvre et gestion sont proportionnels. La sécurité est forcément proportionnelle..

Nous ne nous intéresseront pas trop à ces concepts. En effet, à part pour les connexions, les considérations Peer To Peer, serveurs ou Wan sont plus déterminés par le système d'exploitation et l'utilisation que par les machines.

. Win 95/98/me/ Xp home/ XP Pro pour les Peer To Peer

. Win NT, 2000 serveur, Windows 2003 serveur, lynux ou Netware pour les réseaux lourds

. système Unix ou propriétaires (spécifique au fabricant) pour les autres, même si un Wan est de plus en plus configuré à l'aide de rassemblement de réseaux lourds. Internet ne fait pas exception à la règle.

2.5. Les applications réseaux.

Connecter des ordinateurs en réseau ne sert pas à grand chose sans des applications. L'utilisation d'un réseau permet:

1. **Jeux**. La mise en réseau local d'ordinateurs permet de jouer à plusieurs en même temps si le jeu inclue cette possibilité. Dans ce cas, un simple réseau Peer to Peer de type Win98 est suffisant.
2. **Partage de fichier**. Selon le niveau de sécurité et d'administration centralisée souhaités, on peut opter soit pour un réseau Peer To Peer, soit pour un réseau lourd. Dans un réseau Peer To Peer, la sécurité et l'administration est quasiment nulle mais l'installation est relativement facile et souple. De plus, il est plus facile d'effectuer une sauvegarde d'un seul ordinateur (le serveur) que sur tous les PC connectés. Les peer to peer ne sont donc utilisés que pour un nombre restreint de PC. Vous pouvez également utiliser un [NAS](#) en remplacement d'une serveur.
3. **Application centrale**. Dans des applications de gestion au sens large, on fait appel à un programme gérant une (ou plusieurs) bases de données. Ces programmes nécessitent généralement un serveur lourd. Ceci permet à plusieurs PC de travailler sur la même base de donnée en même temps à partir de PC différents (comptabilité, gestion de fabrication, facturation et gestion de stock, ...). La sécurité se fait à deux niveaux: accès aux dossiers et limitations des droits d'accès dans le programme lui-même. Prenons un exemple, une entreprise utilise une gestion commerciale (facturation, gestion des stocks, ...). Si la secrétaire ne doit pas avoir accès à la base de données, son accès serveur n'inclura pas l'accès au dossier. De même, le responsable des achats sera limité au niveau du programme pour ne pas avoir l'accès aux factures de sorties ou seulement en consultation. Ceci nécessite des serveurs particulièrement musclés avec généralement un système d'exploitation dédié serveur.
4. **Partage de connexion Internet**. Se connecter simultanément sur Internet à partir de chaque PC via leur propre connexion revient à terme très chère. La mise en réseau des ordinateurs permet de partager une seule connexion (modem, ADL ou haute vitesse). Cette possibilité passe par un partage de connexion Internet sous Win98 se et supérieur ou par l'utilisation d'un routeur ou d'un logiciel spécifique pour des utilisations plus professionnelles.
5. **Partage de périphériques**. Utiliser une imprimante par PC permet une souplesse d'utilisation. Néanmoins, l'utilisation simultanée d'une seule imprimante de grosse capacité peut s'avérer rentable avec l'achat d'une imprimante plus rapide (généralement, plus l'imprimante est chère, moins chère est le prix à la page).

Cette liste n'est pas exhaustive.

2.6. Les types de serveurs.

Dans le chapitre précédant, nous avons parlé de serveurs au sens large. Dans l'informatique, on distingue trois types de serveurs:

- Un **serveur de fichier** stocke et distribue les fichiers de programmes ou les données partageables par les utilisateurs du réseau local. Il résulte d'une combinaison de matériel et de logiciel qui peut être spécifique. Ils sont également utilisés comme serveurs d'impression.
- Un **serveur d'application** permet d'exploiter une application (un programme) sur un serveur à partir de tous les clients. Ceci est typique aux applications basées sur des bases de données (gestion de fabrication, gestion commerciale, comptabilité, ...). Elle permet par exemple de facturer, gérer les stocks, ... à partir de plusieurs PC en même temps dans une gestion commerciale. Ces applications doivent être dédiées à ce mécanisme de partage. La configuration de ces serveurs sont généralement nettement plus musclée. Le serveur envoie en permanence les parties de programme et données vers chaque station, ce qui augmente nettement le trafic réseau. Les serveurs de ce type sont en monde PC multi-processeurs. Le programme doit être conçu pour comme application centralisé. En effet, un fichier (texte, tableau, ...) ne peut être utilisé que par un programme (1 PC client dans notre cas) à la fois. Ceci pose des problèmes pour les sauvegardes lorsque le serveur travaille par exemple. Dans le cas des bases de données, le programme dédié permet le travail simultané sur la même base de donnée. Pour éviter les risques d'erreurs (modification du même enregistrement par 2 utilisateurs à la fois et corruption des données), le programme dédié va bloquer chaque enregistrement utilisé par une station. Pour rappel, dans les bases de données, l'enregistrement d'une modification se fait à fait, sans besoin d'utiliser la commande enregistrer du menu fichier. Par contre, si la base de donnée est utilisée, il est impossible de sauvegarder la base de donnée. La sécurité (contrôle d'accès, sauvegardes, ..) est cependant facilitée car centralisée.
- Un **serveur d'imprimante** permet de partager des imprimantes connectés sur un seul PC. Certaines imprimantes réseaux peuvent être directement connectés sur le réseau sans passer par un PC, des boîtiers spécifiques peuvent également être utilisés.

Dans la pratique, un serveur rassemble souvent les trois applications. Les configurations (puissances) sont différentes pour chaque application, les serveurs d'applications sont les plus performants..

2.7. Caractéristique d'un réseau.

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entre stations de travail. Si l'on énumère la liste des composants d'un réseau local, on sera surpris d'en trouver une quantité plus grande que prévue:

1. Le **câblage** constitue l'infrastructure physique, avec le choix entre paire téléphonique, câble coaxial et fibre optique. Ce choix détermine le type de concentrateurs (switch, HUB) du réseau. Ceux-ci constituent les nœuds internes dans le cas de réseaux en étoile. Dans ce cours, les liaisons hertziennes (sans fils) sont vues comme un câblage particulier.
2. La **méthode d'accès** décrit la façon dont le réseau arbitre les communications des différentes stations sur le câble : ordre, temps de parole, organisation des messages. Elle dépend étroitement de la topologie et donc de l'organisation spatiale des stations les unes par rapport aux autres. La méthode d'accès est essentiellement matérialisée dans les cartes d'interfaces, qui connectent les stations au câble.
3. Les **protocoles** de réseaux sont des logiciels qui "tournent" à la fois sur les différentes stations et leurs cartes d'interfaces réseaux. C'est le langage de communication. Pour que deux structures connectées sur le réseau, ils doivent "parler" le même protocole.
4. Le **système d'exploitation** du serveur réseau (ou NOS pour Network Operating System), souvent nommé gestionnaire du réseau, est installé sur le ou les serveurs. Il gère les partages, droits d'accès, ... Pour Microsoft, on retrouve Windows NT serveur, Windows 2000 serveur, Windows 2003 (.NET). Ce sont des versions spécifiques. Linux est utilisé sous différentes versions serveurs. Novell Netware est un système dédié principalement efficace comme serveur de fichier.
5. Le **système de sauvegarde** est un élément indispensable qui fonctionne de diverses manières soit en recopiant systématiquement tous les fichiers du ou des serveurs, soit en faisant des sauvegardes régulières, éventuellement automatisées.
6. Un **pont**, un **routeur** ou **passerelle** constituent les moyens de communication qui permettent à un de ses utilisateurs de "sortir" du réseau local pour atteindre d'autres réseaux locaux ou des serveurs distants.
7. Le **système de gestion et d'administration** du réseau envoie les alarmes en cas d'incidents, comptabilise le trafic, mémorise l'activité du réseau et aide le superviseur à prévoir l'évolution de son réseau. Cette partie est typiquement software.

2.8. Sécurité et administration.

Un des aspect important d'un réseau informatique local est la centralisation de l'administration des données. Ceci permet de sauvegarder et sécuriser les données sur une seule machine, réduisant les pertes de temps liées à cet aspect rébarbatif mais obligatoire de l'informatique.

La sécurité rassemble un ensemble de mesures: intrusion et droits d'accès, virus, sauvegardes des données, continuité de l'application (pas d'arrêts), ...

Il n'y a pas de solutions idéales pour la sécurité des réseaux (et pour la sécurité informatique en générale). Trois solutions sont envisageable: les solutions matérielles que nous verrons, des solutions basées sur Linux et des solutions basées sur Windows ou des programmes rajoutés sur ces stations Windows. Le mélange de plusieurs solutions est possible dans certains cas. Certaines solutions sont d'ailleurs complémentaires. Sur un gros réseau "sensible", mettre un VPN hardware n'est pas suffisant. Une sécurité logicielle complémentaire incluant des contrôles d'accès au niveau administration serveur (serveur, dossier, droits d'accès) et logiciels de sécurités vérifiant le trafic sur le réseau interne n'est pas superflu.

- Les **routeurs** peuvent être remplacés par le logiciel WinGate ou par des applications spécifiques en Linux sur un PC dédié par exemple
- Les **serveurs proxy** sont parfois intégrés dans les routeurs
- Les **firewall anti-intrusion** sont intégrés dans certains routeurs mais des logiciels assurent (presque) des fonctions équivalentes (ex.:Symantec, zonealarm)
- Les **réseaux privés intégrés (VPN)** permettant un accès à un réseau lourd par Internet sont inclus dans certains systèmes d'exploitation ou logiciels.
- Les **anti-virus** sont généralement logiciels, mais parfois inclus dans les routeurs qui possèdent leur propre logiciel anti-virus. Ces appareils renvoient directement tous messages contenant un virus à son expéditeur.

Selon l'application, le concepteur - administrateur du réseau utilisera l'un ou l'autre ou une combinaison des deux. Les solutions logicielles sont réservées aux [autres cours de la formation technicien PC / réseaux](#). D'autres programmes de gestion réseaux permettent de gérer les trafics, les utilisateurs, ... Ils sont spécifiquement logiciels. Les droits d'accès peuvent être bloqués d'une station vers un serveur dans son intégralité, pas au niveau des ressources. En clair, par hardware, vous pouvez bloquer l'accès complet à un serveur, par software, autoriser seulement une partie des ressources d'un serveur.

[Comment monter un petit réseau](#)

Installation d'un réseau local interne

[Réseau Ethernet](#)

Les normes de connexions réseaux Ethernet, cartes, câblage, ...

[Aménagements de locaux](#)

Tous le matériel et les produits pour aménager votre entreprise

[Serveur réseau](#)

Les particularités des serveurs utilisés en réseau local

La suite du cours Hardware 2 > Chapitre 3: [Base de transmission réseau](#)

Révision 26/06/2004



Le [cours "Hardware 1": PC et périphériques](#), le [cours "Hardware 2": Réseaux, serveurs et communications](#).

[Le cours informatique hardware](#)

© YBET informatique 2005

