

Master 1
Année scolaire 2006-2007

Réseaux & Sécurité

Ahmed Mehaoua
Professeur

BIBLIOGRAPHIE

Les principales références bibliographiques en français sont :

- Andrew Tannebaum - **Réseaux Informatiques** - Interéditions.
- Douglas Comer - **TCP/IP, architectures, protocoles et applications**. - Interéditions.
- Solange Ghernaoui-Hélie – **Sécurité Informatique et Réseaux** – Dunod
- Raymond Panko - **Sécurité des Systèmes d'information et des Réseaux** - Pearson Education

Objectifs de ce cours

• **objectif générale** : approfondir les technologies des réseaux et les solutions de sécurité qui sont associées.

• **Points clés de ce cours** :

- Etude des réseaux locaux sans fils et des mécanismes de sécurité associés
- Etude des réseaux hauts débits et des mécanismes de contrôle de la qualité du service
- Etude des nouveaux protocoles de l'Internet : IPv6, transport temps réel
- Approfondissement des applications de l'Internet : DHCP, Web, FTP, Annuaire LDAP, Téléphonie et Vidéo
- Typologie des incidents de sécurité et des attaques
- Principes de Cryptographie et les certificats
- Protocoles de sécurité pour les Réseaux locaux et l'Internet : VLAN, IPsec, SSL/TLS, PGP
- Etude des réseaux privés virtuels (RPV ou VPN)
- Logiciels de protection des systèmes et des réseaux : Sniffer, Pare-feux, Antivirus, détection d'intrusion

Partie 1

Fondement des Réseaux & des Télécommunications

QU'EST CE QU'UN RESEAU DE COMMUNICATION ?

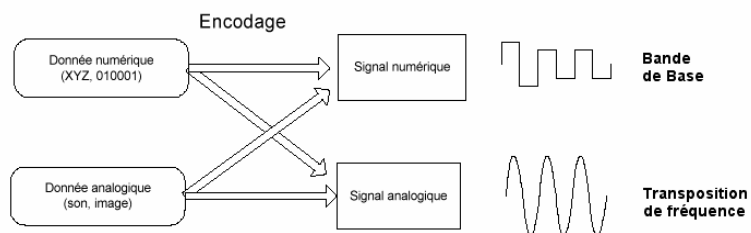
Définition :

Un réseau de communication peut être défini comme l'**ensemble des ressources matériels et logiciels** liées à la transmission et l'**échange d'information** entre différentes **entités**. Suivant leur organisation, ou architecture, les distances, les vitesses de transmission et la nature des informations transmises, les réseaux font l'objet d'un certain nombre de **spécifications** et de **normes**.

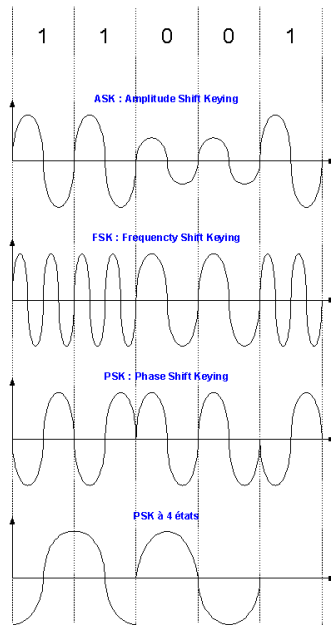
TRANSMISSION EN BANDE DE BASE OU PAR TRANSPOSITION DE FREQUENCE

◆ **4 combinaisons** possibles entre les différents types d'information et les modes de transmission :

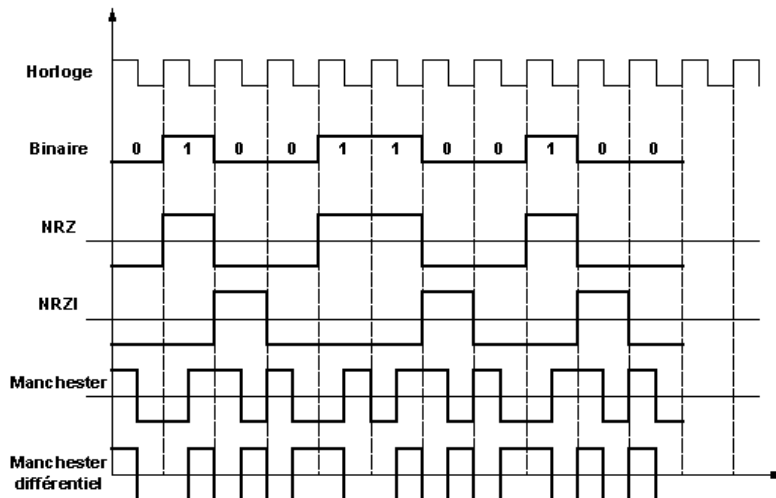
1. Information **Analogique** - Transmission **Analogique** (voix sur Réseaux Téléphonique Commuté)
2. Information **Analogique** - Transmission **Numérique** (voix sur Numéris)
3. Information **Numérique** - Transmission **Analogique** (Ordinateur via RTC avec modem)
4. Information **Numérique** - Transmission **Numérique** (Ordinateur sur LAN)



Transmission analogique Codage de l'information



Transmission numérique Codage de l'information sur le support



CLASSIFICATION DES RESEAUX DE COMMUNICATION

Les **réseaux de communications** peuvent être **classés** en fonction du **type d'informations** transportées et de la **nature des entités** impliquées. On distingue ainsi trois principales catégories de réseaux :

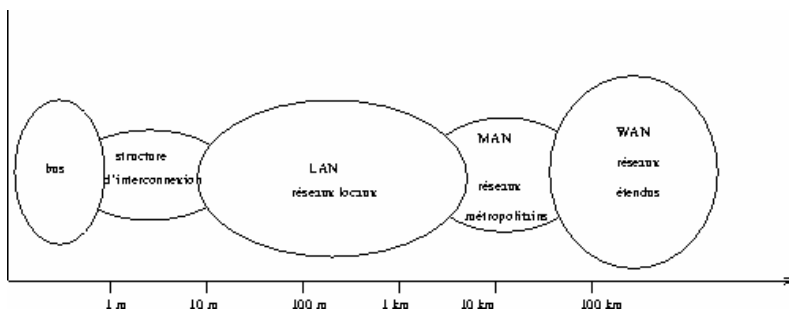
1. Les réseaux de **télécommunications** :
Ce sont les réseaux les plus **anciens**. Ils ont pour objectif **l'acheminement de communications vocales** entre **individus**. **Exemples** : Réseau Téléphonique Commuté Public, Numéris, Réseaux mobiles GSM/DCS
2. Les réseaux de **télédiffusion** :
Plus récents, ils servent à la diffusion de canaux de **télévisions** entre les studios TV et les particuliers. On retrouve les réseaux de distribution terrestre des câblo-opérateurs et les réseaux satellites (TDF, EutelSat, Noos, Numericable).
3. Les réseaux **Téléinformatiques** :
Ils servent à l'échange de **données numériques** et le partage de ressources (Imprimantes, disques, ...) entre systèmes et applications informatiques tels que les traitements de textes, ou les navigateurs Web.

page 9

CLASSIFICATION DES RESEAUX TELEINFORMATIQUES

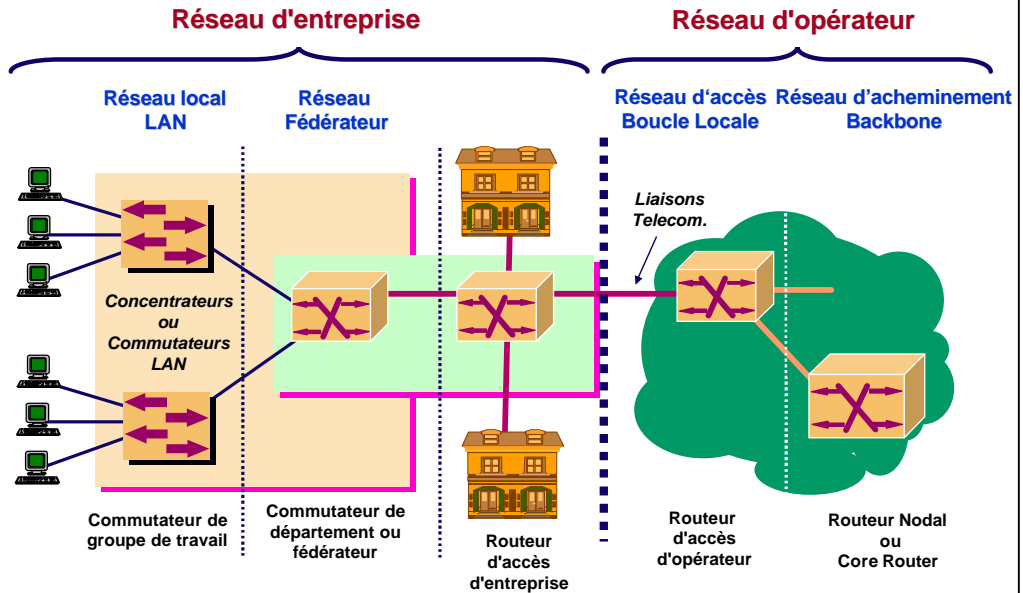
◆ Taille (distance) du réseaux :

- **Bus des ordinateurs** ISA, MCA, PCI
- **Structures d'interconnexion** Fiber Channel, ATM
- **Réseaux Privés (PAN)** Bluetooth, HomeRF
- **Réseaux locaux (LAN)** Ethernet, Wifi, ATM, Token Ring
- **Réseaux départementaux (DAN)** Fast Ethernet, ATM
- **Réseaux métropolitains (MAN)** Gigabit Ethernet, ATM
- **Réseaux étendus (WAN)** RTCP, RNIS, GSM, Internet, Frame Relay, ATM



page 10

INTERCONNEXION DES RESEAUX



EQUIPEMENTS D'INTERCONNEXION DES RESEAUX

- Les Répéteurs
- Les Concentrateurs ou hubs
- Les Ponts ou Bridge
- Les Commutateurs ou Switches
- Les Routeurs
- Les Par-feux ou FireWall
- Les Passerelles ou Gateways

REPEATER / HUB / SWITCH

Répéteur/adaptateur (UNICOM)



hubs 16/8 ports (HP)



Commutateur/ Switch Netgear



Switch multi Protocole (3com)



Switch empilables

ROUTEURS / FIREWALL / DSLAM



Netgear Wireless
Firewall / Router



Alcatel DSLAM 7301 et 7300 Compact



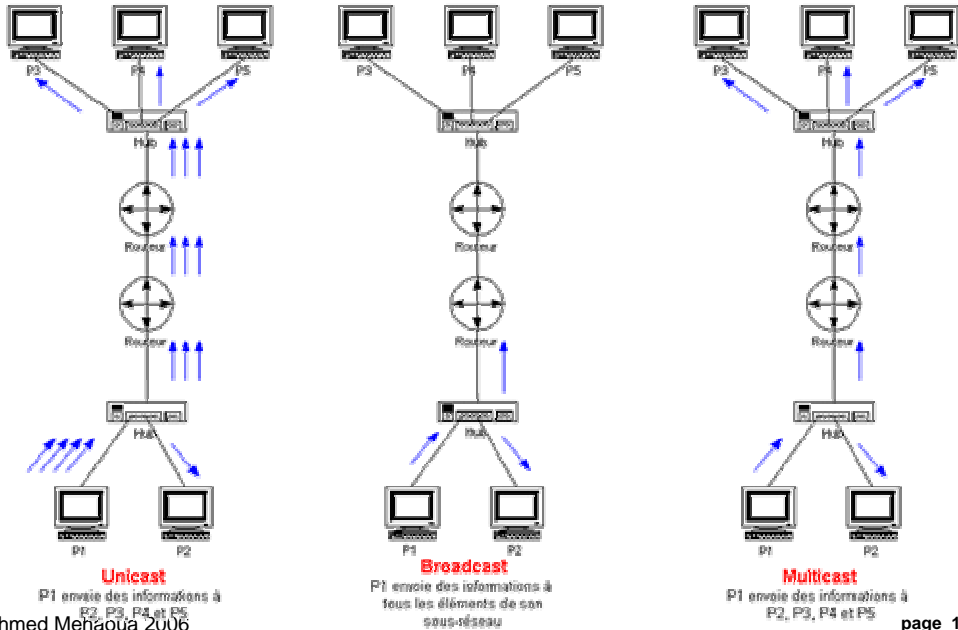
Routeur cisco serie 2600



Routeur cisco serie 12 000



3 modes d'échange



page 15

Mode de fonctionnement des terminaux

Quelle que soit l'architecture physique d'un réseau, les entités communicantes utilisent **2 modes** de fonctionnement différents lors du transfert d'information :

- **Mode Connecté :**
 - **Avantages :** permet une sécurisation des échanges et la négociation à l'avance des paramètres de communications (vitesse, qualité, ...).
 - **Défauts :** Temps de connexion plus long, communication multipoint peu aisée.
- **mode non connecté**
 - **Avantages :** simplicité, efficacité et robuste aux pannes du réseau
 - **Défauts :** déséquencement des paquets à l'arrivée, engorgement de la mémoire tampon des équipements réseaux, pas de qualité négociée.

page 16

MODE CONNECTE

◆ Principe du téléphone / Minitel

● 1 : Établissement de la connexion

- A demande une connexion avec B par l'envoi d'un message spécial (**paquet d'appel**)
- Le paquet d'appel est **routé** dans le réseau avec l'adresse du destinataire B
- Le paquet d'appel trace un chemin entre A et B dans le réseau : le **circuit**
- B confirme ou non la connexion avec un autre message spécial (**paquet d'acquiescement**)

● 2 : Transfert des données

- Tous les paquets du message sont envoyés à B en suivant le même chemin dans le réseau
- Les paquets du message contiennent le **numéro du circuit** et non plus l'adresse de B.
- Les paquets de données sont **commutés** sur le circuit virtuel

● 3 : Libération de la connexion

- un **paquet de libération** du circuit est envoyé à l'initiative de A ou B.
- ce paquet est **commuté**

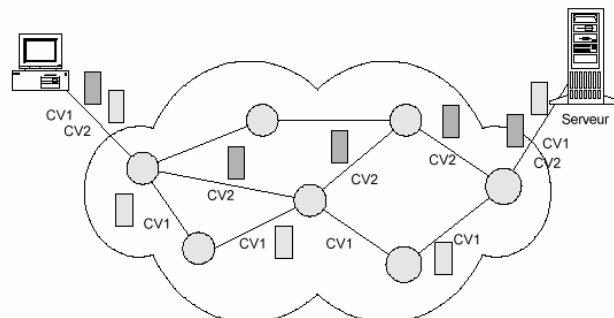
page 17

LE MODE CONNECTE - LE CIRCUIT VIRTUEL -

Application aux réseaux :

- Le chemin pré-établi est identifié par des numéros appelé n° de circuit virtuel.

Exemples : Réseau Transpac, Numéris, Frame Relay, ATM.



page 18

MODE NON CONNECTE

◆ Principe du courrier postal

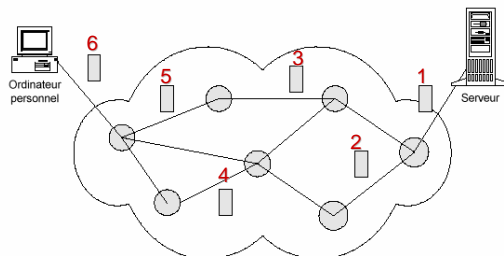
- ◆ le client poste une lettre dans une boîte aux lettres
- ◆ chaque lettre porte le nom et l'adresse du destinataire
- ◆ chaque client a une adresse propre et une boîte aux lettres
- ◆ le contenu de l'information reste inconnu du prestataire de service
- ◆ les supports du transport sont inconnus de l'utilisateur du service

MODE NON CONNECTE - MODE DATAGRAMME -

Application aux réseaux :

- A envoi vers B les différents paquets de son messages avec l'adresse de B sans demande préalable de connexion (pas de circuit virtuel entre A et B).
- C'est aux équipements du réseau d'acheminer ces paquets **individuellement** par des chemins pouvant être différents, et en les **temporisant** si nécessaire.

Exemples : Internet, Réseaux locaux



ORGANISMES DE NORMALISATION

◆ Les Organismes Internationaux :

Les organismes de normalisation internationaux cités ci-dessous sont sous l'égide de l'**ONU** et sont les plus **actifs** dans le domaine des **réseaux** et des **télécommunications**.

- **OSI** (Organisation Internationale de Standardisation) ou **ISO** (International Organisation for Standardisation)
- **CEI** (Commission Électrotechnique Internationale)
- **UIT** (Union Internationale des Télécommunications) anciennement **CCITT** (Comité Consultatif International Télégraphique et Téléphonique)

◆ Les Organismes Multinationaux :

A ces organismes internationaux, s'ajoutent encore des organismes de différents continents comme l'Europe et les Etats-Unis :

- **ECMA** (European Computer Manufacturer Association)
- **CEPT** (Conférence Européenne des Postes et Télécommunications)

LES ORGANISMES DE NORMALISATION (2)

◆ Les Organismes nationaux :

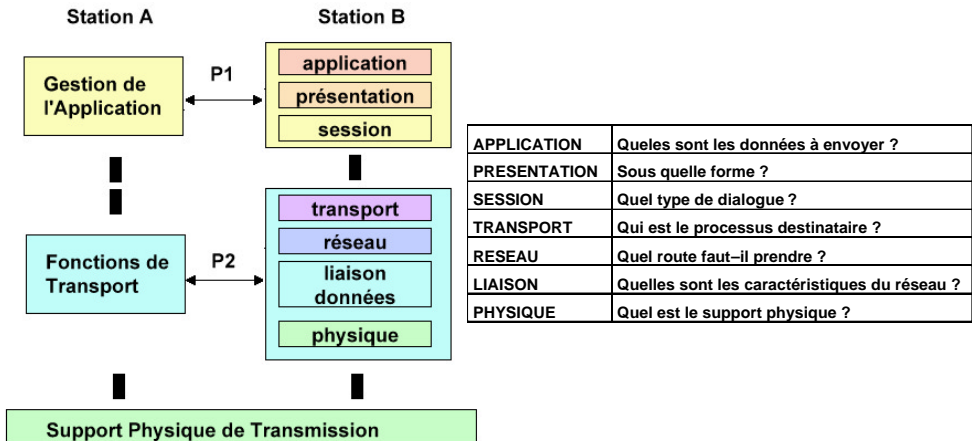
- **AFNOR** (Association Française de Normalisation)
- **ANSI** (American National Standard Institute) (USA)
- **DIN** (Deutsches Institut für Normung) (GER)
- **BSI** (British Standardization Institut) (UK),
- **SEV** (Schweizerischer Electrotechnischer Verein)

◆ Les Organismes privés :

- **DARPA** du DoD (USA);
- **IEEE** (Institute of Electrical and Electronics Engineers) (USA)
- **EIA** (Electronic Industries Alliance)
- **ATM Forum** et **Gigabit Ethernet Alliance**
- **IETF** (Internet Engineering Task Force) (USA)

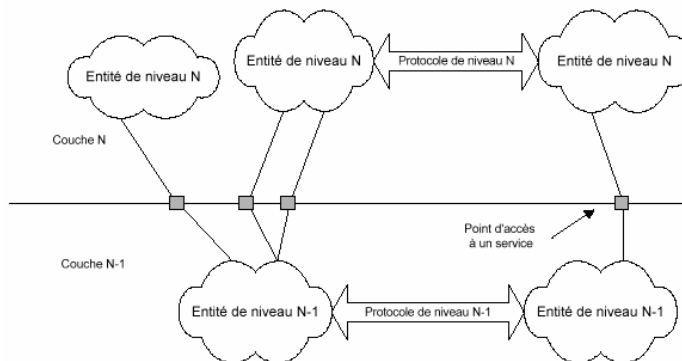
LE MODELE OSI

Open System Interconnection



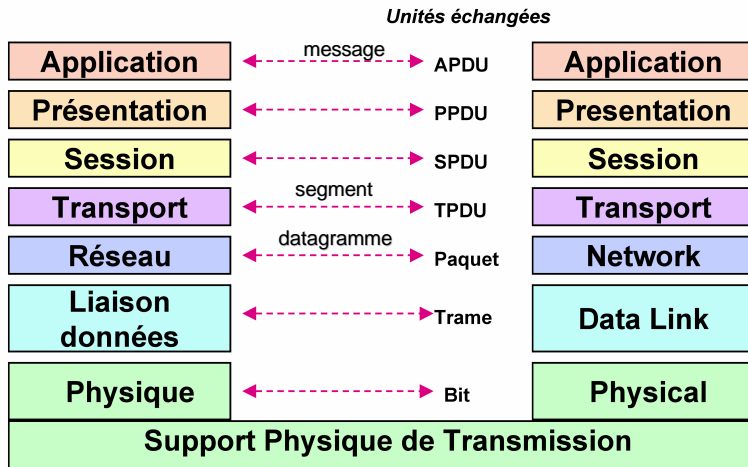
LE MODELE OSI

PRINCIPES ENTITE – PROTOCOLE - SAP



- les **entités** (N) représentent les éléments actifs (processus) de la couche (N)
- le **protocole** (N) définit les règles d'échanges à l'intérieur de la couche (N)
- Les **entités** d'une même couche communiquent entre elles selon un ensemble de règles d'échange, appelé **protocole**, à travers **les points d'accès au service** (SAP Service Access Point).

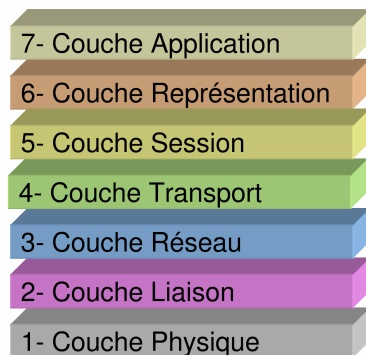
LE MODELE OSI COUCHES ET UNITES DE DONNEES (PDU Protocol Data Unit)



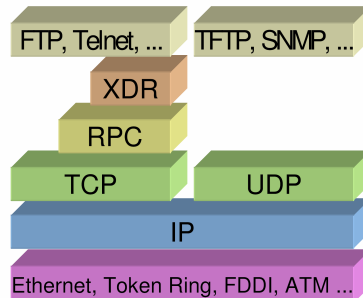
PDU : Protocol Data Unit

OSI vs INTERNET

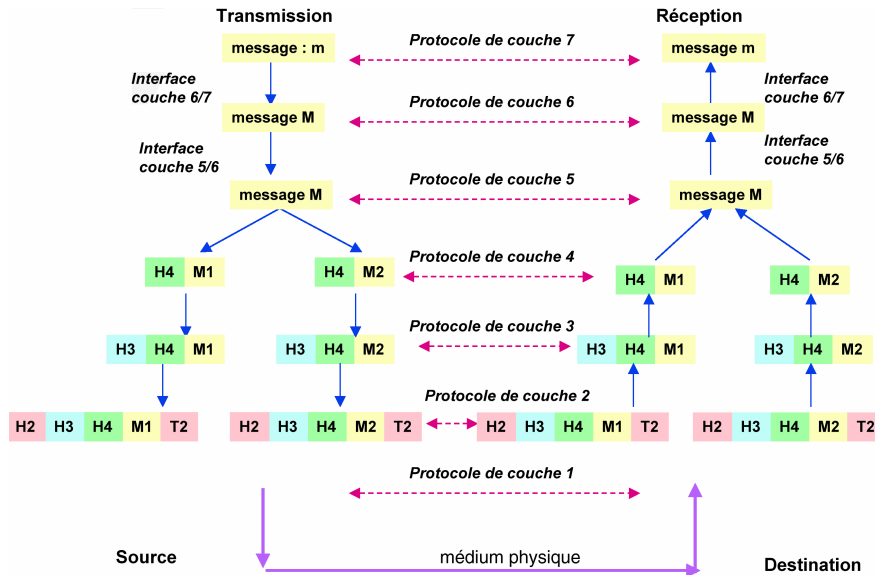
Le modèle OSI



Internet



LE MODELE OSI PRINCIPE DE L'ENCAPSULATION



LE MODELE OSI PRINCIPE DU RELAIS

