



Pourquoi les réseaux?

- Problématiques des entreprises : Eviter la duplication équipements et ressources ? & Communiquer efficacement ? Services multimédia
- Solutions : déploiement réseaux avec
 - À partir de 1960 : architecture centralisée (Relie des terminaux distants à un site central)
 - À partir de 1980 : architecture décentralisée (Relie des ordinateurs entre eux)
 - À partir de 2000 : architecture client-serveur (Relie des machines terminales telles que des stations de travail ou des serveurs)
- Architecture Client - Serveur :
 - Client : application sur une machine qui peut initier une connexion et émettre une requête.
 - Serveur : application sur une machine qui accepte les requêtes, les traite et y répond.
 - Internet fonctionne en tant qu'architecture client – serveur.
- Architecture Poste à Poste : Chaque nœud du réseau peut être client et serveur.



Types de réseaux

- 4 catégories selon la portée : PAN (WPAN), LAN (WLAN), MAN (WMAN) et WAN (WWAN).
- 1. PAN (Personal Area Network) : interconnecte sur une dizaine de mètres des équipements personnels (GSM, PDA, PC , ...). PAN le plus souvent sans fil. Exemple : Bluetooth, IrDA (Infrared Data Association)
- 2. LAN (Local Area Network): interconnecte des PC, périphériques, terminaux et autres unités à l'intérieur d'une enceinte privée.
 - topologie (Bus, Anneau, Etoile, ...); dimension (qlq km, hors intervention des opérateurs); débits (qlq Mb/s à qlq Gb/s) et taux d'erreur peu élevé.
 - deux grandes catégories : Réseaux locaux généraux et Réseaux locaux industriels.



Types de réseaux

- Réseaux locaux généraux :
 - Ethernet filaire IEEE 802.3 à 10 Mb/s (Fast Ethernet 100 Mb/s, Gigabit Ethernet 1 Gb/s); Token Ring IEEE 802.5 à 4 Mb/s - 16 Mb/s; FDDI (Fiber Distributed Data Interface) ISO 9314 à 100 Mb/s proche de IEEE 802.5; WIFI IEEE 802.11 à 1 à 54 Mb/s
 - Réseaux locaux peuvent aussi être utilisés dans un environnement de production automatisée. Ils permettent d'interconnecter divers équipements de contrôle et de mesure, des capteurs et des actionneurs pour échanger des informations qui doivent être exploitées très rapidement.
 - Token Bus IEEE 802.4; FIP (Factory Instrumentation Protocol), Profibus, CAN, ...
3. MAN (Metropolitan Area Network) :
- Câblé ou hertzien; Infrastructure privée ou publique, Longue portée qlq Km (entreprise de plusieurs sites, campus universitaire,...); Services (vidéoconférence, audioconférence, TV, images animées, ...); Débit : 64 Kb/s à 155,52 Mb/s; Exemple (DQDB IEEE 802.6, FDDI, ATM,...)



Types de réseaux

4. WAN (Wide Area network) :
 - s'appuie sur les services d'un opérateur
 - appartient à un opérateur,
 - terrestre ou satellitaire.
 - dimension : un pays, un continent.
 - constitution : Hôtes , Routeurs, Commutateurs.
 - Taux d'erreur : relativement élevé.
 - Exemple :
 - RTC, RNIS, GSM, GPRS, UMTS, Téléx
 - X.25, Frame Relay, ATM, LS, ...
 - Internet
 - WAN (débits accès) :
 - Téléx : 200 b/s; RTC : 14,4 à 32 Kb/s; RNIS : $n \cdot 64$ Kb/s; X25 : 19,2 à 2 Mb/s; FR : 34 Mb/s; LS : 2,4 Kb/s à 2 Mb/s



Qu'est ce que l'Internet ?

- 1962 : Groupe de chercheurs américains chargé de créer un réseau capable de résister à une attaque nucléaire. Concept repose sur un système décentralisé.
- 1964 : Modèle de Paul Baran
 - système centralisé vulnérable (destruction du noyau \Rightarrow anéantissement des communications) \Rightarrow mise au point d'un réseau hybride (architectures étoilées et maillées) où les données se déplacent de façon dynamique en cherchant le chemin le moins encombré et en patientant si toutes les routes sont encombrées (commutation des paquets).
- 1969 : Création du réseau expérimental ARPANET (Advanced Research Projects Agency Network) pour relier 4 instituts universitaires.
 - Communication entre machines ARPANET se faisait sans machine centralisée intermédiaire.
- 1972 : Présentation de ARPANET au grand public lors de la conférence internationale.



Qu'est ce que l'Internet ?

- ARPANET : réseau précurseur d'internet, comportait déjà à l'époque certaines caractéristiques fondamentales du réseau actuel et protocoles utilisés étaient basiques.
- INTERNET : réseau d'ordinateurs qui interconnecte les matériels informatiques à l'échelle mondial. Les ordinateurs interconnectés sont aussi des serveurs de LAN. Interconnexion de plusieurs réseaux hétérogènes de toutes tailles. Sa structure est décentralisée et non hiérarchique. Il permet la communication multimédia.
- Les offres d'Internet
 - Editions électronique,
Distribution d'information,
Moyen de publication, Forum public, Télé-enseignement, Téléachat, Divertissement
- Qu'est ce qu'on trouve sur l'Internet
 - Ressources les logiciels,
Ressources documentaires,
Ressources informatives,
Radio, TV, ...



Aller vers une offre Internet ?

- RTC : abonné avec un numéro unique VS Internet : on se sert de « adresse IP ».
- RTC : abonné avec un nom VS Internet : on se sert du « nom de domaine » : yahoo.fr
- Nécessité d'un annuaire qui fait correspondance «nom de domaine» ↔ « adresse IP ». Annuaire = Domain Name Service (DNS).
- Adresse URL (Uniform Ressource Locator) : permet d'accéder à des hypertextes.
 - lien hypertexte = chemin électronique vers une autre page web.
- A chaque page web correspond une adresse unique URL qui indique le protocole utilisé par le serveur ainsi que le nom du domaine.
 - Adresses URL peuvent être de différents types:
 - <http://www.microsoft.com> ; <ftp://nic.sys.edu> <telnet://micros.bpo.fr>



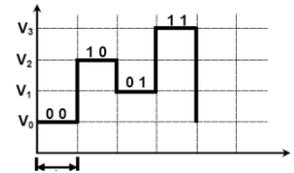
Intranet et Extranet ?

- Intranet :
 - Réseau privé caractérisé par mise en œuvre des mêmes technologies et protocoles d'Internet (protocoles TCP/IP)
 - ⇨ réseau Internet protégé et privé
 - L'entreprise peut ne pas être raccordés à l'Internet
 - Utilise des routeurs pour extension,
 - Services applicatifs: web, email, ...
- Extranet :
 - Réseau intranet permettant aux usagers extérieurs d'accéder à ses ressources
 - Problème de sécurité



Paramètres de performance d'un réseau

- Débit D: vitesse à laquelle le réseau est capable de transmettre l'information. [bits / seconde].
 - Si T temps de commutation → Rapidité de commutation
 $R=1/T$. [bauds]
 - $D = R \log_2 V$, où V est la valence.



- Temps de propagation : temps mis par l'information pour traverser le réseau de bout en bout.
- Taux d'erreur : nombre d'erreurs détectées par quantité d'information transmise. Erreurs Bits, Trames, ...
- Taux de couverture : étendue du réseau (local, national, planétaire)



Nature et caractéristiques des informations transmises sur un réseau

- Voix :
 - analogique; parole: 300 à 3400 Hz; Peut être convertie en numérique; Peu sensible aux erreurs de transmission; Très sensible aux problèmes de retards, délais, synchro, ...
- Données (data) :
 - numérique; nécessite un codage; peut-être transmis en analogique (Modems); Peu sensibles aux problèmes de retards, délais, Très sensibles aux erreurs (intégrité des réseaux)
- Image, Vidéo :
 - peut être transmise en analogique ou numérique; codage dépend de la définition (pixels, couleurs); Très sensible aux problèmes de délais, synchro...; Sensibilité accrue aux erreurs en cas de compression (intégrité des algorithmes de compression).



Principes de la communication sur un réseau

- Pour échanger des informations sur un réseau, on définit une chaîne de communication constituée de 3 éléments nécessaires:
1. Source 2. Canal 3. Destinataire
- Communication a pour but d'assurer un ou plusieurs services à l'utilisateur.
 - Services offerts varient en fonction de l'évolution technologique de la télématique :
 - Transmission de la voix; Transmission de données; Transmission des images; Multimedia
- Systèmes de transmission numérique véhiculent l'information en utilisant un support. La tâche du système de transmission est d'acheminer l'information avec le plus de fiabilité possible : techniques de commutation et transmission.
- Les signaux transportés peuvent être soit directement d'origine numérique soit d'origine analogique mais convertis en numérique.



Transmission & Commutation

- Transmission : acheminer l'information jusqu'à l'utilisateur final
 - Equipement d'extrémité, Eléments de Codage/Modulation, Médiants de communication
- Commutation :
 - Réseau = Σ voies de transmission et des moyens nécessaires pour les relier entre elles et les attribuer aux usagers. Si réseau déploie une assignation dynamique des voies, le réseau est commuté. Les liaisons entre correspondants ne sont pas permanentes mais établies de cas en cas selon des ordres. Les commutateurs interprètent et exécutent les ordres.
 - Commutation permet d'aiguiller la communication à l'intérieur du réseau et d'optimiser les réseaux de télécommunications.
 - 4 types de commutation : 1. Commutation de circuits; 2. Commutation de messages; 3. Commutation de paquets; 4. Commutation de cellules.



Commutation

- Commutation de circuits : établir, par les commutateurs, en préalable à la communication, une liaison bout à bout. Liaison maintenue tant que les usagers le désirent même s'il y a du silence.
- Commutation de messages : n'établit aucun lien entre les deux extrémités. Chaque message porte l'adresse du destinataire et est acheminé individuellement à travers le réseau. Message = fichier complet, ligne tapée sur un terminal,..
- Commutation de paquets : chaque paquet acheminé dans le réseau indépendamment des autres. Message segmenté en paquets ne dépassent pas une taille bornée fixée à l'avance par le réseau. Les paquets sont mémorisés dans les files d'attente pendant quelques millisecondes ⇒ Incompatibilité de transport de la voix et la vidéo.
- Commutation de cellules : cellule=53 octets (5 pour entête). Exemple réseau ATM où pas de fonctions de mémorisation.
 - Fonctionnement en mode connecté (cellules arrivent dans l'ordre).

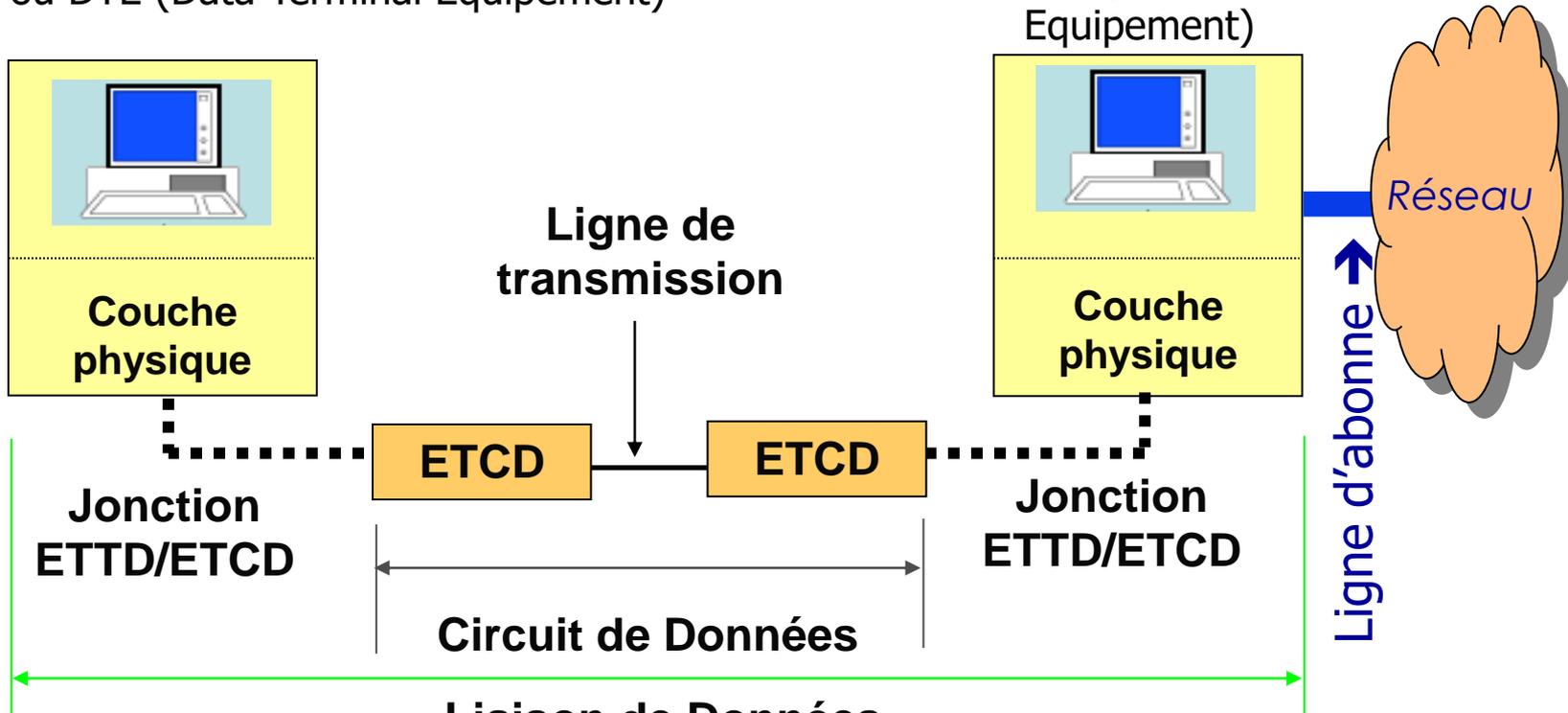


Standardisation de la chaîne de communication

ETTD : Equipement Terminal de Traitement des Données ou DTE (Data Terminal Equipment)

ETTD : Equipement Terminal de Circuit de Données ou DCE (Data Communication Equipment)

Architecture TCP/IP



ETTD :

- Source et collecteur des données,
- Traitement des données,
- Stockage des données,
- Contrôle des communications
- Exemples: stations, routeurs, ...

ETCD :

- Adaptation au media de transmission
- Codage et décodage
- Modulation et démodulation
- Contrôle de la liaison : établissement, maintien et libération de la ligne,
- Exemples: modems, concentrateurs, ...

- ETCD caractérisé par débit, mode de transmission (synchrone ou asynchrone), type de ligne de transmission, le mode d'exploitation du circuit (simplex, duplex...etc), type d'interface avec l'ETTD,...



Paire torsadée et coaxial utilisés en réseau

- Câble = Σ paires de fils de cuivre identiques isolés et toronnés.
 - Selon le niveau de qualité : Paire non blindée (UTP), Paire écrantée (FTP), Paire blindée (STP) et Paire blindée et écrantée (SFTP).
Diamètre fils de 0,2 à 1 mm, Utilisation : RTC et réseaux locaux,... ;
Blindage pour protection contre influences extérieures; Immunité aux interférences : moyenne si blindée; Supporte tous les réseaux voix, données et images; Techniques modernes : possibilité de transmission de 140 Mb/s (PDH), 155 Mb/s (SDH) et 622 Mb/s (SDH) sur de très courtes distances.
- Câble constitué de 2 conducteurs concentriques séparés par isolant. Deux types : fin si diamètres 1,2 - 4,4 mm et épais si diamètres 2,6 - 9,5 mm.
 - Conducteur extérieur concentrique : protection des données;
Conducteur intérieur : transport de données; Isolant : évite le contact entre les deux conducteurs; Gaine en plastique: protection de l'environnement extérieur.
- Débits permis câble cuivre inversement proportionnel à la portée.

Fibre optique utilisée en réseau

- Fibre optique : transmission de données à haut débit grâce à des rayons optiques. Principe : réflexion totale à travers la fibre d'indice de réfraction cœur $n = c/v$. c : la célérité et v : la vitesse de l'onde dans le cœur.
- Constitution fibre optique: Cœur (silice) d'indice n_1 : sert à la propagation des rayons lumineux; Gaine (silice) entourant le cœur et d'indice $n_2 < n_1$ pour confiner la propagation des rayons lumineux; Revêtement de protection : protection de la gaine optique des dégradations physiques; Selon le diamètre du cœur, deux types de fibre: fibre monomode SMF (diamètre cœur $< 10 \mu\text{m}$) et fibre multimode MMF (diamètre cœur $> 10 \mu\text{m}$).
- Quelques avantages : Très grande bande passante; Très faible atténuation; Débit important sur grandes portées; Très bonne fiabilité; Protection contre l'écoute; Immunité très élevée au bruit et aux interférences électromagnétiques; ...

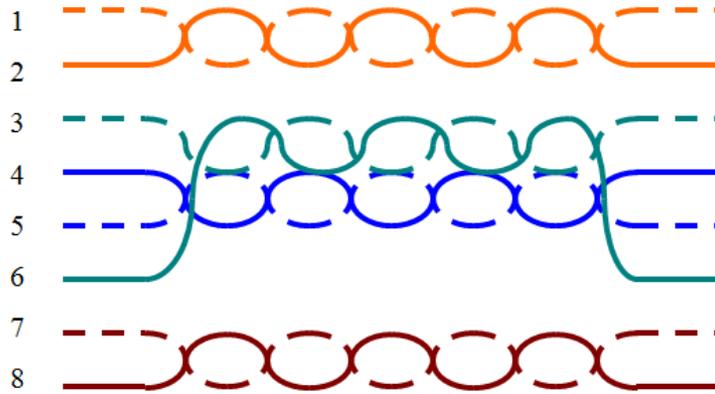
Raccordement paire torsadée

- Câble informatique UTP catégorie 5 : câble à 4 paires torsadées (8 broches).
- Code de couleur (norme T568B) :

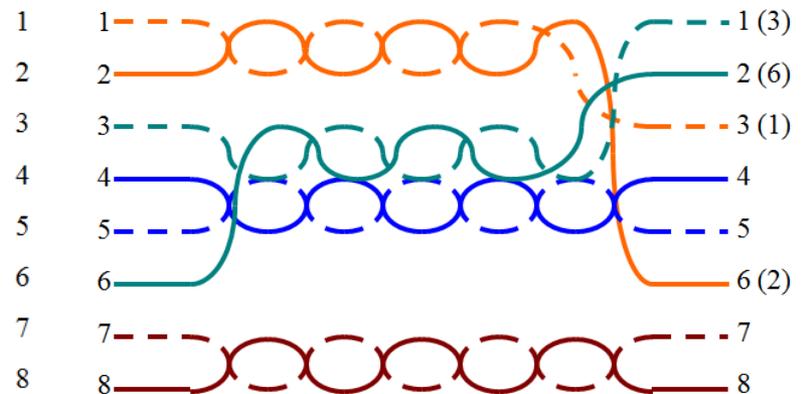
N° broche	N° de paire	Couleurs	Fonction
1	2	 Blanc-orange	Transmission
2	2	 Orange	Transmission
3	3	 Blanc-Vert	Réception
4	1	 Bleu	--
5	1	 Blanc-Bleu	--
6	3	 Vert	Réception
7	4	 Blanc-Marron	--
8	4	 Marron	--

- Câble droit (straight-through) : ETTD-ETCD → PC-Hub, PC-Switch et Switch-Routeur.
- Câble croisé (Crossover) : ETTD-ETTD ou ETCD-ETCD → Switch-Switch, Hub-Hub, Switch-Hub, Routeur-Routeur et PC-PC.
- Câble console (Rollover cable) : exploiter l'OS d'un module → PC-Routeur ou PC-Switch.

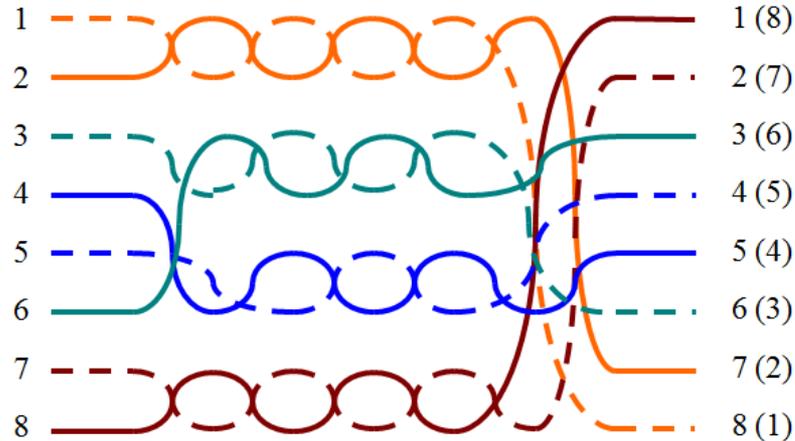
Types de câble RJ45



Câble droit



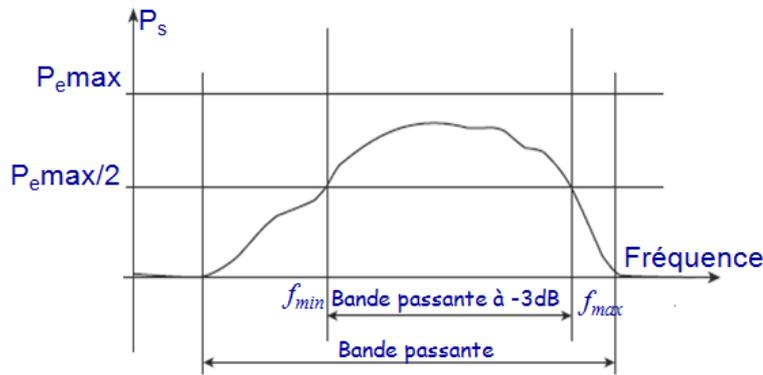
Câble croisé



Câble console

Caractéristiques des supports de transmission

- BP $[f_{\min} - f_{\max}]$ définie pour une atténuation en puissance de moitié $\Leftrightarrow -3$ dB: BP à 3 dB.



- Affaiblissement dB :

$$A_{dB} = 10 \log_{10} \frac{P_e}{P_s}$$

- $A \leq 3$ dB $\Leftrightarrow P_s \geq P_e / 2$ (P_s puissance en sortie et P_e en entrée)

- Capacité = nombre de bit transitant sur canal par unité de temps. Capacité maximale C un canal bruité (BP W) : $C = w \log_2 \left(1 + \frac{S}{B}\right)$
 - S/B : rapport puissance signal sur bruit.
- Temps d'acheminement : temps total mis par un message pour parvenir d'un point à un autre = $Tp + Tt$.
 - Temps de propagation Tp : temps nécessaire à un signal pour parcourir un support d'un point à un autre et temps de transmission Tt : délai entre le début et la fin de la transmission d'un message sur une voie = longueur du message/ débit sur la ligne.

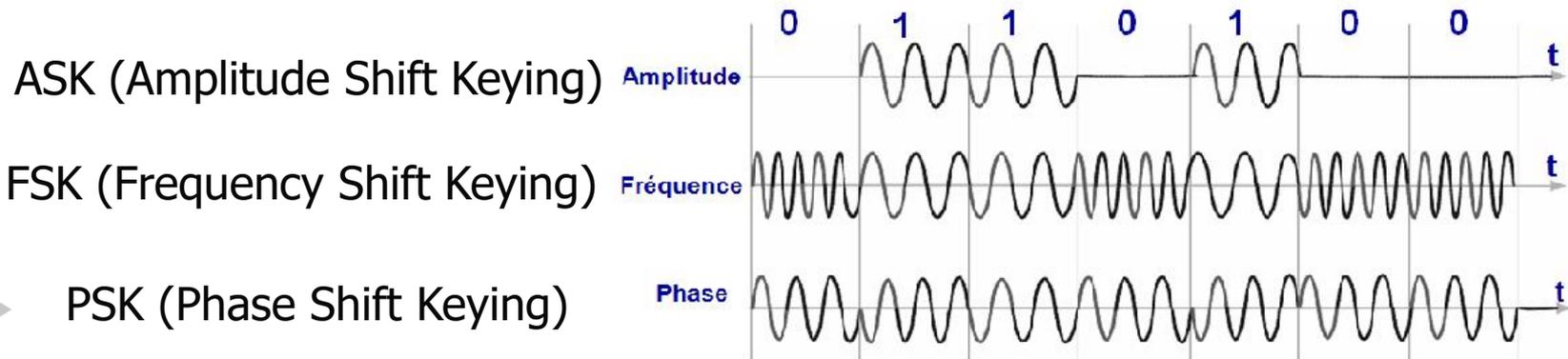


Techniques de transmission sur un support

- Transmission des informations numériques : transformer le signal en signal mieux adapté aux contraintes physiques du système de transmission.
- 2 techniques de transmission : Bande de Base BdB et large bande
 - BdB : signal transmis sous forme numérique → codage du signal pour adaptation : Bipolaire, NRZ, Manchester, HDB3, ... Quelques caractéristiques de la BdB: Impulsions discrètes, électriques ou lumineuses; Transporte sur support un seul signal à la fois; Possibilité de grand débit mais sur faible portée. Mais : Dégradation très rapide des signaux avec la distance ⇒ Récepteur incapable de comprendre les signaux reçus ⇒ Régénération répétitive.
 - BdB limitée à moins de 5 Km et spectre des signaux émis doit coïncider avec BP support afin que ces derniers ne soient pas filtrés → Recours à la modulation.

Techniques de transmission sur un support

- Transmission par modulation large bande : signal transmis sous forme analogique.
 - Modulation \Leftrightarrow moduler une porteuse sinusoïdale par le signal informatif.
 - Possibilité de transmettre simultanément Σ messages indépendants dans des BP juxtaposées pour rentabiliser médium.
 - Caractéristiques Broadband : transporte les signaux analogiques sur une plage de fréquence; transporte les ondes électromagnétiques ou optiques; transporte éventuellement Σ signaux simultanément si BP support suffisante; transporte les signaux dans un seul sens.
 - Modulation en émission et de démodulation en réception réalisée par MODEM (Modulateur-Demodulateur).





Types de liaisons et modes de connexion dans un réseau

- Liaison parallèle (fil/bit) \neq liaison série (tous les bits/fil).
- Liaison asynchrone : Séparateurs Start/Stop, Simplicité mais allongement du délai \neq Liaison synchrone : Fil d'horloge pour synchronisation ou récupération horloge du signal reçu, Permet très hauts débits mais problèmes longues distances.
- Mode simplex : Liaison dans un seul sens \neq Mode semi-duplex : Liaison alternativement dans un sens puis dans l'autre \neq Mode duplex intégral : Transmission simultanée dans les deux sens, mode le plus performant pour transmission multimédia.
- Mode connecté: transmission précédée d'une demande de connexion réussie. Etablissement, transfert et coupure. Permet l'authentification des intervenants, contrôle de flux, erreurs et ordre. Les ressources mobilisées ne sont pas forcément utilisées,... \neq Mode non connecté : Pas de négociation entre les intervenants, une seule phase de transfert de données, pas de contrôle de flux ou d'erreur,... Réseau à commutation par paquets peut offrir différents services :
 - Service sans connexion « Datagrammes » service non fiable, sans garantie de délivrance, de l'ordre ou des délais. Exemple Internet.
 - Service orienté connexion « Circuit Virtuel » : Service fiable. Exemples X.25, ATM.



Topologies de réseau

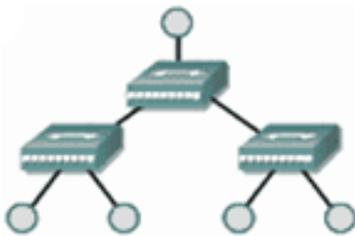
- Organisation structurelle (topologie) spécifique comment les organes sont interconnectés entre eux. On a Bus, Etoile, Anneau, Maillé, ...
- 1. Bus (réseau de diffusion) : 1 seul chemin entre 2 éléments; Communications point à point; Toutes les stations connectées reçoivent les signaux émis; Si défaillance d'un élément le réseau reste opérationnel mais si support défectueux le réseau est neutralisé; Faible coût de mise en place.
- 2. Etoile (Σ liaisons point à point) : éléments reliés à un nœud central; Topologie très utilisée où gestion réseau plus simple mais plus onéreuse (concentrateur et longueur des câbles importante); Panne nœud provoque le non fonctionnement des éléments raccordés à ce nœud.
- 3. Anneau : nœuds connectés en chaîne les unes aux autres par liaison bipoint; Éléments communiquent chacun à son tour; Toute station, hormis celle qui génère la trame, réémet le signal reçu (diffusion de la trame); Défaillance d'un nœud rompt l'anneau et manque de fiabilité en cas de rupture du support → doubler le support: les 2 anneaux d'une boucle peuvent transmettre dans même sens ou sens opposés.

Topologies de réseau

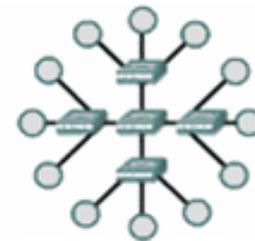
4. Maillée : plusieurs liaisons point à point et chaque élément relié à tous les autres; Si N éléments, nombres de liaisons = $N(N-1)/2$; Information peut parcourir le réseau suivant divers itinéraires grâce à des méthodes de routage; Topologie rencontrée dans les grands réseaux (Internet); En cas de défaillance élément ou support, communications sont toujours possibles.

- Topologies dérivées :

- Topologie hiérarchique :



- Topologie étoile prolongée :



- Réseaux multipoints :

- Trames diffusées à tous : adresse destination permet de vérifier que la station est bien destinataire.
 - Possibilité de faire broadcast : une machine s'adresse à plusieurs avec une seule trame.



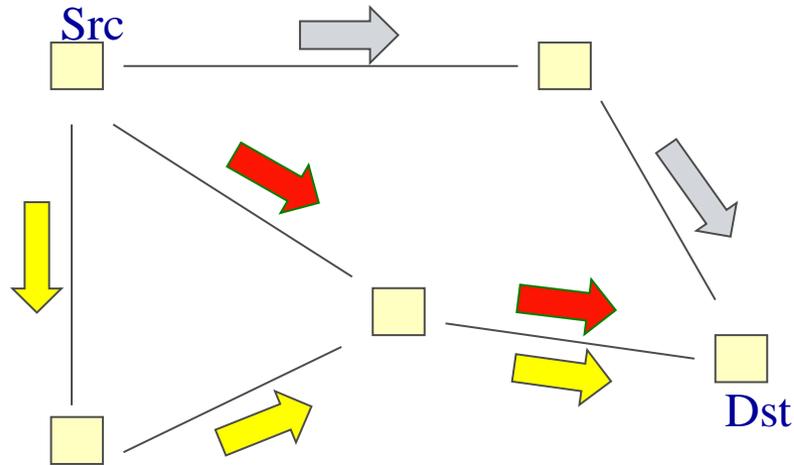
Types de liaisons et modes de connexion dans un réseau

- Dans un réseau, on distingue :
 1. Liaison point à point : chaque machine relié par un lien dédié à une seule autre machine et canal dédié spécifiquement à la connexion de ces deux machines. Exemples : liaison entre nœuds du même réseau ou entre ordinateur et terminal. Topologie étoile avec Hub ou Switch.
 2. Liaison multipoint : même support partagé par plusieurs nœuds ou utilisateurs. Exemples : Machines reliées en bus ou boucle.

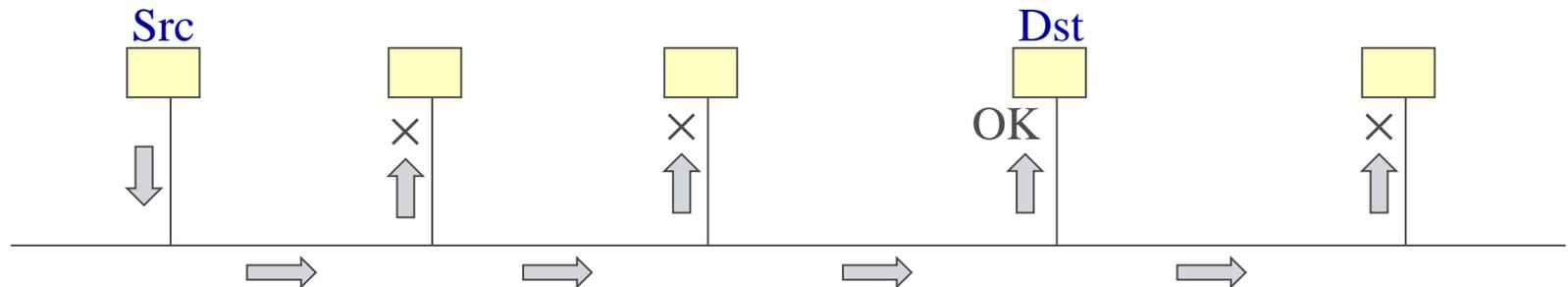


Routeage – Unicasting – Multicasting – Broadcasting- Collision

- Routeage : Processus de choix du chemin par lequel les paquets sont acheminés.



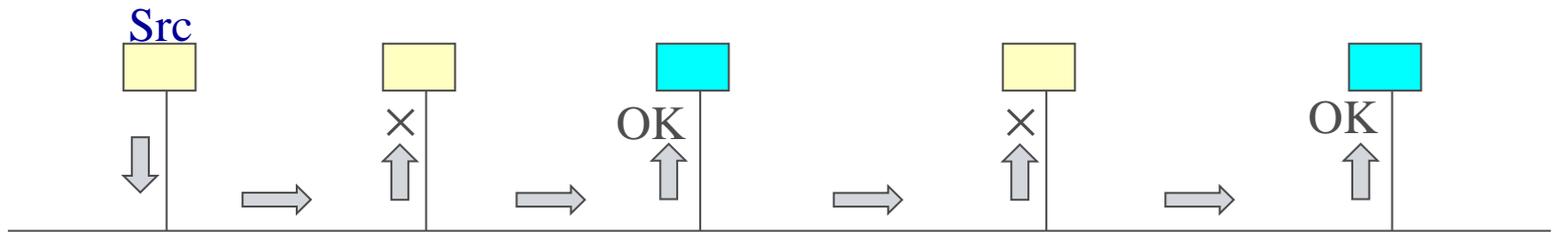
- Unicast : une source envoie un message à une destination.



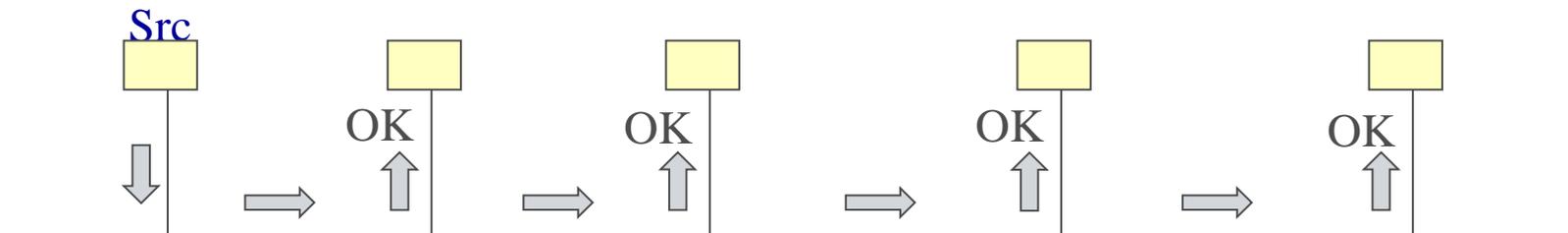


Routeage – Unicasting – Multicasting – Broadcasting- Collision

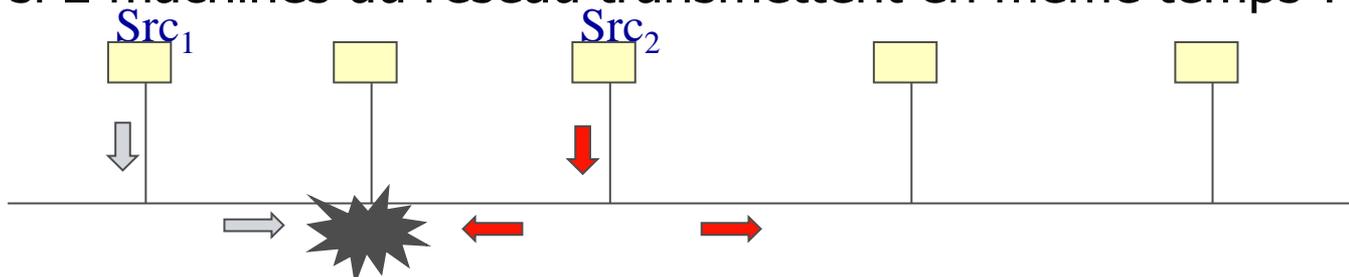
- Multicast : diffusion restreinte → une source envoie à la fois un message aux machines d'un groupe (routeage).



- Broadcast : diffusion générale → une source envoie un message à toutes les machines d'un réseau.



- Collision: si 2 machines du réseau transmettent en même temps ?



- Pour permettre des communications à travers un réseau, il faut instaurer des règles prédéterminées (Protocoles de communication).



Extension et composantes d'un réseau

- Carte réseau : circuit imprimé; fonctions : préparation des données pour transmission sur média et contrôle du flux entre machine et système de câblage.
- Répéteur : reçoit un signal, le régénère et le transmet au niveau du bit pour lui permettre d'aller sur de plus longues distances via les media.
 - Répéteur régénère aussi les distorsions.
 - Possibilité de plusieurs répéteurs par LAN.
- Concentrateur (Hub) \equiv répéteur multiports. Bits entrant dans un port reconnus et régénérés sur tous les autres ports et même sur les fils émission du port sur lesquels ils arrivent.
 - Il y a les Hub intelligents qui sont administrables à distance et d'autres sont passifs et actifs.
 - Les Hub peuvent être chaînés entre eux.



Extension et composantes d'un réseau

- Pont (bridge) : conçu pour connecter au moins 2 segments du même LAN.
 - On regroupe moyennant le pont des machines qui ont entre elles un dialogue privilégié (moins d'utilisateurs par segment).
 - Filtre le trafic pour conserver le trafic local au niveau local, tout en établissant une connectivité avec d'autres segments du LAN pour le trafic qui y est destiné et ceci en se basant sur les adresses physiques.
 - Réduit le taux de collisions et améliore l'utilisation de la BP.
 - L'action du pont n'est plus que physique mais aussi logique puisque il lit et interprète les octets véhiculés.
 - Sur même réseau, possibilité pont à translation entre Ethernet et Token Ring.



Extension et composantes d'un réseau

- Commutateur (Switch) \equiv pont multiport, segmente LAN et élimine l'effet des collisions, peut être utilisé pour interconnecter deux LAN à 10 Mb/s ou 1 Gb/s.
 - Switch prend des décisions en fonction des adresses MAC (Switch commute les données uniquement au port auquel le bon hôte est connecté en fonction de l'adresse physique du destinataire) mais le Hub ne prend aucune décision (Hub achemine les données à tous les ports, de sorte que tous les hôtes doivent accepter ou rejeter les données).
 - Si une trame est à destination d'un port qui est occupé, le Switch la mémorise pour la délivrer après.
 - Switch : Latence peu élevée et hauts débits d'acheminement des trames à chaque port d'interface (permet de mettre simultanément plusieurs ports en relation sans que le débit de chacun en souffre).
 - Switch peut fonctionner par port ou par segment.



Extension et composantes d'un réseau

- Routeur : examine les paquets entrants, choisit le meilleur chemin et les commutent ensuite au port de sortie approprié
 - Utilise des adresses logiques pour faire le routage \Rightarrow utilisation d'un protocole routable.
 - Permettent à n'importe quel type d'ordinateur de communiquer avec n'importe quel autre dans le monde.
 - Dotés d'au moins 2 interfaces physiques et sont administrables à distance.
- Passerelle : ensemble des ressources matérielles et logicielles nécessaires pour offrir aux équipements connectés à des réseaux hétérogènes les moyens de communiquer entre eux.
 - Traduit les protocoles des deux réseaux de technologie différente.
 - Passerelle par défaut est le nom du routeur par défaut permettant de quitter un réseau.



Problématique d'interconnexion

- Début années 70: chaque constructeur a développé sa solution propriétaire (SNA d'IBM, DECNET de Digital, TCP/IP, ...),
- Début années 80 : croissance phénoménale des technologies réseaux,
- Milieu années 80 : apparition de problèmes d'interconnexion dus aux nombreuses technologies de réseau incompatibles.
 - Nécessité de réunir les constructeurs pour trouver une solution: ensemble de règles communes qui permettra d'interconnecter des systèmes de technologies différentes \Leftrightarrow standardisation \Leftrightarrow modèle de réseau (Établir des spécifications et des tests, Comparer des solutions équivalentes, Établir des théories).
 - Utilité des normes: pouvoir interconnecter et communiquer des équipements hétérogènes au travers réseau et permettre aux intervenants de se comprendre sur un langage commun, ...
 - Toute norme est basée sur un compromis, la meilleure norme est celle qui s'impose, les normes sont faites pour évoluer (2 fois par an), ...



Exemples de standards

- Organismes de standardisation:
 - Niveau mondial : ISO, UIT-T, IEEE, IETF,
 - ISO : organisation internationale non gouvernementale de normalisation créée en 1947. Fédération mondiale d'organismes nationaux de normalisation de quelques 140 pays.
 - Résultats des travaux de l'ISO : accords internationaux publiés sous forme de normes internationales.
 - Niveau continent : ETSI, ANSI,
 - Niveau national : AFNOR, ANSI, DIN, BSI,
- Organismes de standardisation aboutissent à des standards.
- Deux types de standards :
 - « Standards propriétaires » : réservés à un constructeur.
 - SNA d'IBM, ■ NetWare de Novell, ■ DECnet de Digital, ...
 - « Standards ouverts » :
 - OSI de l'ISO, ■ IEEE 802.x, ■ TCP/IP, ■ Ethernet, ...



Concept de l'architecture réseau

- Transport des données entre 2 extrémité au travers un réseau nécessite support. Mais pour que les données arrivent correctement au destinataire, avec la QoS exigée, il faut en outre implémenter dans le réseau un grand nombre de fonctionnalités qui seront chargées du contrôle des données dans le réseau.
 - Exemples de fonctionnalités : Transmission physique filaire ou sans fil, Choix du chemin pris dans un réseau, Détection d'erreurs, Gestion d'une situation d'erreur, ...
- Pour réduire la complexité des réseaux, faciliter l'implémentation des fonctionnalités et organiser les interactions entre les différentes activités, les architectes réseau ont décomposé les processus mise en œuvre dans les réseaux en couches protocolaires + support physique.
 - Solutions matérielles et logicielles mises en œuvres constituent l'organisation fonctionnelle ou l'architecture réseau qui spécifie comment les différentes fonctionnalités sont organisées entre elles.
- Modèle en couches argumenté par :
 - réduit la complexité, uniformise les interfaces, facilite la conception modulaire, assure l'interopérabilité de la technologie, accélère l'évolution, simplifie l'enseignement et l'acquisition des connaissances,...



Concept de l'architecture réseau

- Architecture ou modèle en couches permet au réseau de traiter en parallèle les fonctions attribuées aux différentes couches.
- 3 grandes architectures se disputent le marché des réseaux :
 - Architecture OSI (Open System Interconnection) ou interconnexion de systèmes ouverts provenant de la normalisation de l'ISO,
 - Système ouvert = équipement voulant échanger dans un environnement hétérogène. Caractéristiques: interopérabilité, portabilité, compatibilité.
 - Architecture TCP/IP utilisée dans Internet,
 - Architecture introduite par l'UIT pour l'environnement ATM.
- ISO a publié et a mis en œuvre en 1984 un modèle de référence OSI.
 - Modèle réseau = représentation du fonctionnement du réseau et non pas le réseau réel.
- Modèle OSI se base sur plusieurs couches simples à vocation précise afin d'en faciliter la compréhension et l'implémentation.
 - Processus mise en œuvre dans les réseaux sont décomposés en couches protocolaires plus un support physique (Protocoles sont structurés en couches).



Concept de couche & protocole

- Protocole de communication : ensemble de procédures et informations préétablies et standardisés nécessaires pour réaliser et gérer un échange fiable de données entre deux systèmes distants.
 - Protocoles désignés pour normaliser temps de réponse, qualité, le type de support ... et prennent en compte les contraintes d'atténuation, du bruit, des pertes, du délai, segmentation, ...
 - Divers périphériques peuvent accéder au réseau et doivent communiquer à l'aide des mêmes protocoles → les protocoles doivent être indépendants de la technologie.
- Protocoles sont liés au type de réseau et de données échangées. Les formats des informations échangées par un protocole font partie intégrante de ce protocole.
- Lors de l'échange de données, une couche ou un protocole d'une couche sera en charge d'assurer par exemple : Délimitation des blocs de données échangés, Contrôle d'erreur, Organisation et contrôle de l'échange, Contrôle de la liaison, ...



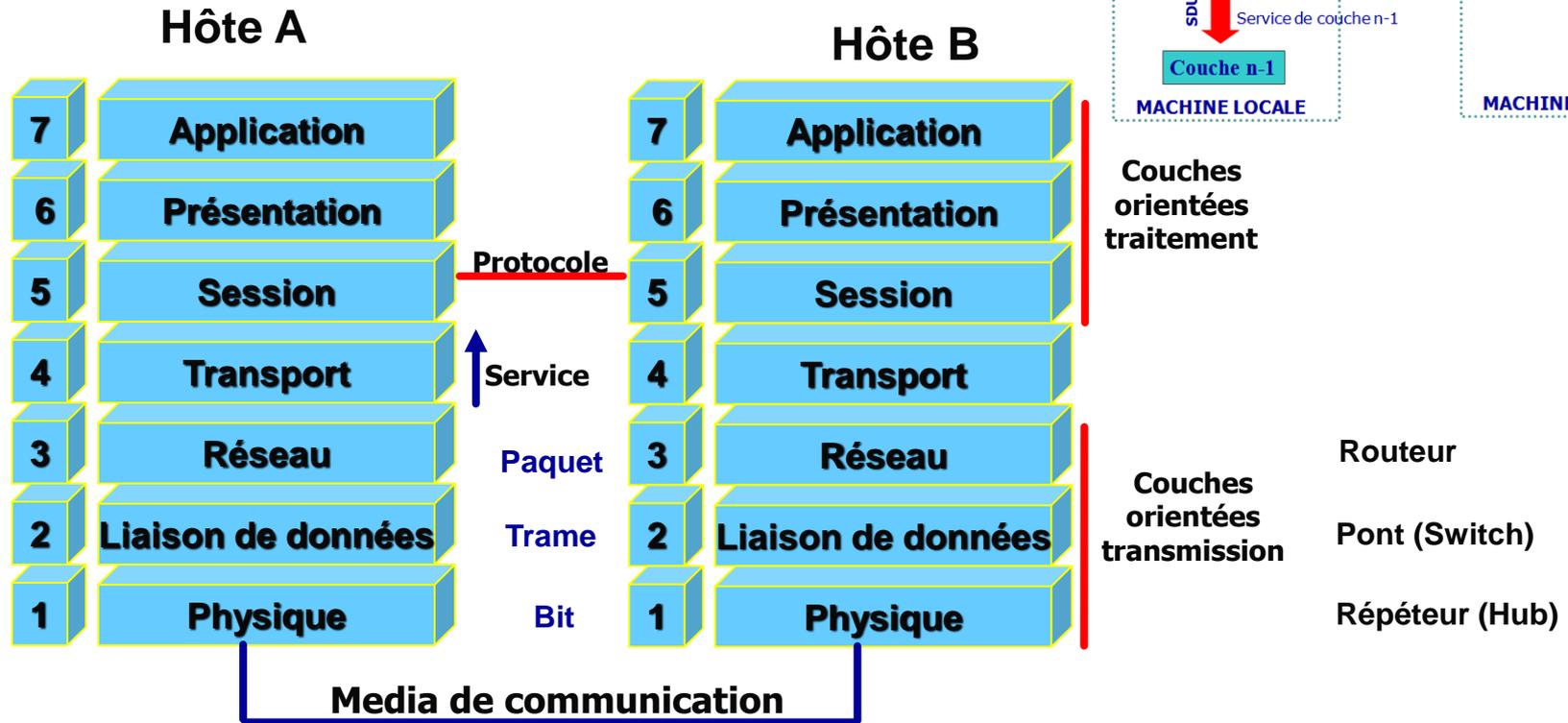
Couches & protocoles du modèle de référence OSI

- Modèle OSI basé sur 7 couches: 1 → 7
- Classement des couches :
 - Couches 1 à 3 : couches basses orientées transmission.
 - Couche 4 : couche charnière entre couches basses et couches hautes, qui gère le transfert de l'information.
 - Couches 5 à 7 : couches hautes orientées traitement.
- Chaque couche fournit des services à la couche immédiatement supérieure, utilise des services de la couche immédiatement inférieure, ne communique qu'avec les couches qui lui sont adjacentes, échange de l'information suivant un protocole avec des couches distantes de même niveau.
- Modèle OSI repose sur protocoles et interfaces.
 - Règles et conventions utilisées lors du dialogue entre deux couches n sont appelées protocole de communication de la couche n.
 - Interface est un ensemble de services proposés par les couches aux autres couches.
 - Données transférées par les services : SDU (Service Data Unit).
 - Données transférées par le protocole : PDU (Protocol Data Unit).



Couches & protocoles du modèle de référence OSI

Architecture TCP/IP



- Passage d'une couche à l'autre se fait par l'ajout des informations de contrôle relatives au protocole → Encapsulation (en descendant dans les couches, les données reçoivent des en-têtes, des en-queues et d'autres informations). Dans l'autre sens, c'est la désencapsulation.



Couches & protocoles du modèle de référence OSI

- Couche physique: assure l'interface entre le système d'extrémité et le support de transmission :
 - S'occupe de la transmission brute entre les entités physiques (ETTD et ETCD) des bits consécutifs des trames sur un circuit de communication suivants des spécifications électriques, optiques, mécaniques, procédurales et fonctionnelles définies par des normes (Ethernet, RS232, ...) sans connaître ni la structure ni la signification de ces bits, les données sont transmises sous forme binaire et traduites par des impulsions électriques ou lumineuses.
 - Au niveau de cette couche, on s'intéresse à l'amplitude du signal, au temps bit, à la possibilité de transmettre dans les deux sens, à l'établissement de la connexion, ...
- Couche liaison de données : définit des règles pour l'émission et la réception de données à travers la connexion physique de deux systèmes distants :
 - Fractionne les données en trames, permet la détection et éventuellement la correction des erreurs, gère les trames d'acquittement et par suite permettra la résolution des problèmes des trames erronées, perdues ou dupliquées, permet le contrôle de flux, détermine la méthode d'accès au support, s'occupe de l'adressage physique et de la topologie, ...



Couches & protocoles du modèle de référence OSI

- Couche réseau : gère la façon dont les paquets sont acheminés de l'émetteur vers le récepteur qui peuvent être situés sur des réseaux géographiquement éloignés :
 - Permet le choix des chemins à partir des adresses en assurant le routage des paquets entre les nœuds. Si nœud surchargé ou hors-service, les paquets seront déroutés vers un autre nœud,
 - Doit résoudre les problèmes d'interconnexion entre les réseaux hétérogènes,
 - Peut prendre part au contrôle du flux et à la gestion des erreurs.
- Couche transport : assure essentiellement le transport fiable, transparent et efficace de bout en bout au travers le réseau de l'information selon un niveau de qualité demandé par l'utilisateur.
 - Connexion de transport = canal point à point délivrant des messages sans erreur dans l'ordre d'émission.
 - Avec la couche de transport, on aborde les couches de "bout en bout" (couches hautes), c'est-à-dire que le même programme s'exécute sur l'émetteur et le destinataire en utilisant des messages d'en-tête et de contrôle. Cette couche doit gérer l'initialisation et la fin des connexions sur le réseau.



Couches & protocoles du modèle de référence OSI

- Couche session : orientée traitement,
 - Sert d'interface entre les fonctions liées à l'application et celles liées au transport de données,
 - Assure l'ouverture, la gestion et la fermeture des sessions de travail pour le compte des applications entre les utilisateurs distants opérant sur différentes machines, En plus de la mise en place du dialogue entre les tâches distantes, la couche assure le contrôle du dialogue : connexion, gestion (interventions en cas d'incident..), Assure la synchronisation du dialogue entre les hôtes, Définit les règles d'organisation et de synchronisation du dialogue entre les utilisateurs opérant sur différentes machines.
- Couche présentation : met en forme les informations échangées pour les rendre compatibles avec l'application destinataire dans le cas de dialogue entre des systèmes hétérogènes.
 - Assure trois fonctions principales : formatage des données (présentation), encryptage des données, compression des données.



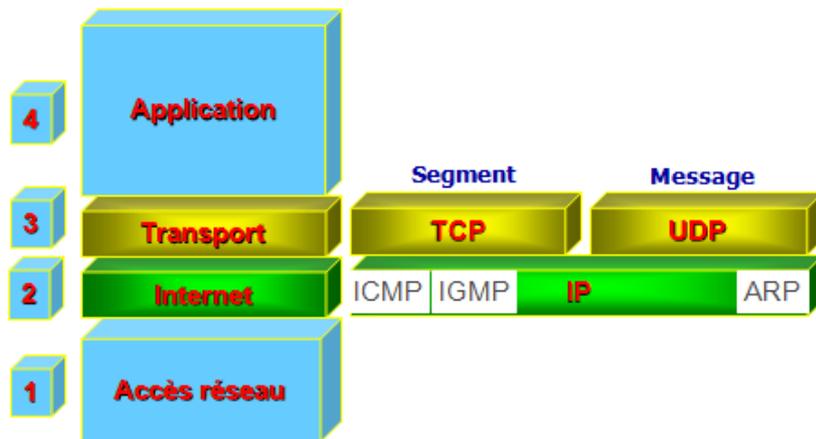
Couches & protocoles du modèle de référence OSI

- Couche application : Point de contact entre l'utilisateur et le réseau :
 - Crée une interface directe avec le reste du modèle OSI par le biais des applications réseau (navigateur, messagerie, transfert de fichier, Telnet, ...) ou une interface indirecte par le biais des applications autonomes (comme les traitements de texte, les logiciels de présentation ou les tableurs extérieurs du modèle OSI) avec des logiciels de redirection réseau.
 - Chargée de l'exécution des applications et de dialogue avec la couche 7 du destinataire en ce qui concerne le type ou la signification des informations à échanger : transfert de fichier, interrogation de bases de données, ...



Architecture du protocole TCP/IP vs OSI

- TCP/IP (Transfert Control Protocol/ Internet Protocol) protocole de base de l'Internet, développé par DARPA et University of Southern California, fait référence à une multitude de protocoles, tient son nom de deux les plus importants de ses protocoles pourtant il y a un bon nombre d'autres protocoles encapsulés dans ce nom. TCP/IP est indépendant de l'architecture matérielle et des systèmes d'exploitation. TCP/IP se base sur la philosophie OSI: 4 couches et encapsulation.



Fonctionnalités des couches:

Application: Représente les données pour l'utilisateur, assure le codage et le contrôle du dialogue. **Protocoles** : FTP, HTTP, ...

Transport: Prend en charge la communication entre les différents périphériques à travers divers réseaux. **Protocoles** : TCP, UDP.

Internet: Détermine le meilleur chemin à travers le réseau. **Protocoles** : IP, ARP, ...

Accès réseau: Contrôle les périphériques matériels et les supports qui constituent le réseau. **Protocoles** : Ethernet, Token Ring, FDDI, ...



Protocole IP

- Protocole niveau 3 OSI: offre un service de transmission de datagrammes IP non connecté et non fiable → pertes et duplications possibles, déséquencelement, aucun contrôle de flux.
- Datagramme IP: message avec adresse émetteur et destinataire



- IP puissant grâce à ses deux adresses. Chaque routeur dans le réseau peut trouver le chemin adéquat dans le monde entier.
- Permet les fonctionnalités suivantes :
 - Encapsulation des données de la couche supérieure (format du datagramme),
 - Définir le routage.
- IP transporte presque toutes les données qui transitent dans le monde. Toutes les nouvelles applications sont construites avec ce protocole. Il est indépendant du type de technologie utilisée.

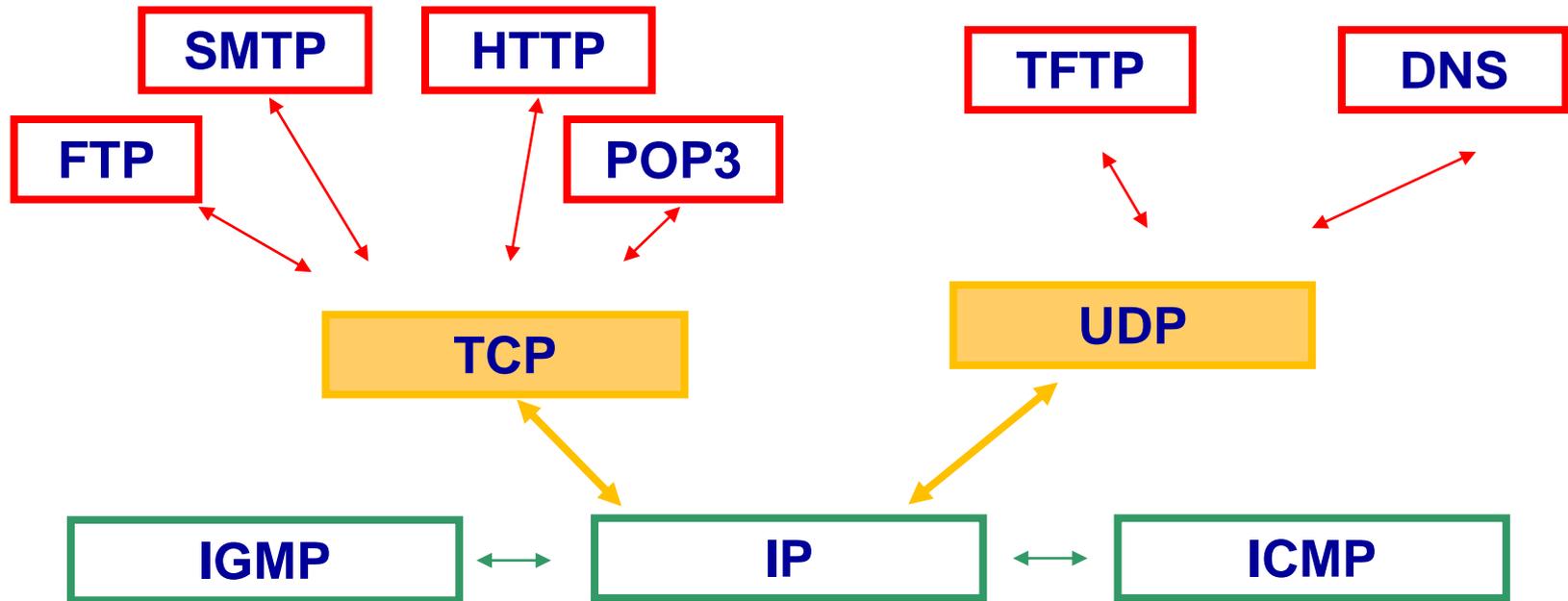


Protocoles TCP & UDP

- TCP niveau 4 OSI: protocole de transmission orienté connexion, fiable → sans perte, sans duplication, acquittement positif avec retransmission sur Time-Out, séquençement. Permet le contrôle du flux par fenêtre de réception.
- TCP orienté connexion ⇔ les applications dialoguant sont considérées l'un comme serveur, l'autre comme client et qu'elles doivent établir une connexion avant de pouvoir dialoguer.
 - Protocoles applicatifs appropriés: Telnet, FTP, HTTP,
 - TCP permet le multiplexage.
- UDP (User Datagram Protocol) niveau 4 OSI : Protocole de transmission orienté non connexion, transmission non fiable → sans acquittement, perte, duplication, déséquençement. Sans contrôle du flux. Application utilisant UDP doit prendre en charge la gestion de la perte, déséquençement, duplication,
 - Protocoles applicatifs appropriés: RIP, SNMP, RADIUS, VOD, ...



Applications TCP/IP et protocoles couche transport



- HTTP : HyperText Transfer Protocol.
- TELNET : service de connexion à distance sur des machines éloignées.
- FTP (File Transfer Protocol) : service de transfert de fichiers. Permet de télécharger de nombreux logiciels et documents publics.
- SMTP (Simple Mail Transfert Protocol) : protocole de transfert de courrier électronique.
- SNMP : Simple Network Management Protocol.



Ports TCP/UDP

- TCP et UDP introduisent la notion de « port »: une application fournit un service particulier sur une machine donnée. Service identifié par le numéro de port tandis que la machine identifiée par une adresse.
- Port: destination abstraite sur une machine et correspond à une application sur la machine. Une station oriente les données vers la bonne application de destination grâce au port utilisé pour le transport. Le port est identifié par un numéro qui sert d'interface à l'application pour recevoir et émettre des données.
- UDP offre un service supplémentaire par rapport à IP, il permet de distinguer plusieurs applications destinataires sur la même machine par l'intermédiaire des ports.



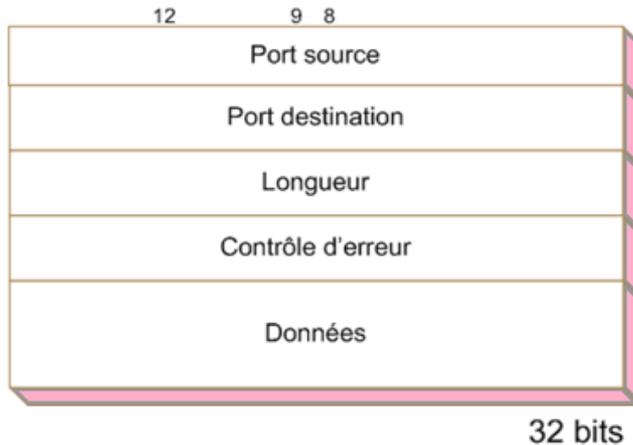
Ports TCP/UDP

- Trois types de ports :
 - Ports reconnus, utilisés par des services réseau d'usage général et commun. N°: 0 → 1023. Exemple : HTTP, SMTP, FTP, ...
 - Ports réservés, correspondent à des services d'usage moins général. N°: 1024 → 49151. Exemple : 17500 pour Dropbox
 - Ports libres, utilisés pour des durées limitées. N°: 49152 → 65535
- Chaque application utilise un numéro de port :
 - Exemples : tftp: 69/udp; snmp: 161/udp; 25: SMTP; 21: FTP; 53: DNS; 80: HTTP; 20: FTP data; 21: FTP control; 23: Telnet; 25: SMTP; 110: POP3; 520: UDP Router; ...
- Relation client-serveur: port source client choisi par le système d'exploitation (le premier disponible) alors que port serveur identifié avec une application spécifique. La combinaison {adresse IP, numéro de port } correspond à un processus sur le client ou le serveur.
- Comme TCP démultiplxe les données venant d'applications différentes, la notion de port permet de distinguer la destination ultime sur une machine.

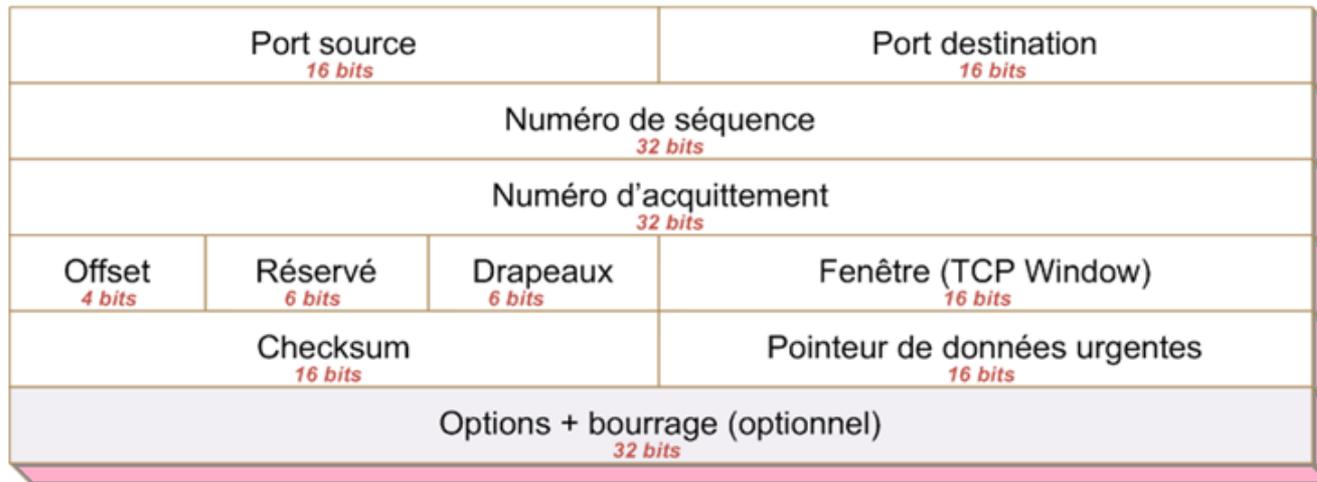


Ports TCP/UDP

Les ports UDP et TCP sont distincts (deux espaces), N° port = 16 bits.



Message UDP

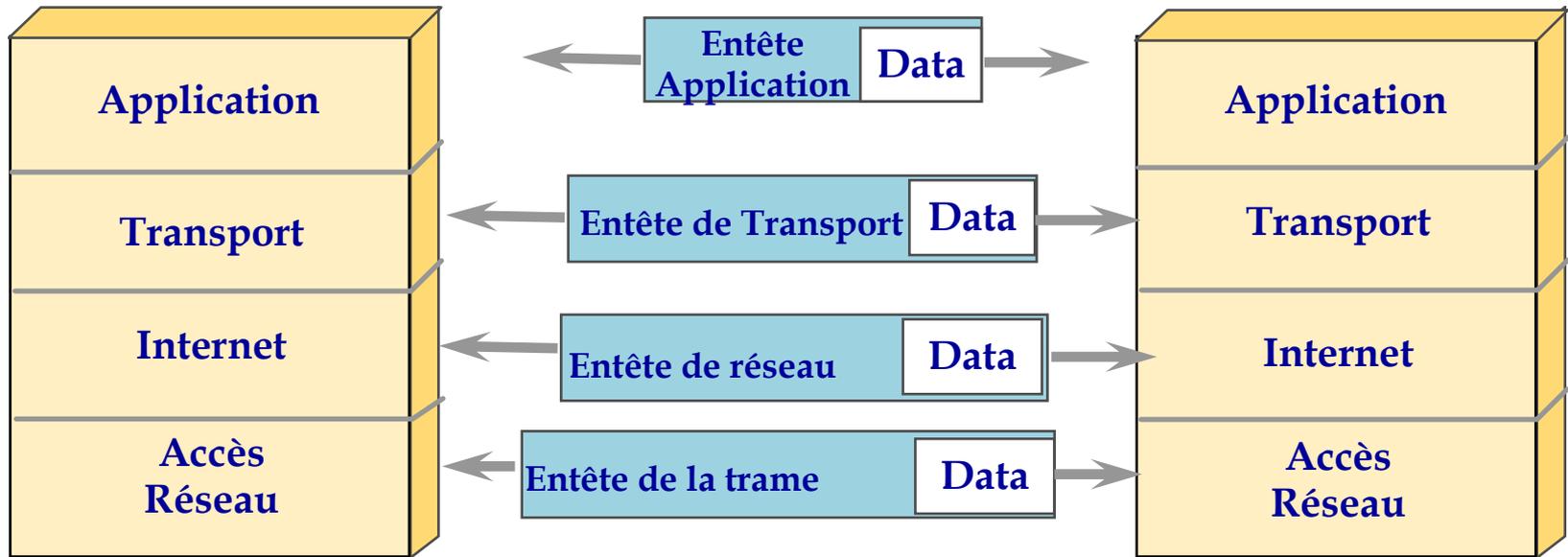


Entête
segment TCP

En associant les ports source et destination avec les adresses IP source et destination du datagramme, on identifie de manière unique une connexion.

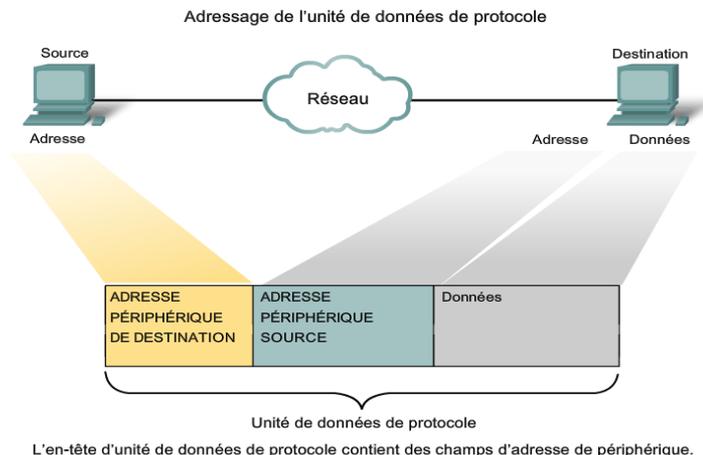


Encapsulation & Décapsulation



Adressage dans les réseaux

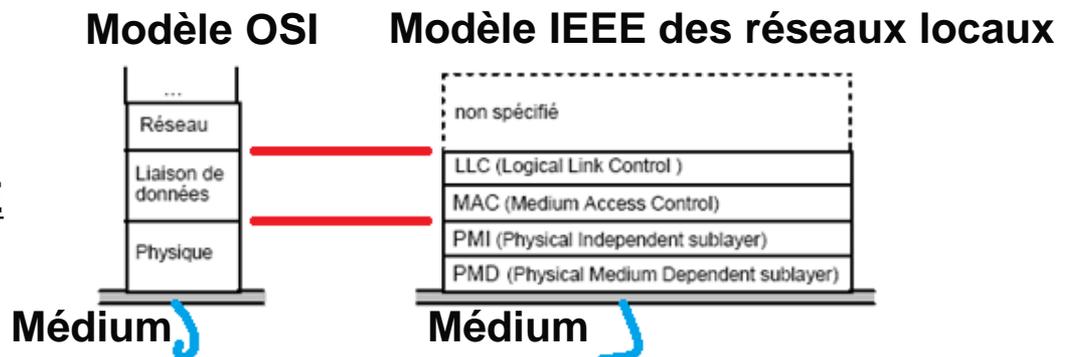
- Adressage :
 - Adresses MAC (couche 2),
 - Adresses IP (couche 3),
 - Ports TCP/UDP.
- Protocoles de la couche 3 : principalement conçus pour déplacer des données depuis un LAN vers un autre LAN au sein d'un inter-réseau.
- Adresses couche 2 et couche 3 différentes : adressage au niveau de chacune de ces couches n'a pas le même rôle : adressage MAC permet d'identifier les machines sur un même réseau et adressage IP permet d'adresser les machines sur des réseaux distincts.



Architectures des réseaux locaux

- Réseau local = câblage reliant différents nœuds suivant une certaine topologie.
 - Partage du support (méthode d'accès) + Adressage (identifier chaque nœud) + Protocoles + Applications
- Protocoles d'accès respectent la structuration en couches.
 - Requièrent une partie des fonctionnalités des couches OSI et peuvent ne mettre en jeu qu'une partie de ces couches. Réseaux locaux couvrent les couches 1 et 2 du modèle OSI.
- Particularités :
 - Sous-couche MAC et sous couche LLC.
 - Couche physique découpée en une sous couche PMI et une sous couche PMD.

Comparaison des modèles OSI et IEEE





Architectures des réseaux locaux

- Rôle des sous-couches :
 - MAC : contrôler le partage du medium, filtrer les trames reçues pour laisser passer celles réellement destinées à la station et contrôler les erreurs.
 - LLC : établissement et rupture des connexions ainsi que leur gestion.
 - Grâce à MAC, la LLC fait de sorte comme si les stations du réseau étaient toutes reliées deux à deux.
 - L'adoption d'une architecture en couches permet de disposer d'une même couche LLC quelle que soit la technique du partage du support utilisée.
 - PMI : détecter le signal et assurer son codage en ligne.
 - PMD : assurer l'émission physique des bits sur différents supports.
- Normalisation ne concerne pas les couches au-dessus de LLC. Possibilité d'implanter directement des protocoles applicatifs ou des protocoles d'interconnexion de réseaux.



Protocoles d'accès aux ressources de communication

- LAN nécessite un mécanisme efficace de contrôle d'accès aux ressources de communication pour permettre à chaque station d'établir des communications.
- 3 groupes de protocole d'accès avec plusieurs techniques. Le type d'accès est très lié à la topologie.
 1. Accès statique : BP répartie entre les stations de façon définitive.
 - 2 techniques déterministes AMRF accès multiple par répartition de fréquence et AMRT accès multiple par répartition du temps.
 2. Accès dynamique : allocation dynamique de la BP aux stations. Si station a besoin d'émettre, elle sollicite une BP. Mécanisme de décision permet d'élire parmi plusieurs stations, celle invitée à émettre. 2 techniques: polling / selecting & jeton.
 - Méthode d'accès déterministe Token Ring. Organisation de réseau en anneau fermé où les systèmes présents s'échangent un ou des jetons (token) qui leur donne le droit d'accès. Quand une station termine une émission ou épuisé son délai, elle cède le jeton à la suivante.



Protocoles d'accès aux ressources de communication

3. Accès aléatoire : station qui désire émettre n'a pas besoin d'autorisation et sollicitation matérialisé par l'accès directe au canal → possibilité de conflit d'accès. Plusieurs techniques proposées pour qu'en cas de conflit une seule station soit autorisée à émettre.

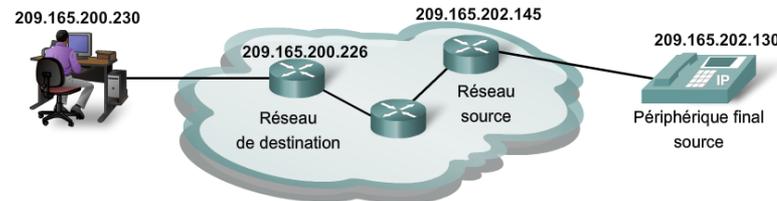
1. CSMA (Carrier Sens Multiple Access) : écoute du canal, s'il est silencieux émission. Collisions non absentes mais moins nombreuses.
2. CSMA/CD (CSMA with Collision Detection) : transmission et suspension lors de détection d'une collision et reprise ensuite après temporisation aléatoire. Avant de transmettre, le réseau est testé et si voie libre, la transmission commence → on émet et on écoute, il y a collision si le signal écouté différent de celui émet, on arrête l'émission qu'on réessaye après un temps aléatoire.
3. CSMA/CA (CSMA with Collision Avoidance): envoie trame test (TRRS: Request To Send), si ne collisionne pas, on peut émettre.
 - CSMA /CD utilisée sur toute topologie surtout bus.

Adresse IP

- Machine \Rightarrow adresse permettant de la distinguer de manière unique dans le monde entier dite @ IP. Constituée de 4 entiers entre 0 et 255 représentant chacun un octet et séparés par un point (32 bits). @ IP n'a pas de lien avec un emplacement géographique, indépendante de la couche matérielle.
- @ IP = identificateur du réseau (@ réseau) + identificateur machine sur ce réseau : @ IP = (identif_res, identif_ord)



L'en-tête d'unité de données de protocole contient également l'adresse réseau.

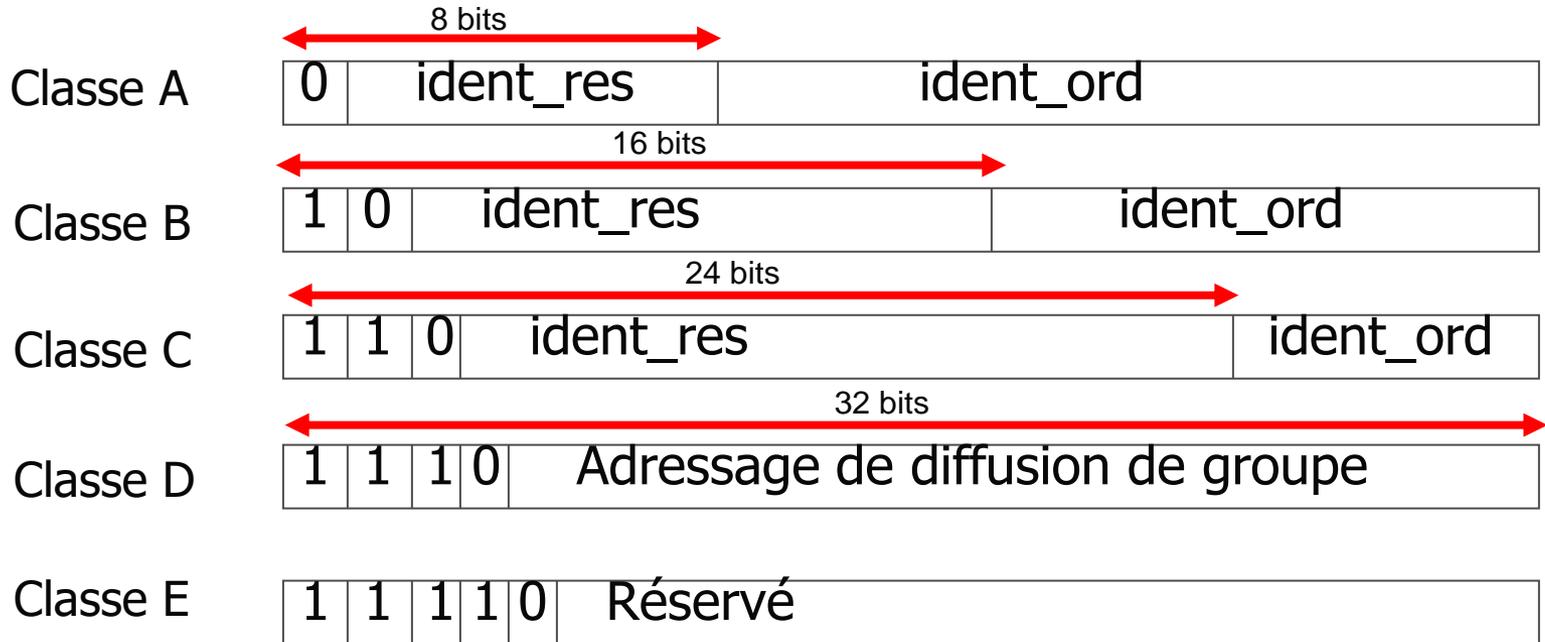


- @ IP publique attribuée par un organisme central, le NIC (Network Information Center) qui gère le plan d'@ et garantit son unicité.
 - @ IP publiques sont celles qui sont utilisées sur Internet.



Adresse IP

- 5 classes d'@ IP publique (A,B,C,D,E) : Classe A (Grand Réseau), Classe B (Réseau intermédiaire) et Classe C (petit réseau).



- @ IP : plus le N° du réseau est grand et plus le nombre d'hôtes sera petit.
- Réseau défini par son identité de réseau sur 7, 14 ou 21 bits selon la classe et @ IP ne spécifie pas réellement un ordinateur mais le point d'accès de cet ordinateur au réseau.



Classe d'adresse IP

- | ■ Classe | @ basses | @ hautes |
|----------|-----------|-----------------|
| A | 1.0.0.0 | 126.0.0.0 |
| B | 128.1.0.0 | 191.254.0.0 |
| C | 192.0.1.0 | 223.255.254.0 |
| D | 224.0.0.0 | 239.255.255.255 |
| E | 240.0.0.0 | 247.255.255.255 |
- Classe A : 126 réseaux avec 16777214 machines.
 - Classe B : 16383 réseaux avec 6445534 machines.
 - Classe C : 2097151 réseaux avec moins de 255 machines.
 - @ IP où ident_ord vaut 0 fait référence au LAN,
 - ident_res d'une @ IP vaut 0 fait référence au rang de la machine dans le LAN,
 - ident_ord ne comportant que des 1 réservé à la diffusion Broadcast.



Plan d'adressage

- Routeurs s'appuient sur les identif_res pour prendre les décisions de routage des datagrammes.
- Routeur dispose de 2 ou plusieurs interfaces (multi-connecté).
- Administrateur attribue l'ident_ord selon un plan d'adressage.
- Un LAN utilise des adresses privées.
- Dans chaque classe, une plage d'@ réservée à des fins privées
⇒ @ IP privées : non visibles sur Internet. La liste des @ privées autorisées :
 - Classe A : de 10.10.0.1 à 10.255.255.254 : 10/8
 - Classe B : de 172.16.0.1 à 172.31.255.254 : 172.16/12
 - Classe C : de 192.168.0.1 à 192.168.255.254 : 192.168/16



Sous-réseaux

- Classes A,B et C mal adaptées aux besoins croissants des réseaux. Pour combler cette lacune des classes, on fait appel au subnetting.
 - Subnetting : technique pour subdiviser un réseau en sous-réseaux \Leftrightarrow Réseau divisé en branches et les branches sont précisées au niveau des @.
 - On étend la partie identi_res de @ IP en empruntant un nombre variable de bits à la partie ident_ord, donc 2 ou 3 parties dans une adresse IP :
 - @ de réseau – (@ sous réseau) - @ machine
 - Identification du sous-réseau c`ad spécification du découpage est réalisée à l'aide d'un masque qui a le même format que @ IP et qui donne la partie de l'@ IP consacré au numéro du réseau.
 - Tous les bits à 1 du masque indiquent que les bits correspondants de l'@ IP décrivent l'identi_res et tous les bits à 0 permettent de définir chaque bit correspondant de l'@ IP comme un bit faisant partie de l'ident_ord.
 - Il ne faut pas qu'il y ait des "1" et des "0" croisés.



Sous-réseaux

- Les masques réguliers :

Classe	Exemple @ IP	Masque
A	10.0.0.0	255.0.0.0
B	128.2.0.0	255.255.0.0
C	192.9.201.0	255.255.255.0

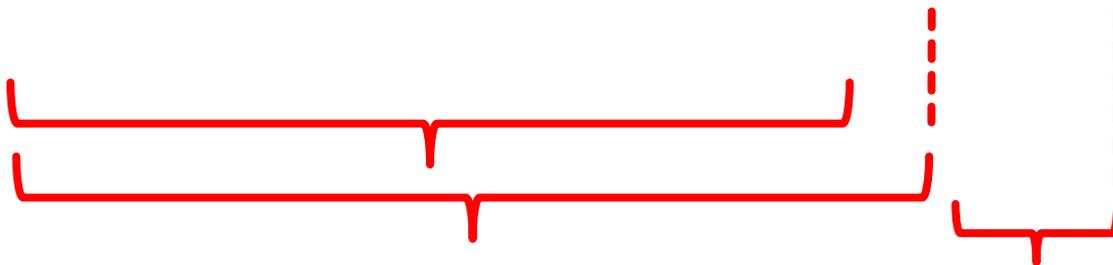
- Notation : @ IP 192.168.1.13 et masque 255.255.255.0 \Leftrightarrow 192.168.1.13/24.
- Sous réseaux d'un même réseau doivent avoir une taille identique (contrainte routeurs)

Sous-réseaux

- Masque irrégulier :

Dans l'exemple suivant basé sur un classe C, le masque de sous réseaux est de 27 bits, le numéro de sous réseaux sur 3 bits :

- 192 . 168 . 5 . 0
11000000.10101000.00000101.00000000



Bits du n° de la machine

Masque du sous réseau sur 27 bits :

11111111.11111111.11111111.11100000 càd 255.255.255.224

- Masque sous-réseau permet de créer des sous-réseaux qui ne respectent plus le découpage en classes A, B, C. Le masque sous-réseau définit la limite des bits d'adressage du réseau des bits d'adressage de la machine.



Sous-réseaux

- 192.168.10.5/255.255.255.0 ou 192.168.10.5/24 \Leftarrow 24 bits
ident_res sur 32 \rightarrow 192.168.10.0 \rightarrow 192.168.10.255
- 192.168.10.5/255.255.255.128 ou 192.168.10.5/25 \Leftarrow 25 bits
ident_res sur 32 \rightarrow 192.168.10.0 \rightarrow 192.168.10.127
- 192.168.10.5/255.255.252.0 ou 192.168.10.5/22 \Leftarrow 22 bits
ident_res sur 32 \rightarrow 192.168.8.0 \rightarrow 192.168.11.0