

LA COUCHE RESEAU



Par Dr GILBERT TINDO

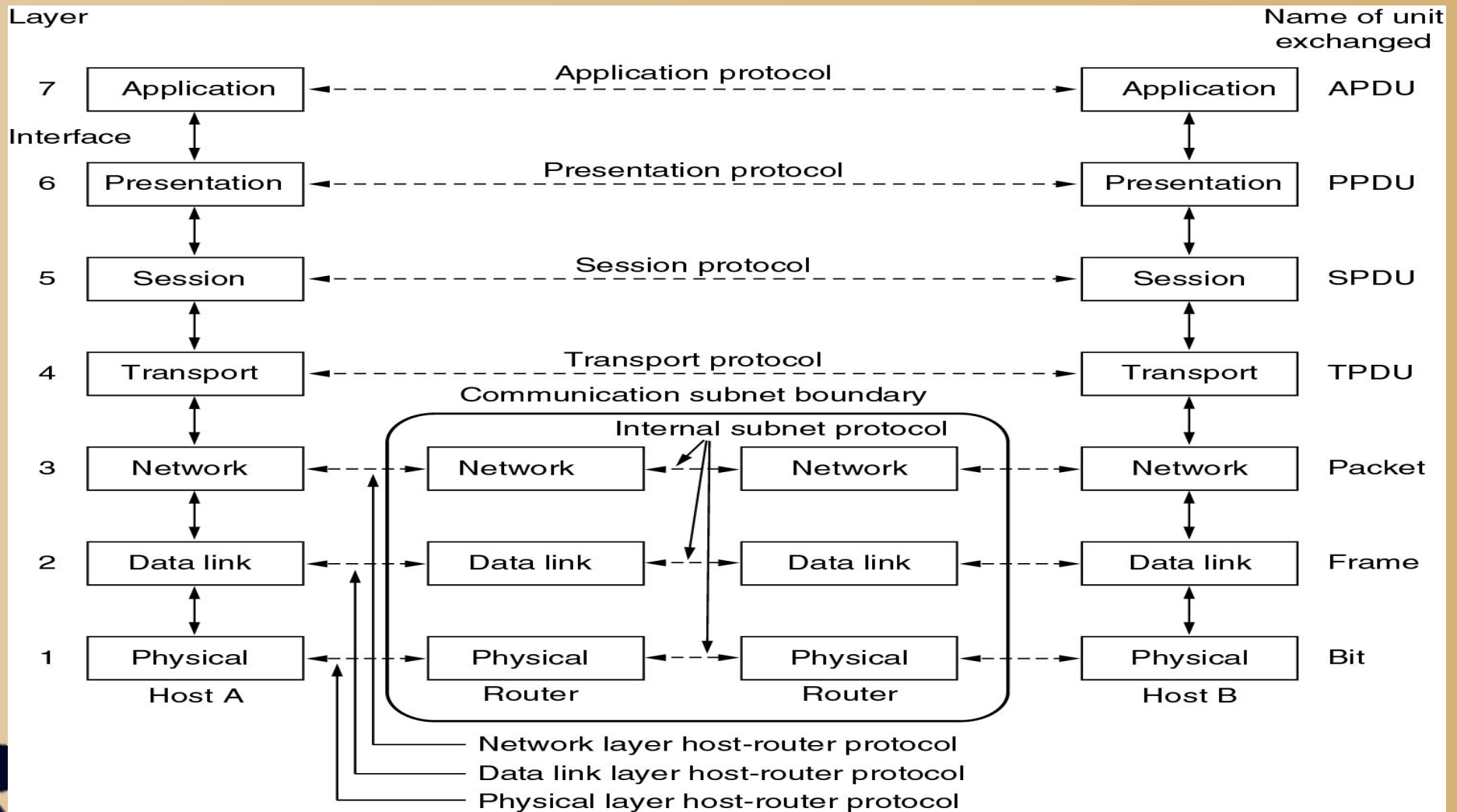
NB : Les illustrations de ce cours sont tirées du livre « Réseaux » de Andrew Tanenbaum, et des slides mis en ligne sur son site web.



COUCHE RESEAU

- PLAN :
- Services de la couche réseau
- Contrôle de flux
- contrôle de congestion
- Fragmentation
- Algorithmes de routage
- Le protocole IP
- Le protocole X.25
- Interconnexion de réseaux


Couche réseau dans le modèle ISO



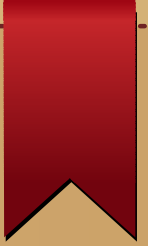
Equipements de la couche réseau



Les équipements intervenant dans cette couche peuvent être discriminés en deux classes :

- Ceux appartenant aux opérateurs de télécommunication
 - Les routeurs
 - Ceux appartenant aux clients de ces opérateurs
 - Les passerelles
 - Les postes de travail
 - Les commutateurs/routeurs
- 

Acheminement de paquets dans la couche réseau



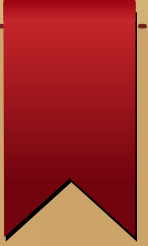
- La commutation de paquets
 - Algorithme de type « store and forward »
 - Paquet entièrement reçu , ensuite retransmission vers le routeur voisin
- La commutation de circuits
 - Un circuit= support physique entre deux noeuds
 - Réserver des circuits entre l'émetteur et le destinataire
 - Toutes l'information passe par ces circuits



Services de la couche réseau

- Services sans connexion (internet)
 - Les routeurs se contentent de transférer les paquets
 - Le sous réseau manque de fiabilité
 - Les hôtes doivent assurer les différents contrôles
- Services avec connexion (opérateur télécommunication)
 - établir les routes pour le transfert des paquets
 - Faciliter la gestion de la qualité de services

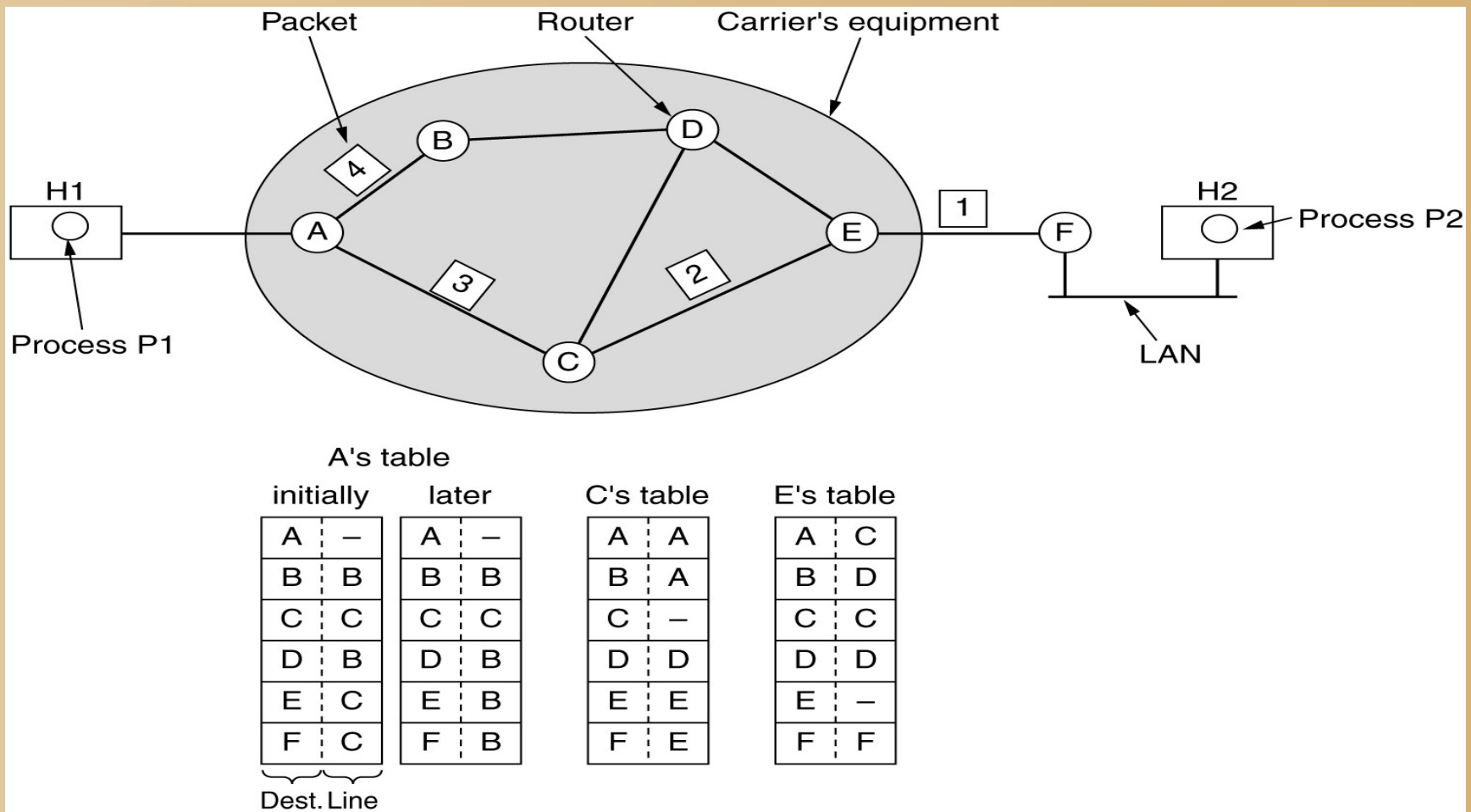
Implémentation service sans connexion



- Les paquets sont transférés individuellement et indépendamment les uns des autres
- Chaque paquet suit une route quelconque
- Chaque routeur maintient une table de routage qui peut être statique ou mise à jour dynamiquement
- Une entrée de la table indique :
 - Une destination
 - Le routeur voisin à qui envoyer le paquet (indique l'interface sur laquelle envoyer le paquet)



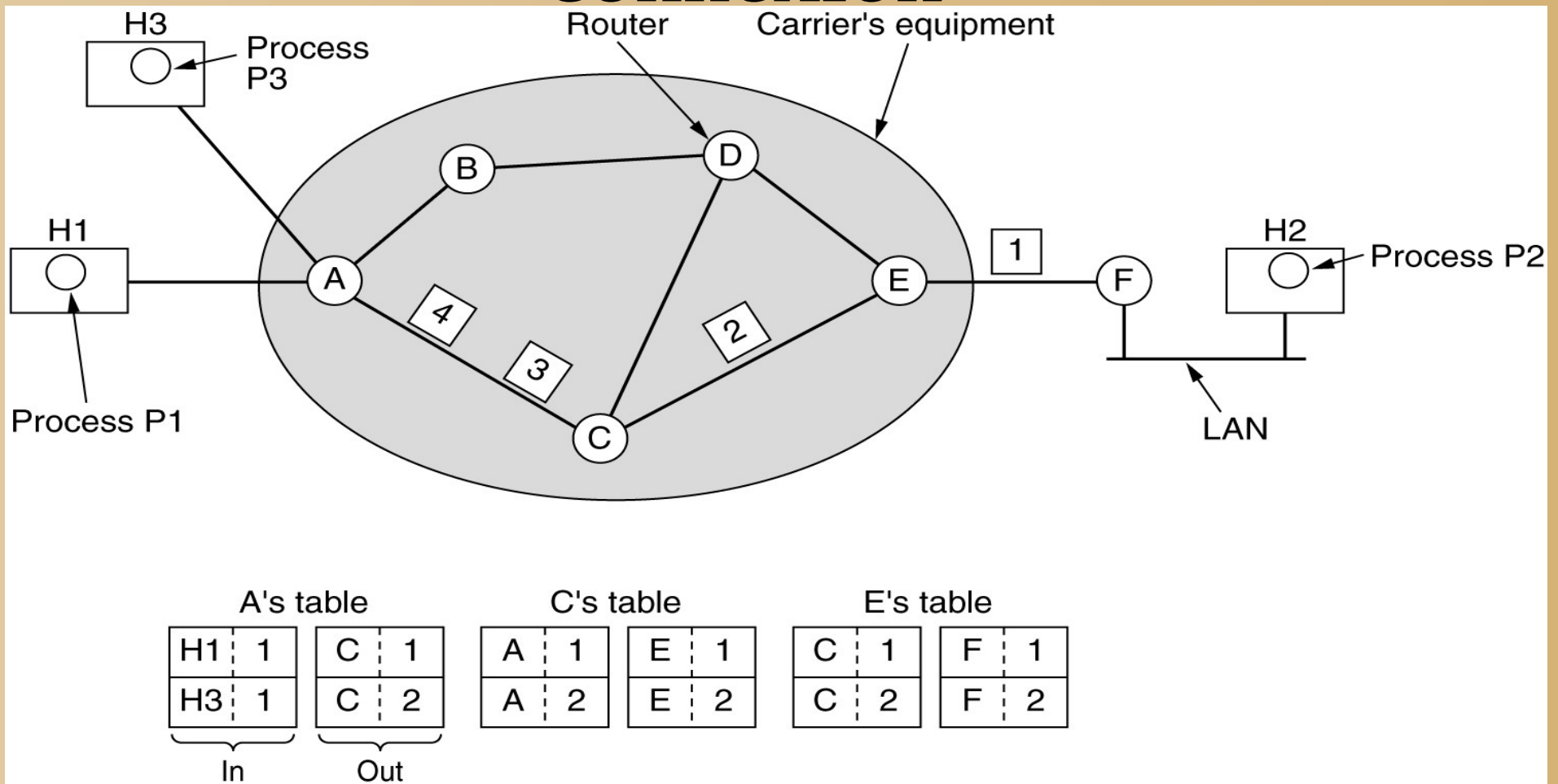
Implémentation service sans connexion



Implémentation service avec connexion

- Un circuit virtuel est établi entre la source et la destination
- Un circuit virtuel a un numéro
- Une entrée de la table de routage a quatre champs :
 - Adresse hôte émetteur
 - Numéro du circuit virtuel
 - Adresse hôte destination
 - Numéro circuit virtuel

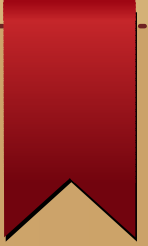
Architecture de communication : Implémentation de services avec connexion



Comparaisons service sans connexion service avec connexion

Aspect	Datagrammes	Circuits virtuels
Phase d'établissement	Non nécessaire	Requise
Adressage	Adresse source et destination dans chaque paquet	Identification de circuit dans chaque paquet
Routage	Chaque paquet routé indépendamment	Tous les paquets suivent la même route
Impact d'une panne de routeur	Aucun	Tous les circuits virtuels passant par ce routeur sont perdus

Comparaisons service sans connexion service avec connexion



Aspect	Datagrammes	Circuits virtuels
Qualité de service	Difficile à garantir	Facile à garantir si suffisamment de ressources peuvent être allouées par avance
Contrôle de congestion	Difficile	Facile à garantir si suffisamment de ressources peuvent être allouées par avance

Contrôle de flux


- Définition d'un flux (flot):
 - Un flux (flot) est un ensemble de paquets circulant dans le réseau et ayant un même émetteur et un même destinataire.
 - C'est donc un ensemble de paquets IP donc les champs adresse source et adresse destination sont exactement les mêmes

Contrôle de flux

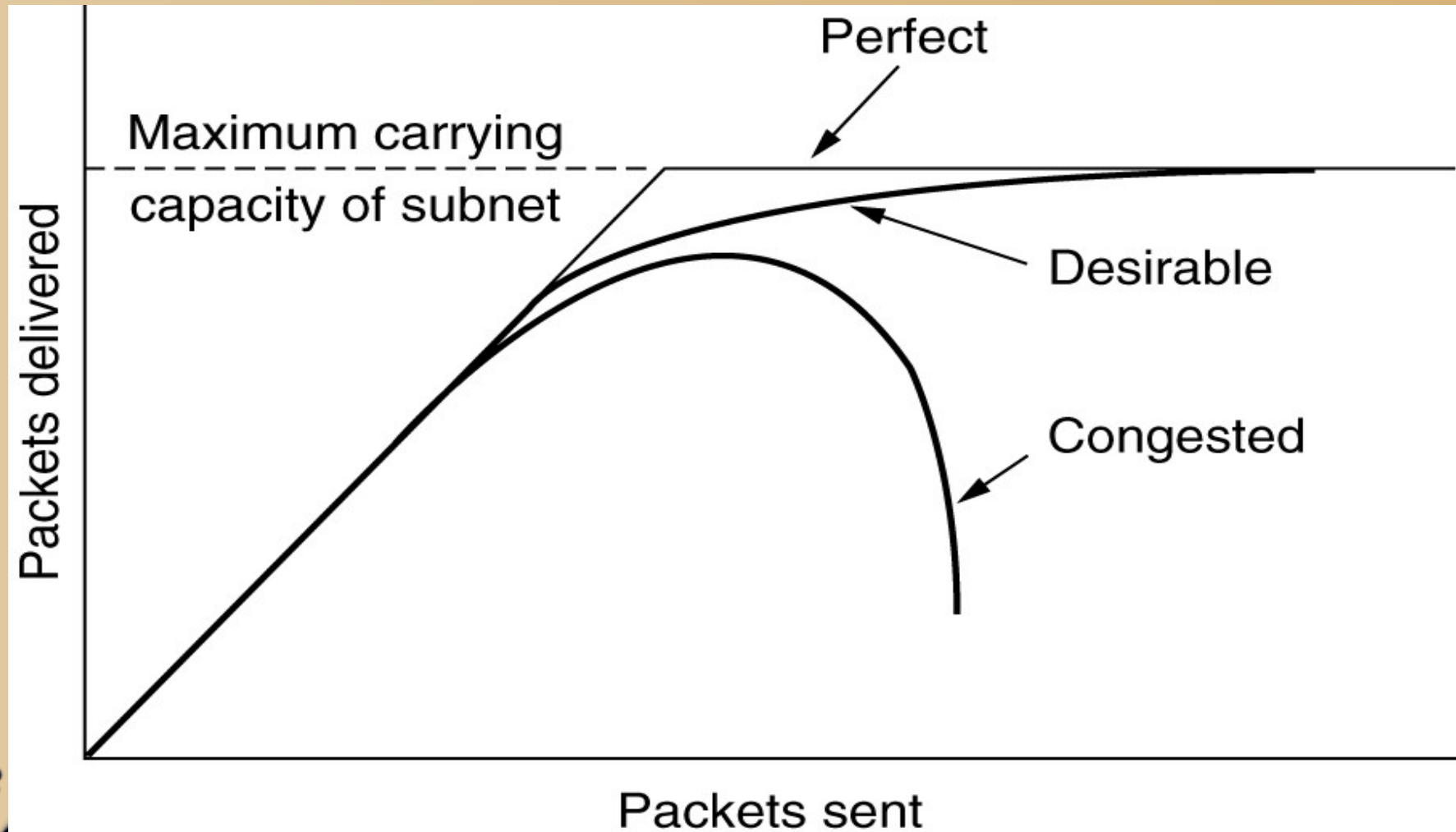
- Objectifs :
 - Gérer les paquets d'un flux pour qu'ils arrivent au destinataire dans un laps de temps le plus court possible
 - Eviter les pertes des paquets par écrasement dans les mémoires tampons des nœuds intermédiaires en cas de surcharge
- Le contrôle de flux s'effectue en général par une contrainte sur le nombre de paquets circulant dans le réseau.

Contrôle de congestion



- Quand un sous réseau a un moment donné a trop de paquets à transmettre, il se produit une dégradation des performances appelée congestion
 - Le nombre de paquets injectés par les hôtes dans le sous réseau est supérieur à la capacité du sous réseau
 - Des paquets seront perdus quand il y a congestion
- 

Contrôle de congestion



Contrôle de congestion

- Causes de la congestion :
 - Mémoire insuffisante aux noeuds :
 - Plusieurs paquets arrivent sur un nœud et doivent sortir par la même liaison → une file d'attente pour les contenir
 - Si la mémoire n'est pas suffisante pour les contenir, des paquets seront perdus
 - Trop de mémoire pour les files aux noeuds :
 - Les paquets peuvent attendre très longtemps avant d'être transmis
 - Les délais expirent et les hôtes retransmettent les paquets → surcharge du réseau

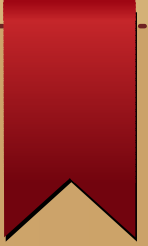
Contrôle de congestion

- Processeur lents dans les nœuds :
 - Temps de traitement d'un paquet long → les paquets s'accumulent et remplissent les files d'attente
 - Temps de la mise à jour des tables de routage long → les paquets attendent pour être routés
- Petite bande passante des différents liens entre les noeuds
- NB : Apporter une solution à l'un de ces problèmes ne va améliorer les performances que partiellement

Contrôle de congestion

- Le contrôle de congestion concerne les performances d'un sous réseau de façon globale
- Les métriques à utiliser pour contrôler la congestion sont :
 - Le pourcentage des paquets éliminés par manque d'espace dans les tampons
 - Les longueurs moyennes des files d'attente
 - Le nombre de paquets retransmis pour délais expirés
 - Le temps moyen d'acheminement des paquets
 - L'écart type du temps d'acheminement

Fragmentation



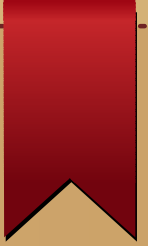
- Chaque réseau a une taille maximale pour les paquets qu'il transporte
- Cette limitation peut être due à plusieurs raisons :
 - Le matériel utilisé
 - Les protocoles mis en œuvre
 - Exigence de certaines normes internationales
 - Faciliter la gestion des erreurs
 - Diminuer le temps d'acheminement des paquets



Fragmentation

- Dans la couche réseau la taille des paquets varie de 48 octets (cellule ATM) à 65535 octets (paquet IP)
- Un routeur qui interconnecte deux sous réseaux gérant les paquets de tailles différentes doit trouver des stratégies pour que les paquets soient acceptés de part et d'autre de la frontière :
 - Un petit paquet va vers un réseau acceptant de plus gros paquet : Pas de problème. A la limite on peut faire du bourrage
 - Un grand paquet va vers un réseau acceptant de plus petits paquets : Problème → Fragmenter le paquet.

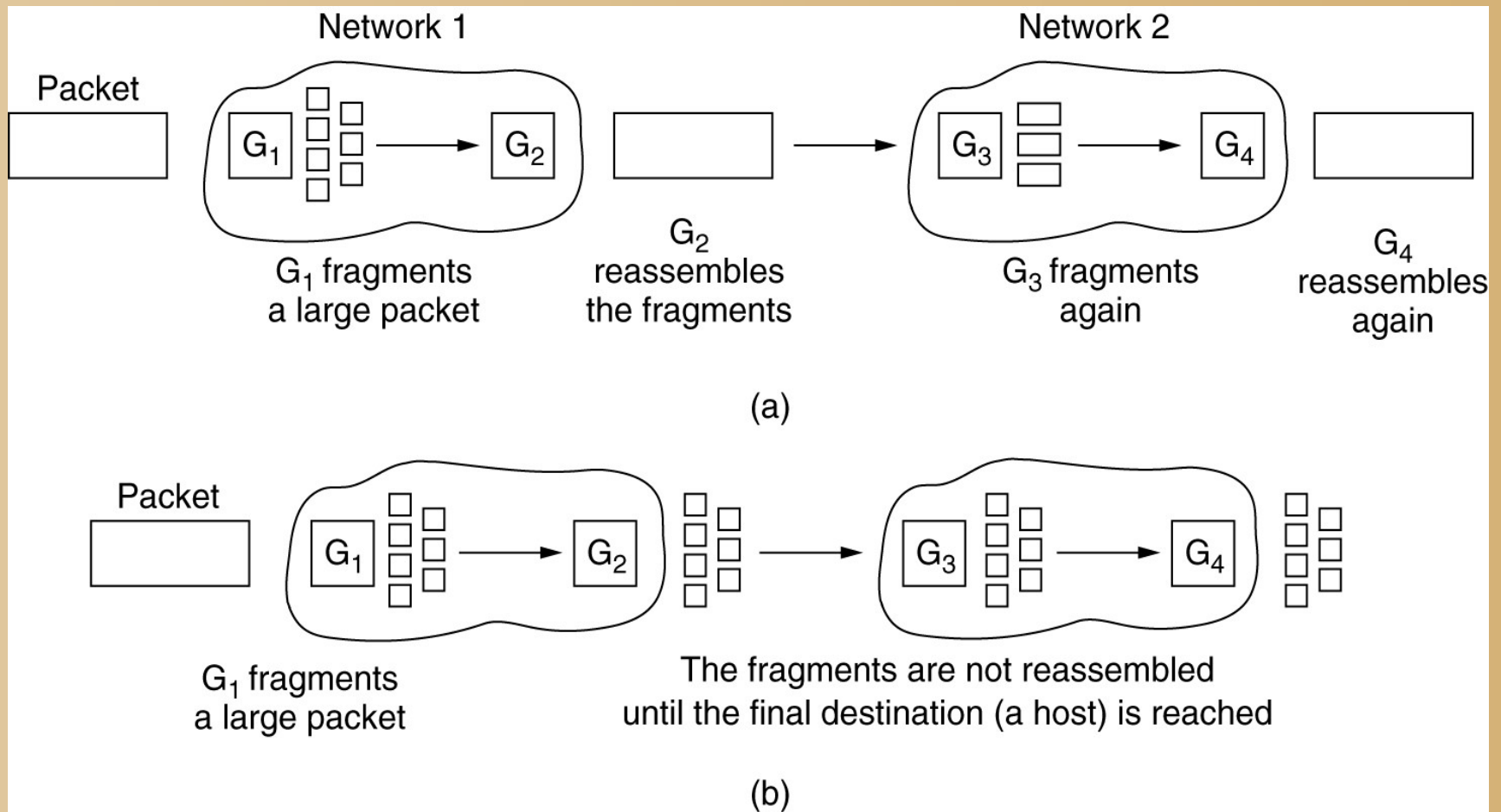
Fragmentation



- - Fragmentation transparente
 - Le routeur de bordure du réseau intermédiaire fragmente les gros paquets
 - L'autre routeur de bordure du réseau intermédiaire par lequel les morceaux doivent quitter le réseau intermédiaire assemble les morceaux pour former le paquet original
 - Fragmentation non transparente
 - Le routeur de bordure fragmente les paquets qui seront acheminés ainsi jusqu'à la destination
 - C'est le destinataire qui fera le réassemblage pour former le paquet initial



Fragmentation



Fragmentation

- Problèmes de la fragmentation transparente :
 - Tous les fragments doivent quitter un réseau intermédiaire en passant par le même routeur de bordure
 - Les fragments doivent être numérotés et il faut un code de fin pour le dernier fragment d'un paquet
 - La fragmentation et l'assemblage des paquets consomme du temps processeur au niveau des routeurs : surcharge du réseau

Fragmentation

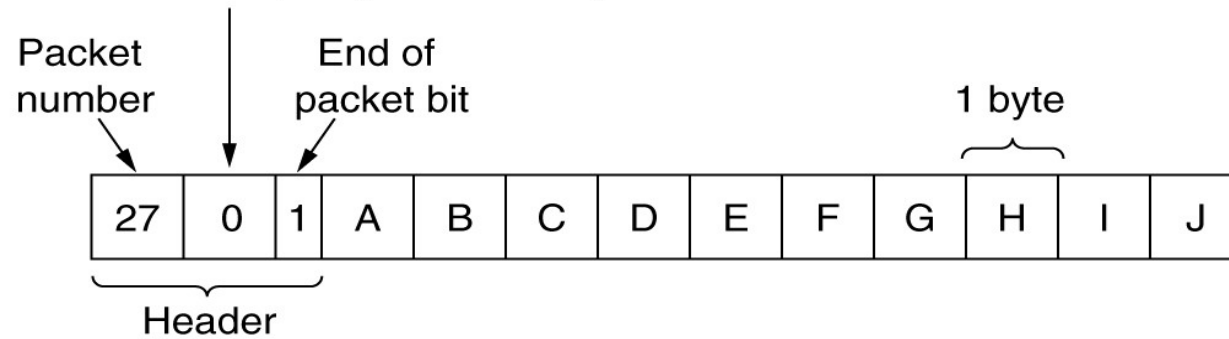
- Problèmes de la fragmentation non transparente :
 - Chaque destinataire doit être capable de faire le réassemblage
 - Chaque fragment a aussi des entêtes et éventuellement des enqueues → surcharge du réseau
- Avantages de la fragmentation non transparente :
 - Chaque fragment peut suivre n'importe quel chemin
 - La fragmentation se fait une seule fois
 - augmentation des performances

Fragmentation

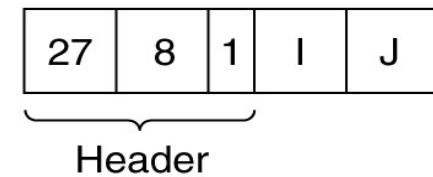
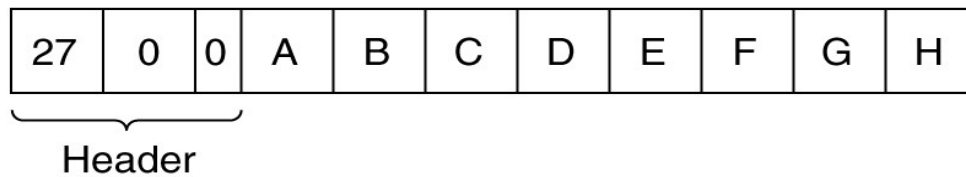
- Numérotation des fragments :
 - La taille du fragment élémentaire doit être suffisamment petite pour qu'il puisse traverser n'importe quel réseau sans être à nouveau fragmenté
 - Un fragment doit contenir le numéro du paquet d'origine
 - Le numéro d'un fragment doit être attribué par rapport à l'origine du paquet fragmenté

Fragmentation

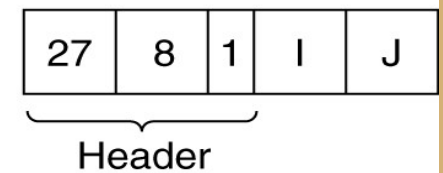
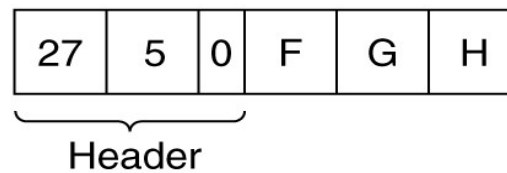
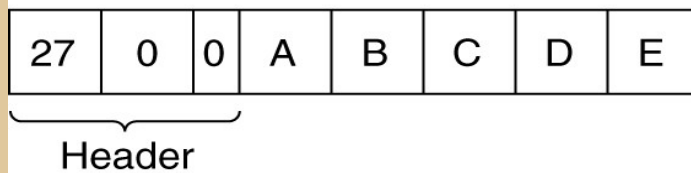
Number of the first elementary fragment in this packet



(a)



(b)



(c)

Algorithmes de routage

- Permettre de router des paquets d'une source vers une destination
- Il existe deux grands types d'algorithmes :
 - Les algorithmes non adaptatifs ou algorithmes statiques
 - Les routes sont calculées d'avance et transmises aux différents routeurs lors de l'initialisation
 - Les algorithmes adaptatifs
 - Les routes sont modifiées dynamiquement en fonction généralement de la topologie du réseau ou du trafic

Algorithmes de routage

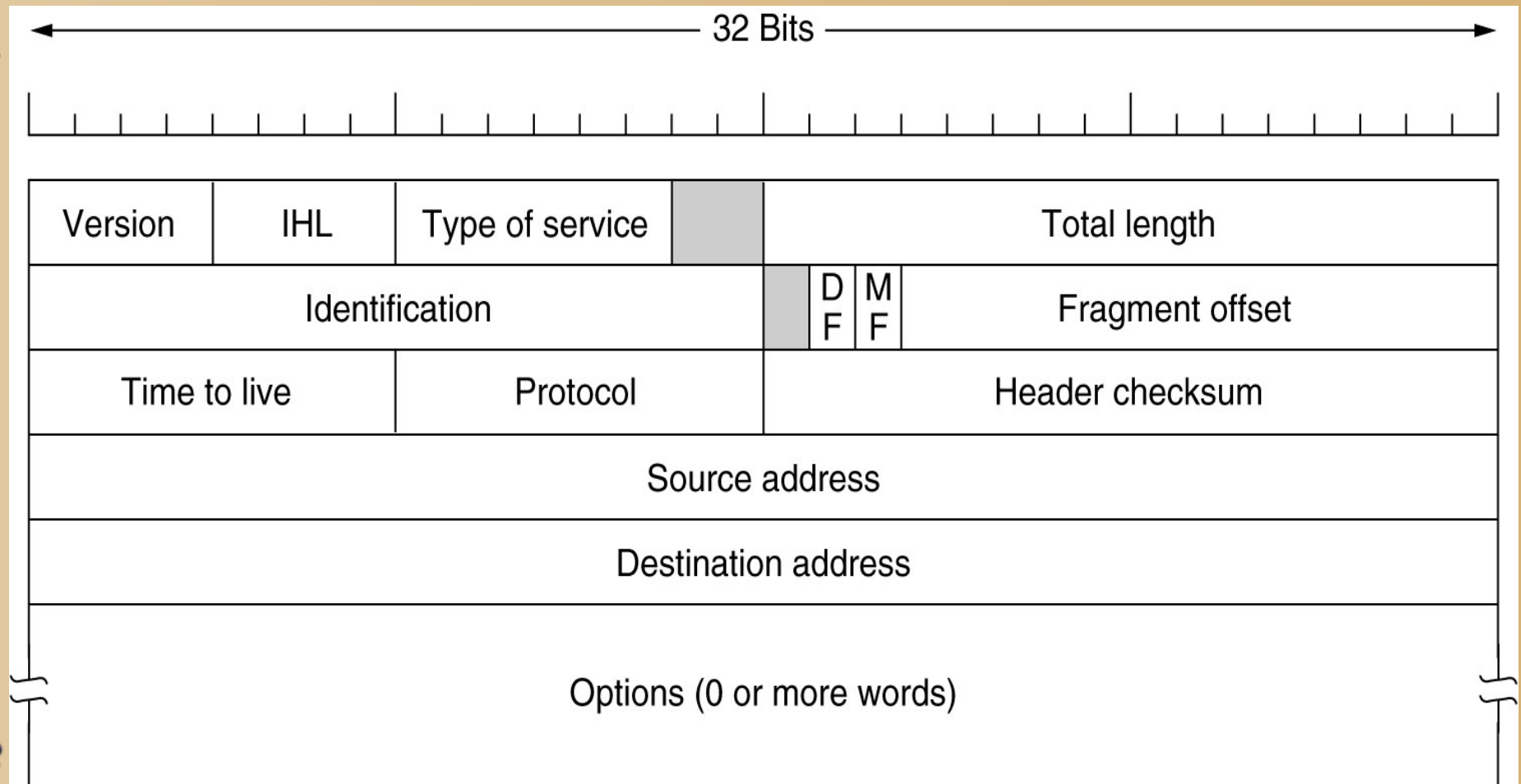
- Propriétés d'un bon algorithme :
 - L'exactitude
 - La simplicité
 - La robustesse (résister aux pannes des routeurs, aux changement de topologie)
 - La stabilité (doit converger vers un état d'équilibre)
 - L'équité

Le protocole IP

- La cohésion est assurée par le protocole IP qui a été conçu pour être un protocole d'interconnexion.
- La couche réseau doit faire de son mieux pour délivrer les paquets aux destinataires → il n'y a pas de garantie
- Un paquet émis par un hôte doit traverser plusieurs réseau intermédiaire avant d'arriver à la destination.

Le protocole IP

- Datagramme IPv4 :



Le protocole IP

- Datagramme IPv4:
 - Deux parties : entête et des données
 - L'entête comprend une partie fixe de 20 octets et une partie variable
 - L'entête est transmis suivant le mode gros-boutiste (big endian)
 - Champ version:4bits, indique la version du protocole
 - Champ LET : 4 bits indique la longueur de l'entête en nombre de mots de 32 bits → 60 octets maximum pour l'entête

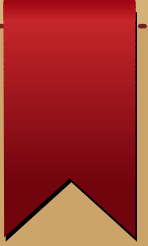
Le protocole IP

- Le champ type de service : (8 bits dont 6 utilisés)
 - Initialement :
 - 3 bits pour la priorité du paquet
 - 1 bit D → Evaluer chemin sur la base du délai de transmission
 - 1 bit T → Evaluer le chemin sur la base du débit de transmission
 - 1 bit R → Evaluer le chemin sur la base de la fiabilité de la transmission
 - 2 bits réservés
 - Après les six bits indiquent une classe de services :
 - Ils permettent de mettre en œuvre la qualité de services en divisant les paquets en classes de priorités
- Le champ suivant donne la longueur totale du datagramme : (16 bits → Max:65535 octets)

Le protocole IP

- Identification du paquet : 16 bits
- Un bit inutilisé
- Un bit DF (don't fragment), qui positionné indique de ne pas fragmenter le paquet
- Un bit MF (More fragment), qui positionné indique qu'un autre fragment du même paquet suit.
- Position du fragment (13bits), indique la position du fragment dans le datagramme : la taille d'un fragment doit être un multiple de 8 octets

Le protocole IP



- Le champ TTL (Time to live) : 8 bits, est un compteur servant à limiter la durée de vit d'un datagramme en secondes. Il est décrémenté d'une unité à chaque saut de routeur ou chaque fois que le paquet dure plus d'une seconde dans le tampon. Le paquet est détruit dès qu'il atteint zéro.
- Un champ protocole : (8 bits), indique le protocol encapsulé :
 - 1=ICMP, 2=IGMP, 6=TCP, 17=UDP, 46=RSVP, 54=NHRP, 89=OSPF
- Un champ total de contrôle:(16 bits), permet de contrôler les erreurs de transmission de l'entête
- Adresse source (32 bits)
- Adresse de destination (32 bits)



Le protocole IP

- Le champ option doit être un multiple de 4 octets. Une option peut indiquer :
 - Le degré de sécurité du datagramme
 - Décrire le chemin à suivre par le paquet
 - Donner une liste de routeurs à emprunter absolument
 - Enregistrer la route suivie par le paquet
 - Obliger chaque routeur à enregistrer la date où il a vu le paquet

Le protocole IP

- adresses Ipv4 :
 - Chaque nœud d'un réseau a une adresse Ipv4 sur 32 bits
 - Les adresses sont regroupées en classes :

← 32 Bits →				Range of host addresses
Class				
A	0	Network	Host	1.0.0.0 to 127.255.255.255
B	10	Network	Host	128.0.0.0 to 191.255.255.255
C	110	Network	Host	192.0.0.0 to 223.255.255.255
D	1110	Multicast address		224.0.0.0 to 239.255.255.255
E	1111	Reserved for future use		240.0.0.0 to 255.255.255.255

Le protocole IP

- Quelques adresses spéciales :

•	0 0	This host
•	0 0 ... 0 0 Host	A host on this network
	1 1	Broadcast on the local network
	Network 1 1 1 1 ... 1 1 1 1	Broadcast on a distant network
	127 (Anything)	Loopback

Le protocole IP

- Avec ce regroupement en classes des adresses IP, une organisation peut se voir attribuer une classe de réseau, et pourtant elle ne dispose pas du nombre d'hôtes prévus dans cette classe → Il y a pertes d'adresses IP
- Dans la table de routage d'un routeur, on a comme information :
 - Un numéro d'adresse de réseau pour les classes A et ou un haché pour les réseaux de classe C.
 - Un nom d'interface sur laquelle envoyer le paquet
 - Quand un paquet arrive :
 - Extraire l'adresse de réseau du paquet à l'aide du masque
 - Parcourir la table à la recherche d'une correspondance

Le protocole IP : Solutions au problème de manque d'adresses

- Les réseaux privées :
 - Classe A : 10.0.0.0 le masque de réseau est : 255.0.0.0
 - Classe B : 172.16-31.0.0 le masque est 255.255.0.0
 - Classe C : 192.168.0-255.0 le masque est 255.255.255.0
- Les adresses privées ne doivent pas se retrouver sur internet. Elles peuvent être réutilisées pour définir des réseaux locaux différents
- Pour se connecter à internet, un hôte privé doit utiliser les services d'une passerelle ayant une adresse publique.

Le protocole IP : Solutions au problème de manque d'adresses

- La passerelle permettant de relier des hôtes privées à internet fait de la translation d'adresse réseau (NAT : Network Address Translation)
- La passerelle utilise une table de translation pour faire la NAT. On distingue la NAT statique, la NAT dynamique et la NAT par port.
- Dans internet, c'est la passerelle et son adresse publique qui sont connues.

Le protocole IP : Solutions au problème de manque d'adresses

- Dans la NAT statique : La passerelle a autant d'adresses privées que d'adresses publiques.
- Dans la NAT dynamique : La passerelle gère moins d'adresses publiques qu'il y a d'adresses privées.
- Dans la NAT par adresses et par port (NAPT) : La passerelle gère une seule adresse publique pour toutes les adresses privées. Elle se sert des ports pour faire la translation.

Le protocole IP : Solutions au problème de manque d'adresses

- Les sous réseaux avec classes à adressage fixe :
 - Tous les sous réseaux ont le même masque
 - Le principe consiste à étendre l'adresse réseau à quelques bits consécutifs de poids forts de la partie adresse d'hôte
 - Le masque de sous réseau est calculé en y ajoutant autant de 1 que de bits de la partie hôte pris en compte dans l'adresse de réseau.
 - Le masque de réseau est alors noté /n où n est le nombre de bits à 1 consécutifs de poids forts du masque réseau
 - Si L est la longueur du masque, alors le nombre d'hôte est $N=2^{(32-L)}-2$.

Le protocole IP : Solutions au problème de manque d'adresses

• Nombre d'hôtes maximum	Longueur de masque de sous-réseau	Masque de sous-réseau
• 2	/30	255.255.255.252
• 6	/29	255.255.255.248
• 14	/28	255.255.255.240
• 30	/27	255.255.255.224
• 62	/26	255.255.255.192
• 126	/25	255.255.255.128
• 254	/24	255.255.255.0
• 510	/23	255.255.254.0
• 1022	/22	255.255.252.0
• 2046	/21	255.255.248.0

Le protocole IP : Solutions au problème de manque d'adresses

- Les sous réseaux avec classes à adressage variable : (VLSM:Variable Length Subnet Mask)
 - Les sous réseaux n'ont pas le même masque
 - Les sous réseaux ont un nombre d'hôtes différents
 - Commencer par les sous réseaux ayant le plus grand nombre d'hôtes
 - Terminer par les réseaux ayant le plus petit nombre d'hôtes
 - **Exemple** : Une entreprise veut découper son réseau de classe B d'adresse 173.120.0.0 en :
 - 09 sous réseaux de 2500 machines
 - 10 sous réseaux de 1500 machines

Le protocole IP : Solutions au problème de manque d'adresses

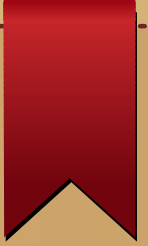
- Principes du partitionnement en sous réseaux avec classes
 - Tenir compte du nombre de sous réseaux. Choisir toujours un nombre de bits minimum pouvant représenter tous les sous réseaux
 - Le nombre de bits restant doit pouvoir représenter tous les hôtes
 - Tenir compte en général des sous réseaux tout à zéro (subnet zero). Seul 0.0.0.0 est encore utilisé
 - Tenir compte en général des sous réseaux tout à un (all-ones subnet) → La diffusion dans tous les sous réseaux n'est plus autorisée : Problèmes de sécurité

Le protocole IP : Solutions au problème de manque d'adresses

- Avantages du découpage en sous réseaux :
 - Une entreprise qui a plusieurs réseaux physiques peut se contenter dans certains cas d'une seule adresse publique
 - La taille des tables de routage se trouve ainsi réduite
 -

Utilisation de plusieurs media (câbles, supports physiques). La connexion de tous les noeuds à un seul support de réseau peut s'avérer impossible, difficile ou coûteuse lorsque les noeuds sont trop éloignés les uns des autres ou qu'ils sont déjà connectés à un autre media.

Le protocole IP : Solutions au problème de manque d'adresses



Avantages de l'organisation en sous réseaux :

- **Réduction de l'encombrement.** Le trafic entre les noeuds répartis sur un réseau unique utilise la largeur de bande du réseau. Si les noeuds d'un sous réseau communiquent principalement avec d'autres noeuds du même sous réseau, l'encombrement global est réduit. ---> Bande passante globale nécessaire réduite.



Le protocole IP : Solutions au problème de manque d'adresses



Avantages de l'organisation en sous réseaux :

- **Economise les temps de calcul.** Les diffusions sur un sous-réseau reste dans le sous-réseau. Les autres nœuds gagnent en temps de traitement de cette diffusion.
- **Isolation d'un réseau.** La division d'un grand réseau en plusieurs réseaux de taille inférieure permet de limiter l'impact d'éventuelles défaillances sur le réseau concerné.




Le protocole IP : Solutions au problème de manque d'adresses

Avantages de l'organisation en sous réseaux :

- **Renforcement de la sécurité.** Sur un support de diffusion du réseau comme Ethernet, tous les noeuds ont accès aux paquets envoyés sur ce réseau. Si le trafic sensible n'est autorisé que sur un sous réseau, les autres hôtes du réseau n'y ont pas accès.
- **Optimisation de l'espace réservé à une adresse IP.** Si un numéro de réseau de classe A, B ou C vous est assigné et que vous disposez de plusieurs petits réseaux physiques, vous pouvez répartir l'espace de l'adresse IP en multiples sous-réseaux IP et les assigner à des réseaux physiques spécifiques. Cette méthode permet d'éviter l'utilisation de numéros de réseau IP supplémentaires pour chaque réseau physique.

GESTION DE L'ADRESSAGE IP



- Chaque machine de l'internet est identifiée de façon unique par son adresse IP
 - Les adresses IP sont gérées au niveau mondial par ICANN (Internet Corporation for Assigned Names and Numbers)
 - Il définit les procédures d'attribution et de résolution de conflits dans l'attribution des adresses.
 - Il délègue le détail de la gestion de ces ressources à des instances régionales (RIR :Regional Internet Registries)
 - Les instances régionales travaillent avec les LIR (Local Internet Registries) de chaque pays.
- 

GESTION DE L'ADRESSAGE IP

- Il y a cinq RIR au monde :
 - APNIC pour la région Asie-Pacifique,
 - ARIN pour l'Amérique
 - RIPE NCC pour l'Europe
 - AfriNIC pour l'Afrique
 - LACNIC pour l'amérique latine
- NB : un LIR peut être un FAI ou une grande entreprise comme CAMTEL.
- Pour obtenir une adresse IP, un utilisateur s'adresse à son LIR

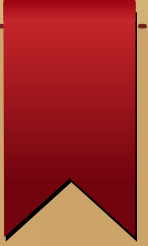
GESTION DE L'ADRESSAGE I

- Certaines adresses sont réservées :
 - Tous les bits sont à zéro=Cet hôte inconnu sur ce réseau. Adresse utilisée par une machine n'ayant pas encore d'adresse
 - Tous les bits de la partie réseau à zéro : Cet hôte sur ce réseau
 - Tous les bits de la partie hôte à zéro= Adresse du réseau
 - Tous les bits de la partie hôte à un= Adresse de diffusion, c'est-à-dire tous les hôtes du réseau
 - Tous les bits de la partie réseau à un et tous les bits de la partie hôte à zéro=Masque de réseau
 - Tous les bits à un=Tous les hôtes de tous les réseaux

GESTION DE L'ADRESSAGE IP

- Avec ce regroupement en classes des adresses IP, une organisation peut se voir attribuer une classe de réseau, et pourtant elle ne dispose pas du nombre d'hôtes prévus dans cette classe → Il y a pertes d'adresses IP
- Dans la table de routage d'un routeur, on a comme information :
 - Un numéro d'adresse de réseau pour les classes A et ou un haché pour les réseaux de classe C.
 - Un nom d'interface sur laquelle envoyer le paquet
 - Quand un paquet arrive :
 - Extraire l'adresse de réseau du paquet à l'aide du masque
 - Parcourir la table à la recherche d'une correspondance

LES SUPER RESEAUX

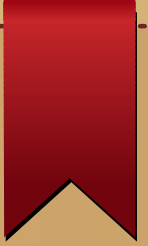


LES SUR-RESEAUX (Super réseaux) : supernetting

- Regrouper plusieurs réseaux consécutifs d'une même classe en unique réseau géré comme un seul réseau au niveau des routeurs.
- La partie adresse réseau est réduite de k bits. On regroupe donc 2^k réseaux de même classe pour former un unique réseau.
- La partie adresse hôte est étendue de k bits.
- Il y a au niveau des routeurs, une seule entrées pour tous les k réseaux.



LE CIDR



LE CIDR (Classless InterDomain Routing) :

- C'est une généralisation des super-réseaux
- Dans les routeurs, les masques de réseaux ne sont plus liés au classe, mais sont indiqués par leur longueur en bit de type /n.
- Le nombre d'adresses allouées est une puissance de deux et elles sont consécutives.
- Une entrée de la table de routage contient une adresse et son masque.



LE CIDR

- Routage CIDR (Classless InterDomain Routing)
 - Il n'y a plus de notion de classes
 - Le masque est représenté /n
 - On alloue des blocs de k adresses où k est une puissance de deux et dont la première adresse est un multiple de k.
 - Permet de faire le super netting, aggrégation de plusieurs réseau
- Une entrée d'une table de routage contient :
 - Une adresse de réseau destinataire
 - Un masque de réseau sous la forme /n
 - Un nom d'interface
 - NB : Quand un paquet arrive, parcourir la table à la recherche du plus long masque qui coïncide

Une autre solution au problème de manque d'adresses

- Adresses dynamiques (dhcp):
 - Un ensemble d'adresses IP est distribué à un nombre plus grand de machines
 - Une même adresse IP peut être attribuée à des machines différentes à des moments différents
 - On profite du fait qu'à un instant donné toutes machines d'un réseau ne sont pas toutes actives
 - Une machine qui n'est active n'a donc pas d'adresse

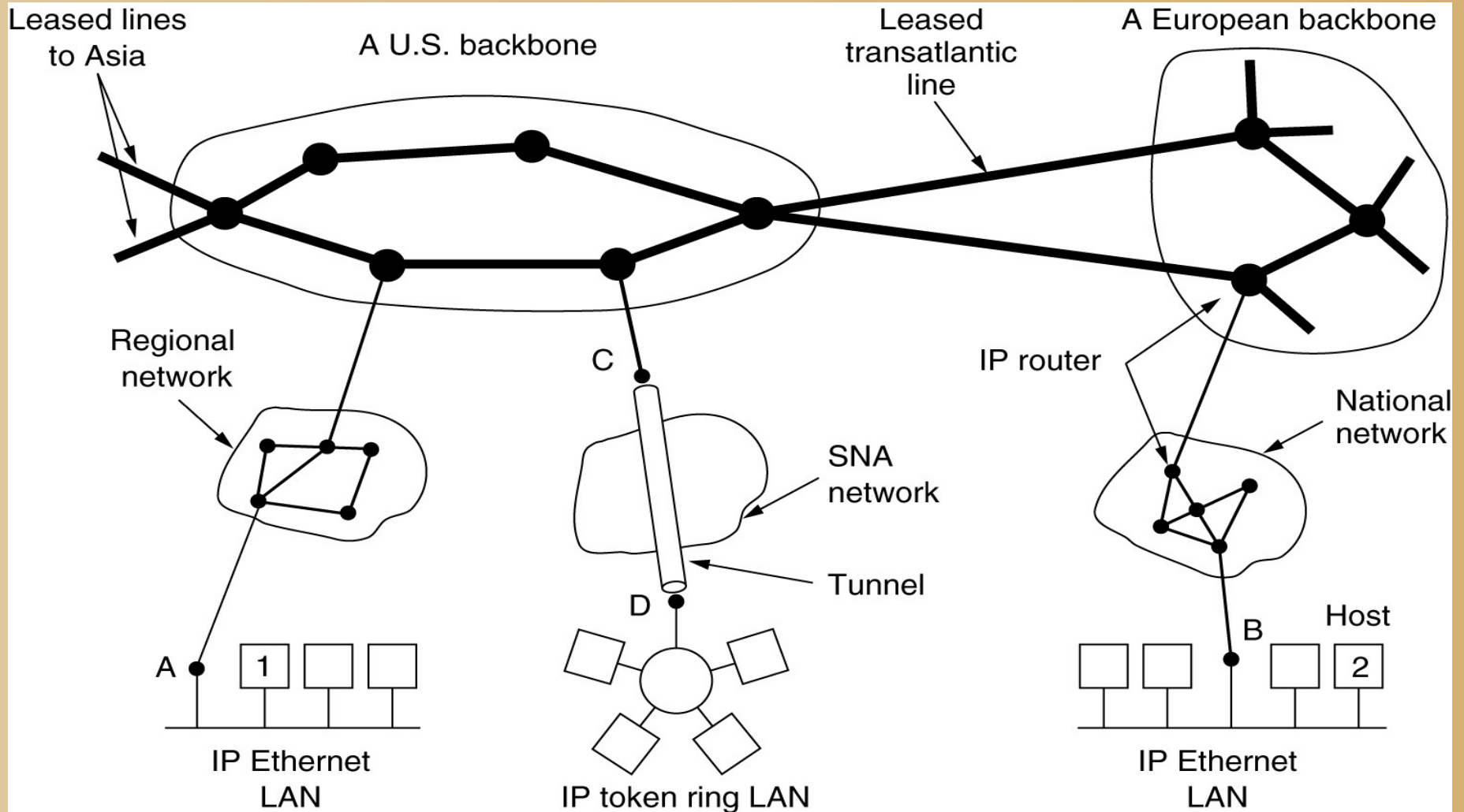
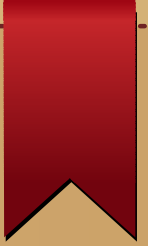
Interconnexion de réseaux

- Un inter-réseau est une interconnexion d'un vaste ensemble de réseaux différents ; exemple : Internet
- Les différences peuvent se situer au niveau :
 - Des services offerts (avec ou sans connexion)
 - Des protocoles (IP,IPX, AppleTalk, ...etc)
 - Adressage (linéaire ou hiérarchique)
 - Diffusion (supportée ou non supportée)
 - Taille des paquets(chaque réseau définit sa taille des paquets)

Interconnexion de réseaux

- De la qualité de service (disponible ou non)
- Gestion des erreurs (liaisons fiables ou non fiable)
- Contrôle de flux (disponible ou non, utilisation ou non de fenêtre)
- Contrôle de congestion (types d'algorithmes implémentés)
- Sécurité (les règles d'authentification et de confidentialité utilisée)
- Facturation (par temps, par paquet, par octets ou pas de facturation)

Interconnexion de réseaux



Interconnexion de réseaux

- Dans un interréseau, un paquet émis d'une source vers une certaine destination, doit traverser un ensemble de réseaux pouvant être complètement différents du réseau émetteur et du réseau récepteur.
- On peut y rencontrer les problèmes suivants dûs aux différences :
 - Un paquet avec connexion qui doit traverser un réseau n'offrant que les services sans connexion

Interconnexion de réseaux



- La réalisation des conversions de protocoles peut être difficile si l'un n'offre pas toutes les primitives fournies par l'autre
- Les traductions d'adresses peuvent être difficiles et exiger l'existence d'annuaires
- Un paquet qui exige une livraison en temps réel traverse un réseau qui n'offre pas de temps réel
- ... etc



Interconnexion de réseaux

- L'interconnexion de deux réseaux peut se faire :
 - Au niveau physique
 - Au niveau liaison de données
 - Au niveau réseau
 - Transport
 - application
- Au niveau physique on utilise des hubs et des répéteurs :
 - Ils permettent de transférer des bits entre deux réseaux et ne font que régénérer les signaux
 - Ils ne comprennent pas les protocoles numériques

Interconnexion de réseaux

- Au niveau de la couche liaison de données, on utilise des ponts et des commutateurs :
 - Ils sont capables de recevoir des trames entrantes, examiner leurs adresses MAC, et les retransmettre en réalisant un minimum de modifications
 - Ils permettent par exemple de transférer une trame d'un réseau ethernet vers un réseau 802.11
- Au niveau de la couche réseau, on se sert des routeurs. Un routeur multiprotocole est un routeur capable de gérer plusieurs protocoles.

Interconnexion de réseaux

- Au niveau transport et application on utilise des passerelles :
 - Les passerelles de niveau transport relient deux réseaux utilisant des protocoles de transport différents
 - Les passerelles de niveau application, s'occupent en général du format des messages
 - Les transformations entre protocoles sont faites dans des hôtes en général munies de plusieurs interfaces réseau par un logiciel approprié.

Interconnexion de réseaux

- Un hôte A appartenant à un sous réseau veut émettre un paquet à un hôte B appartenant à un autre sous réseau
- Modèle à circuits virtuels concaténés :
 - L'hôte établit un circuit avec le routeur le plus proche de son sous réseau
 - Le routeur le plus proche de A, établit un circuit virtuel avec le routeur de son sous réseau qui est le plus proche de la destination

Interconnexion de réseaux

- Le routeur le plus proche de la destination construit un circuit virtuel avec un routeur multiprotocole
- Chaque routeur traversé consigne l'existence du circuit dans ses tables internes
- Le routeur multiprotocole construit un circuit virtuel avec un routeur d'un sous réseau le plus proche du sous réseau de destination.
- Le processus se poursuit de cette façon jusqu'à ce qu'on atteigne la destination.

Interconnexion de réseaux

- Modèle à datagrammes :
 - Les paquets sont acheminés individuellement et peuvent éviter les routeurs multiprotocoles
 - Les adresses sur les différents sous réseau peuvent être différents et ne pas avoir le même format. Il faudrait que le routeur multiprotocole garde une base de données sur les conversions d'adresses (difficile)
 - La solution est d'utiliser un paquet d'interréseau universel et faire en sorte qu'il soit reconnu par tous les routeurs
 - Les routeurs qui relient un sous réseau à un autre sous -réseau doit tout simplement savoir convertir IP au format propriétaire.

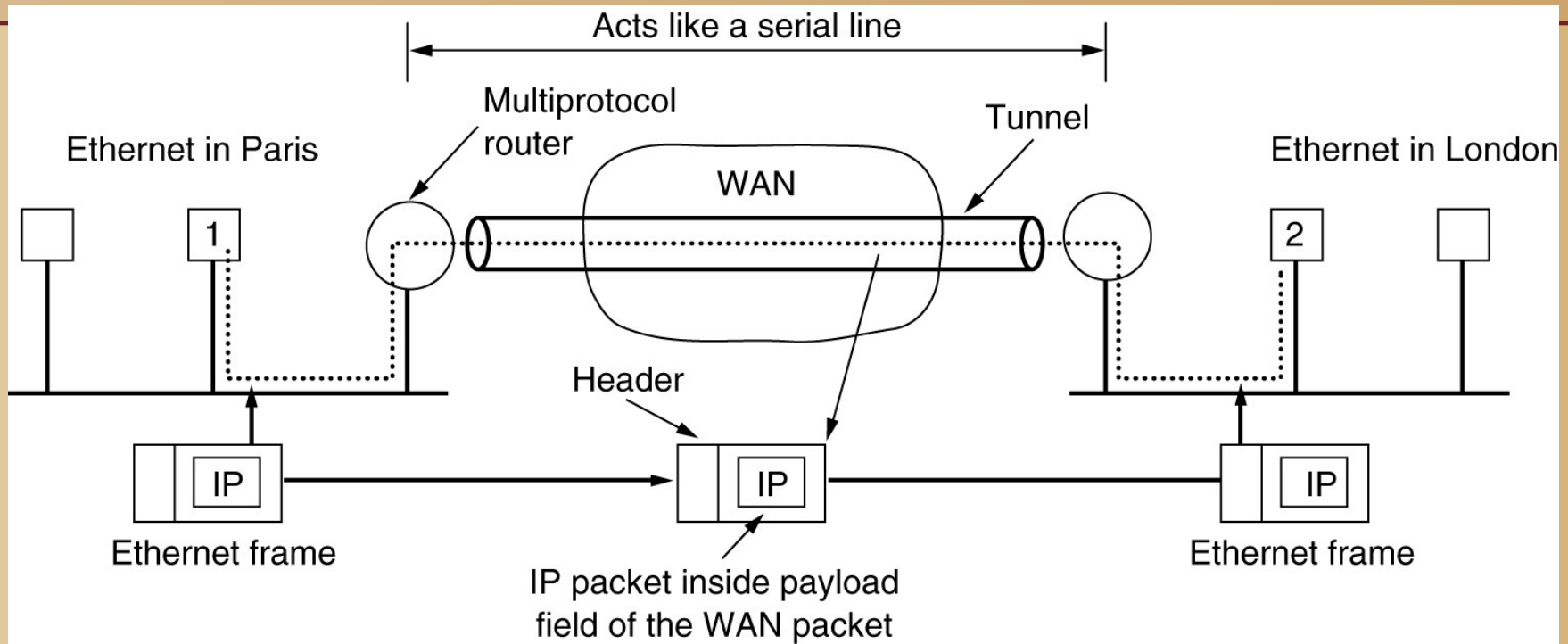
Interconnexion de réseaux

- Technique de tunnel :
 - Elle consiste à relier deux sous réseaux de même type à travers un sous réseau de type différent
 - Les routeurs de bordure des deux sous réseaux doivent être des routeurs multiprotocoles
 - L'hôte A prépare et encapsule un paquet IP dans une trame qu'il expédie à son routeur de bordure multiprotocole
 - Le routeur de bordure multiprotocole du sous réseau de l'hôte A, récupère le paquet IP de la trame et l'encapsule dans un paquet de couche réseau du sous réseau intermédiaire

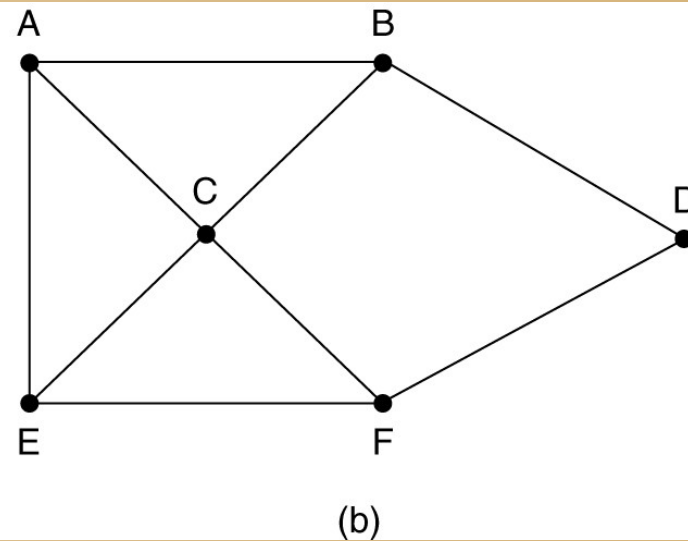
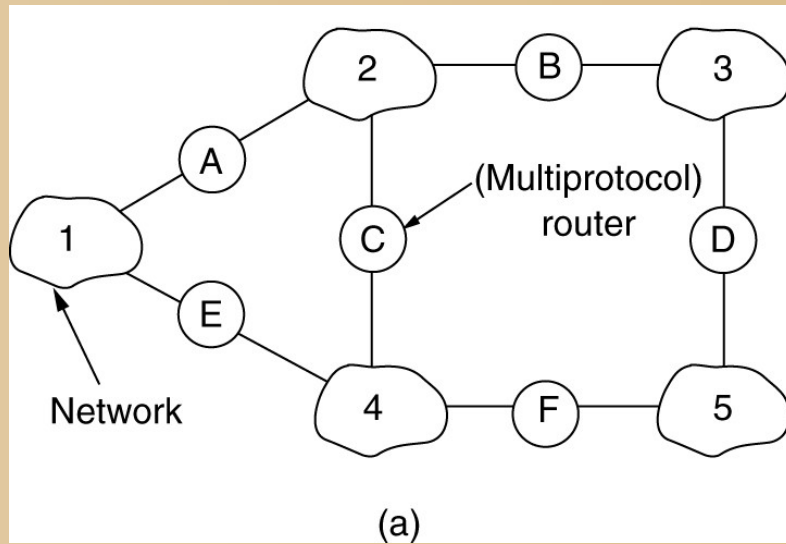
Interconnexion de réseaux

- Le routeur de bordure du réseau de destination récupère le paquet IP et l'encapsule dans une trame qu'il expédie dans le sous réseau de destination
- Le sous réseau intermédiaire se présente juste comme un long tunnel reliant le sous réseau source et le sous réseau de destination
- Le paquet IP traverse juste ce tunnel enfermé dans un paquet du réseau intermédiaire → Technique du tunnel.

Interconnexion de réseaux



Interconnexion de réseaux



Interconnexion de réseaux

- Le routage peut se situer à deux niveaux :
 - Utiliser un protocole de routage interne dans chaque sous réseau (Interior Gateway Protocol:IGP)
 - Utiliser un protocole de routage externe (Exterior Gateway Protocol:EGP)
- Supposons qu'un hôte du réseau 1 veuille envoyer un paquet à un hôte du réseau 3 :
 - Il fait un paquet IP qui sera encapsulé dans une trame et envoyé disons au routeur multiprotocole A

Interconnexion de réseaux

- Le routeur multiprotocole A découvre dans ses tables internes que le paquet va vers un hôte donc le routeur de bordure le plus proche est B.
- Si le sous réseau 1 et le sous réseau 2 utilise les mêmes protocoles alors le paquet est introduit dans 2 tel quel
- Sinon le paquet est encapsulé dans un paquet du protocole réseau du sous réseau 2 et dans ce cas le sous réseau 2 sert de tunnel vers l'hôte 3

Interconnexion de réseaux

- Le routage inter-réseau est rendu difficile par plusieurs problèmes :
 - Il peut traverser plusieurs frontières internationales ou des lois très strictes et différentes sont appliquées
 - Les métriques à utiliser pour calculer les coûts peuvent être complètement différentes
 - La qualité de service offert par les différents sous réseaux peut ne pas être la même