IFT-6800, Automne 2016

Cours #7–Introduction aux réseaux informatiques

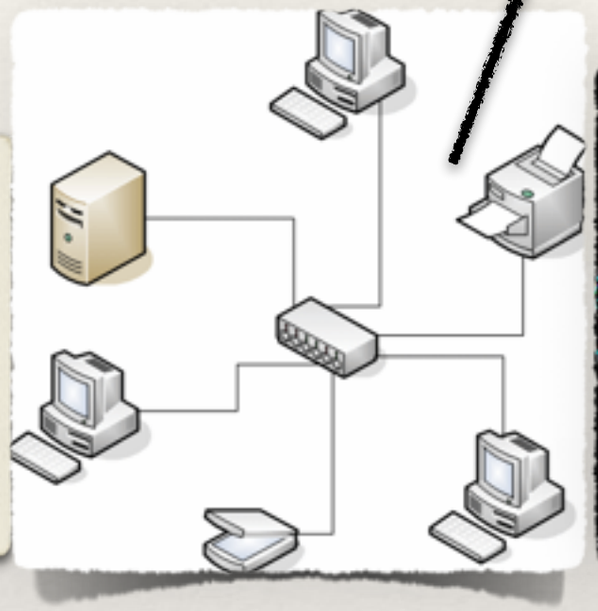
Louis Salvail
André-Aisenstadt, #3369
salvail@iro.umontreal.ca

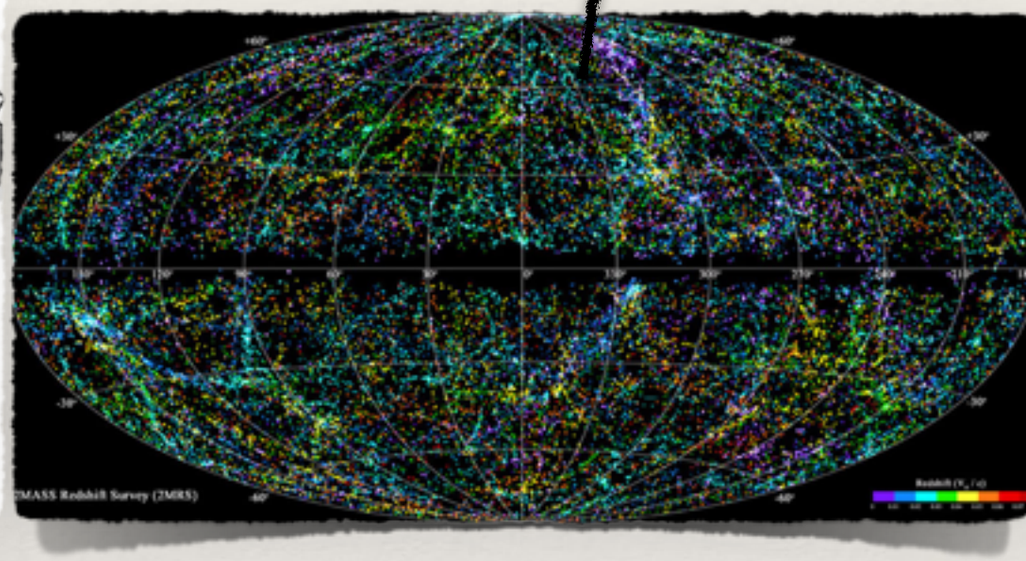
Les réseaux

réseau local comme dans un immeuble, un campus, une compagnie,…

Le plus gros des réseaux

- Un réseau est constitué d'ordinateurs reliés les uns aux autres.
- Des réseaux de toutes tailles existent, le plus petit d'entres-eux contient 2 ordinateurs:





- Les réseaux ne contiennent pas que des ordinateurs:
  - Imprimantes, scanners, ou autre matériel.
- Le but: permettre aux ordinateurs de communiquer entre-eux!

de s'échanger des données…

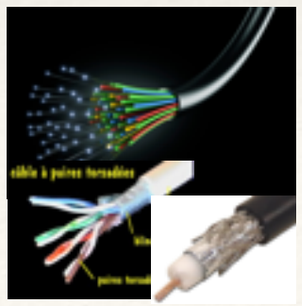
Réseaux locaux

- Ils sont appelés *Réseaux Locaux d'Entreprise* (*Local Area Networks 'LAN'* en anglais).
- Ils permettent d'interconnecter les ordinateurs et le matériel d'une entreprise ou d'une organisation.
- La circonférence d'un tel réseau est habituellement d'une centaine de mètres. Au-delà, les réseaux seraient nommés *Réseaux de Région Métropolitaine* (*Metropolitan Area Networks 'MAN'*).
- Concept qui date des années 1970, les employés d'une entreprise ont à disposition un système permettant:
    - d'échanger des information,
    - de communiquer et
    - d'avoir accès à des services divers.

Constituants matériel

- Un réseau local d'entreprise est composé d'un ensemble d'ordinateurs et de pièces matériels reliés par des éléments matériels et logiciels. Les éléments matériels utilisés pour interconnecter les composantes sont:
  - Carte réseau: Un ensemble de composants électronique sur un circuit imprimé. Elle assure l'interface entre l'équipement ou l'ordinateur dans lequel elle est installée et d'autres équipements connectés sur le même réseau.

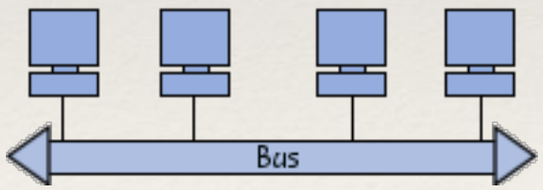
  - Adapteur (transceiver): Il permet d'assurer la transformation des signaux. C'est le premier élément électronique qui fait le lien entre l'ordinateur et le câblage réseau.
  - Prise: L'élément qui fait la jonction mécanique au réseau.

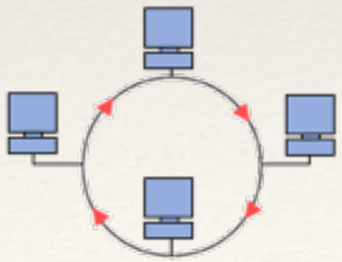


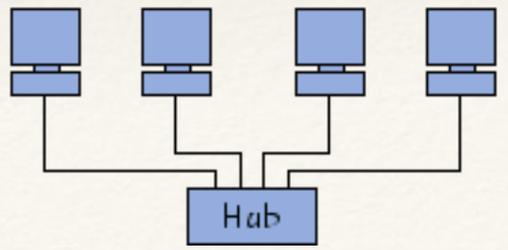
  - Support physique d'interconnexion: Le support sur lequel l'information est communiquée entre les ordinateurs et les éléments matériels. (fibres optiques, câbles en paires torsadées, câble coaxial, ondes Hertziennes,…)

Topologies des réseaux locaux

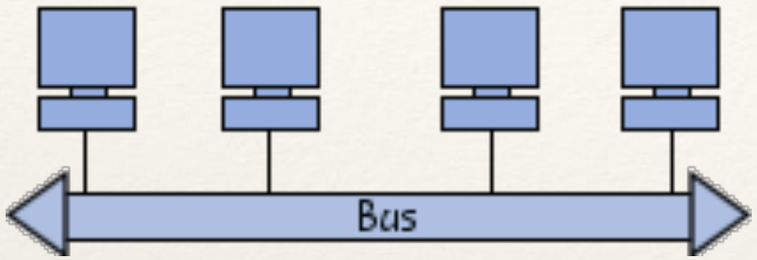
- Il n'est pas suffisant d'avoir les bonnes ressources matérielles pour mettre en place un réseau local. Il faut également que les ordinateurs connaissent la méthode d'accès aux informations transmises et reçus sur le réseau, en particulier lorsqu'il y a plus de deux ordinateurs. Ceci est appelé *topologie logique* du réseau. Le plus populaire:
  - *Ethernet*: Les ordinateurs sont reliés à une même ligne de transmission et la communication se fait à l'aide du protocole CSMA/CD. Ce protocole permet à toute les machines d'émettre lorsque désiré.
- La façon de connecter les ordinateurs physiquement sur le réseau est appelée topologie physique:
  - Topologie en bus:
  - Topologie en anneau:
  - Topologie en étoile:





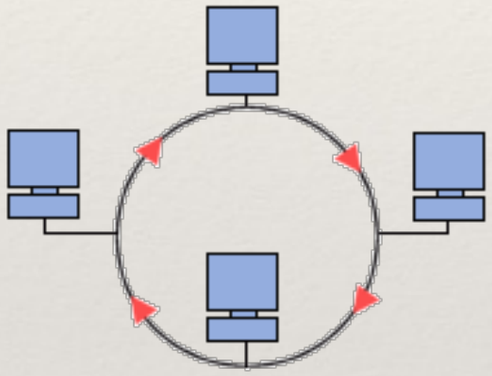


Topologies physiques

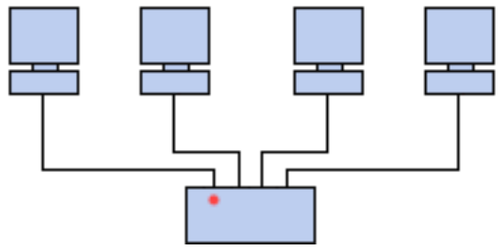


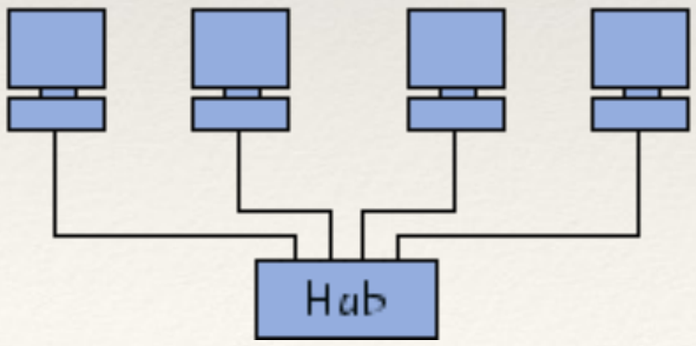
Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.



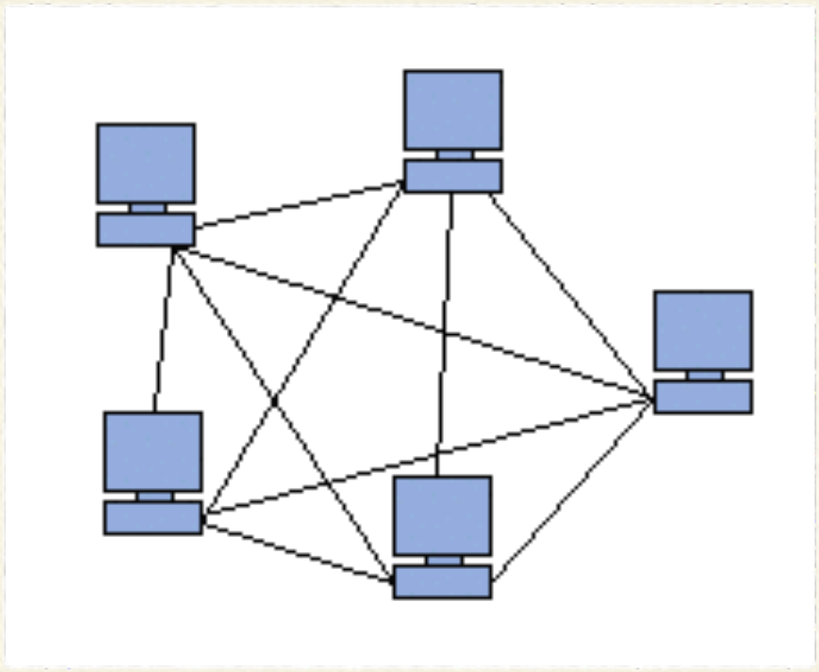
Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.
En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé *MAU*, *Multistation Access Unit*) qui va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





Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais *hub*, littéralement *moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.
Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.
En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub) défectueuse, l'ensemble du réseau en est affecté.

Topologies physiques (II)



Une **topologie maillée**, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1,N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.
Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.
L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée.

Elle existe aussi dans le cas de couverture Wi-Fi. On parle alors bien souvent de topologie mesh mais ne concerne que les routeurs WiFi.

Ethernet

- Un standard de transmission de données pour réseau local basé sur le fait que:
  - Toutes les machines du réseau Ethernet sont connectées à une même ligne de communication, constituée de câbles cylindriques.
  - La topologie physique du réseau Ethernet est ou bien en bus ou bien en étoile.
- Le protocole de communication est le CSMA/CD. Toute machine peut transmettre en tout temps. La communication est simple:
  - Chaque machine vérifie qu'il n'y a rien sur la ligne avant d'émettre,
  - Si deux machines émettent en même temps alors il y a collision. Plusieurs trames de données sur la ligne en même temps.
  - Les deux machines attendent un délai aléatoire avant de ré-émettre. La première à le faire aura transmis son message.

Les réseaux locaux modernes

- Un des premiers réseau local moderne a été installer au centre Xerox PARC dans les années 1970. IBM a lancé son propre réseau dans les années 1980, l'anneau à jeton ou Token Ring.

- Les réseaux locaux sont les plus courants parce qu'ils sont simples à installer, à administrer et sont à forts débits: 10Mbit/s au début, 100Mbit/s ensuite, 1Gbit/s maintenant.

- Ces réseaux permettent aux terminaux qui y participent de transmettre des trames au niveau de la couche de liaison (sans passer par internet).

Standards Réseau

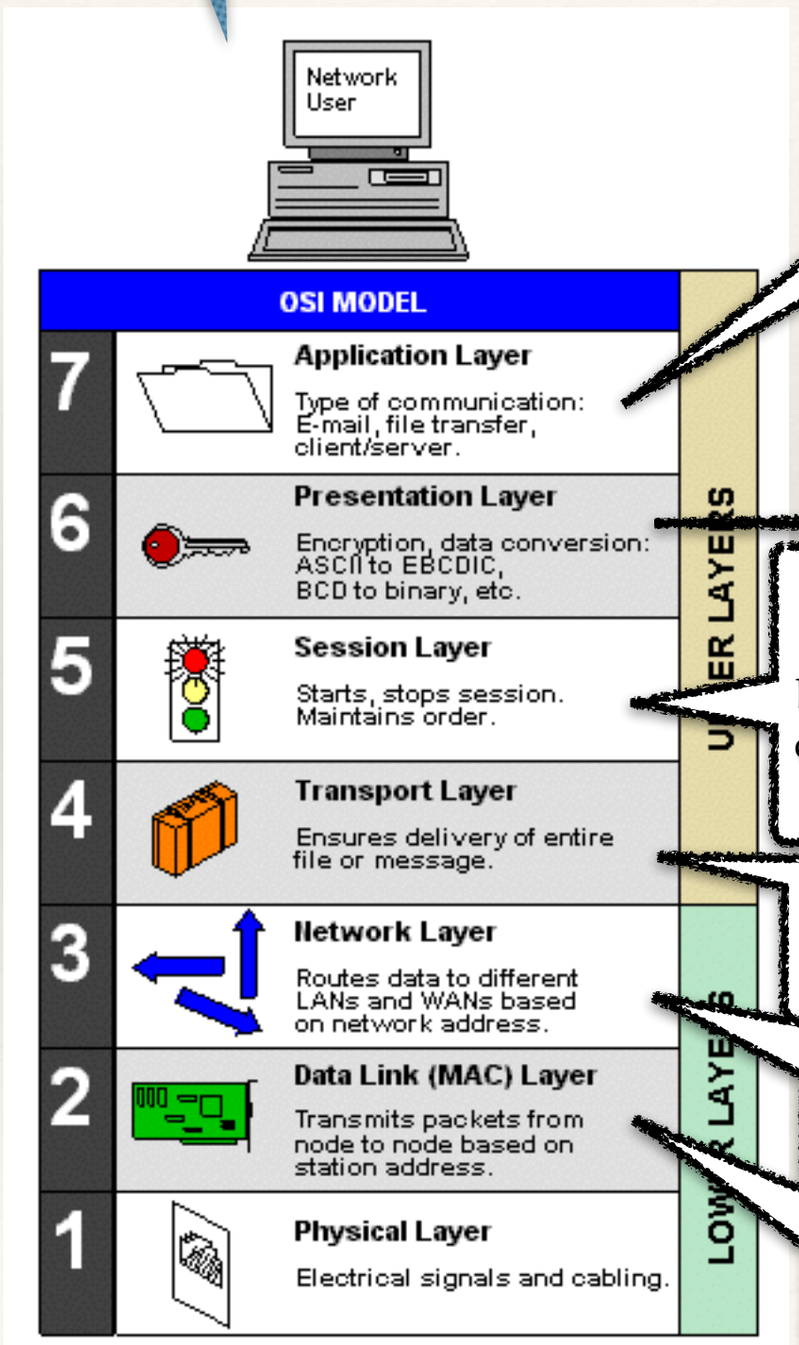
- Le standard OSI (Open Systems Interconnection, 1970) traite de communication en réseau de tous les systèmes informatiques.
- Le résultat d'une rivalité entre trois architectures:
  - DSA—CII-Honeywell-Bull qui innove dans le domaine de l'informatique distribuée avec les mini-ordinateurs Mitra15 et Mini6.
  - Decnet de DEC et SNA d'IBM donnent une plus grande place au site central qui contrôle l'ensemble des ressources matérielles et logicielles. Les utilisateurs y accèdent par une session sur des terminaux passifs.

Standards Réseau (II)

- Hubert Zimmermann travaille à l'IRIA (France, 1971) avec Louis Pouzin pour le développement de Datagramme, une nouvelle technologie.
- Le datagramme est un paquet de données dans un réseau informatique transmis par des protocoles via un service non fiable. Il n'y aucun moyen de s'assurer que le paquet est arrivé à destination.
- Cyclades(1971-1978) est le premier projet expérimental ayant pour but de créer un réseau global qui utilise le datagramme.
- Zimmermann conçoit le première version du standard OSI.

Le modèle réseau OSI

Encore une architecture par couches…



Définition du langage et de la syntaxe que les programmes utilisent pour communiquer avec d'autres. Un programme sur l'ordi d'un client utilise des commandes pour obtenir des données d'un programme sur le serveur: `ouvrir, fermer, lire, écrire des fichiers.`

Lorsque les données transitent entre des ordinateurs distincts, ce niveau négocie et administre la façon que les données sont représentées et encodées. Par exemple, une façon de transférer entre les machines ASCII et EBCDIC. Responsable également du chiffrement et du déchiffrement.

Assure que les communications sont coordonnées et mises en ordre. Détermine le type de communication: sens unique ou bidirectionnelle. Assure que le requête précédente est terminée avant d'envoyer la suivante. Ajoute aux données des points de vérification pour récupération rapide en cas d'erreurs de connection.

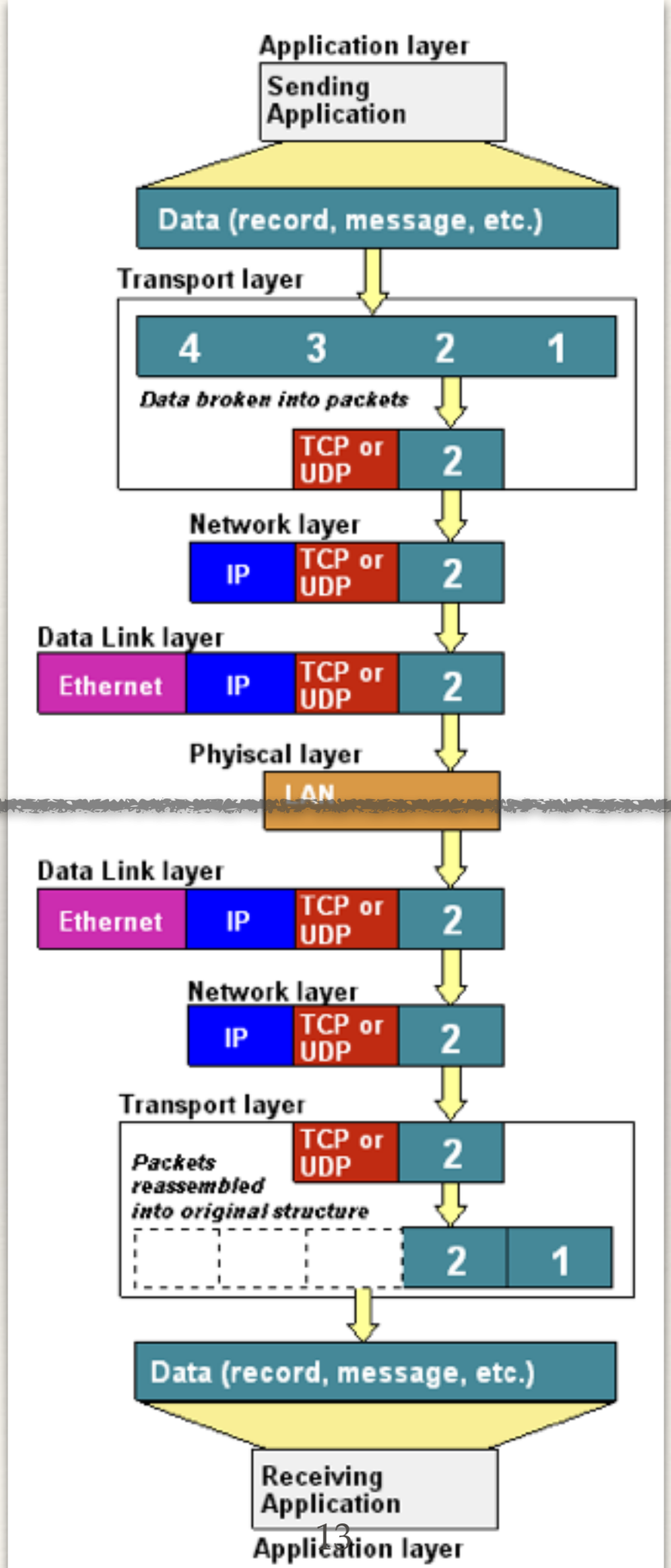
Responsable de s'assurer de la validité et de l'intégrité des données transmises et reçues. Le niveau réseau peut perdre des paquets qui sont récupérés.

Responsable de trouver le bon chemin entre l'envoyeur et le reçeveur au travers de points de commutation (comme des routeurs)

Responsable pour la transmission noeud à noeud (entres voisins), de sa validité et de son intégrité. Les bits transmis sont groupés en trames de données (frames). Ex: trames Ethernet, trames Token Ring, etc….

Envoyeur

Reçeveur



Globalisation des réseaux

- Les premiers réseaux étaient de courte portée (quelques dizaines de mètres) et servaient à la communication entre terminaux, instruments de mesure, périphériques et mini-ordinateurs ou mainframes (1960).
- Des groupes travaillent sur l'aiguillage de paquets comme manière d'assurer la communication même si des parties du réseau sont dégradées comme lors de combats (1960).
- Le bureau de traitement de l'information de l'ARPA (*Defense Advanced Research Projects Agency*) introduit un réseau, l'ARPANET, qui connecte UCSB et le Stanford Research Institute (1969). Le protocole NCP voit le jour.
- Les réseaux filaires entre sites éloignés sont introduits chez *IBM* et *DEC* avec les architectures *SNA* et DECnet (1970). Elles vont être utiles pour la digitalisation du réseau téléphonique de *AT&T*. Le protocole NCP est utilisé.
- Le réseau français Cyclades utilise la commutation de paquets à la sauce moderne: des paquets sont transmis indépendamment les uns des autres et ré-assemblés à la destination en utilisant le datagramme(1972).

Globalisation des réseaux (II)

- L'ARPANET continue de croître jusqu'en 1981, il regroupait alors 213 hôtes. Des centres académiques essentiellement. Il s'agit de l'ancêtre de l'internet, l'architecture sur laquelle le réseau des réseaux sera érigé.

- Les réseaux à ordonnance de paquets (comme pour Cyclades) ont été développé par l'UIC à partir des travaux sur l'ARPANET et le datagramme. Les formes de X.25 sont utilisées en 1974 pour *SERCnet* qui connecte les centres de recherche. Le premier standard X.25 en 1976.

- Le X.25 était disponible dans le monde de l'entreprise contrairement à l'ARPANET. Il sera utilisé pour les premiers réseaux téléphoniques publics: *CompuServe, Tymnet* (1979).

Globalisation des réseaux (III)

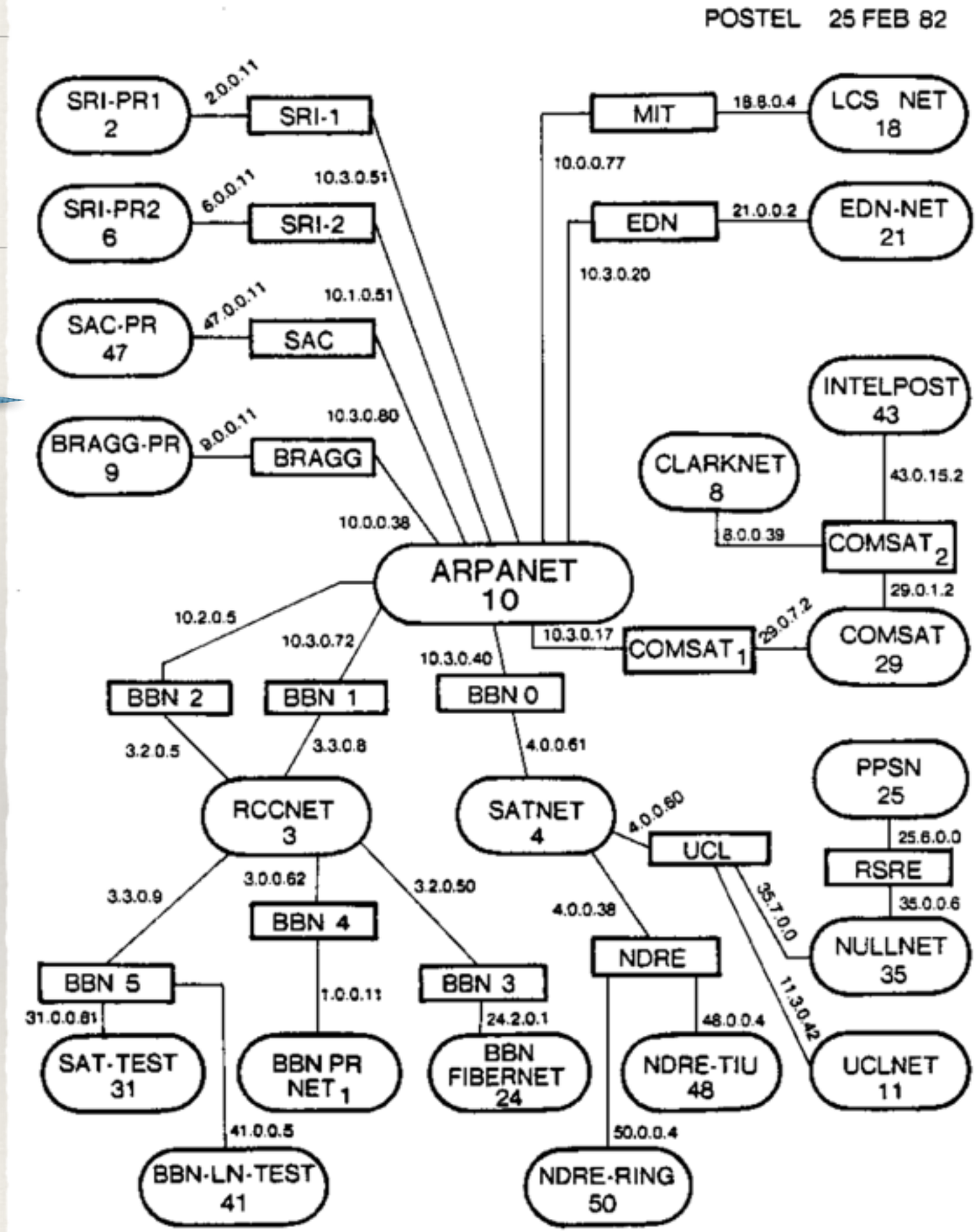
- C'est CompuServe qui offre les premiers un service de courriel et un service de support technique aux utilisateurs de PC (1979). Elle offre ensuite des discussions en temps réel avec son simulateur radio (1980).

- Un besoin d'uniformiser les méthodes de communication devenait nécessaire parce que ces méthodes étaient trop variées. Kahn et Cerf apporteront une reformulation profonde: Les différences entre ces protocoles sont minimisées par l'emploi d'un protocole de communication. Au lieu de faire reposer la fiabilité du réseau sur les connexions (ARPANET), les hôtes en deviennent responsables. Basé sur les travaux antérieurs de Zimmermann et Pouzin sur Cyclades (1973).

Globalisation des réseaux (IV)

- Maintenant que le rôle du réseau physique est réduit au minimum, il devint possible de fusionner à peu près n'importe quel réseaux sans tenir compte de leur caractéristiques. Le DARPA finance le développement du logiciel. La première démonstration de ce qui deviendra le protocole TCP/IP eut lieu en 1977.
- En 1983, l'ensemble des protocoles TCP/IP est le seul utilisé sur l'ARPANET, il remplace le protocole NCP.
- l'ARPANET était financé par le gouvernement et était donc restreint à des activités non commerciales.
- Au départ, l'ARPANET était réservé aux sites de l'armée et aux universités. En 1980, *DEC* et *HP* entrent sur l'ARPANET en participant à des projets de recherche ou en offrant des services aux connectés.

La carte du test réseau TCP/IP de 1982.



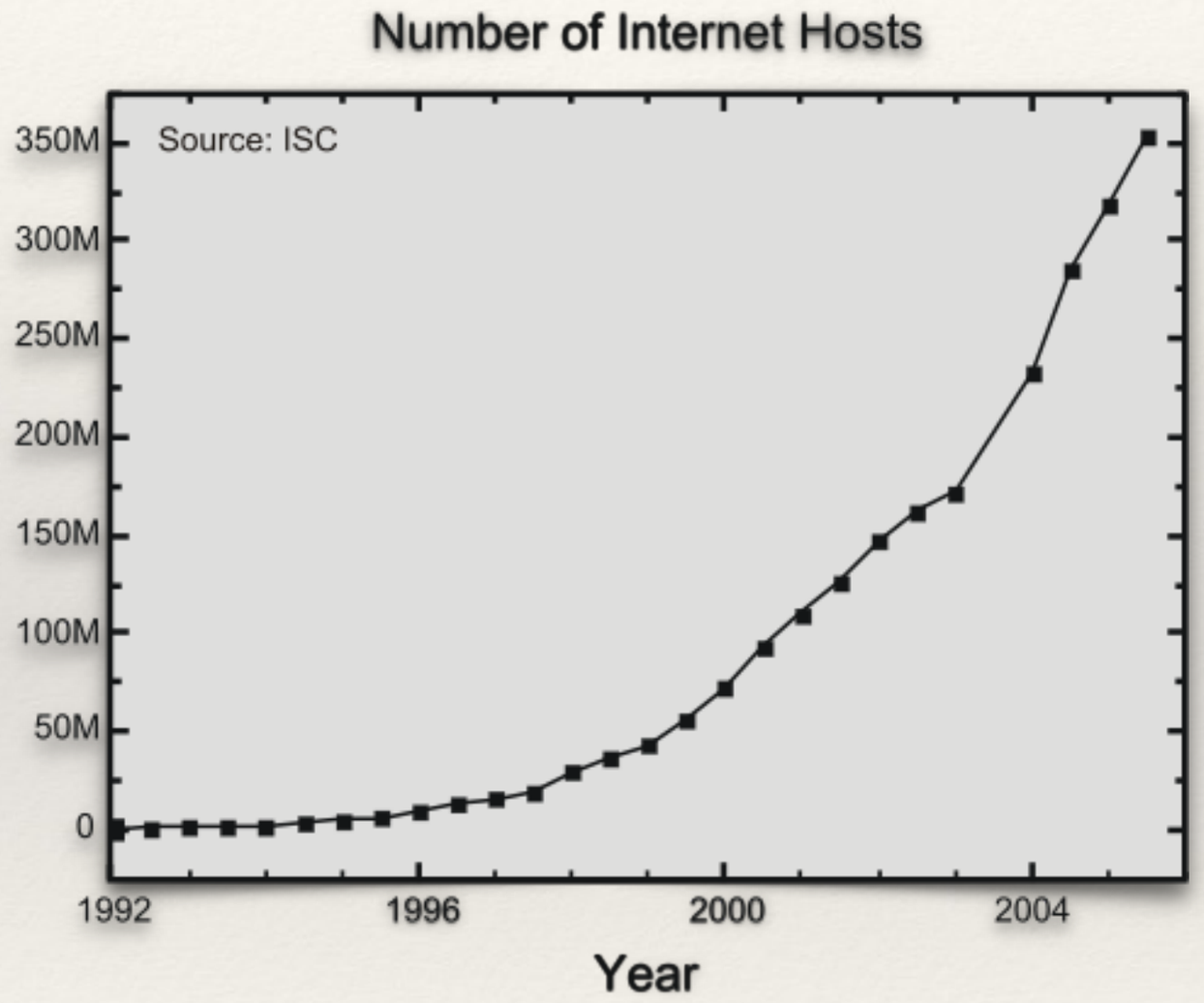
Naissance d'internet

- Le NSF (*National Science Foundation*) s'impliqua dans la recherche nécessaire au remplacement du réseau ARPANET. Le premier réseau étendu conçu spécialement pour TCP/IP apparaît (1984).
- Le réseau s'étendit ensuite au NSFNet (1986), qui fournissait accès au super-ordinateurs du NSF.
- Cette fusion entre ARPANET et NSFNet suggérait le nom **internet** pour un réseau qui utilise le protocole TCP/IP.
- L'utilisation de TCP/IP permet de transporter des messages vers et à partir de n'importe quel réseau, comme les X.25.
- Des sites incapables de se connecter à l'internet directement auront besoin de portails pour le routage des courriels. La connexion au portail pouvait se faire par modem. Le portail avait accès à internet. Les services se diversifient, des sites permettent le transfert de fichiers (*FTP*).
- TCP/IP devient mondial!

L'internet et le commerce

- L'utilisation commerciale d'internet devient un sujet délicat. Même si l'utilisation commerciale était interdite, la définition *d'utilisation commerciale* était subjective.
- L'ARPANET tolérait l'utilisation de UUCP (*Unix to Unix Copy*) qui pouvait être le moteur pour une utilisation commerciale du réseau.
- À la fin des années 1980, les premiers fournisseurs internet sont fondés. Il assiste les réseaux de recherche régionaux en permettant l'accès à l'internet: courriels et nouvelles *usenet*.
- Le premier fournisseur internet par modem était World en 1989.
- Les utilisateurs universitaires étaient plutôt fermés à l'utilisation de l'internet pour des missions non-éducatives. Cependant, les fournisseurs d'accès permettaient aux écoles d'y accéder après la baisse des tarifs d'accès.
- Le successeur de l'ARPANET, NSFNet n'était plus l'épine dorsale de l'internet lorsque les fournisseurs et les institutions gouvernementales installèrent leur propre structure. Les dernières restrictions commerciales disparurent.

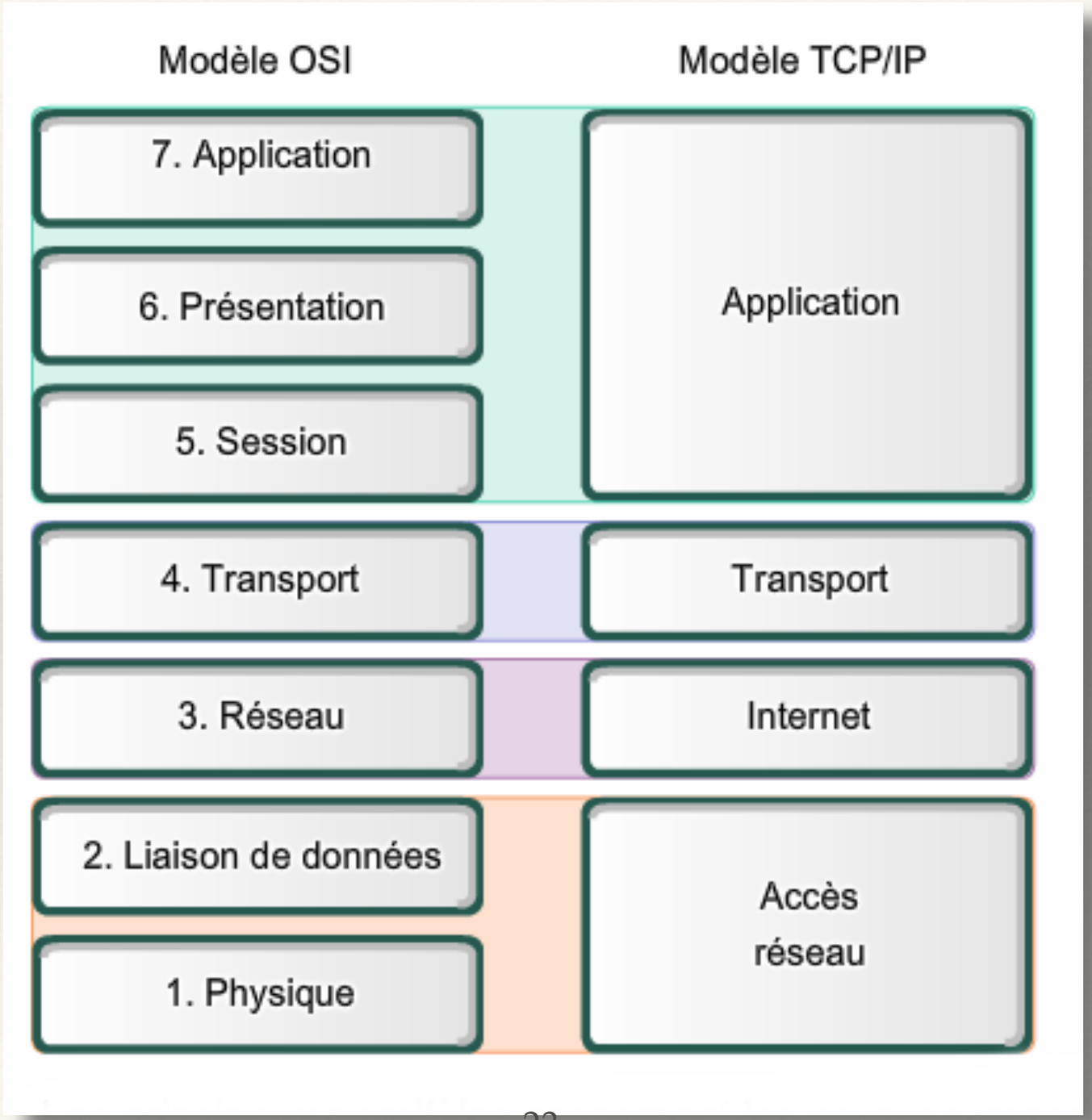
L’évolution du nombre des fournisseurs/hébergeurs



TCP/IP

- L'ensemble des protocoles utilisés sur internet pour le transfert de données. Les deux premiers protocoles dans son développement étaient:
    - TCP: transmission control protocol
    - IP: internet protocol.
        - Ont été inventés par Vincent G. Cerf et Bob Kahn.
- Comme le modèle OSI, TCP/IP décompose les protocoles en couches (4 au lieu de 7). Cependant, les couches OSI ne correspondent pas toujours aux habitudes internet. OSI est théorique tandis que TCP/IP est pratique. Les mêmes principes généraux s'appliquent aux deux.
- Chaque couche TCP/IP résout un certain nombre de problèmes relatifs à la transmission des données et fournit des services aux couches supérieures.
- Les couches hautes sont proches de l'utilisateur et les couches basses sont proches du matériel physique qui compose le réseau…

OSI vs TCP/IP


Modèle OSI
Modèle TCP/IP
7. Application
6. Présentation
5. Session
Application
4. Transport
Transport
3. Réseau
Internet
2. Liaison de données
1. Physique
Accès
réseau

Les couches TCP/IP

- **Accès réseau:** Décrit les caractéristiques physiques de la communication, les conventions sur la nature du média utilisé, les détails associés comme les connecteurs, les types de codage ou de modulation, le niveau des signaux, les longueurs d'ondes, la synchronisation est les distances maximales. Spécifie également comment les paquets sont transportés sur la couche physique comme le tramage qui indique les séquences de bits qui marquent le début et la fin des paquets. Par exemple, les trames Ethernet contiennent des champs qui indiquent à quelle(s) machine(s) du réseau la paquet est destiné.

Les couches TCP/IP (II)

- **Couche internet:** un groupe de protocoles responsables pour la transmission des paquets (*datagrammes*) à partir de l'origine travers les frontières entres réseaux vers la destination. Le receveur est décrit par son adresse IP définie par le protocole internet. Cette couche connecte les réseaux par des passerelles(gateways).
  - Pour un paquet sortant, détermine le prochain hôte à recevoir le paquet sur le chemin.
  - Pour un paquet entrant, intercepte le paquet et le transmet au bon protocole de la **couche de transport**.
  - Permet la détection d'erreurs et produit des diagnostiques.
- La couche internet ne donne pas de protocole pour les communications entre noeuds locaux. Ceci est traité dans la couche **accès réseau**.

Les couches TCP/IP (III)

- **Couche transport:** permet d'établir des services de communication d'un bout à l'autre (de l'envoyeur au receveur). A ce niveau, une connexion est créée entre deux adresses IP et la communication qui s'y déroule respecte l'ordre d'envoi pendant la durée de la connexion.
    - Les communications sont vues comme des flux de données sans mention des datagrammes (les données sont ici des *segments*). Les applications (plus haut) peuvent donc abstraire la mécanique de la communication et ne traiter que ce qui est communiqué.
    - Les paquets peuvent être perdus ou modifiés en cours de route. La couche de transport s'assure que ces erreurs sont détectés et corrigés (par ré-émission).
    - Évite les congestions de trafic en ralentissant la transmission des paquets lorsque nécessaire.
    - Certains ports peuvent offrir plusieurs point d'arrivé sur un seul noeud. La couche transport est responsable du multiplexage (comme le nom associé à une adresse postale permet de livrer à des personnes différentes à la même adresse) qui permet d'adresser plusieurs récipients à la même adresse en livrant à des ports particuliers.

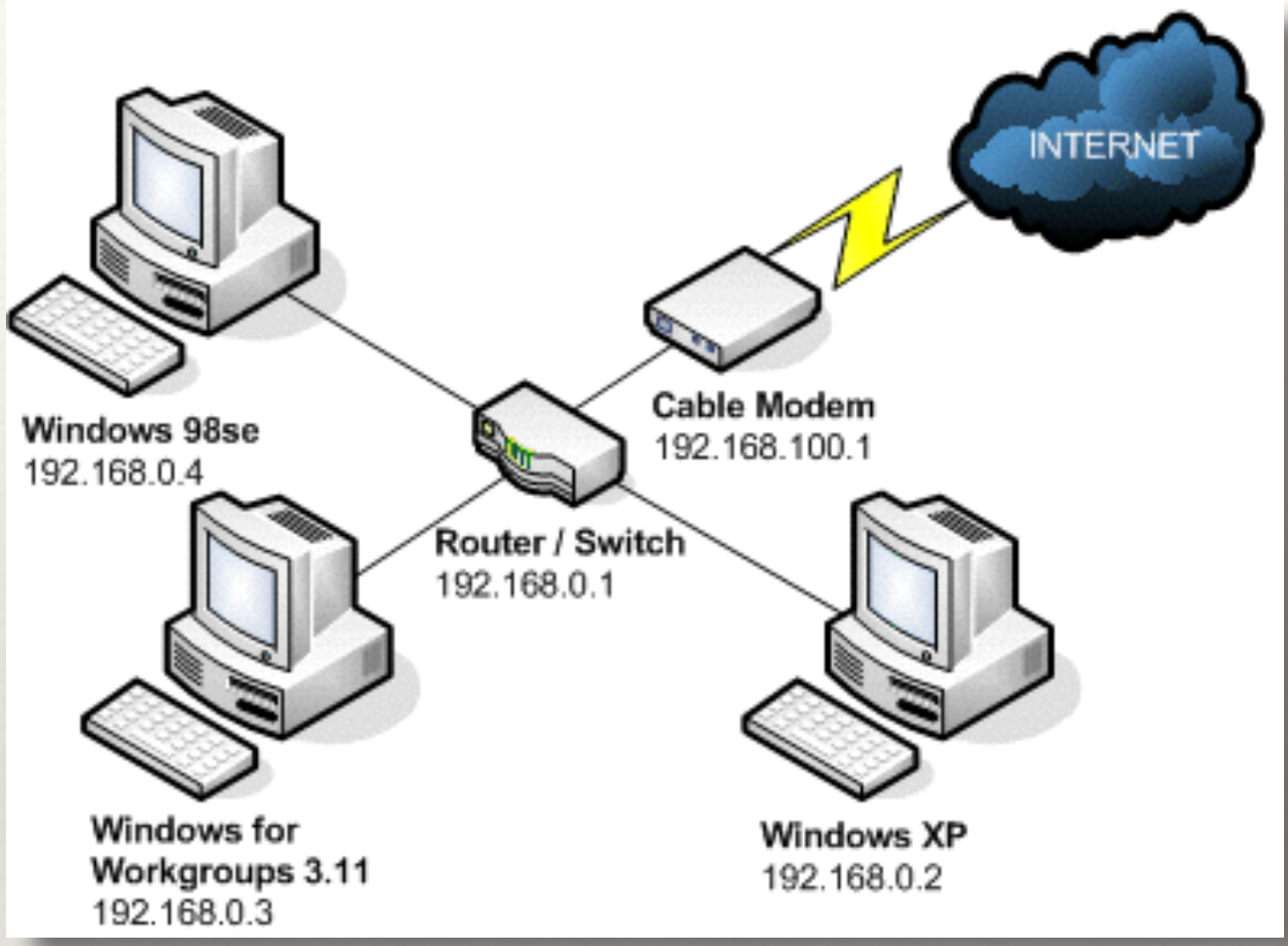
Les couches TCP/IP (IV)

- **La couche application:** Elle comprend les applications standards du réseau (Telnet, SMTP, FTP, HTTP, etc…). Elle est située au sommet de la pile TCP/IP. Elles contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent à l'aide d'un des deux protocoles de la couche Transport: TCP ou UDP. Ces applications sont des services réseaux, pour la plupart. Des applications fournies à l'utilisateur pour assurer l'interface avec le SE:
  - Services de transfert de fichier et d'impression,
  - Services de connexion réseau,
  - Services de connexion à distance,
  - utilitaires internet.

Les données à transmettre sont appelées *message* dans cette couche.

Connexions internet-LAN

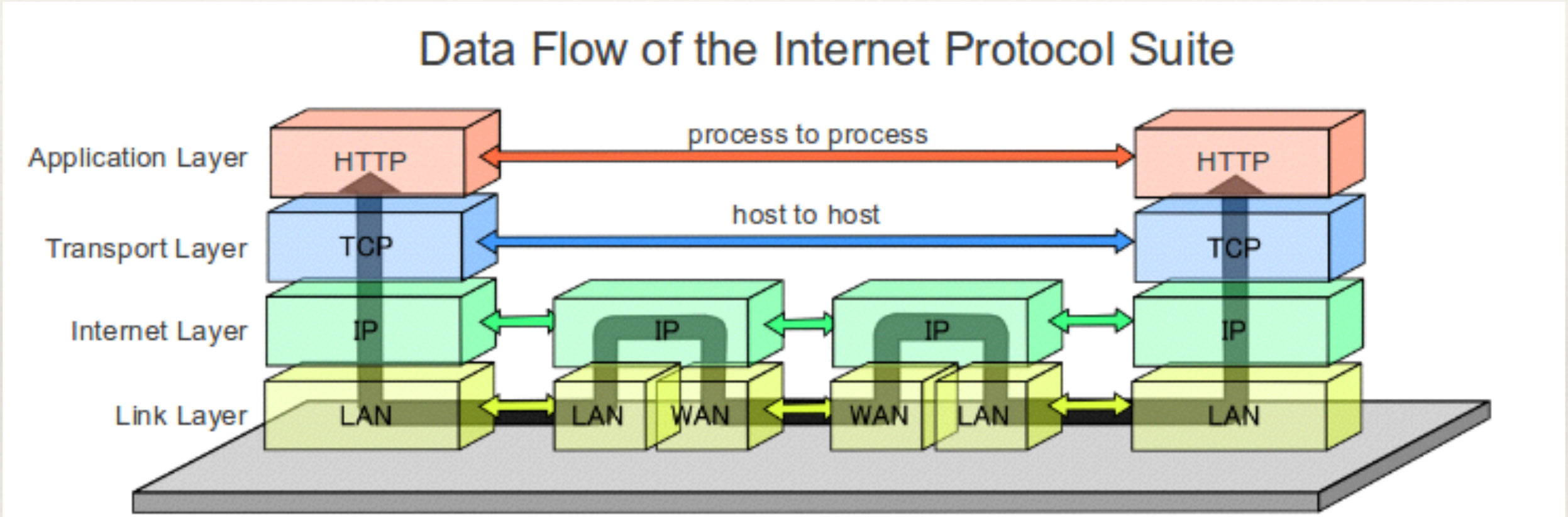
Adresse IP: Numéro d'identification permanent ou provisoire associé à chaque appareil qui utilise le protocole IP. Généralement représentée en décimale par 4 octets séparés par des '.'. Les adresses sont données à chaque interface réseau de tout matériel informatique. Attribuée soit individuellement par l'administrateur LAN soit automatiquement par le protocole DHCP.



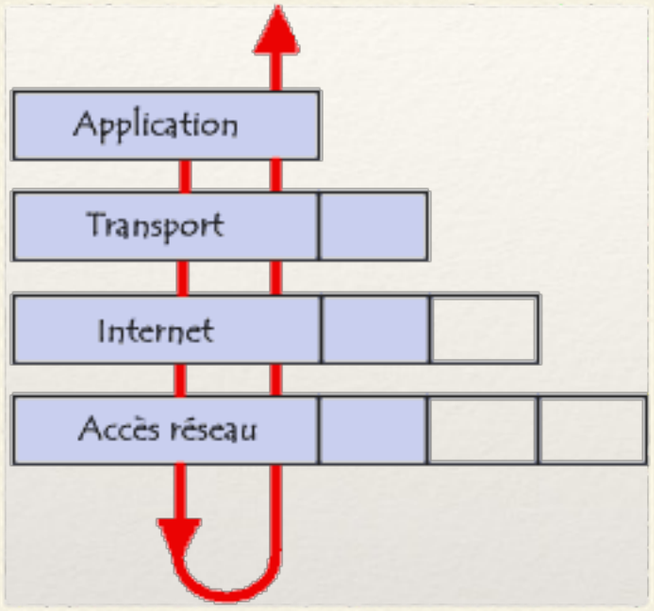
Routeur: Élément de réseau assurant le routage des paquets. Il fait transiter les paquets d'un réseau à un autre. Le premier était le IMP pour l'ARPANET(1969).

Modem câblé: type de modem qui permet de se connecter à Internet en étant relié à un réseau de télévision par câble. Le modem-câble est bidirectionnel, il n'utilise qu'un seul câble coaxial pour les deux directions, en aval pour les données du réseau vers l'utilisateur et en amont pour les données de l'utilisateur vers le réseau.

Flux de données sur l'internet



Encapsulation des données



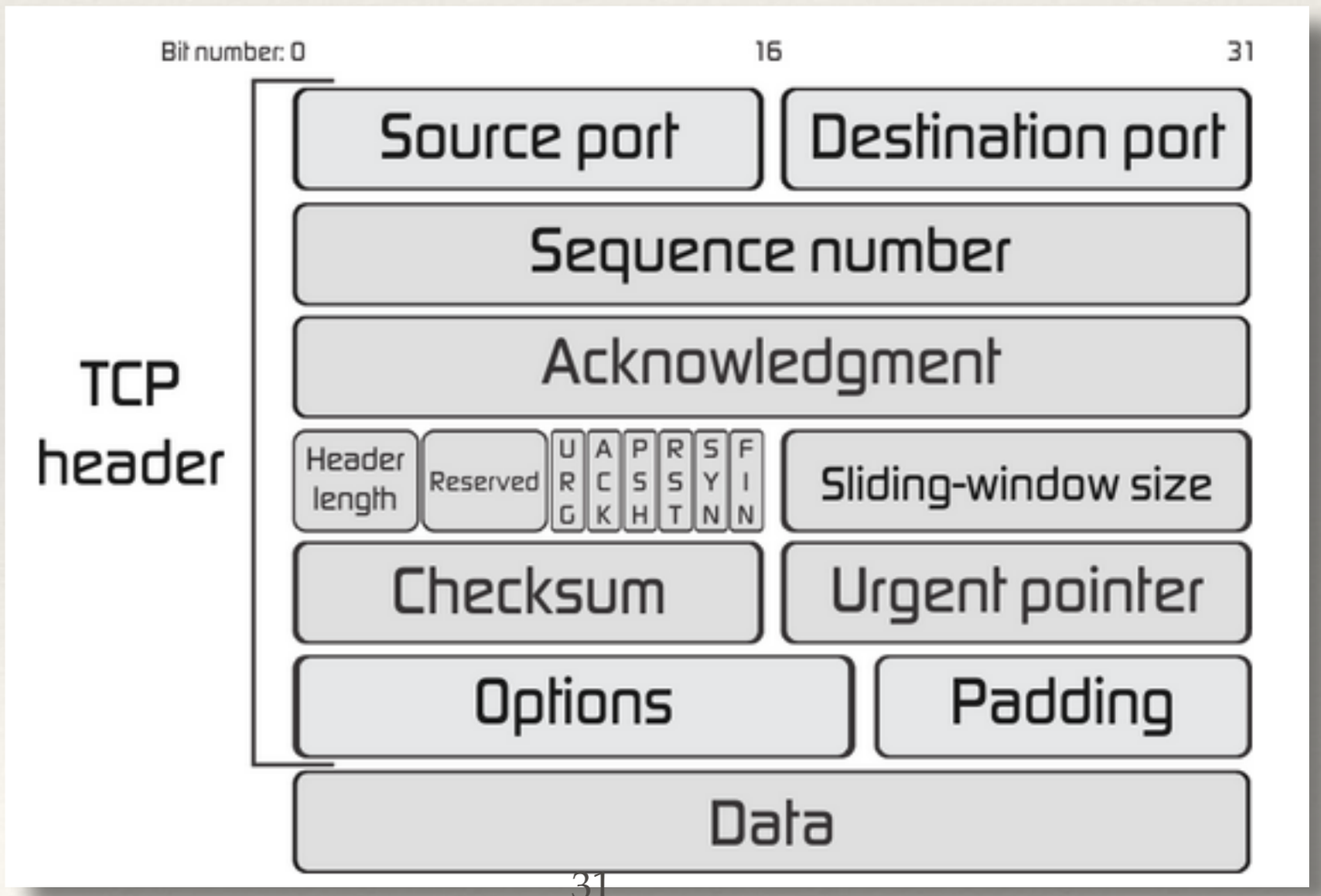
Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantit la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel...

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

- Le paquet de données est appelé **message** au niveau de la couche **Application**
- Le message est ensuite encapsulé sous forme de **segment** dans la couche **Transport**
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**
- Enfin, on parle de **trame** au niveau de la couche **Accès réseau**

Segments TCP/IP

port informatique: Correspond à la couche de transport du modèle OSI, la notion de **port** logiciel permet, sur un ordinateur donné, de distinguer différents interlocuteurs. Ces interlocuteurs sont des programmes informatiques qui, selon les cas, écoutent ou émettent des informations sur ces ports. Un port est distingué par son numéro: 0..65535.



Sessions TCP

Pour établir une connexion:

- L'hôte A initialise la connexion en envoyant une commande SYN (synchronisation).
- Lorsque B reçoit la commande SYN il retourne SYN+ACK dans l'entête TCP.
- Lorsque A reçoit SYN+ACK il retourne ACK à B.
- B reçoit ACK et la connexion est établie.

Pour terminer la session A procède de cette façon.

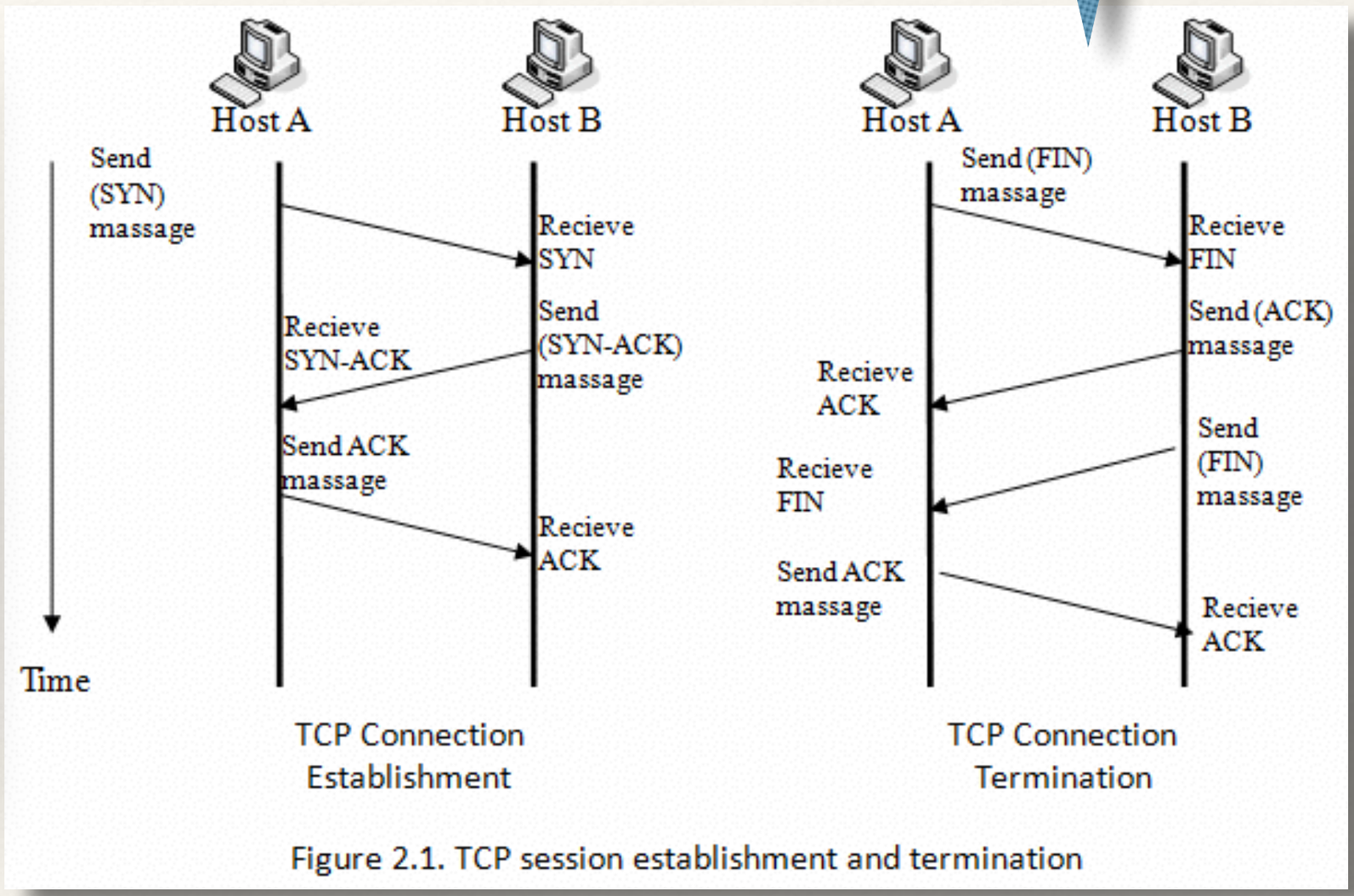
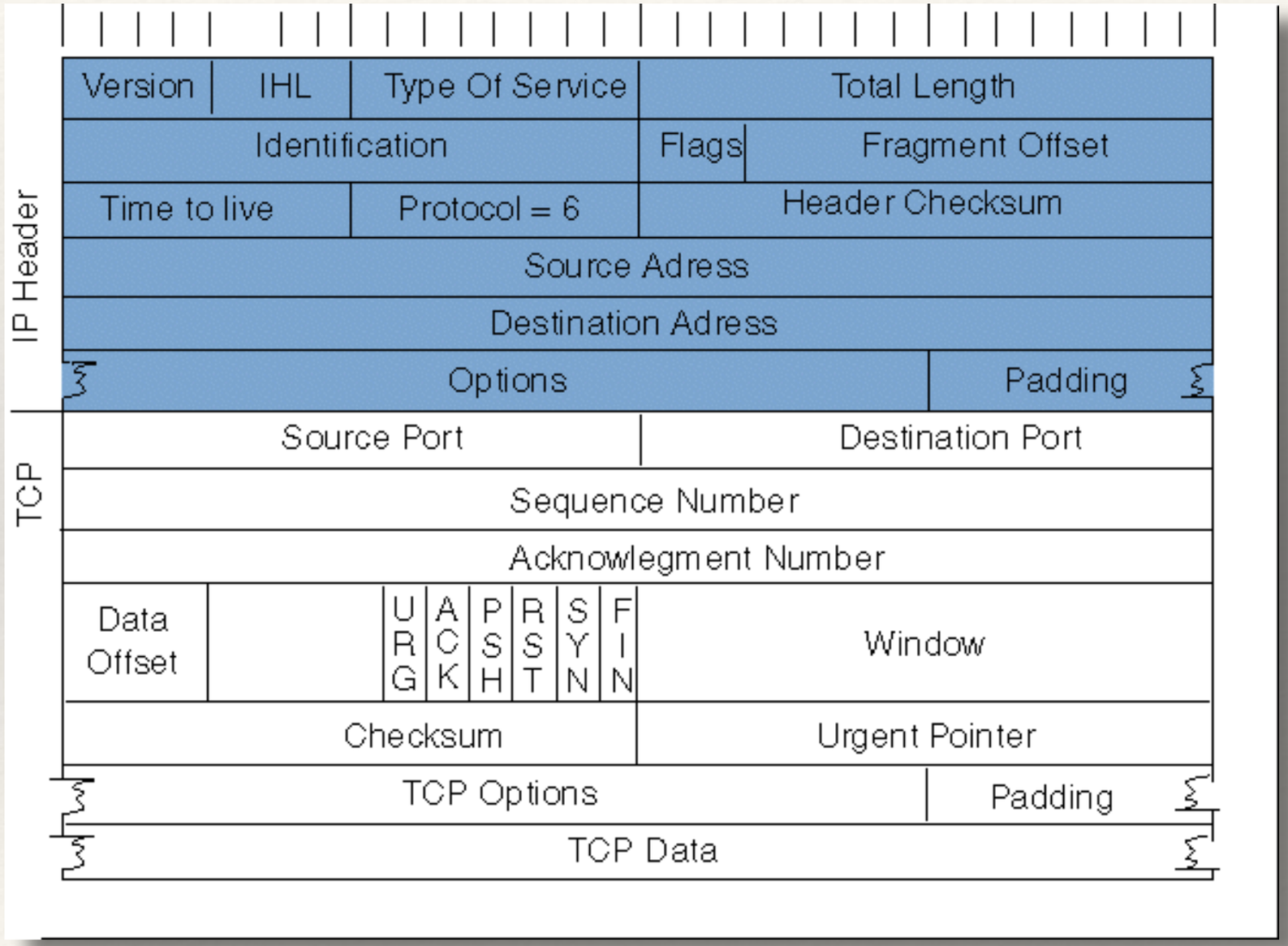


Figure 2.1. TCP session establishment and termination

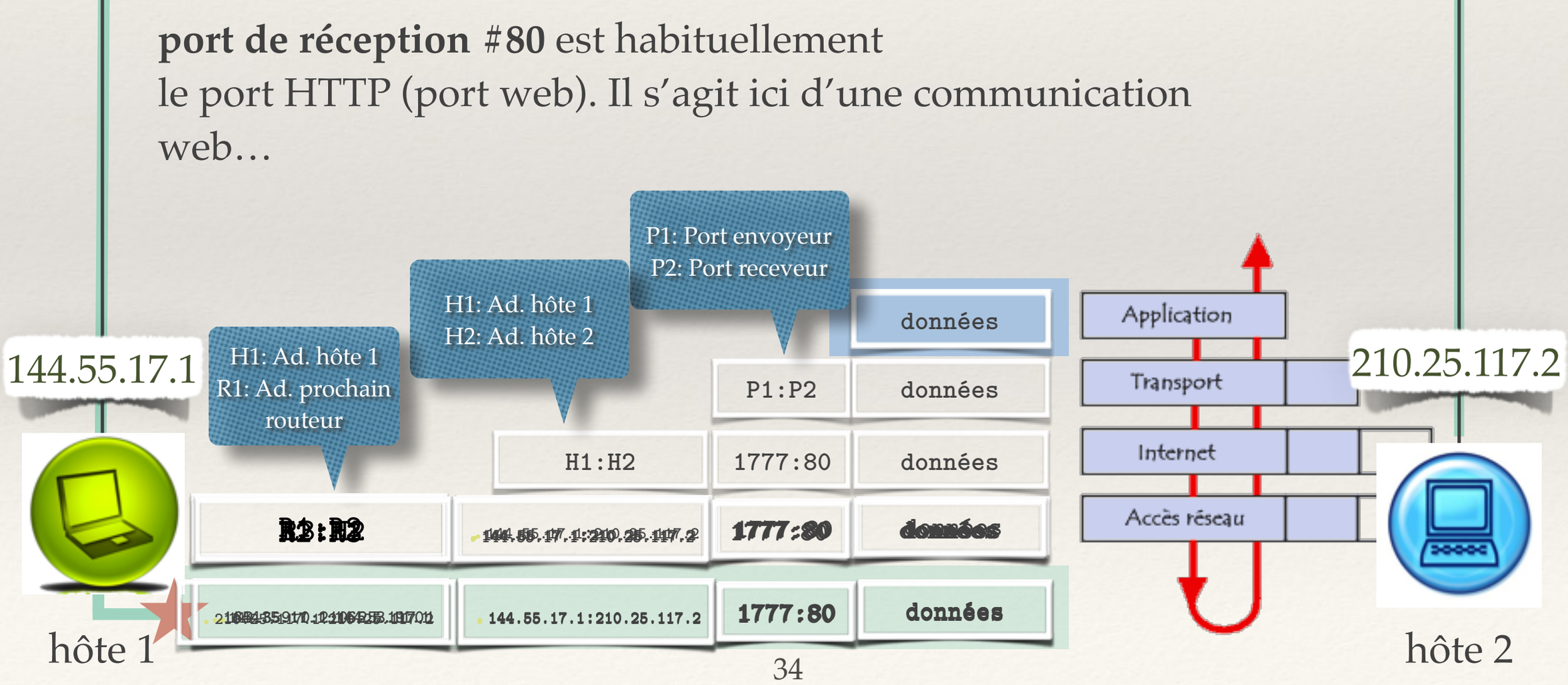
datagrammes TCP/IP



Routage des paquets

144.5.11.1 — routeur R1 — 165.3.9.0 — routeur R2 — 210.25.117.1 — routeur R3

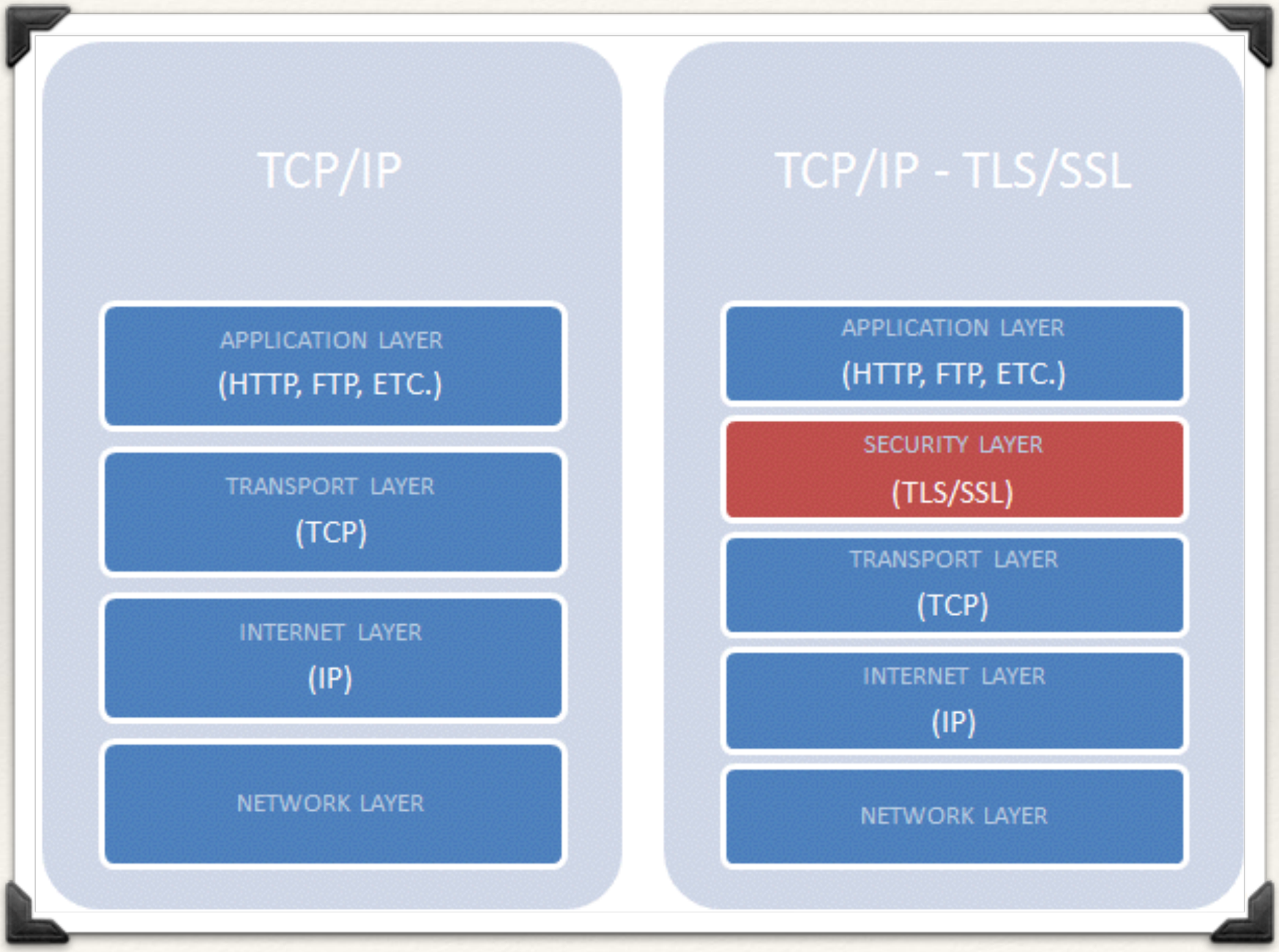
port de réception #80 est habituellement le port HTTP (port web). Il s'agit ici d'une communication web…



Connexions sécurisées

- Les protocoles TCP/IP peuvent assurer l'intégrité et la confidentialité des messages en passant à travers une autre couche appelée couche SSL/TLS.
  - SSL: Secure Socket Layer, (ancien nom)
  - TLS: Transport Layer Security. (nouveau nom)
- Cette couche est entre la couche *Applications* et *Transport*. Elle permet d'obtenir des communications chiffrées et authentifiées.
- Ceci est très important lorsque l'on utilise une connexion TCP/IP pour faire du commerce électronique.
- Permet de s'assurer que seul le serveur et le client connectés peuvent lire et modifier les messages transmis comme les mots de passe, les numéros de carte de crédit, etc…

TCP/IP avec SSL/TLS



SMTP: transmission de courriels

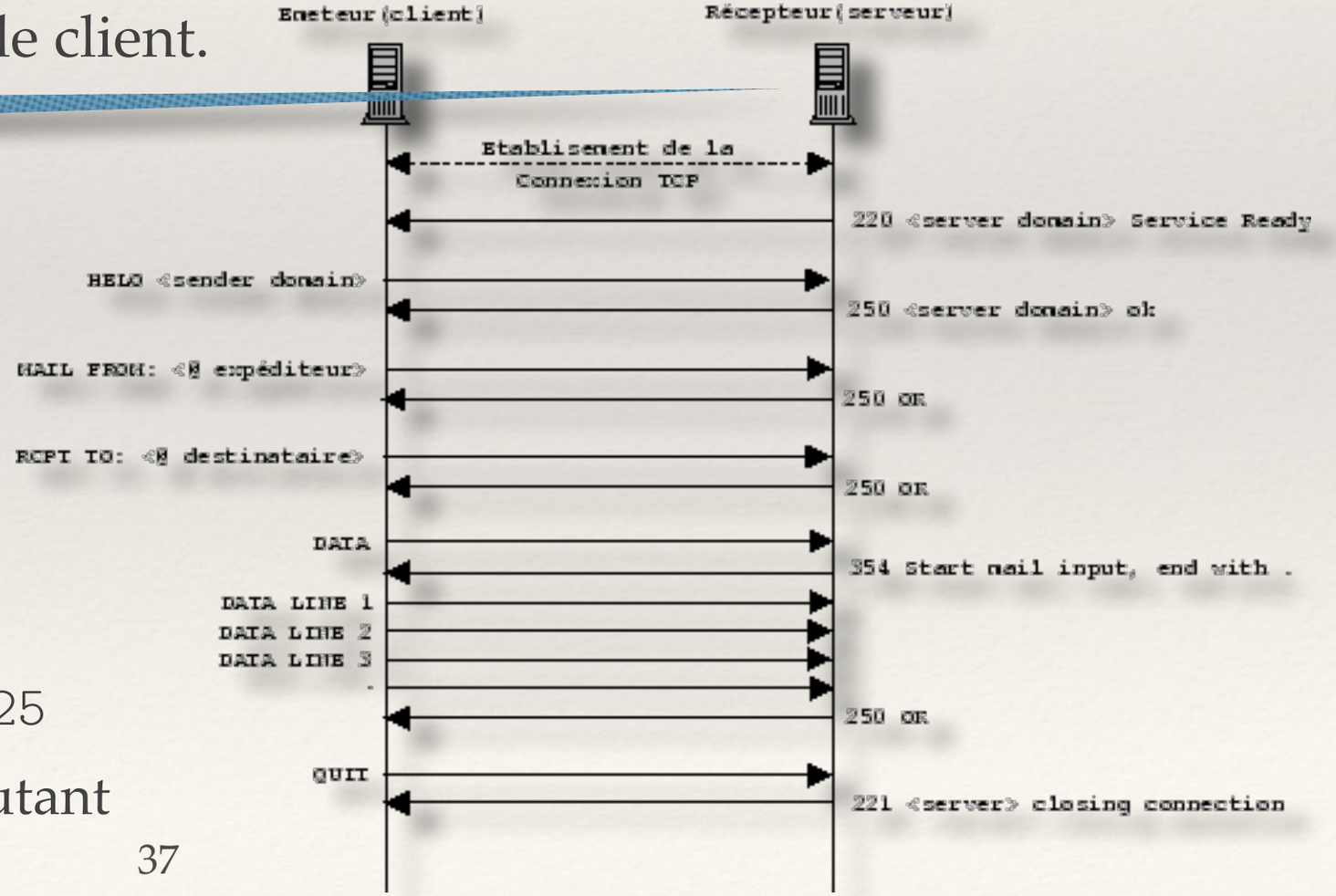
- SMTP = Simple Mail Transfer Protocol.
- Transmet un courriel en ouvrant une session TCP avec le serveur de courriel du destinataire.
- Les données sont transférées jusqu'à une ligne qui ne contient qu'un '.' et `<RTN>`.
- La session termine avec `QUIT` par le client.

Le serveur écoute sur le port de courriel: port #25
dans sa version simple.

la commande UNIX `telnet` permet de débuter une session TCP à l'adresse du serveur sur le port indiqué:

```
telnet smtps.iro.umontreal.ca 25
```

et un courriel peut être envoyé en exécutant le protocole SMTP…



Exemple d'utilisation de SMTP

Au DIRO, une version sécurisée de SMTP est utilisée: SMTPS. Pour utiliser le protocole, il faut se connecter à partir d'un compte du DIRO avec `ssh` avant de faire `telnet`. Ceci peut aussi se faire en utilisant la commande UNIX `openssl`.

```
ssh frontal.iro.umontreal
telnet smtps.iro.umontreal.ca 25
```

port d'écoute standard #25

ou

```
openssl s_client -connect smtps.iro.umontreal.ca:465
```

Port SSL où écoute smtps.iro.umontreal.ca

```
SSL handshake has read 3284 bytes and written 335 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID:
2540FE735DC37DC2F800C1CDED7D574D6E37D36CD350DEE9AA178DD8F8
56660C
    Session-ID-ctx:
    Master-Key:
3095810EB71C07ACC5E07C3A7DAFDDC11907F1E467199BA0102FF6D934
F29A8FDD64F8EBBEFA580DC82BA0ED304FC0D2
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1446325996
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
220 hidalgo.iro.umontreal.ca ESMTP Postfix
HELO salvail@iro.umontreal.ca
250 hidalgo.iro.umontreal.ca
MAIL FROM: salvail@iro.umontreal.ca
250 Ok
rcpt to: salvail@iro.umontreal.ca
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Test Test
Allo comment ca va!
.
250 Ok: queued as A36B91E5B8B
QUIT
DONE
```

Comment lire ses courriels

- Les protocoles qui permettent de lire ses courriels sur un serveur de courriel sont POP et IMAP (entres autres):
  - IMAP est plus puissant. Il fait certaines choses mieux que POP.
  - Le serveur de courriel du DIRO utilise IMAP.
  - Comme pour SMTPS, on peut utiliser IMAP en:
    - se connectant au serveur en utilisant openssl
    - envoyant des commandes pour lire ses messages et les organiser…

Exemple d'utilisation d'IMAP

Dans un Shell UNIX vous pouvez faire:

```
ssh frontal05.iro.umontreal.ca
openssl s_client -connect imap.iro.umontreal.ca:993
```

Le port SSL pour IMAPP

Une session IMAP où je demande les CAPABILITY, j'utilise LOGIN et ensuite je sélectionne ma INBOX.

```
* OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS AUTH=GSSAPI AUTH=PLAIN AUTH=LOGIN]
mercure.iro.umontreal.ca IMAP4rev1 2004.357 at Sat, 31 Oct 2015 13:55:10 -0400 (EDT)
10 CAPABILITY
* CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT
THREAD=REFERENCES THREAD=ORDEREDSUBJECT MULTIAPPEND SASL-IR LOGIN-REFERRALS AUTH=GSSAPI
AUTH=PLAIN AUTH=LOGIN
10 OK CAPABILITY completed
30 LOGIN salvail <MOTDEPASSE>
30 OK [CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT
THREAD=REFERENCES THREAD=ORDEREDSUBJECT MULTIAPPEND] User salvail authenticated
40 SELECT INBOX
* 2928 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1425420477] UID validity status
* OK [UIDNEXT 36785] Predicted next UID
* FLAGS ($NotJunk $Junk $Forwarded JunkRecorded $MDNSent $MailFlagBit1 $MailFlagBit0
$MailFlagBit2 NotJunk Junk Forwarded Old \Answered \Flagged \Deleted \Draft \Seen)
* OK [PERMANENTFLAGS ($NotJunk $Junk $Forwarded JunkRecorded $MDNSent $MailFlagBit1
$MailFlagBit0 $MailFlagBit2 NotJunk Junk Forwarded Old \* \Answered \Flagged \Deleted \Draft
\Seen)] Permanent flags
* OK [UNSEEN 62] first unseen message in /export/home/mail3/salvail/inbox
40 OK [READ-WRITE] SELECT completed
60 quit
60 BAD Command unrecognized: QUIT
60 logout
* BYE mercure.iro.umontreal.ca IMAP4rev1 server terminating connection
60 OK LOGOUT completed
read:errno=0
```