TCP/IP - Protocoles de base

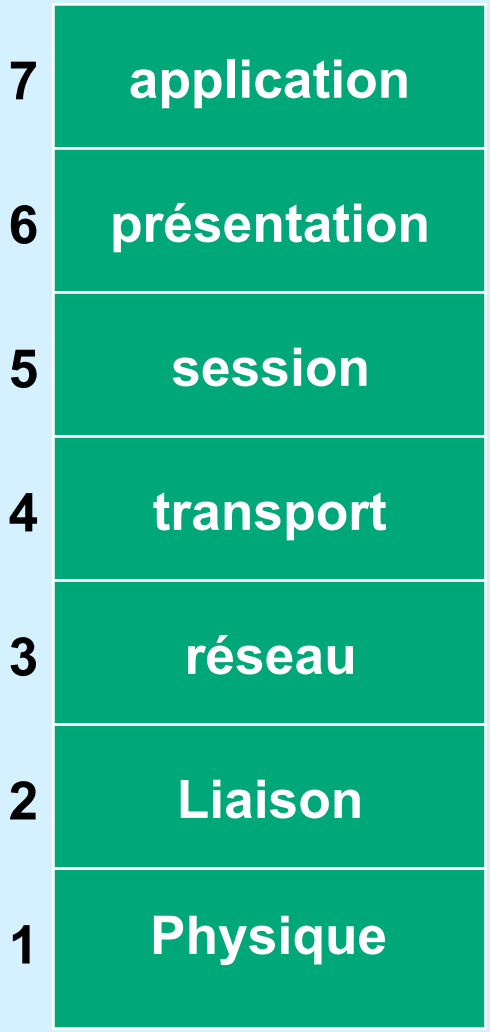
Plan

- Introduction
- Couche réseau : IP (fonctions, adressage, datagramme)
- ARP : protocole de résolution d'adresse
- RARP : Protocole de résolution d'adresse inverse
- Protocole ICMP
- Couche de transport: TCP et UDP
- Conclusion

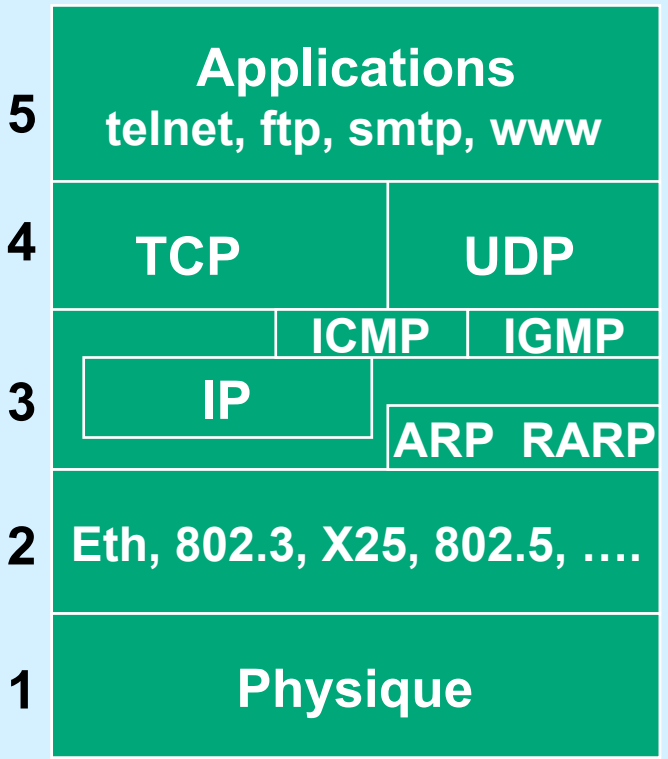
Introduction sur Internet

- Technologie issue des années 1970, de projets DARPA
  (Defense Advanced Projects Research Agency)
- TCP/IP : but = interconnexion de réseaux sur une base planétaire
- ARPANET est le premier réseau à commutation de paquets
- La mise en œuvre de TCP/IP en 1980 sur le réseau de recherche de DARPA est le début d'Internet
- La transition est complète quand DARPA exige que toutes les machines de ARPANET utilisent TCP/IP
- TCP/IP intégré dans l'unix BSD
  - entrée dans le monde universitaire,
  - développement d'applications avec les sockets

Modèle en couches

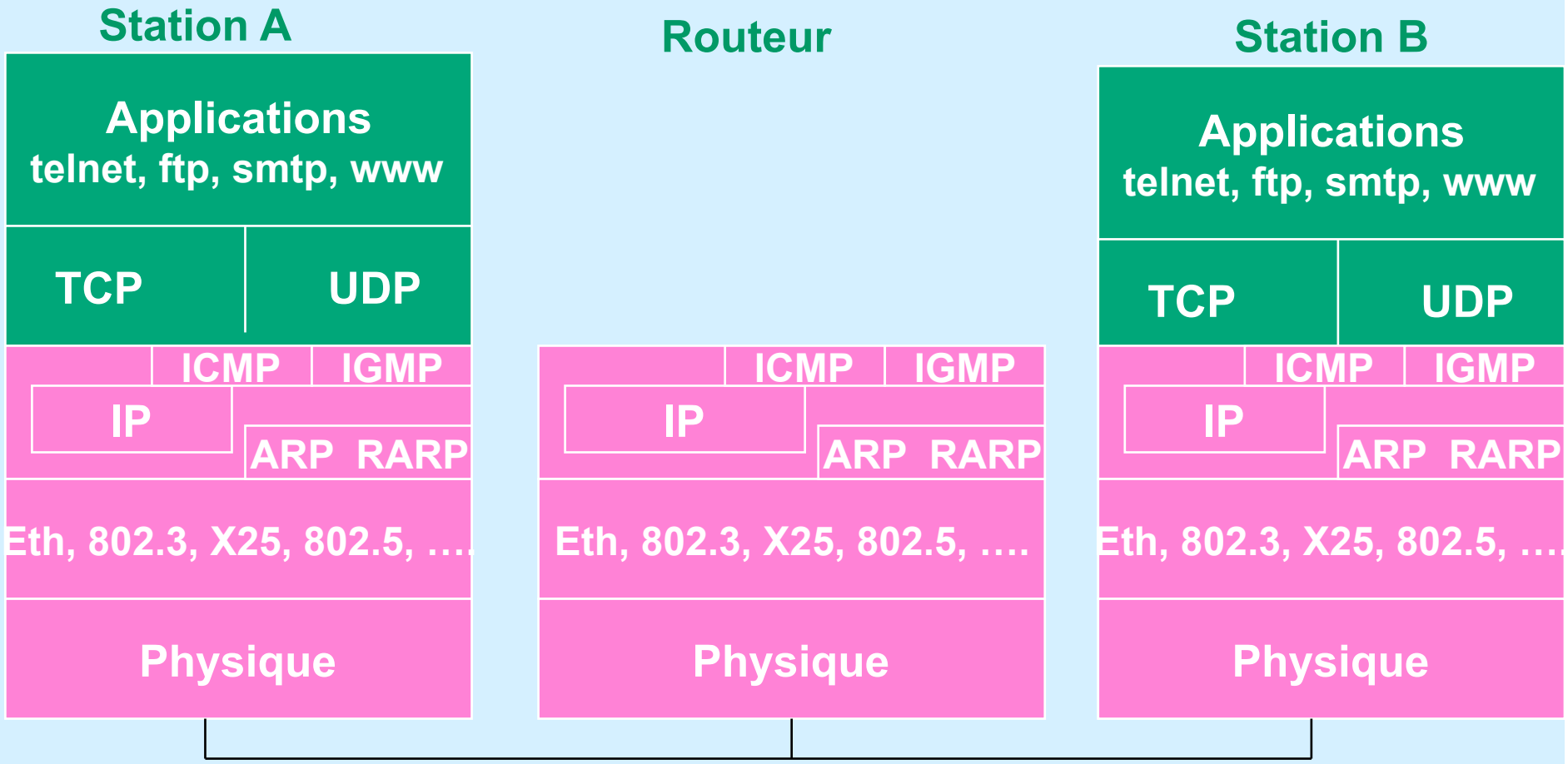


Modèle OSI



Modèle TCP/IP

Modèle en couches



Introduction sur Internet

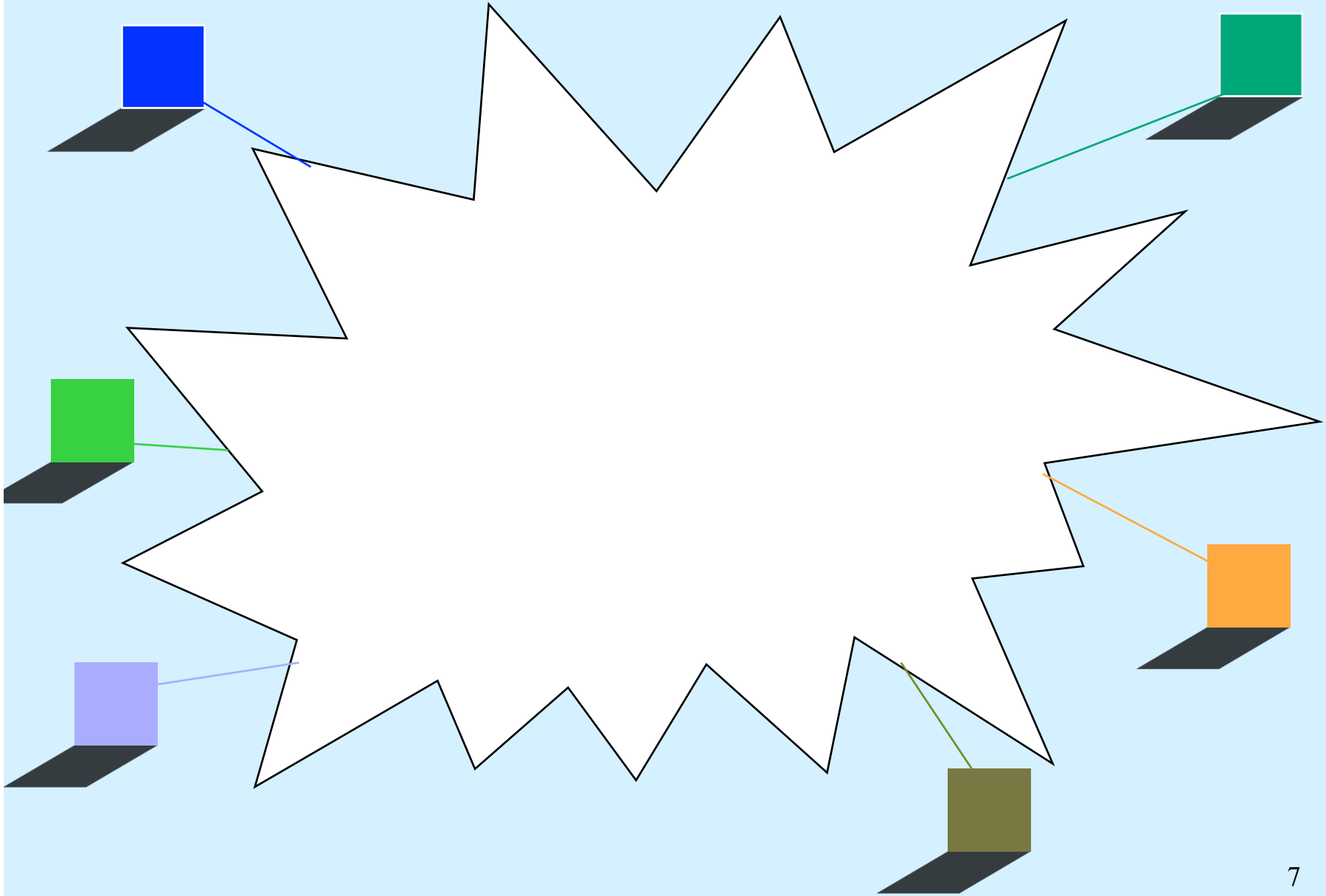
• Interconnexion universelle : les machines ont une adresse unique sur l'Internet. Deux machines reliées au réseau, communiquent grâce aux autres noeuds du réseau qui routent de manière coopérative sur la base de l'adresse destinataire.

• Interconnexion d'égal à égal (peer to peer systems) : il n'y a pas de machines prioritaires (en opposition à une structure hiérarchique).

•Technologie indépendante des constructeurs et disponible sur tous types de matériel (micro, station, super-calculateur et équipements de réseaux)

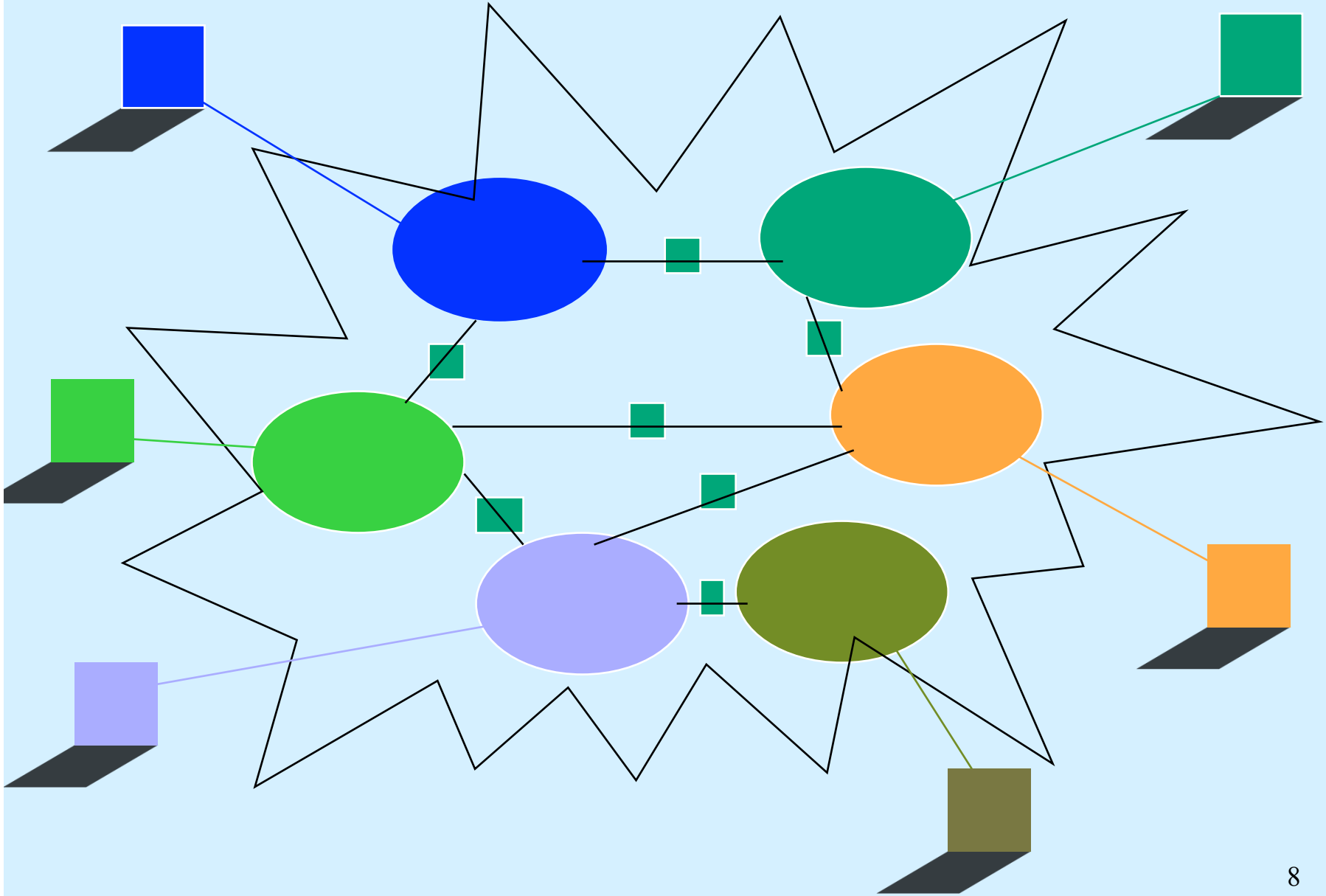
• Largement validée depuis de nombreuses années dans un monde hétérogène.

Architecture de l'Internet Vue de l'utilisateur



Architecture de l'Internet

La réalité



Les services de l'Internet

- Interopérabilité aux niveaux des applications

- Les utilisateurs invoquent les applications sans avoir besoin de connaître la technologie de l'Internet ni son architecture

- Les plus populaires sont :
  - Le courrier électronique (smtp)
  - Le transfert de fichiers (ftp, tftp)
  - L'accès à l'information distante (www)
  - L'accès à des machines distantes (telnet)
  - Les forums (News)

L'adressage Internet

- But : fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion
- Une machine doit être accessible aussi bien par des humains que par d'autres machines
- Une machine doit pouvoir être identifiée par :
  - un nom (mnémotechnique pour les utilisateurs),
  - une adresse qui doit être un identificateur universel de la machine,
  - une route précisant comment la machine peut être atteinte.

L'adressage Internet

Solution : adressage binaire compact assurant un routage efficace

- **Adressage "à plat" par opposition à un adressage hiérarchisé permettant la mise en oeuvre de l'interconnexion d'égal à égal**
- **Utilisation de noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base)**

- **Les classes d'adressage**
  - **Une adresse = 32 bits dite "Internet address" ou "IP address"**
  - **Adresse découpée en deux**

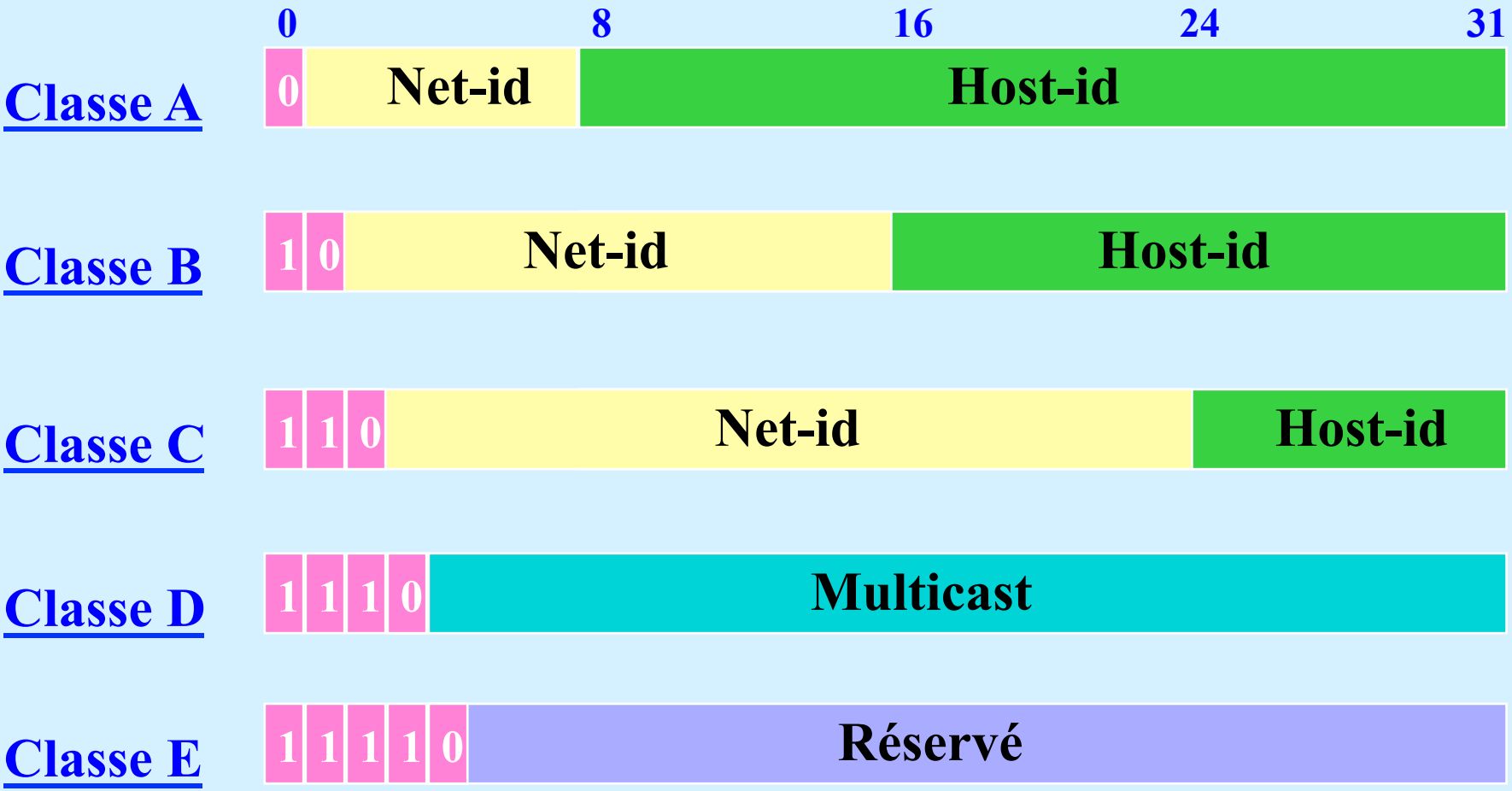
    - adresse de réseau ou *netid*,

    assigné par une autorité, identifie le réseau

    - identificateur local de machine ou *hostid*

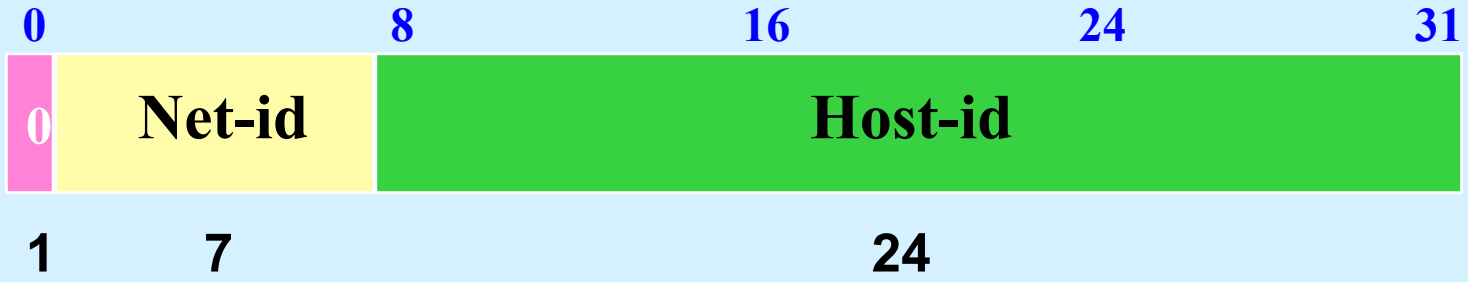
    assigné par l'administrateur du réseau, identifie ma machine sur le réseau
  - **Le découpage précis dépend de la classe d'adresses. Cinq classes d'adresse sont définies**

L'adressage Internet



Adressage IP: classe A

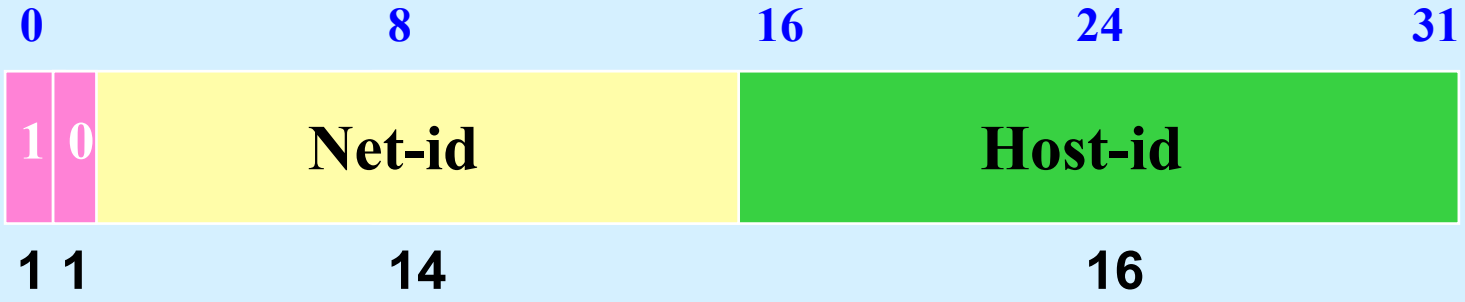
- **7 bits pour le numéro de réseau**
  - **1.0.0.0 à 126.0.0.0**
- **24 bits pour l'adressage local**
  - **256^3 @ locales possibles**



Adressage IP: classe B

- **16 bits pour le numéro de réseau**
  - **128.1.0.0 à 191.255.0.0**

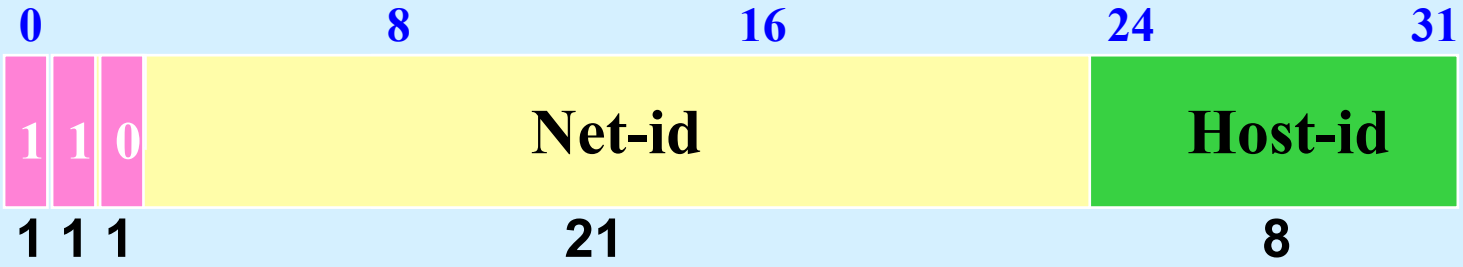
- **16 bits pour l'adressage local**
  - **256^2 @ locales possibles**
    Ex: 129.175 (LRI-Paris-Sud) 134.157 (Jussieu)



Adressage IP: classe C

- **24 bits pour le numéro de réseau**
  - **192.0.1.0 à 223.255.255.0**

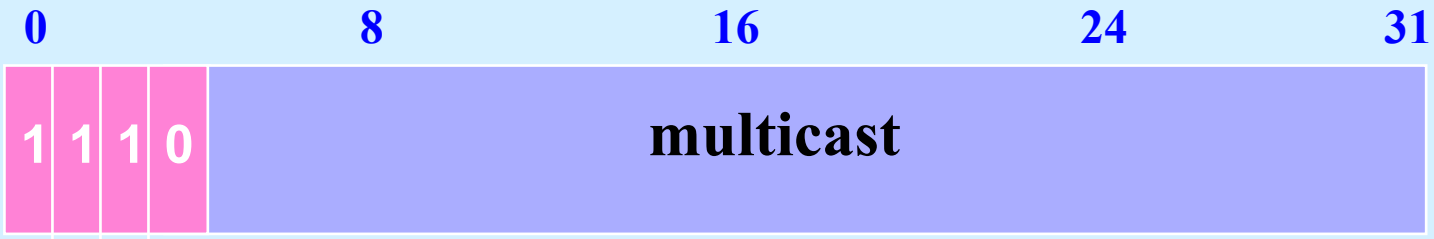
- **8 bits pour l'adressage local**
  - **256 @ locales possibles**
    Ex: 193.52.236 (Département Informatique IUT-Dijon)



Adressage IP: classe D

- **adresse multicast (RFC 1700)**
  transmission point à multipoint: exemple vidéo-conférence

- **réseau 224 à 231**
  Ex: 224.4.4.4



Adressage IP

- **Classe E: réservée pour des utlisations futures**
- **Adresses particulières**

  - tous les bits du réseau sont à 0 => adresser une machine locale

  - tous les bits du réseau sont à 1 => concerne uniquement le réseau physique associé

  - soi-même: 127.0.0.1 (loopback ou localhost)
  test logiciels, communication inter-processus sur la station

  - tous les bits de la machine à 0 => réseau
  130.190.0.0 désigne le réseau de classe B : 130.190

  - tous les bits de la machine à 1 => toutes les machines du réseau diffusion, broadcast IP
  130.190.255.255 désigne toutes les machines du réseau 130.190

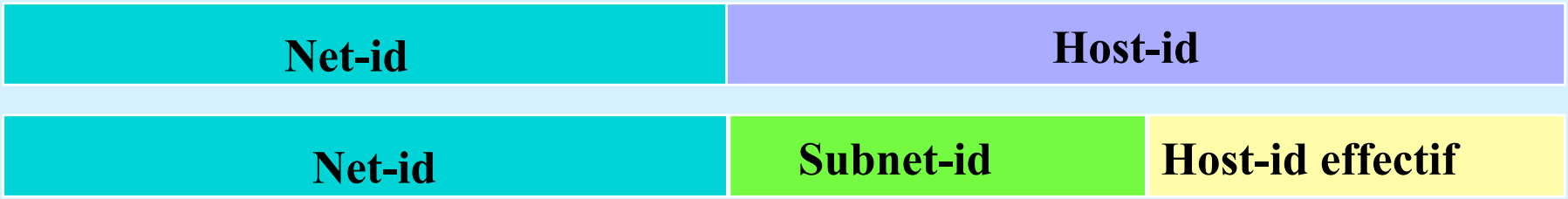
  - 0.0.0.0 une machine ne connaît pas son adresse (station sans disque qui utilise RARP)

Adressage IP

- **Résumé**

Sous-réseaux IP

- **Découpage d'un réseau en entités plus petites**
  - sous-réseau ou 'subnet'
  - permet meilleur structuration du réseau du site
  - décidé par l'administrateur du site
  - adresse de sous-réseaux prélevée sur la partie 'Host-id'
  - longueur compter en bits décidée par l'administrateur

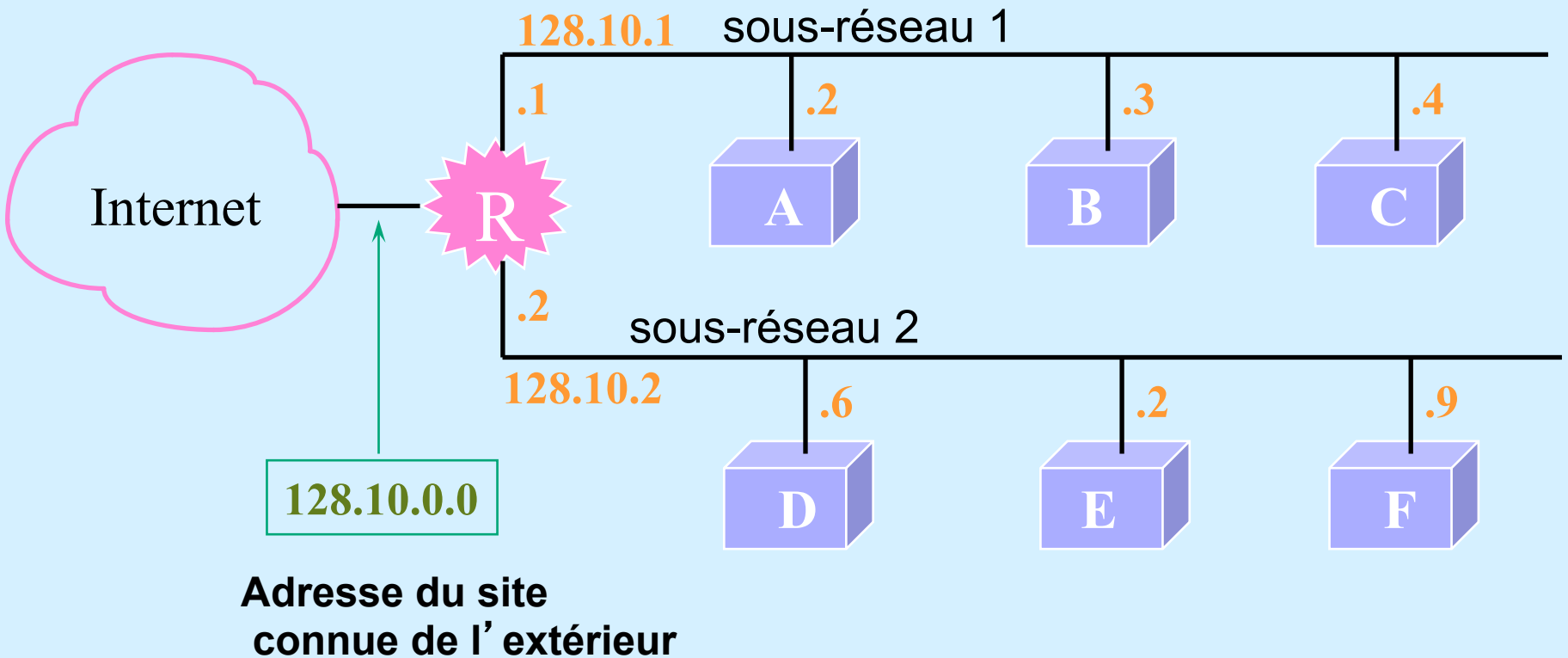


- tous les équipements réseaux doivent utiliser la notion de sous-réseau (stations, serveurs de terminaux, routeurs, imprimantes, …)
- interconnexion des sous-réseaux impérativement par des routeurs

Sous-réseaux IP

Exemple :

- découpage en 2 sous-réseaux, numérotation par le 3ème octet



Sous-réseaux IP

- **Le découpage est inconnu de l'extérieur !**
- **Passe par l'utilisation d'un subnet-mask**
  - **même notation que l'adresse IP:**
    - * bits réseau à 1
    - * bits de la partie sous-réseau à 1
    - * bits de la parite host à 0
  - **Exemple: 130.190.0.0; réseau de classe B**
    - * masque par défaut 255.255.0.0 si pas de sous-réseau
    - * masque 255.255.255.0 si présence de (au plus 256) sous-réseaux
- **utilisation**
  - **@IP & subnet -mask =adresse net-id+subnet**
    - utilisée pour le routage local au site
  - **@IP & ~(subnet-mask)=host-id effectif**

IP: fonctions

- **Assure le routage :savoir où envoyer le datagramme**
  - Les équipements IP ne connaissent que le prochain équipement sur le chemin (next hop)

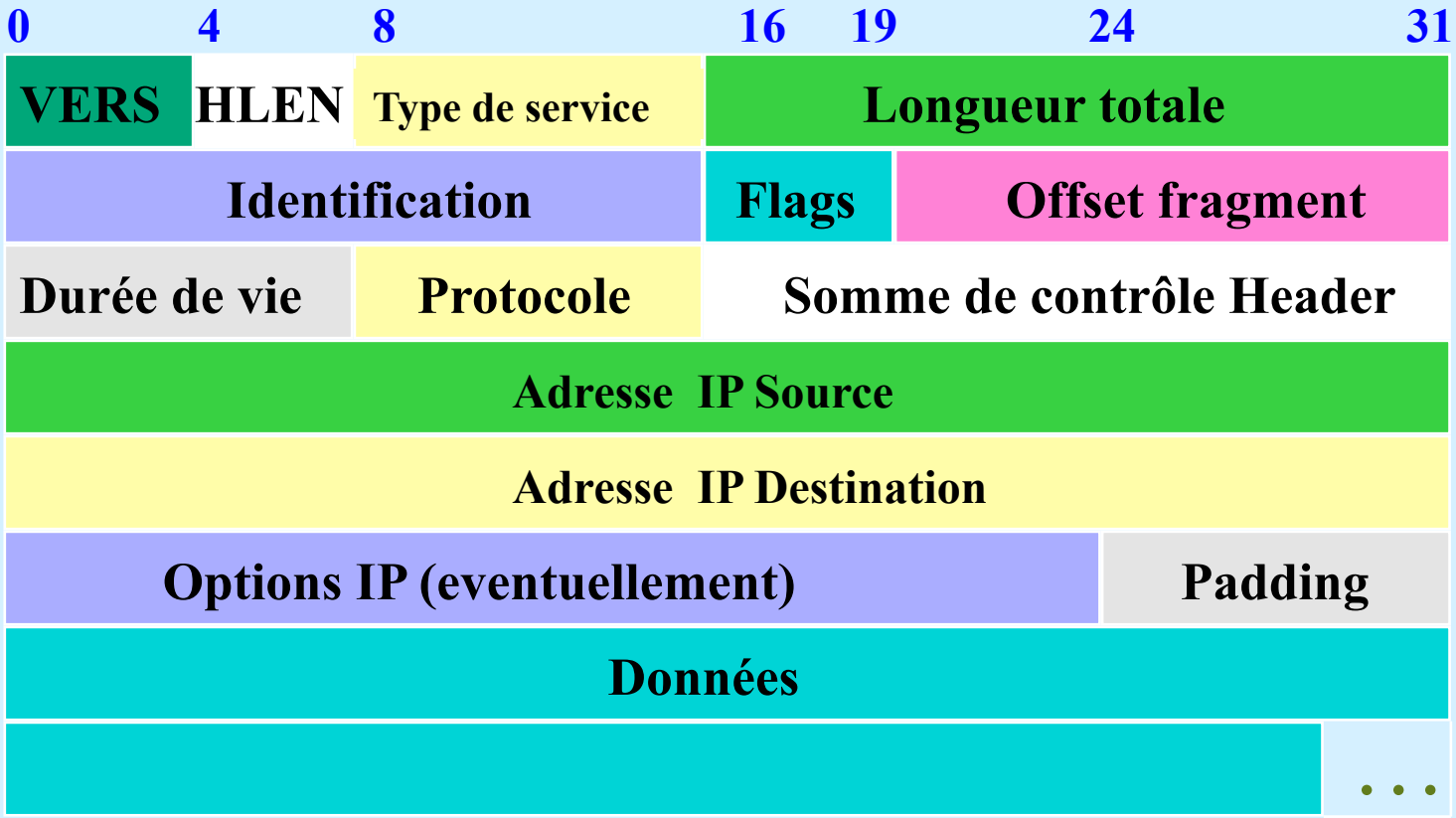
- **La fragmentation**
  - C'est la machine destinataire qui réassemble non le routeur à la frontière d'un type de réseau

- **IP n'assure pas**
  - le multiplexage
  - la vérification du séquencement
  - la détection de perte
  - la retransmission en cas d'erreur
  - le contrôle de flux
    - ICMP assure partiellement cette fonction

Datagramme IP

✦ **Le datagramme IP**

L'unité de transfert de base dans un réseau Internet est le datagramme qui est constituée d'un en-tête et d'un champ de données:



Datagramme IP

Signification des champs du datagramme IP :

- **VERS : numéro de version de protocole IP, actuellement version 4,**
- **HLEN : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),**
- **Longueur totale : longueur totale du datagramme (en-tête + données)**
- **Type de service : indique comment le datagramme doit être géré :**

  - **PRECEDENCE (3 bits) : définit la priorité du datagramme; en général ignoré par les machines et passerelles (pb de congestion).**
  - **Bits D, T, R : indiquent le type d'acheminement désiré du datagramme, permettant à une passerelle de choisir entre plusieurs routes (si elles existent) : D signifie délai court, T signifie débit élevé et R signifie grande fiabilité.**

Datagramme IP

- **FRAGMENT OFFSET, FLAGS, IDENTIFICATION : les champs de la fragmentation.**
  - **Sur toute machine ou passerelle mettant en oeuvre TCP/IP une unité maximale de transfert (*Maximum Transfert Unit* ou MTU) définit la taille maximale d'un datagramme véhiculé sur le réseau physique correspondant**
  - **lorsque le datagramme est routé vers un réseau physique dont le MTU est plus petit que le MTU courant, la passerelle fragmente le datagramme en un certain nombre de fragments, véhiculés par autant de trames sur le réseau physique correspondant,**
  - **lorsque le datagramme est routé vers un réseau physique dont le MTU est supérieur au MTU courant, la passerelle route les fragments tels quels (rappel : les datagrammes peuvent emprunter des chemins différents),**
  - **le destinataire final reconstitue le datagramme initial à partir de l'ensemble des fragments reçus; la taille de ces fragments correspond au plus petit MTU emprunté sur le réseau. Si un seul des fragments est perdu, le datagramme initial est considéré comme perdu : la probabilité de perte d'un datagramme augmente avec la fragmentation.**

Datagramme IP

- **Champs liés à la fragmentation IP**

- Identification : Identification du datagramme

* Utilisé par l'émetteur et le destinataire pour identifier le datagramme
* Numérotation faite par l'émetteur
* Uniquement utilisé pour la fragmentation

- Flags : Flags pour des fragments

001 : il y a encore des fragments

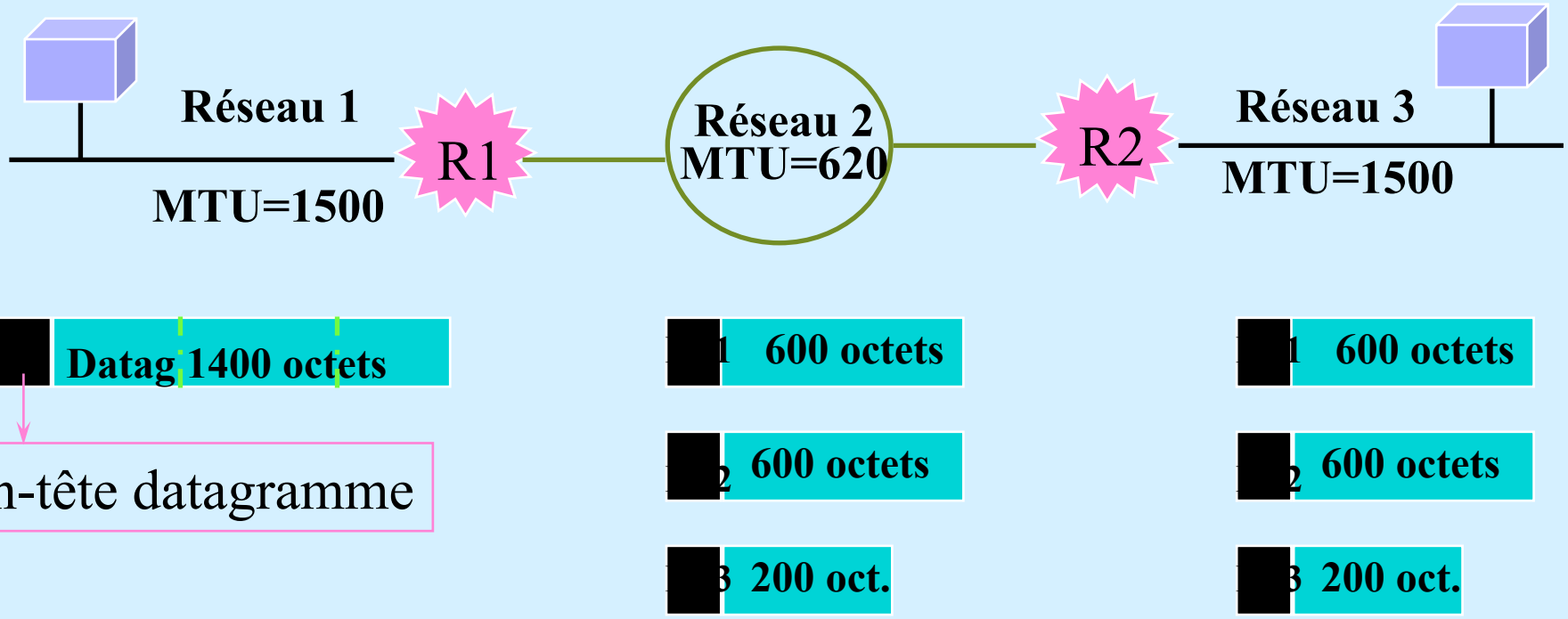
000 : dernier fragment (ou pas encore fragmenté)

01X: ne pas fragmenter

- Offset fragment : Fragment offset

* position du fragment dans le datagramme d'origine,
* calculé en unité de 8 octets,
* premier fragment = 0
* Le destinataire doit récupérer tout les fragments, si un fragment est perdu tout le datagramme est jeté

Datagramme IP



Datagramme IP

- **@ source : Adresse IP de l'émetteur**

- **@ destinataire : Adresse IP du destinataire**

Ce sont des adresses d'extrémité, pas les nœuds intermédiaires !

Datagramme IP

- **Durée de vie**
  - **Ce champ indique en secondes, la durée maximale de transit du datagramme sur l'internet. La machine qui émet le datagramme définit sa durée de vie.**
  - **Les passerelles qui traitent le datagramme doivent décrémenter sa durée de vie du nombre de secondes (1 au minimum) que le datagramme a passé pendant son séjour dans la passerelle; lorsque celle-ci expire le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.**
- **Protocole**

Ce champ identifie le protocole de niveau supérieur dont le message est véhiculé dans le champ données du datagramme :

- **6 : TCP,**
- **17 : UDP,**
- **1 : ICMP.**

Datagramme IP

- **Somme de contrôle de l'en-tête**
  - **Ce champ permet de détecter les erreurs survenant dans l'en-tête du datagramme, et par conséquent l'intégrité du datagramme.**
  - **Le total de contrôle d'IP porte sur l'en-tête du datagramme et non sur les données véhiculées.**

- **Longueur totale : taille du fragment et non pas celle du datagramme initial.**

Datagramme IP

- **Option : variables en taille, permettent des extensions**

- Certaines options sont standards (décrites dans des RFCs)

Exemple : niveau de sécurité. Time stamp (chaque routeur ajoute l'heure de passage)

- Elles se composent

* du code de l'option (1 octet)
* de la longueur de l'option (1 octet)
* des données associées

- **Padding : complète le champs options**

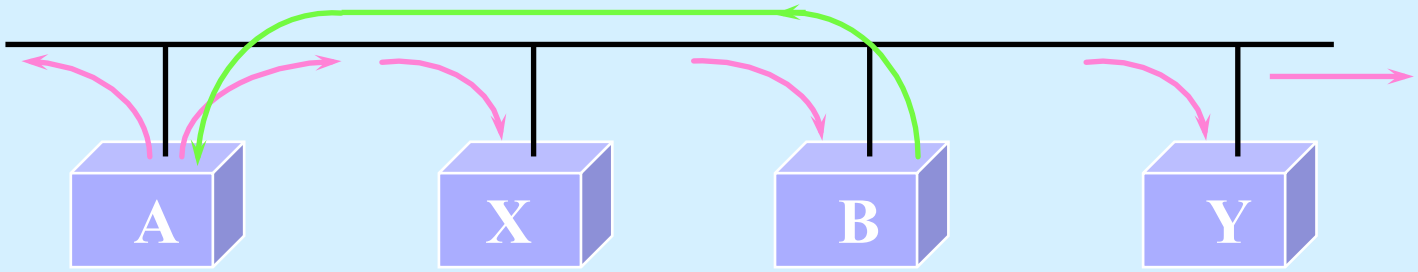
- Pour que la longueur de l'en-tête soit un multiple de 32.

ARP: Address Resolution Protocol

- **Le besoin**
  - **La communication entre machines ne peut s'effectuer qu'à travers l'interface physique**
  - **Les applicatifs ne connaissant que des adresses IP, comment trouver une adresse MAC à partir de l'adresse IP?**
- **La solution : ARP**
  - **Mise en place dans TCP/IP d'un protocole de bas niveau appelé Adress Resolution Protocol (ARP)**
  - **Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine destinatrice**
- **LA technique :**
  - **Diffusion d'adresse sur le réseau physique**
  - **La machine d'adresse IP émet un message contenant son adresse physique**
  - **Les machines non concernées ne répondent pas**
  - **Gestion cache pour ne pas effectuer de requête ARP à chaque émission**

ARP: Address Resolution Protocol

- **L'association adresse physique - adresse IP de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache**



- **Pour connaître l'adresse physique de B, PB, à partir de son adresse IP IB, la machine A diffuse une requête ARP qui contient l'adresse IB vers toutes les machines; la machine B répond avec un message ARP qui contient la paire (IB, PB).**

RARP: Reverse Address Resolution Protocol

- **Problème : déterminer un mécanisme permettant à la station d'obtenir son adresse IP depuis le réseau.**

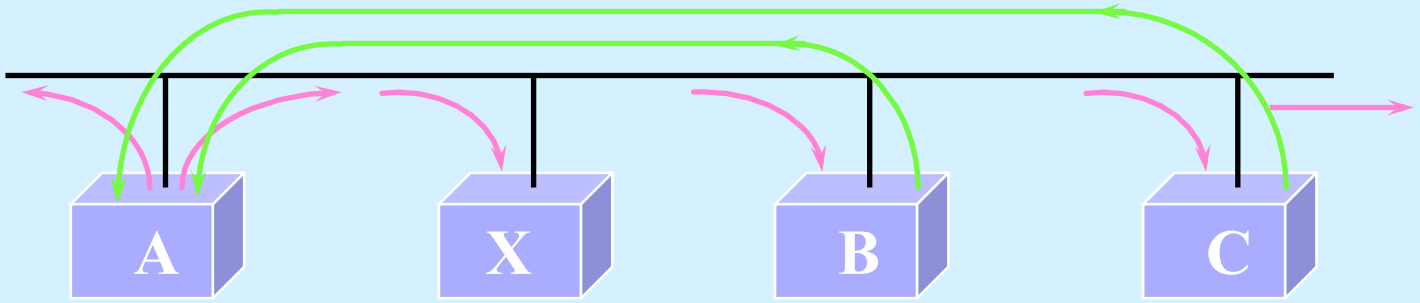
- **La solution**
  - **Protocole de bas niveau appelé Reverse Adress Resolution Protocol**
  - **Permet d'obtenir son adresse IP à partir de l'adresse physique qui lui est associée.**

- **Fonctionnement**

  Serveur RARP sur le réseau physique; son rôle: fournir les adresses IP associées aux adresses physiques des stations du réseau;

RARP: Reverse Address Resolution Protocol

- **Le serveur possède une base de données contenant les couples adresse physique/adresse IP,**
- **les stations émettent une requête RARP sur le réseau, consistant à demander l'adresse IP qui est associée à leur adresse physique,**
- **Les requêtes RARP sont propagées vers le ou les serveur(s) RARP par mécanisme de diffusion. Le(s) serveur(s) RARP réponde(nt) par un message de type RARP.**



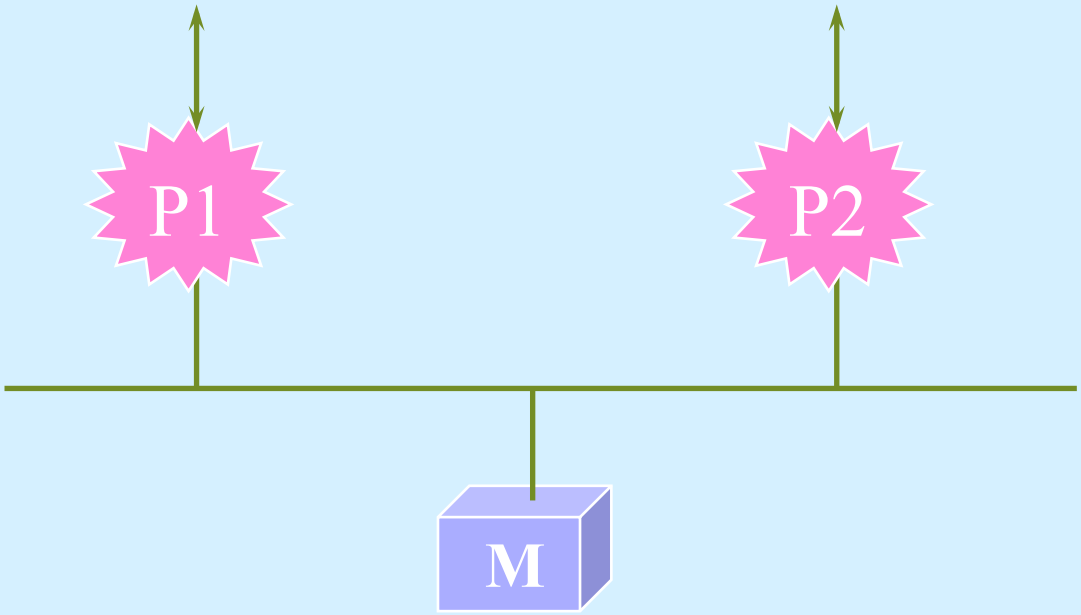
Pour connaître son adresse IP, A diffuse sur le réseau, une requête RARP
qui la désigne comme destinataire

Les Serveurs RARP (B et C) répondent à la requête.

Routage des datagrammes

- **Le routage est le processus permettant à un datagramme d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.**
- **Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.**
- **Les routeurs forment une structure coopérative de telle manière qu'un datagramme transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire. Un routeur possède deux ou plusieurs connexions réseaux tandis qu'une machine possède généralement qu'une seule connexion.**
- **Machines et routeurs participent au routage :**
  - **les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le datagramme doit être acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.**
  - **les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.**

Routage des datagrammes (suite)



M est mono-domiciliée et doit acheminer les datagrammes vers une des passerelles P1 ou P2; elle effectue donc le premier routage. Dans cette situation, aucune solution n'offre un meilleur choix.

Le routage indirect repose sur une table de routage IP, présente sur toute machine et passerelle, indiquant la manière d'atteindre un ensemble de destinations.

Routage des datagrammes (suite)

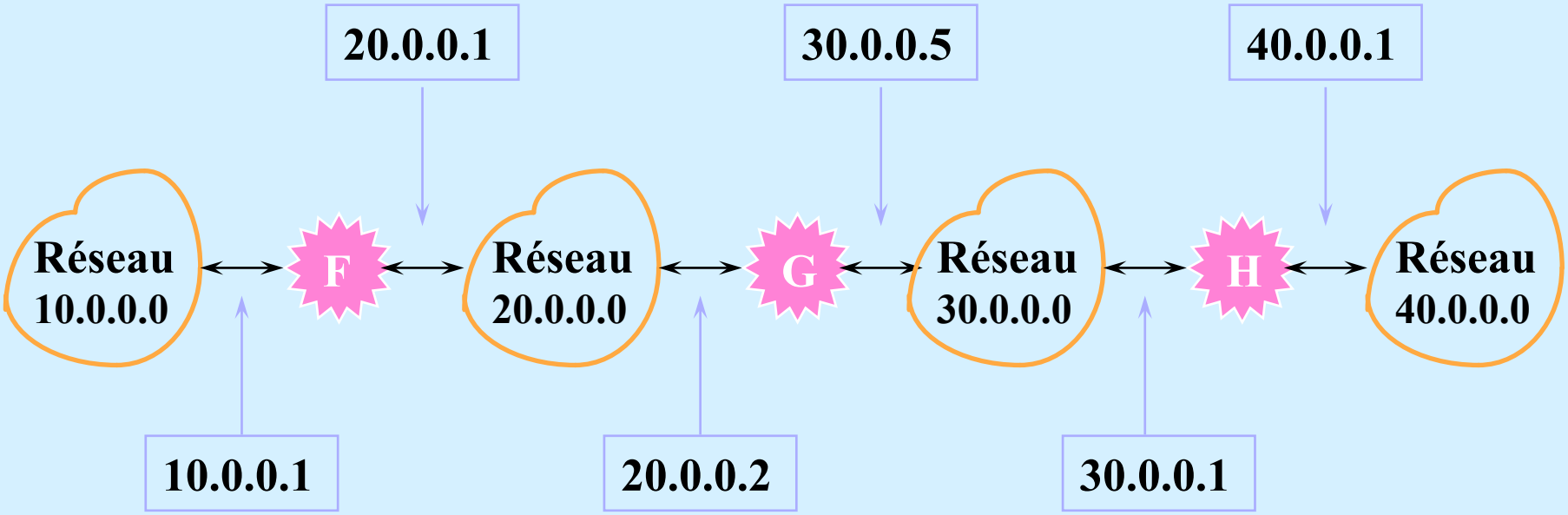
- **Les tables de routage IP, pour des raisons évidentes d'encombrement, renseignent seulement les adresses réseaux et non pas les adresses machines.**

- **Typiquement, une table de routage contient des couples (R, P) où R est l'adresse IP d'un réseau destination et P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire.**

- **La passerelle ne connaît pas le chemin complet pour atteindre la destination.**

- **Pour une table de routage contenant des couples (R, P) et appartenant à la machine M, P et M sont connectés sur le même réseau physique dont l'adresse de niveau réseau (partie Netid de l'adresse IP) est R.**

Routage des datagrammes (suite)



Pour atteindre les machines du réseau	10.0.0.0	20.0.0.0	30.0.0.0	40.0.0.0
Router vers	20.0.0.1	direct	direct	30.0.0.1

Table de routage de G

Routage des datagrammes (suite)

Route_Datagramme_IP(datagramme, table_de_routage)

- **Extraire l'adresse IP destination, ID, du datagramme,**
- **Calculer l'adresse du réseau destination, IN.**
- **Si IN correspondant à une adresse de réseau directement accessible,**

  envoyer le datagramme vers sa destination, sur ce réseau.
- **sinon si dans la table de routage, il existe une route vers ID**

  router le datagramme selon les informations contenues dans la table de routage.
- **sinon si IN apparaît dans la table de routage,**

  router le datagramme selon les informations contenues dans la table de routage.
- **sinon s'il existe une route par défaut**

  router le datagramme vers la passerelle par défaut.
- **sinon déclarer une erreur de routage.**

Routage des datagrammes (suite)

- **Après exécution de l'algorithme de routage, IP transmet le datagramme ainsi que l'adresse IP déterminée, à l'interface réseau vers lequel le datagramme doit être acheminé.**

- **L'interface physique détermine alors l'adresse physique associée à l'adresse IP et achemine le datagramme sans l'avoir modifié (l'adresse IP du prochain saut n'est sauvegardée nulle part).**

- **Si le datagramme est acheminé vers une autre passerelle, il est à nouveau géré de la même manière, et ainsi de suite jusqu'à sa destination finale.**

Routage des datagrammes (suite)

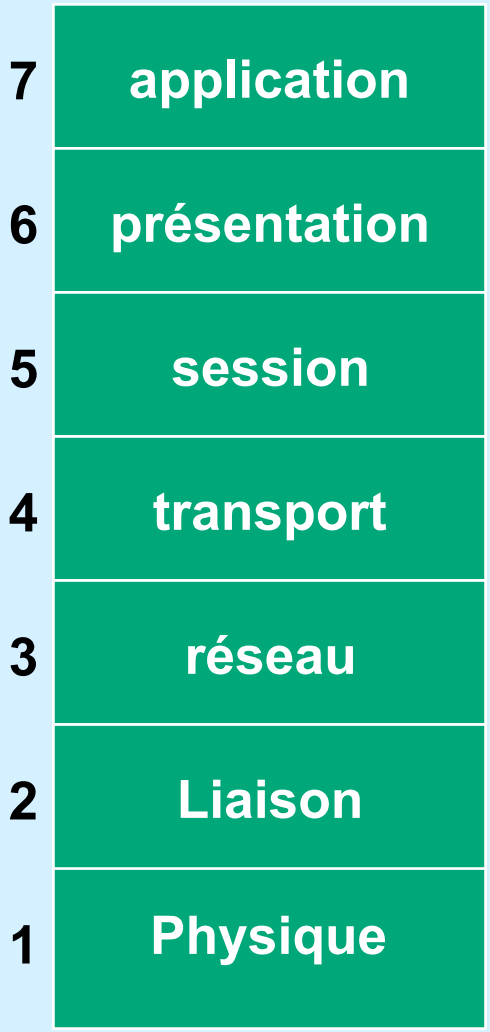
- **Les datagrammes entrants sont traités différemment selon qu'il sont reçus par une machine ou une passerelle :**

- **machine : le logiciel IP examine l'adresse destination à l'intérieur du datagramme**

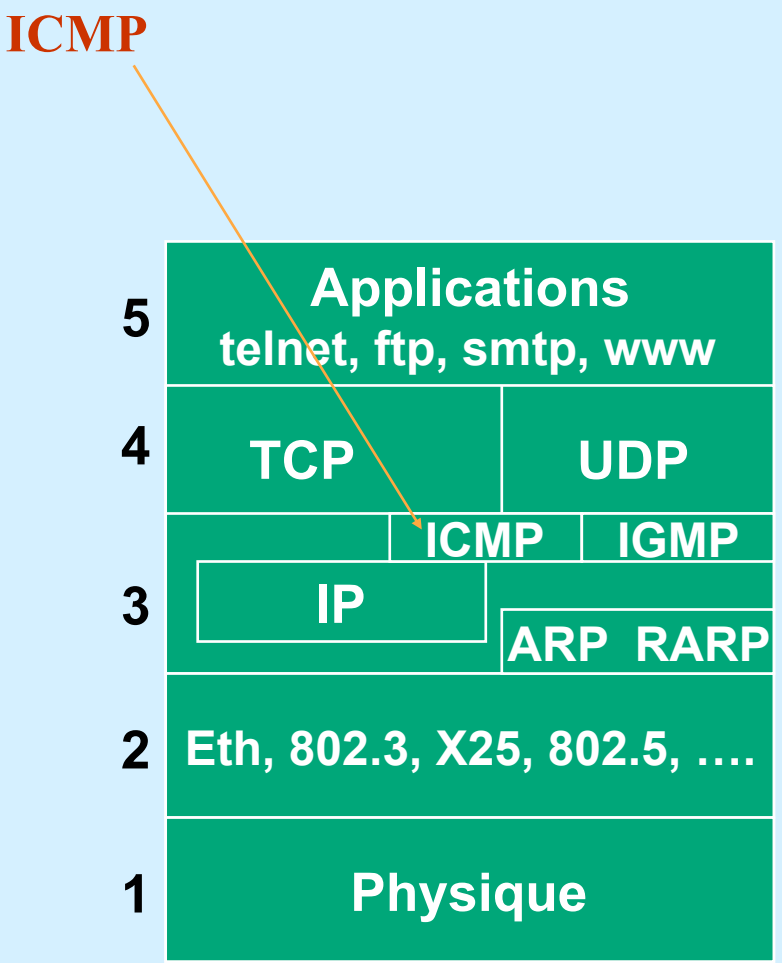
  - **si cette adresse IP est identique à celle de la machine, IP accepte le datagramme et transmet son contenu à la couche supérieure.**
  - **sinon, le datagramme est rejeté; une machine recevant un datagramme destiné à une autre machine ne doit pas router le datagramme.**

- **passerelle : IP détermine si le datagramme est arrivé à destination et dans ce cas le délivre à la couche supérieure. Si le datagramme n'a pas atteint sa destination finale, il est routé selon l'algorithme de routage précédemment décrit.**

Modèle en couches



Modèle OSI



Modèle TCP/IP

ICMP: Internet Control Message Protocol

Protocole de ‘gestion’ de réseau=mécanisme de rapport d’erreur.

- **Implémenté sur tous les équipements IP: stations, routeurs.**
- **Message envoyé par l’équipement destinataire ou un routeur intermédiaire**
  - Quand il s’aperçoit d’un problème dans un datagramme
  - Pour avertir l’émetteur afin qu’il modifie son comportement
  - ex: routeur qui a une mauvaise information de routage

- **Un message ICMP ne doit pas engendrer un autre message ICMP**
  - Il ne demande pas de répondre

ICMP: Internet Control Message Protocol

Le besoin

- **Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles.**
- **ICMP rapporte les messages d'erreur à l'émetteur initial.**
- **Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dûes à des problèmes d'interconnexions rencontrées sur l'Internet :**
  - **machine destination déconnectée,**
  - **durée de vie du datagramme expirée,**
  - **congestion de passerelles intermédiaires.**
- **Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.**
- **Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'Internet.**
- **Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP (évite l'effet cummulatif).**

ICMP : format des messages

TYPE : 8 bits; type de message

CODE : 8 bits; informations complémentaires

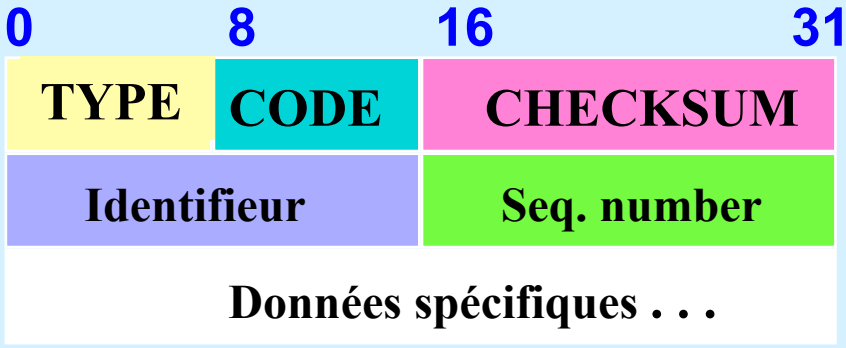
CHECKSUM : 16 bits; champ de contrôle

HEAD-DATA : en-tête datagramme + 64 premiers bits des données.

TYPE	Message ICMP
0	Réponse d'écho
3	Destination inaccessible
4	Source Quench (demande de ralentissement)
5	Redirection (change de route)
8	Demande d'écho
11	Durée de vie expirée
12	Problème de paramétrage

TYPE	Message ICMP
13	Horadatage (Timestamp)
14	Réponse horadatage
15	demande d'information
16	Réponse à la demande d'information
17	Demande du 'netmask'
18	Réponse à la demande de 'netmask'

ICMP : format des commandes



IDENTIFIER et SEQUENCE NUMBER sont utilisés par l'émetteur pour contrôler les réponses aux requêtes, (CODE = 0).

Demande d'écho et réponse d'écho

- **Permettent à une machine ou passerelle de déterminer la validité d'un chemin sur le réseau.**
- **Le champ de données spécifiques est composé de données optionnelles de longueur variable émises par la requête d'écho et devant être renvoyées par le destinataire.**
- **Utilisé par les outils applicatifs tels ping et traceroute.**

ICMP : les commandes

Synchronisation des Horloges et temps de transit

- **Les horloges de deux machines qui diffèrent de manière importante peuvent poser des problèmes pour des logiciels distribués.**
- **Une machine peut émettre une demande d'horodatage (*timestamp request*) à une autre machine susceptible de lui répondre (*timestamp reply*) en donnant l'heure d'arrivée de la demande et l'heure de départ de la réponse.**
- **L'émetteur peut alors estimer le temps de transit ainsi que la différence entre les horloges locale et distante.**
- **Le champ de données spécifiques comprend l'heure originale (*originate timestamp*) émis par le demandeur, l'heure de réception (*receive timestamp*) du destinataire, et l'heure de départ (*transmit timestamp*) de la réponse.**

ICMP : les commandes

Demande et réponse d'information (*Information Request* + *Reply*)

- **Ces messages étaient initialement utilisés pour permettre aux machines de connaître leur adresse IP au démarrage du système.**
- **Ces commandes sont aujourd'hui remplacées par les protocoles RARP et BOOTP.**

Obtention de masque de sous-réseau

- **Une machine peut émettre une demande de masque de sous-réseau (*Subnet Mask Request*) vers une passerelle gérant le sous-réseau en question.**
- **La passerelle transmet par une "*Subnet Mask Reply*", l'adresse de masque de sous-réseau (de longueur 32 bits) dans le champ de donnée spécifique.**

ICMP : les messages d'erreur

Format des messages d'erreur ICMP

- **CODE indique le codage de l'erreur rapportée et est spécifique à chaque type d'erreur,**
- **SPECIFIQUE est un champ de données spécifique au type d'erreur,**
- **IP HEADER + FIRST 64 bits contient l'en-tête IP + les premiers 64 bits de données du datagramme pour lequel le message est émis.**
- **Compte rendu de destination inaccessible**

ICMP : les messages d'erreur

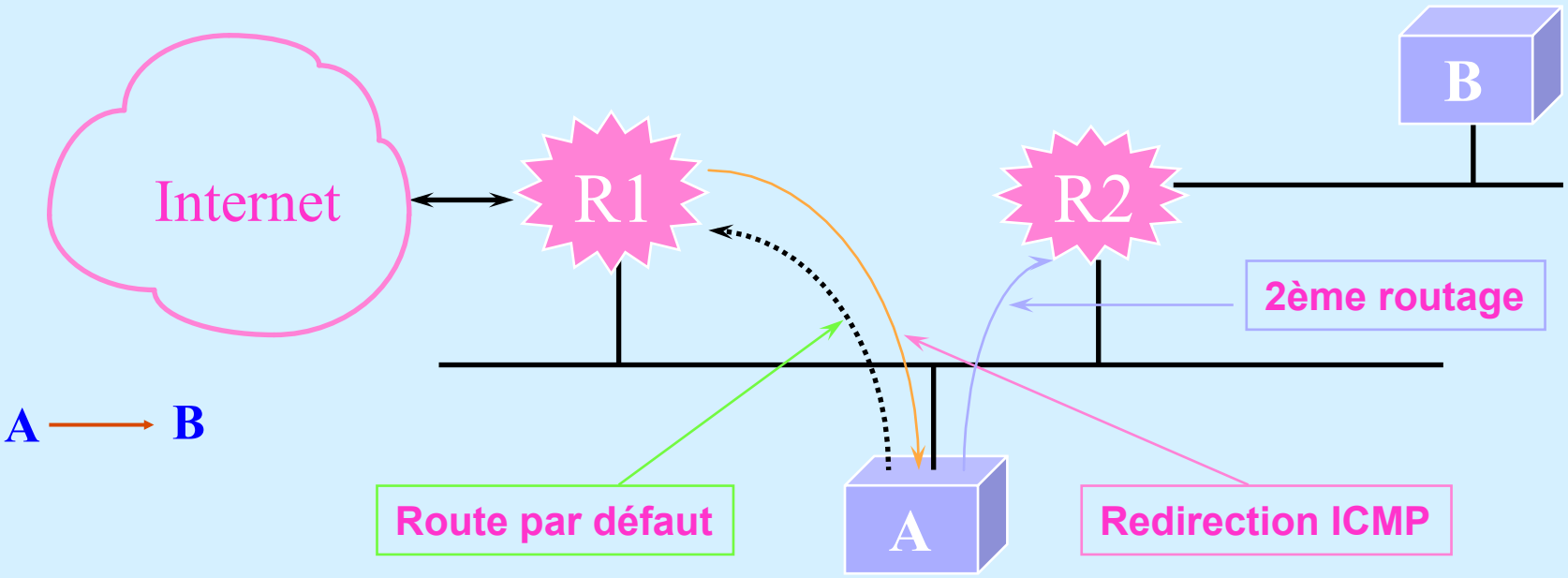
- **Lorsqu'une passerelle émet un message ICMP de type destination inaccessible, le champ code décrit la nature de l'erreur :**
  - **0 Network Unreachable (inaccessible)**
  - **1 Host Unreachable**
  - **2 Protocol Unreachable**
  - **3 Port Unreachable**
  - **4 Fragmentation Needed and DF set**
  - **5 Source Route Failed**
  - **6 Destination Network Unknown**
  - **7 Destination Host Unknown**
  - **8 Source Host Isolated**
  - **9 Communication with desination network administratively prohibited**
  - **10 Communication with desination host administratively prohibited**
  - **11 Network Unreachable for type of Service**
  - **12 Host Unreachable for type of Service**

ICMP : contrôle de congestion

- **Le protocole IP étant un protocole en mode non connecté :**
  - **=> les passerelles ne peuvent réserver à l'avance la quantité de mémoire nécessaire au routage des datagrammes.**
  - **=> des datagrammes sont alors détruits.**
- **Cette situation de congestion se produit :**
  - **lorsqu'une passerelle est connectée à deux réseaux aux débits différents (elle ne peut écouler au rythme imposé par le réseau le plus rapide),**
  - **lorsque de nombreuses machines émettent simultanément des datagrammes vers une passerelle.**
- **Pour palier ce problème, la machine peut émettre un message ICMP de limitation de débit de la source (*Source Quench*) vers l'émetteur.**
- **Il n'existe pas de message d'annulation de limitation de débit. La source diminue le débit, puis l'augmente progressivement tant qu'elle ne reçoit pas de nouvelle demande de limitation.**

ICMP : modification de route

Un message ICMP de redirection de route peut être transmis par une passerelle vers une machine reliée au même réseau pour lui signaler que la route n'est pas optimale.



Une fois la redirection effectuée, les datagrammes seront acheminés vers la passerelle appropriée.

ICMP : modification de route

- **Dans le bloc de commande, le champ SPECIFIQUE indique l'adresse de la passerelle que la machine doit utiliser pour router le datagramme; CODE spécifie la redirection :**

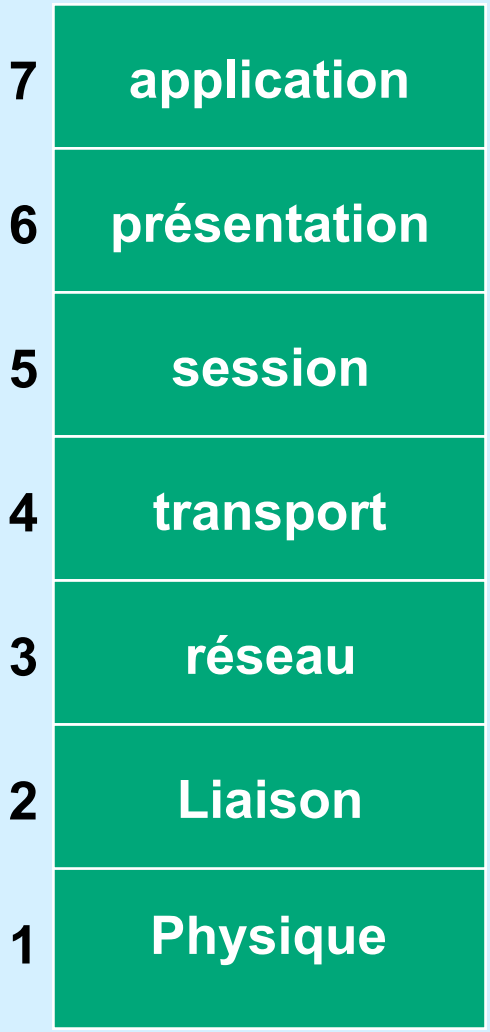
CODE	SIGNIFICATION
0	Redirect datagrams for the Network
1	Redirect datagrams for the Host
2	Redirect datagrams for the Type of Service and Network
3	Redirect datagrams for the Type of Service and Host

Détection de routes circulaires ou excessivement longues

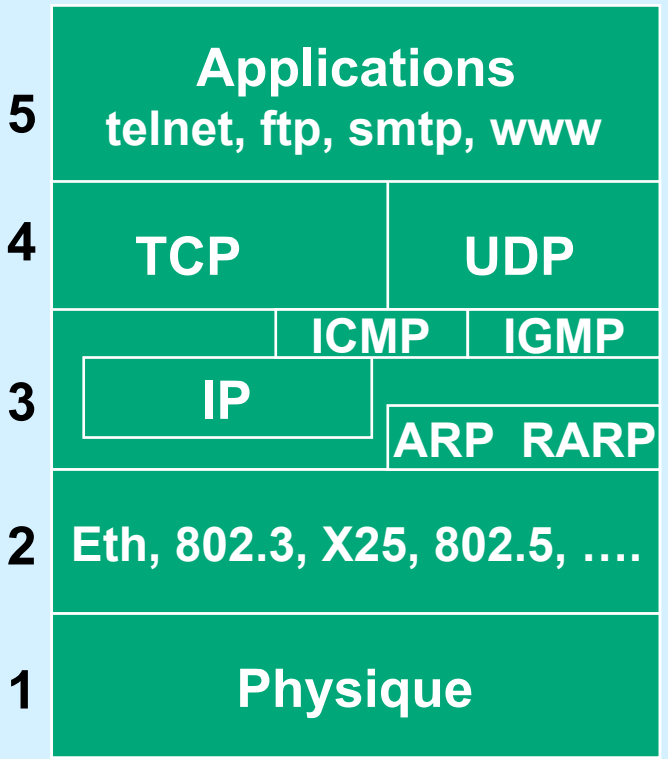
- **Une passerelle détruit les datagrammes dont le champ durée de vie est à zéro et émet un message ICMP de délai dépassé.**

CODE	SIGNIFICATION
0	time to live exceeded in transit
1	fragment reassembly time exceeded

Modèle en couches

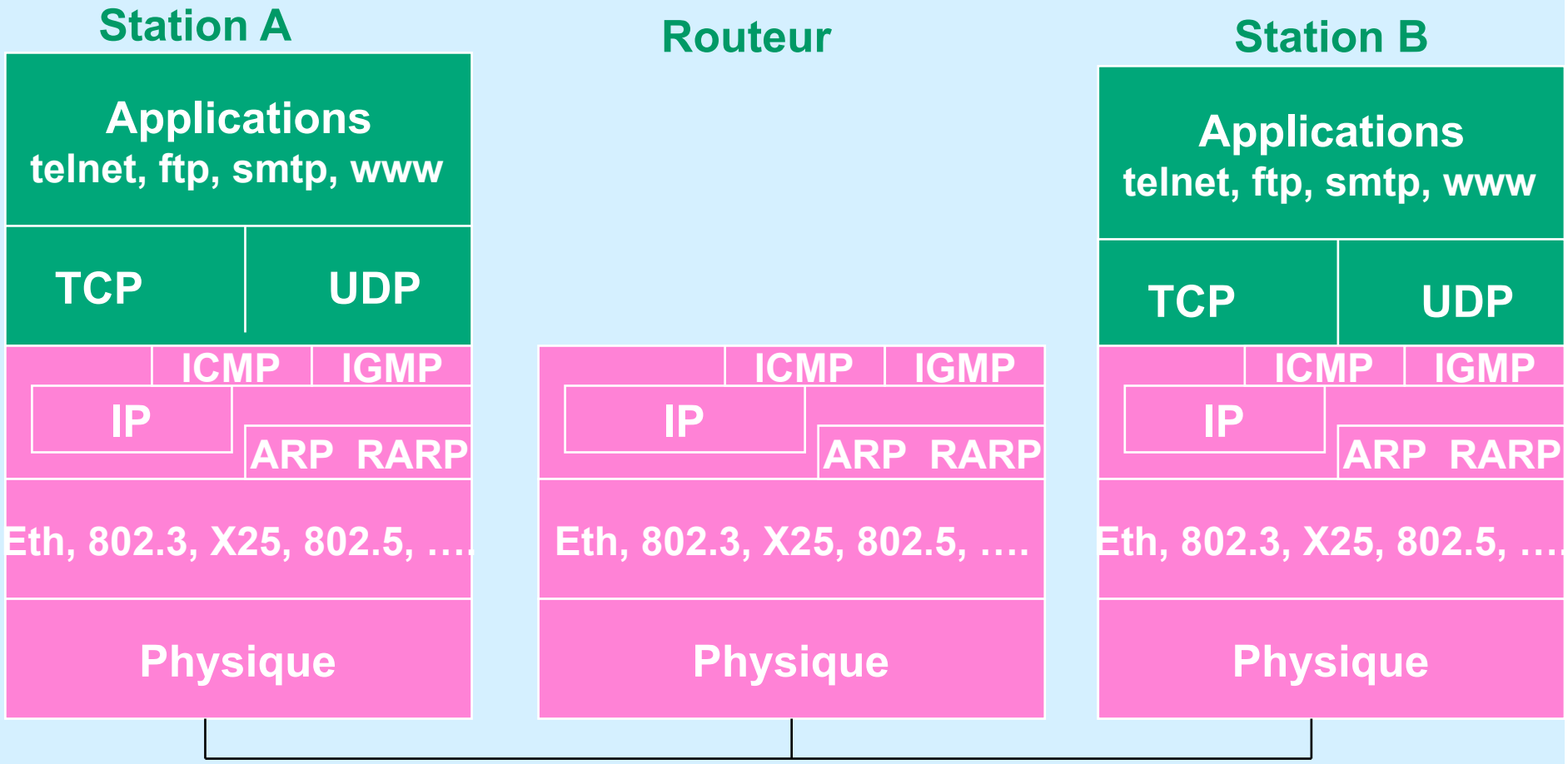


Modèle OSI



Modèle TCP/IP

Modèle en couches



Couche Transport

Définitions

- **Deux protocoles pour la communication entre applications**
- **TCP: Transmission Control Protocol**
  protocole en mode orienté connexion
- **UDP: User Datagram Protocol**
  protocole en mode sans connexion

Couche Transport — Définitions

- **Identification d'une application : numéro de port**
  le port est une destination abstraite utilisé par le protocole
- **Socket = Combinaison @IP- Numéro de port**
  130.190.5.1-23 est le démon telnetd sur la station 130.190.5.1
- **La combinaison de 2 sockets définit complètement une connexion TCP ou un échange UDP**

  Exemple 130.190.5.1-23 et 147.171.150.2-1094

  Connexion entre un processus client qui a pris le numéro 1094 sur la machine 147.171.150.2 et le démon telnetd sur la machine 130.190.5.1.

  Un utilisateur sur 147.171.150.2 a fait un telnet 130.190.5.1

  C'est ce que on peut avoir avec la commande Unix *netstat -a*

Couche de transport

- **Port pré-définis (RFC 1060 'Assigned numbers') pour les services :**

  20 FTP-transfert
  21 FTP-Contrôle
  23 Telnet
  25 SMTP
  53 DNS (Domain Name Server)
  69 tftp

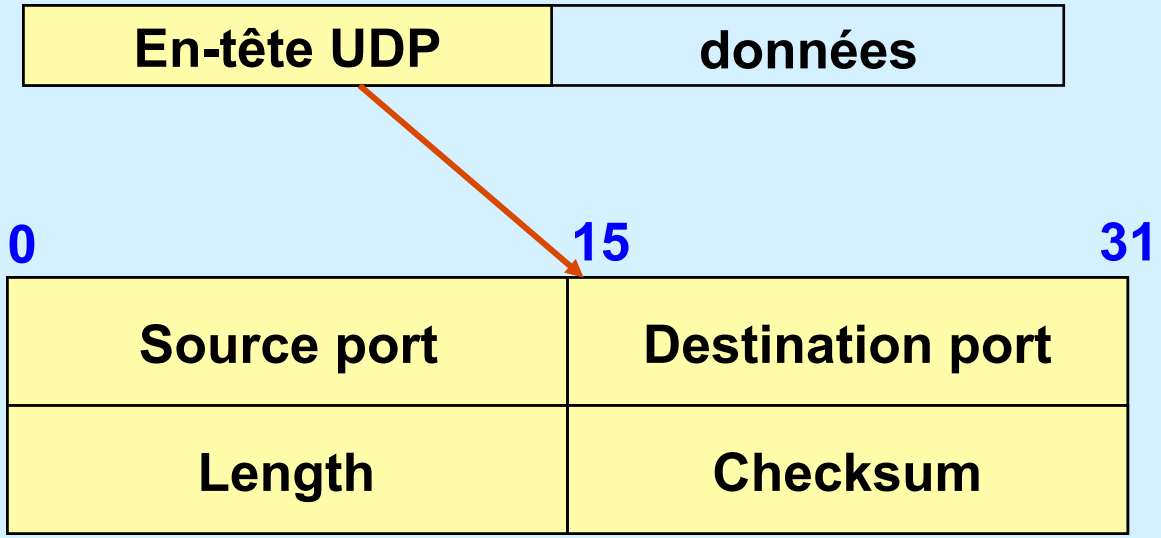
- **Mode client serveur**
  - un **serveur**, on parle de **démons dans Unix**.
  - Le client se voit attribué un numéro de port non affecté (>1000) pour éviter toute confusion avec les ports 'officiels'

- **Tous les équipements TCP/CP respectent cette attribution de ports pré-définis**

UDP (RFC 768)

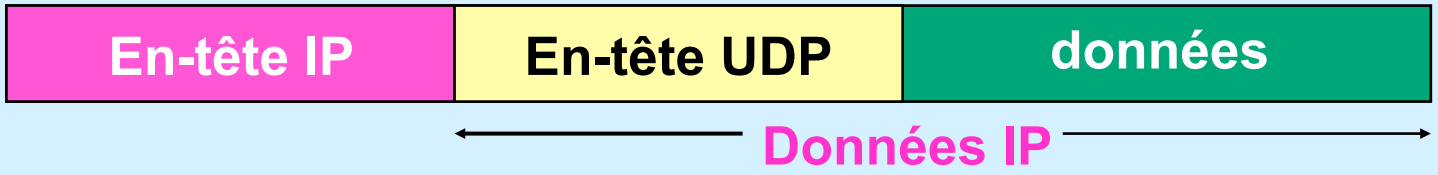
- **User Datagram Protocol**

  - service sans connexion, sans garantie, utilisant IP pour le transport de messages entre machines



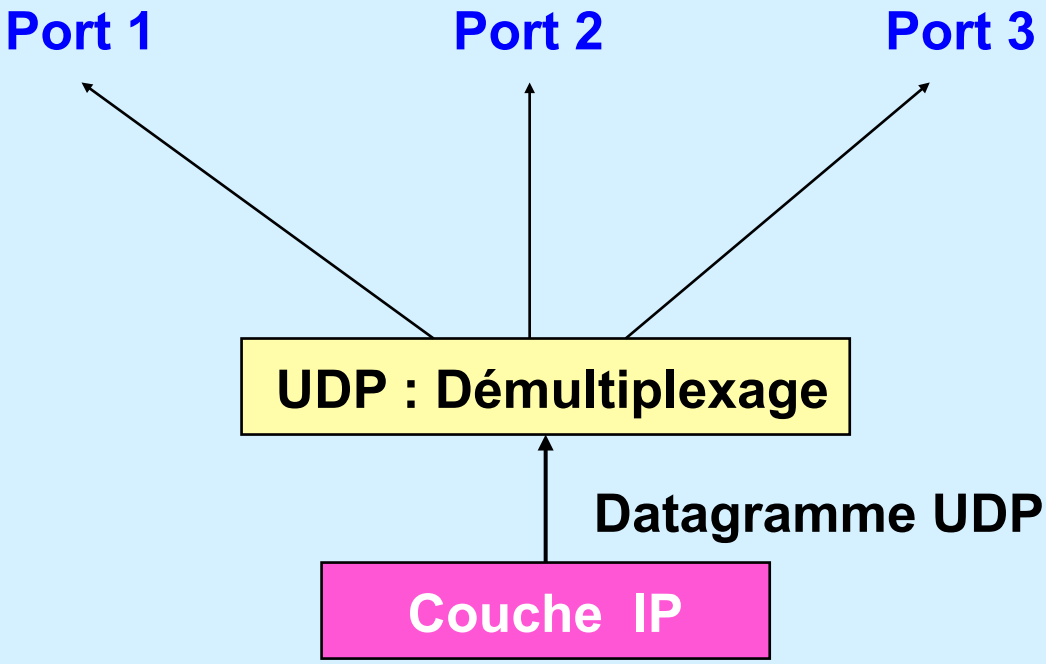
UDP : Champs

- **En-tête de 8 octets**
- **Source port : numéro de port**
  - optionnel, identifie un port pour la réponse.
- **Destination port : numéro de port**
- **Length : taille de l'en-tête et des données**
  - Unité = octet
  - Taille maximale = 64 K octets
- **Cheksum : fonction de l'en-tête et des données**
  - optionnel
  - c'est la seule garantie sur la validité des données qui arrivent à destination
- **Un datagramme UDP est contenu dans un datagramme IP**



UDP

- **Par rapport à IP, UDP rajoute l'information indiquant le service**



TCP : (RFC793) Fonctionnalités

- **Traite les données venant des couches supérieures comme une suite d'octets.**
- **Découpe cette suite d'octets en segments**
  - Taille maximale de 64 K octets
- **1 segment TCP est contenu dans un datagramme IP**
  Champs protocole du datagramme IP = 6
- **Des segments sont échangés pour :**
  - ouvrir les connexions
  - transférer des données
  - envoyés des ACK, gérer le contrôle de flux
  - fermer les connexions

TCP : La connexion

- une connexion de type circuit virtuel est établie avant que les données ne soient échangées : appel + négociation + transferts

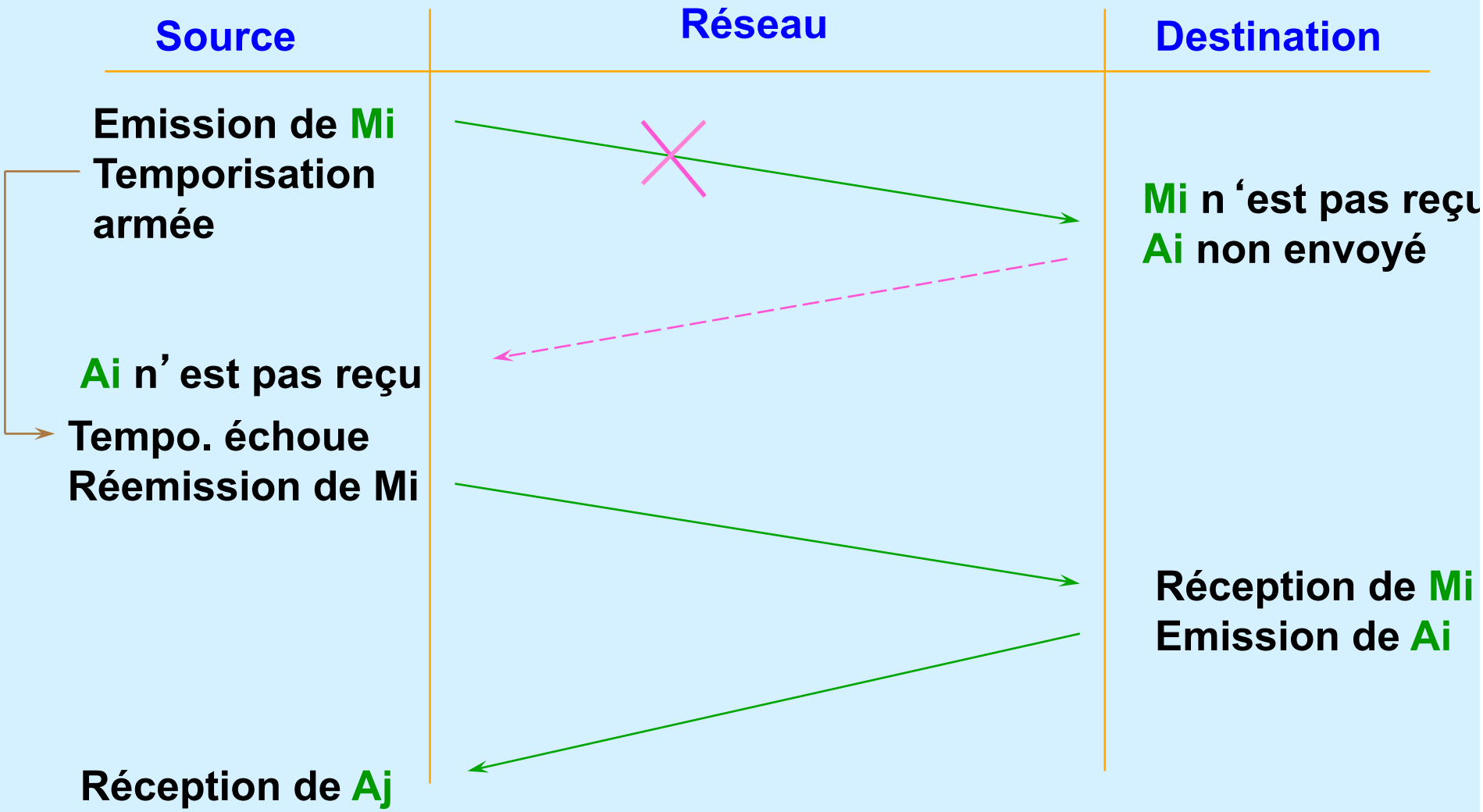
- Une connexion = une paire d'extrémités de connexion
- Une extrémité de connexion = couple (adresse IP, port)
- Exemple de connexion : ((124.32.12.1, 1034), (19.24.67.2, 21))
- Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)
- La mise en oeuvre de la connexion se fait en deux étapes :
  - une application (extrémité) effectue une ouverture passive en indiquant qu'elle accepte une connexion entrante,
  - une autre application (extrémité) effectue une ouverture active pour demander l'établissement de la connexion.

TCP : Segmentation

- **Segmentation, contrôle de flux**
  - **Les données transmises à TCP constituent un flot d'octets de longueur variable.**
  - **TCP divise ce flot de données en segments en utilisant un mécanisme de fenêtrage.**
  - **Un segment est émis dans un datagramme IP.**

- **Acquittement de messages**
  - **Contrairement à UDP, TCP garantit l'arrivée des messages, c'est-à-dire qu'en cas de perte, les deux extrémités sont prévenues.**
  - **Ce concept repose sur les techniques d'acquittement de message : lorsqu'une source S émet un message M_i vers une destination D, S attend un acquittement A_i de D avant d'émettre le message suivant M_{i+1}.**
  - **Si l'acquittement A_i ne parvient pas à S, S considère au bout d'un certain temps que le message est perdu et reémet M_i :**

TCP : Acquittements

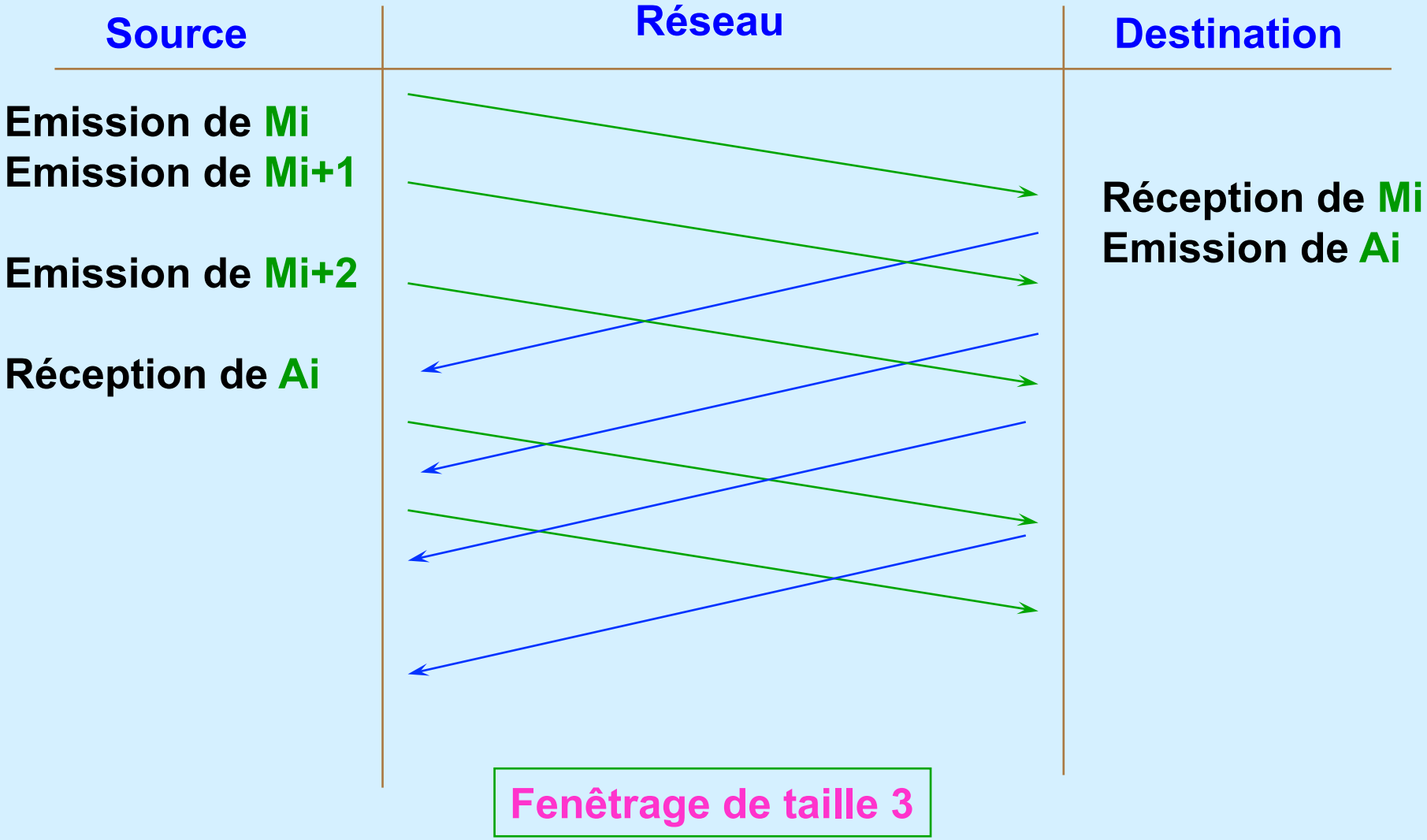


TCP : le fenêtrage

- **La technique acquittement simple pénalise les performances puisqu'il faut attendre un acquittement avant d'émettre un nouveau message. Le fenêtrage améliore le rendement des réseaux.**

- **La technique du fenêtrage : une fenêtre de taille T, permet l'émission d'au plus T messages "*non acquittés*" avant de ne plus pouvoir émettre :**

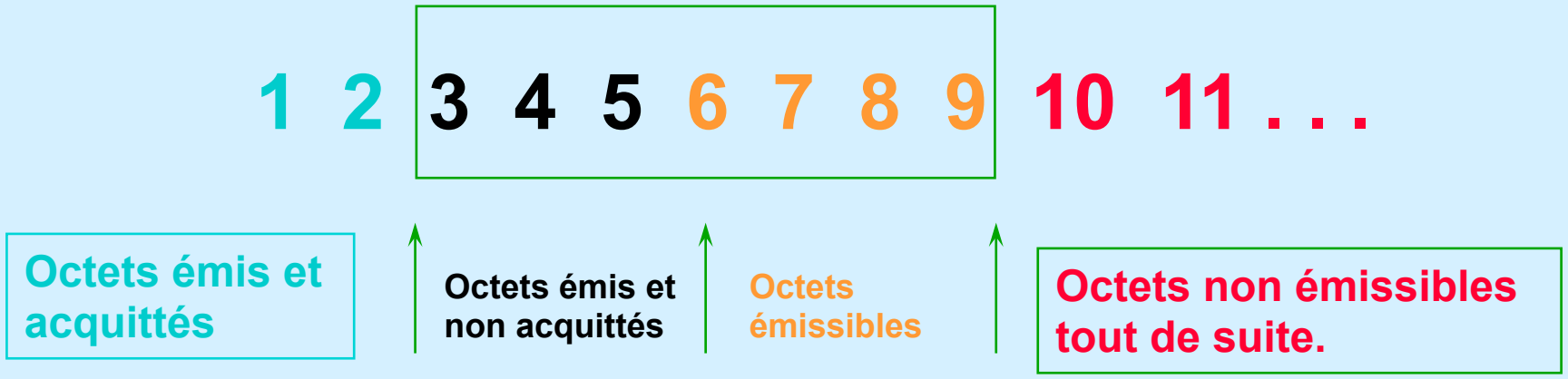
TCP : le Fenêtrage



TCP : Technique de fenêtrage

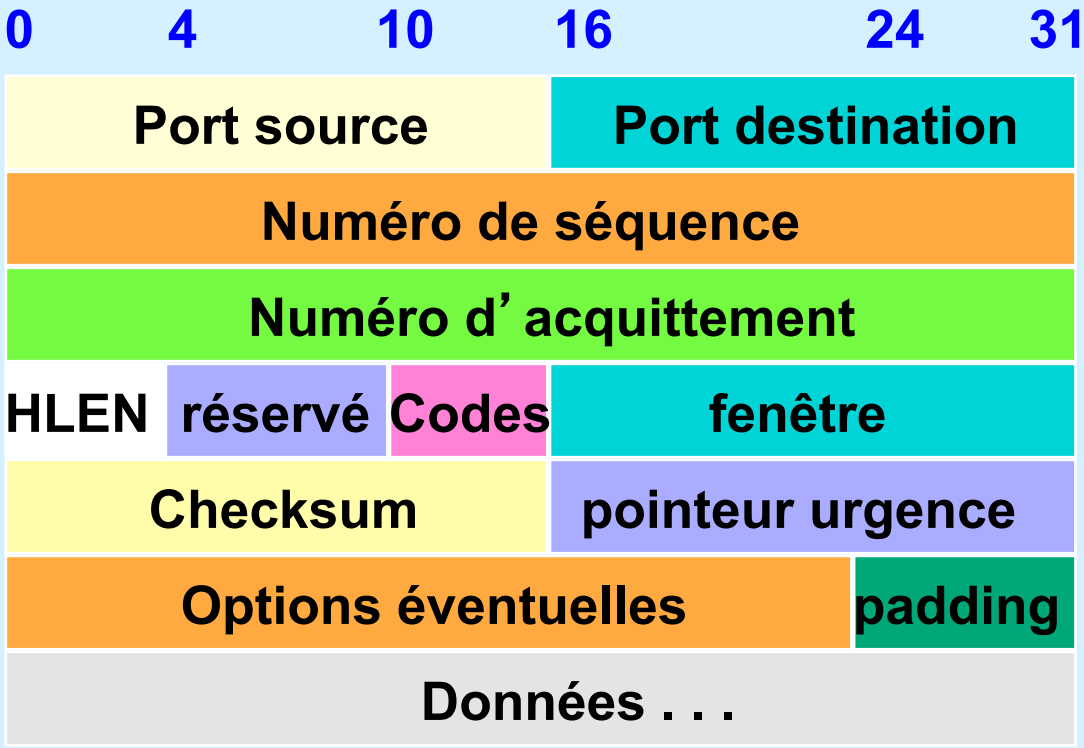
- **fenêtrage glissante permettant d'optimiser la bande passante**
- **permet également au destinataire de faire diminuer le débit de l'émetteur donc de gérer le contrôle de flux.**
- **Le mécanisme de fenêtrage mis en oeuvre dans TCP opère au niveau de l'octet et non pas au niveau du segment; il repose sur :**

  - **la numérotation séquentielle des octets de données,**
  - **la gestion de trois pointeurs par fenêtrage :**



TCP : Segments

- **Segment : unité de transfert du protocole TCP.**
  - **échangés pour établir les connexions,**
  - **transférer les données,**
  - **émettre des acquittements,**
  - **fermer les connexions;**



TCP : Format du segment

- **Code bits : indique la nature du segment :**
  - **URG : Urgent (1 bit)**
    - exemple interruption, Ctrl C dans telnet
  - **SYN : Désire établir une connexion (1 bit)**
  - **FIN : Termine la connexion (1 bit)**
  - **PSH : délivrer immédiatement les données (1 bit)**
    - l'emetteur ne prévoit pas d'envoyer d'autres données dans l'immédiat.
  - **RST** (reset)**: Reprise d'une connexion au départ (réinitialiser la connexion)**
- **Checksum :**
  - Fontion d'ajouter des options
  - Permet de vérifier que le transport s'est effectué sans erreur
  - Si le récepteur s'aperçoit d'une erreur, il fait comme si le segment avait été perdu, il ne l'aquitte pas

TCP : format du segment

Options

- **Permet d'ajouter des options**
- **Permet de négocier la taille maximale des segments échangés.**
- **TCP calcule une taille maximale de segment de manière à ce que le datagramme IP résultant corresponde au MTU du réseau. La recommandation est de 536 octets.**

Pointeur urgence

Indique le dernier octet de données urgentes quand URG=1

TCP : acquittements et retransmissions

Acquittements et retransmissions

- **Le mécanisme d'acquittement de TCP est cumulatif :**
  - Acquitte un nombre d'octets de données (et non obligatoirement un segment entier)
- **Les acquittement peuvent être transportés avec des données**

Les délais de retransmission

- **pour chaque segment envoyé il y a un timer de déclenché, mais la structure de l'Internet impose des timers variables**
- **algorithme adaptatif**
  - adaptation automatique et dynamique, tout au long de la connexion, en fonction des délais d'acquittement des segments précédents

  Ceci permet à TCP de s'adapter sans paramétrage, à tous les débits et à tous les temps de réponse, donc à tous les réseaux.

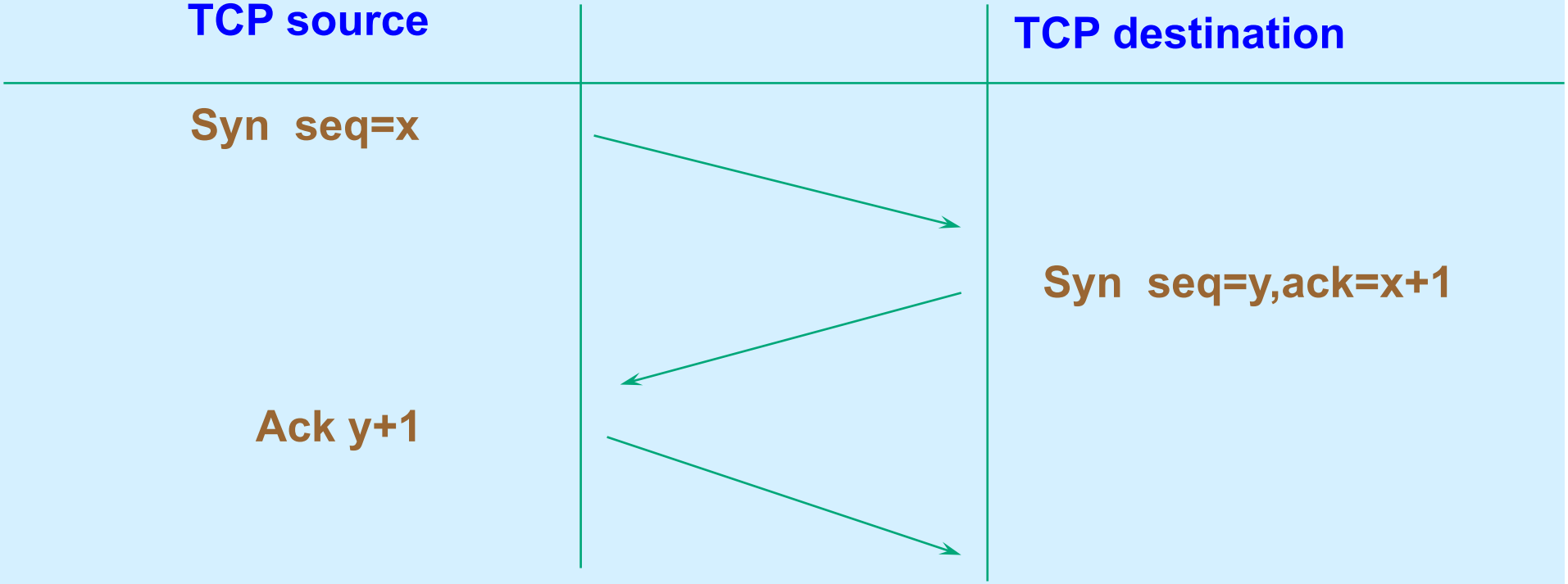
TCP : la congestion

Gestion de la congestion

- **TCP gère le contrôle de flux de bout en bout mais également les problèmes de congestion liés à l'interconnexion.**
- **La congestion correspond à la saturation de noeud(s) dans le réseau provoquant des délais d'acheminement de datagrammes jusqu'a leur pertes éventuelles.**
- **Les extrémités ignorent tout de la congestion sauf les délais. Habituellement, les protocoles retransmettent les segments ce qui aggrave encore le phénomène.**
- **Dans la technologie TCP/IP, les passerelles (niveau IP) utilisent la réduction du débit de la source mais TCP participe également à la gestion de la congestion en diminuant le débit lorsque les délais s'allongent .**

TCP : connexion

Une connexion TCP est établie en trois temps de manière à assurer la synchronisation nécessaire entre les extrémités :



Ce schéma fonctionne lorsque les deux extrémités effectuent une demande d'établissement simultanément. TCP ignore toute demande de connexion, si cette connexion est déjà établie.

TCP : ports standards

No port	Mot-clé	Description
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call

Conclusion TCP/IP aujourd'hui

- **C'est le protocole le plus utilisé actuellement sur tous les types de réseaux (locaux et longues distances)**

- **Quels sera son remplaçant ?**

Conclusion avantage de TCP/IP

- **Gratuit**
- **indépendant des constructeurs**
- **Disponible sur tous les types de matériel**
  - micro, station, super calculateur et équipements de réseaux
- **Facile à installer**
- **Produits éprouvés depuis longtemps dans un monde hétérogène**
- **Inclut de très nombreuses applications**
- **Bien standardisé et documenté**
- **Les protocoles sont simples mais efficaces**

Conclusion inconvénients de TCP/IP

- **Les standards sont édités aux USA**
  - pas une norme internationale
- **La plage d'adresses commence à s'épuiser**
  - surtout classe B
- **Le protocole est très ouvert**
  - on peut créer facilement un réseau que rapidement l'on peut plus gérér
- **La sécurité n'est pas prie en compte dans la conception**
  - De plus le monde non-connecté est un problème difficile pour la sécurité

Sécurité des réseaux informatiques

Vols d'information, attaques virales généralisées, usurpations d'identité, déstabilisation ou encore sabotage à distance… Sur fond d'une concurrence planétaire où tous les coups sont permis, le tissu économique français est la cible de cyberattaques massives. Selon le Club des directeurs de sécurité des entreprises (CDSE), qui tient un colloque sur ce thème jeudi à à l'OCDE, en partenariat avec Europol, les sociétés tricolores sont la cible de plusieurs centaines d'attaques informatiques par jour.

[Le Figaro 06/12/2012]