Protocoles TCP/IP

Mastère "réseaux" - 2000

1- Concepts et modèle d'un internet
2- Adressage IP
3- Protocoles IP
4- Protocoles de transport
5- IPv6

1ère partie: Concepts et modèle d'un internet

- Problème: comment faire communiquer des ordinateurs sur des réseaux hétérogènes ?
- 2 modèles d 'interconnexion:
  - Interconnexion au niveau application:
    - les applications établissent directement les connexions aux réseaux pour communiquer entre elles:
      - supporter "tous" les réseaux possibles (?!)
    - les applications coopèrent entre elles pour acheminer les informations sur les réseaux hétérogènes:
      - passerelle d'application; exemple de la messagerie électronique
  - Interconnexion au niveau réseau:
    - Séparer la communication des données de l'application
    - Offrir un mécanisme de transmissions de paquets indépendant des applications

Interconnexion au niveau réseau

- Deux considérations :
  - Un seul réseau ne peut satisfaire tous les besoins des utilisateurs:
    - LAN rapides mais distances faibles,
    - WAN plus lents,
    - Satellites pour la multi-diffusion,
    - etc...
  - Les utilisateurs souhaitent un moyen d 'interconnexion universel:
    - ne pas être limité aux bornes physiques du réseau
    - ne pas utiliser des applications différentes selon les réseaux utilisés
- Solution d 'un internet:
  - interconnecter les réseaux hétérogènes de manière transparente aux applications en masquant les détails des réseaux
  - Système de communication abstrait

R. CHALON Protocoles TCP/IP 3

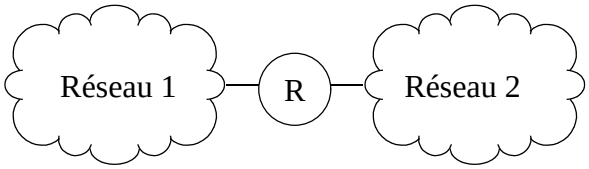
Propriétés d'un internet

- Cacher l'architecture sous-jacente :
  - ➡ les applications ne doivent pas connaître les détails des connexions physiques
- Ne pas imposer de topologie particulière de réseau :
  - ➡ l'ajout d'un nouveau réseau ne doit pas impliquer sa connexion à un ordinateur central ou sa connexion à tous les réseaux existants
- Possibilité d'envoyer des informations à travers des réseaux intermédiaires
  - ➡ notion de réseaux relais
- Tous les ordinateurs doivent partager un ensemble d'identificateurs qui est universel:
  - ➡ notions d'adresses et/ou de noms
- Indépendance de l'interface utilisateur vis-à-vis du réseau :
  - ➡ Les actions pour établir une communication restent indépendantes des réseaux sous-jacents et du type d'ordinateur destinataire

R. CHALON Protocoles TCP/IP 4

Architecture d'un internet

- Interconnexion de 2 réseaux différents:
  - machine spécialisée connectée à chaque réseau
  - passerelle IP [Internet gateway] ou routeur IP [Internet router]
- Le routeur permet d'acheminer les paquets d'informations au travers de l'internet
  - Exemple: R prend sur le réseau 1 les blocs de données destinés aux ordinateurs du réseau 2 et vice-versa

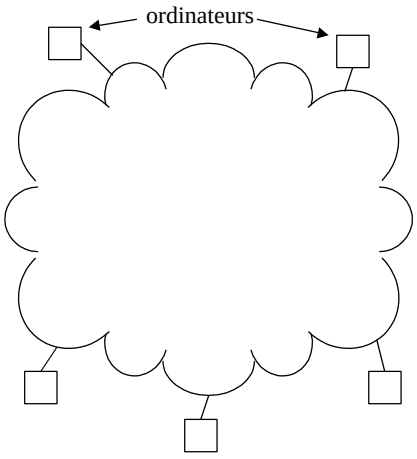


- *Cf. cours sur le routage*

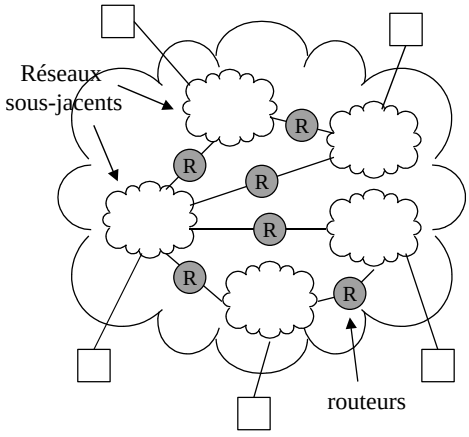
R. CHALON Protocoles TCP/IP 5

Point de vue de l'utilisateur

- Réseau vu par l'utilisateur:
  - chaque ordinateur semble être raccordé à un réseau unique



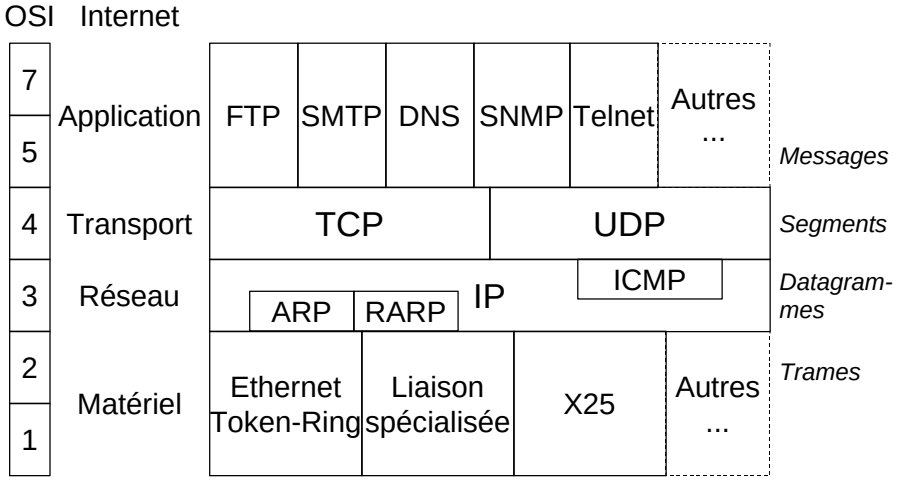
- Réseau réel:
  - les divers réseaux et routeurs qui constituent l'internet



R. CHALON Protocoles TCP/IP 6

Famille de protocoles TCP/IP (1/3)

- La famille TCP/IP se situe aux niveaux 3 et 4 du modèle OSI



Famille de protocoles TCP/IP (2/3)

- Niveau réseau :
  - **IP** [Internet Protocol] : protocole assurant le service de base de remise de paquets non-fiable en mode non-connecté
  - **ARP** [Address Resolution Protocol] : protocole permettant de faire le lien entre une adresse IP et une adresse du réseau sous-jacent
  - **RARP** [Reverse ARP] : protocole permettant à une machine d'obtenir automatiquement une adresse IP au démarrage
  - **ICMP** [Internet Control Message Protocol] : protocole permettant d'échanger des informations d'administration
- Niveau transport:
  - **TCP** [Transmission Control Protocol] : protocole assurant un service de transport fiable en duplex intégral, en mode connecté et de bout en bout
  - **UDP** [User Datagram Protocol] : protocole assurant un service de transport non-fiable en duplex intégral, en mode non-connecté

Famille de protocoles TCP/IP (3/3)

- Niveau application :
  - **FTP** [File Transfer Protocol] : protocole de transfert de fichier entre 2 ordinateurs
  - **SMTP** [Simple Mail Transfer Protocol] : protocole de transfert de message pour le service de messagerie électronique
  - **DNS** [Domain Name Server] : protocole permettant de faire correspondre à un nom de machine son adresse IP
  - **Telnet** : protocole permettant de fournir un service de terminal virtuel pour un accès interactif à des ordinateurs
  - **SNMP** [Simple Network Management Protocol] : protocole pour l'administration de réseaux
  - *Cf. cours sur les Applications sur TCP/IP*

R. CHALON Protocoles TCP/IP 9

Notes sur la normalisation (1/2)

- Normalisation:
  - Un document est écrit par un groupe souhaitant proposer une idée sous la forme d ’un RFC
  - Si cela présente suffisamment d ’intérêt alors il lui est donné l ’état de ***proposed standard*** (PS)
  - Pour devenir DS (***draft standard***) il faut qu’une implémentation ait été testée sur 2 sites différents pendant au moins 4 mois
  - si l ’IAB est convaincu que l ’idée est bonne et si le logiciel fonctionne bien, alors le RFC devient un ***Internet standard*** (IS)
- Les normes ont ensuite des statuts:
  - Exigé [required]: toute machine utilisant IP doit implémenter ce RFC
  - Recommandé [recommanded]
  - Facultatif [elective]
  - Usage limité [limited use]: protocole expérimental (usage déconseillé)
  - Non recommandé [not recommended]: protocole périmé

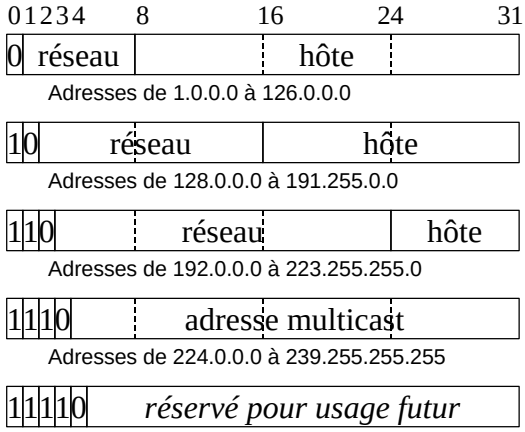
R. CHALON Internet, Intranet et les applications sur TCP/IP 10

Notes sur la normalisation (2/2)

- Les RFC contiennent donc:
  - les normes réseau (exemple: IP: RFC 791)
  - les normes des applications (exemple: FTP: RFC 959)
  - des informations générales
  - ➡ numérotées par ordre croissant. Lorsqu'il y a une nouvelle version d 'un standard elle porte un nouveau numéro mais elle garde le même titre (différent de l 'OSI)
- Il existe aussi les **FYI** [For Your Information] qui sont une sélection de RFC d 'intérêt général
- Les RFC sont disponibles gratuitement sur l 'Internet (contrairement à l 'OSI où les normes sont payantes et chères!):
  - ➡ http://www.pasteur.fr/other/computer/RFC/
- Aujourd'hui plus de 2700 RFC ! (RFC 2795, 1er avril 2000)
- le document STD1 contient la liste des standards et est régulièrement ré-édité (actuellement RFC 2600, mars 2000)

2ème partie: Adressage IP

- Adresses de 4 octets (32 bits) notées : **`www.xxx.yyy.zzz`**
  - 2 parties : numéro de réseau numéro d'hôte



128 réseaux de 16 millions d'hôtes

16384 réseaux de 64536 hôtes

Plus de 2 millions de réseaux de 256 hôtes

Plus de 250 millions de groupes de diffusion

Adresses particulières

- Adresse d'un réseau

N° réseau	Tout à 0

  - exemple: 156.18.0.0 (réseau de l'Ecole Centrale)
- Adresse de diffusion dirigée

N° réseau	Tout à 1

  - permet de s'adresser à tous les hôtes d'un réseau
  - exemple: 156.18.255.255 (tous les hôtes de l'ECL)
- Adresse de diffusion "locale"

Tout à 1

  - ne sort pas du réseau
- "Cet" ordinateur:

Tout à 0

  - utilisable au boot seulement (pour RARP)
- Ordinateur sur "ce" réseau

Tout à zéro	N° hôte

  - utilisable au boot seulement (pour RARP)
- Rebouclage

127	Nb quelconque (souvent 1)

  - ne doit jamais apparaître sur un réseau

Attribution des adresses (1/2)

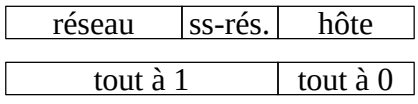
- ICANN [Internet Corporation for Assigned Names and Numbers] est le nouvel organisme chargé :
  - de l'allocation des adresses IP
  - de la gestion des noms de domaine
  - de l'homologation des protocoles et de leurs paramètres
  - de la gestion des serveurs racines
  - Organisme international indépendant et qui se veut géré par la communauté Internet
  - ➡ plus d'info sur: **`www.icann.org`**
- Provisoirement, les adresses sont toujours gérées par l'IANA [Internet Assigned Number Authority] : **`www.iana.org`**
  - organisme dépendant du gouvernement américain
  - Règle d'attribution fixée par le RFC 2050

Attribution des adresses (2/2)

- L'attribution est délèguée à un RIR [Regional Internet Registry] :
  - ARIN [American Registry for Internet Numbers] : **`www.arin.net`**
  - RIPE [Réseaux IP européens] : **`www.ripe.net`**
  - APNIC [Asia Pacific Network Information Center] : **`www.apnic.net`**
- Les fournisseurs d'accès ont eux-mêmes délégation pour attribuer les groupes d'adresses de leurs clients
- Attribution des adresses des machines dans le réseau :
  - par l'administrateur du réseau
- Aujourd'hui, il y a tendance à la pénurie :
  - toutes les classes A sont allouées ou réservées
  - les classes B sont presque toutes épuisées
  - plus de la moitié des classes C sont attribuées
- Solutions transitoires en attendant IP v6

Sous-réseaux IP

- Découpage d'un réseau en entités plus petites :
  - création de sous -réseaux par l'administrateur du site
  - les sous-réseaux ne sont pas visibles à l'extérieur du site
- Les équipements (hôtes et routeurs) doivent savoir les gérer
  - les routeurs sont chargés de l'interconnexion
- Utilisation d'un "masque":



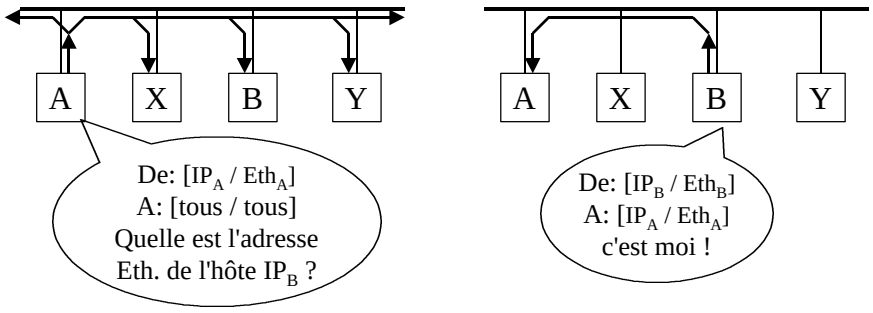
  - Exemple : Ecole Centrale:
    156.18.0.0 (classe B) découpé en 255 sous-réseaux de 255 hôtes
    - 156.18.22.0, masque=255.255.255.0 : sous-réseau du SRI
    - 156.18.36.0, masque=255.255.255.0 : sous-réseau de ICTT
  - On note aussi le nb de bits à 1:
    - 156.18.22.0/24 : masque avec 24 bits à 1 = 255.255.255.0

Faiblesses de l'adressage Internet

- Les adresses ne font pas références à des ordinateurs mais à des points d'accès au réseau:
  - un ordinateur connecté à plusieurs réseaux possède plusieurs adresses
  - un ordinateur doit changer d'adresse s'il change de réseau
  - solution: utiliser DHCP [Dynamic Host Configuration Protocol]
- Les classes sont mal découpées:
  - les classes C sont trop petites, les classes B trop grandes
  - Solution : faire l'agrégation de classes C consécutives et utiliser CIDR [Classless Inter-Domain Routing]
- Pénurie d'adresses:
  - Solution: utiliser des adresses privées en interne et les ré-écrire avec NAT [Network Address Translation]
- Solutions à ces faiblesses : IPv6 !!!

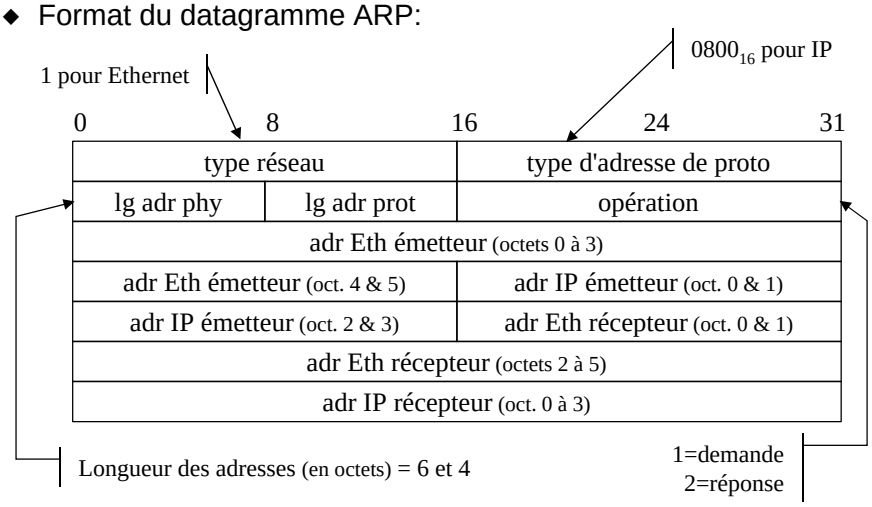
Correspondance adresse IP - adresse réseau

- Les adresses IP sont indépendantes des adresses des réseaux sous-jacents :
  - mise en relation directe :
    - table statique de correspondance (avec X25: IP⇔X121, RFC 877)
    - la partie "hôte" est l'adresse dans le réseau sous-jacent
  - mise en relation dynamique : protocole ARP (RFC 826)
- Principe de ARP sur réseau Ethernet :



Protocole ARP sur Ethernet

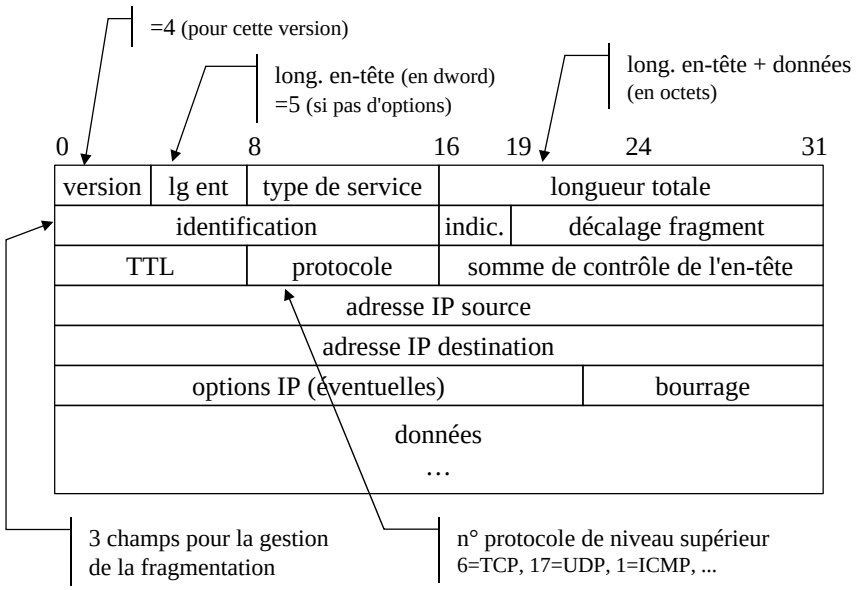
- Utilise des trames Ethernet II, "type"=0806_{16}
- Format du datagramme ARP:



3ème partie: Protocole IP

- IP assure les fonctionnalités de la couche 3 de l'OSI:
  - Il permet le transfert de paquets (appelés datagrammes) entre deux ordinateurs (éventuellement en traversant plusieurs réseaux)
- Caractéristiques :
  - mode **non-connecté**
  - transfert **non fiable** des données (la fiabilité des réseaux traversés) IP fait au mieux (*best effort protocol*)
  - taille maximale d'un datagramme= 64 Ko; il peuvent être fragmentés en fonction de la nature des réseaux traversés
- Services assurés :
  - adressage : tout équipement (ordinateur et routeur) dispose d'une ou plusieurs adresses
  - routage : acheminement des paquets entre deux réseaux sous-jacents
- Version actuelle: version 4 (appelée IPv4) - RFC 791 (STD 5)

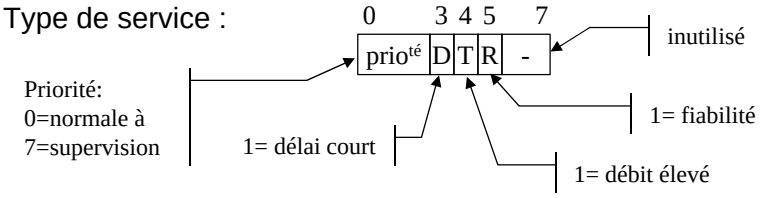
Datagramme IP (1/3)



R. CHALON Protocoles TCP/IP 21

Datagramme IP (2/3)

- Type de service :

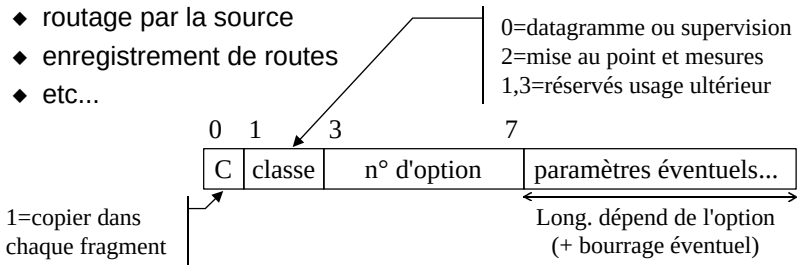


  - la priorité permet, en cas de congestion, que les informations de contrôle du réseau puissent circuler (sans être victimes elles-mêmes de la congestion !)
  - D, T et R permettent aux routeurs de choisir le chemin qui correspond à ces critères (s'ils ont le choix !)
- Somme de contrôle:
  - complément à un de la somme de tous les mots de l'en-tête
  - ne vérifie que l'en-tête pas les données ! C'est aux couches supérieures de vérifier l'intégrité des données

R. CHALON Protocoles TCP/IP 22

Datagramme IP (3/3)

- TTL [Time to Live] = durée de vie
  - exprime en secondes, la durée maximale de transit d'un paquet
  - chaque routeur doit décrémenter la valeur (en pratique, le TTL compte donc le nb de routeurs traversés)
  - le datagramme est détruit quand TTL=0
    - ➡ évite au datagramme de circuler indéfiniment en cas de boucle
- Options:
  - routage par la source
  - enregistrement de routes
  - etc...

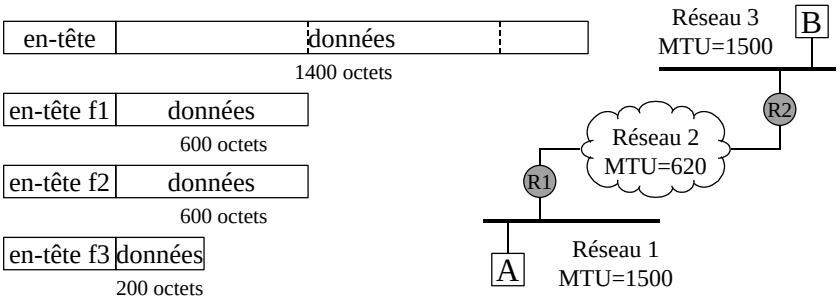


R. CHALON Protocoles TCP/IP 23

Fragmentation des datagrammes IP (1/2)

- **Problème**: un datagramme IP peut être plus grand que la taille maximale de trame admise par le réseau sous-jacent
  - Ethernet = 1500 octets
  - FDDI = 4470 octets

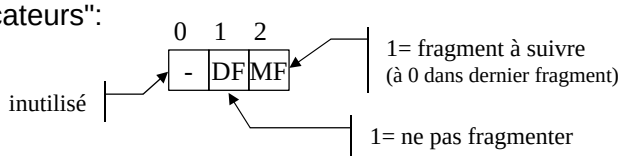
  } MTU [Maximum Transfer Unit] (exprimé en données utiles !)
- **Solution**: un routeur peut fragmenter un datagramme pour qu'il respecte le MTU du réseau sous-jacent



R. CHALON Protocoles TCP/IP 24

Fragmentation des datagrammes IP (2/2)

- Le champ "identification" contient un n° unique de datagramme
- Le champ "décalage fragment" contient la localisation du fragment par rapport au début du bloc initial de données
  - exprimé sous la forme d'un multiple de 8 octets
  - donc les fragments doivent être des multiples de huit !
- Champ "indicateurs":



- Ré-assemblage du datagramme initial :
  - utilisation du champs "identification"
  - les fragments sont ré-assemblés par l'ordinateur destinataire et non par les routeurs

Fonctions non assurées par IP

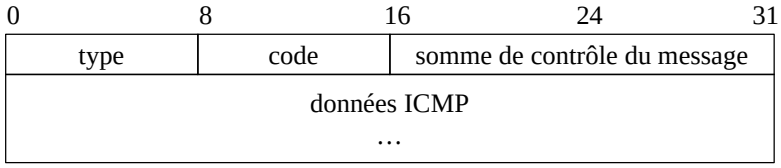
- IP n'assure pas :
  - le multiplexage:
    - plusieurs flux de donnés simultanés
  - la vérification du séquencement :
    - les paquets peuvent arriver en désordre, voire dupliqués
  - la détection de perte:
    - doit être assurée par les couches supérieures
  - la retransmission en cas d'erreur:
    - doit être assurée par les couches supérieures
  - le contrôle de flux:
    - assuré en partie par ICMP

Protocole ICMP (RFC 792)

- ICMP [Internet Control Message Protocol] gère les messages d'erreurs et de contrôle entre les différents systèmes
- Caractéristiques:
  - utilise IP (champ protocole=1)
  - permet de palier au manque de services d'IP
  - Protocole obligatoire sur tous les équipements IP !
  - il ne demande pas de réponse: un message ICMP ne doit pas engendrer un autre message ICMP
- Message renvoyé à l'expéditeur par l'équipement destinataire ou le routeur intermédiaire :
  - Quand il s'aperçoit d'un problème dans le datagramme:
    - par exemple: TTL expiré
  - Pour avertir l'émetteur afin qu'il modifie son comportement
    - par exemple: demande de ralentir l'émission

Message ICMP

- Format du message:



- Chaque type de message a un format particulier:
  - 22 types définis
- Les messages ICMP qui rendent compte d'erreurs renvoient toujours les 64 premiers bits du datagramme IP fautif:
  - permet de localiser facilement les problèmes provenant de protocoles de plus haut niveau

Exemples de messages ICMP

- Messages d'echo (Cf. commande ping):
  - permet de tester la connectivité entre 2 machines
  - demandes (type=8, code=0), réponses (type=0, code=0)
- Compte-rendu de pb de paramètres (type=12, code=0 ou 1):
  - permet de renvoyer des erreurs sur l'en-tête IP ou les options
- Destination inaccessible (type=3):
  - code=0: réseau inaccessible
  - code=1: ordinateur inaccessible
  - code=3: port TCP ou UDP inaccessible
  - etc… (13 codes en tout)
- Contrôle de flux:
  - Demande de ralentissement de l'émission [source quench] (4,0)
- Durée de vie dépassée (type=11, code=0)
- Demande de modifications de routes (type=5, code=0 à3)

4ème partie: Protocoles de transport

- Deux protocoles pour la communication entre applications:
  - TCP [Transmission Control Protocol]:
  - UDP [User Datagram Protocol]:
- Ils sont placés fonctionnellement au niveau 4 de l'OSI
- Comparaison:

	TCP	*UDP*
Orienté connexion	oui	non
Circuit virtuel	oui	non
Fiabilité (contrôle d'erreur)	oui	non
Contrôle de flux	oui	non
multiplexage	oui	oui
Taille des messages	illimitée	64 Ko

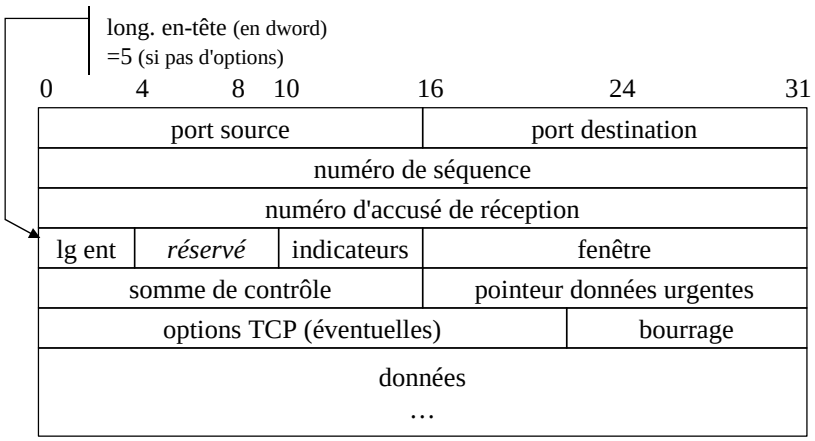
Protocole TCP

- TCP [Transmission Control Protocol] fournit un service de transport fiable de bout en bout entre 2 applications
- Caractéristiques:
  - **mode connecté**
  - établissement d'un **circuit virtuel bidirectionnel**
  - transport fiable: correction d'erreur, re-séquencement, …
  - transferts tamponnés: grouper les petits messages
  - connexions non structurées : transport de flots d'octets
  - contrôle de flux
  - multiplexage : plusieurs connexions simultanées
  - possibilité de données prioritaires (données urgentes + "push")
- Taille des messages non-limitée:
  - ➡ les messages sont décomposés en segments de 64 Ko max pour être passés à la couche IP
- Défini par la RFC 793 (STD 7)

R. CHALON Protocoles TCP/IP 31

Segment TCP (1/3)

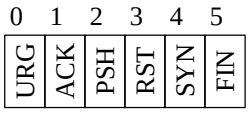
- Format du segment:



R. CHALON Protocoles TCP/IP 32

Segment TCP (2/3)

- Champ indicateurs:

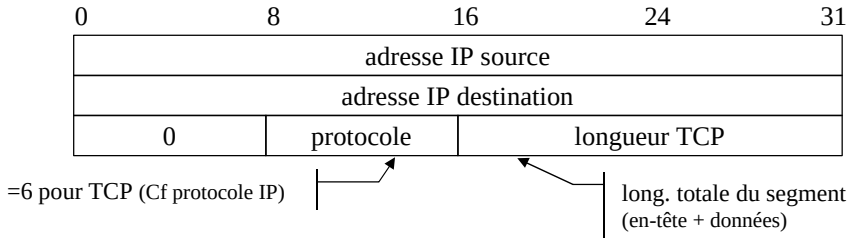


  - URG=1 : données urgente
  - ACK=1 : le champs accusé de réception est valide
  - PSH=1 : "push" requit = envoyer immédiatement les données
  - RST=1 : ré-initialiser la connexion
  - SYN=1 : synchroniser les n° de séquence
  - FIN=1 : l'émetteur a atteint la fin de son flot de données
- En pratique:
  - SYN=1, ACK=0 : demande de connexion
  - SYN=1, ACK=1 : connexion acceptée

R. CHALON Protocoles TCP/IP 33

Segment TCP (3/3)

- Calcul de la somme de contrôle:
  - Avant le calcul un pseudo-en-tête est ajouté:

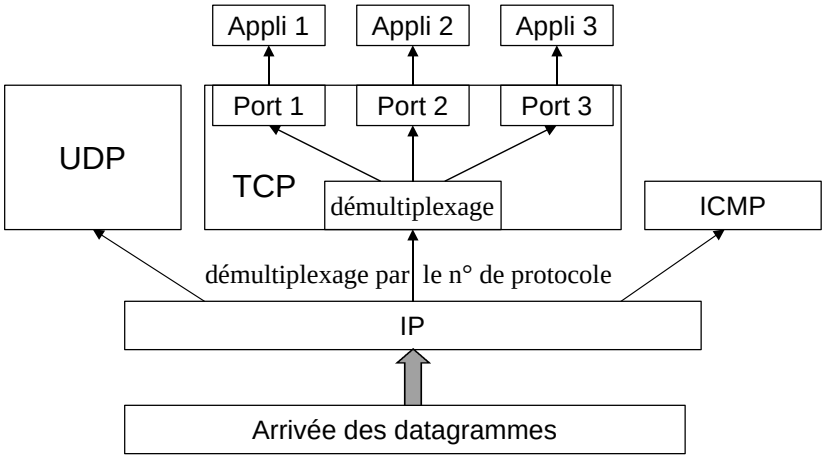


  - + un octet à 0 est évent[ent] ajouté pour obtenir un multiple de 16 bits
  - La somme de contrôle est calculée sur l'ensemble des mots (arithmétique en complément à 1) puis son complément à 1 est rangé dans le champ "somme de contrôle"
  - le pseudo-en-tête et l'octet de bourrage ne sont pas transmis !

R. CHALON Protocoles TCP/IP 34

Ports (1/2)

- Ils permettent le multiplexage des communications :



R. CHALON Protocoles TCP/IP 35

Ports (2/2)

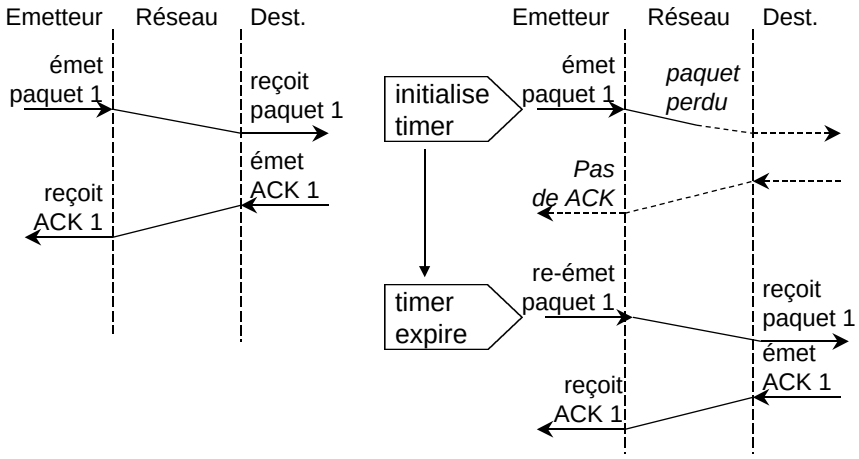
- 2 champs par segment: "port source" et "port destination"
- Toute connexion TCP est identifiée par un quadruplet: <adr IP source, n° port source, adr IP dest., n° port dest>
  - ➡ possibilité d'utiliser plusieurs fois le même port !
- Utilisation en client-server:
  - Il existe des n° réservés pour les applications "classiques":
    - ➡ Donnés par la RFC 1700 (STD 2) "Assigned numbers"
  - Les serveurs "écoutent" ce port pour attendre de nouvelles connexions
  - Les clients doivent donc utiliser des n° de ports >1000 pour éviter toute confusion

N° port	*Protocole*
20	FTP - données
21	FTP - contrôle
23	Telnet
25	SMTP
53	DNS
80	HTTP
	etc...

R. CHALON Protocoles TCP/IP 36

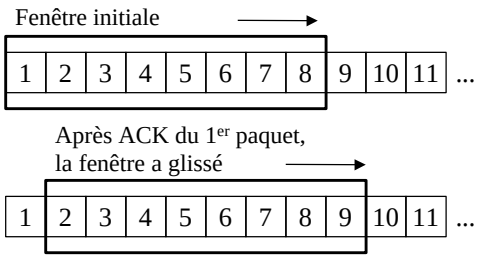
Fiabilité du service de transport (1/3)

- La fiabilité est assurée par des accusés de réception avec retransmission en cas d'erreur:



Fiabilité du service de transport (2/3)

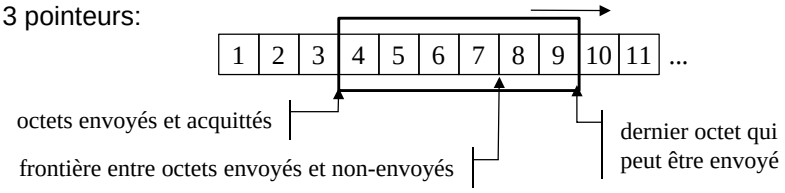
- Problème d'efficacité de l'acquittement paquet par paquet:
  - il faut attendre l'accusé de réception du paquet précédent pour pouvoir transmettre le suivant ==> perte de temps
- Solution: fenêtre glissante [Sliding window]
  - émettre plusieurs paquets d'avance avant d'avoir à attendre un accusé de réception
  - *exemple*: fenêtre de huit paquets



NOTE:
Il faut gérer un tampon à chaque extrémité de la connexion !

Fiabilité du service de transport (3/3)

- TCP utilise une fenêtre glissante au niveau de l'octet:
  - les octets sont numérotés séquentiellement
  - 3 pointeurs:



- Champs utilisés dans l'en-tête:
  - N° de séquence:
    - donne le numéro du 1er octet transmis dans le segment
  - N° d'accusé de réception:
    - donne le numéro du prochain octet attendu, donc tous les octets précédents sont acquittés (attention c'est le flot inverse de ci-dessus !)
- TCP est bidirectionnel ==> 2 fenêtres dans **chaque** sens

Contrôle de flux (1/3)

- La taille de la fenêtre peut être modifiée:
  - le destinataire peut envoyer une nouvelle taille de fenêtre avec l'ACK du paquet précédent
  - diminuer la taille de la fenêtre en cas de surcharge
- Champ utilisé dans l'en-tête:
  - "Fenêtre":
    - donne la taille maximale de la fenêtre en octet que la machine peut accepter
- Un mécanisme de contrôle de flux est indispensable:
  - hétérogénéité des machines:
    - TCP résoud ce problème
  - réseaux et routeurs de différentes capacités:
    - TCP se repose sur ICMP (source quench)

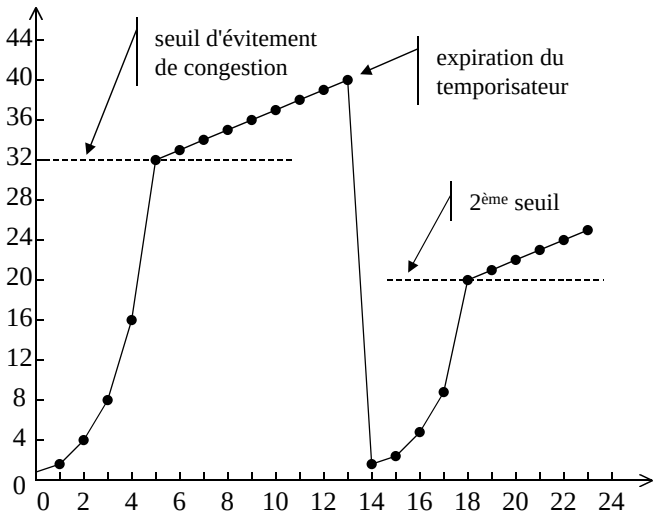
Contrôle de flux (2/3)

- TCP utilise un algorithme adaptatif:
  - prendre en compte le temps de transmission aller/retour
    RTT [Round Trip Time] = temps de boucle moyen
  - prendre en compte le taux de perte
  - but: éviter la congestion
- Principe de l'algorithme:
  - démarrage lent:
    - commencer par fenêtre = 1 segment
    - si ACK OK alors doubler la taille de la fenêtre
    - lorsque taille dépasse le seuil d'évitement de congestion (32 Ko au démarrage) alors augmenter la fenêtre de 1 segment à chaque fois
  - diminution dichotomique:
    - si paquet perdu alors seuil d'évitement de congestion = taille fenêtre /2
    - recommencer le démarrage lent

R. CHALON Protocoles TCP/IP 41

Contrôle de flux (3/3)

- Exemple:



Remarque:

si paquet ICMP "source quench" même effet que perte de paquet

R. CHALON Protocoles TCP/IP 42

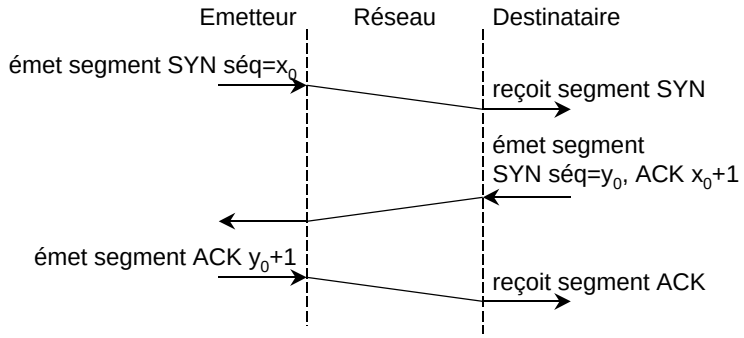
Options et données urgentes

- Négociation du plus grand segment:
  - Utilisation du champ "options" pour négocier le MSS [Maximum Segment Size] = taille maximale de segment
  - Idée: choisir la plus grande valeur mais éviter la fragmentation
  - En général:
    - si sur le même réseau, prendre le MTU du réseau diminué de 40 (exemple sur Ethernet = 1460)
    - sinon on conseille 536 (576-40)
- Données urgentes:
  - Permettre d'envoyer des données prioritaires sur le flot normal ==> utiles pour "interrompre" un programme qui fonctionne mal
  - Champs utilisés:
    - indicateur URG=1
    - "pointeur données urgentes": indique le dernier octet de données urgentes (avant les données normales)

R. CHALON Protocoles TCP/IP 43

Etablissement d'une connexion TCP

- Connexion en 3 temps:

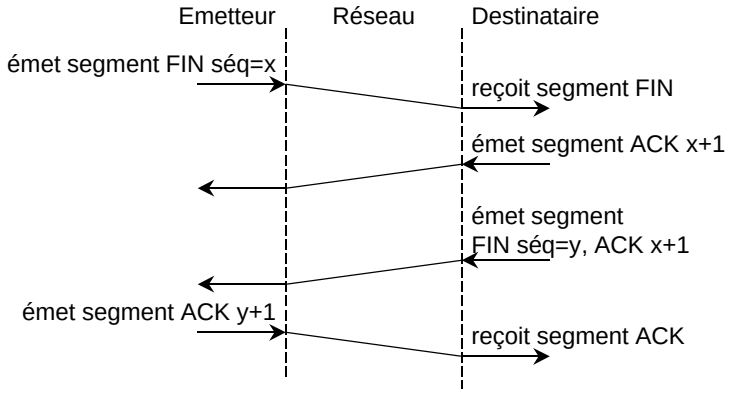


- Toute demande de connexion supplémentaire qui arrive après que la connexion est établie doit être ignorée:
  - permet de résoudre les problèmes posés par la non-fiabilité de IP
  - résout aussi les cas de connexions simultanées

R. CHALON Protocoles TCP/IP 44

Libération d'une connexion TCP

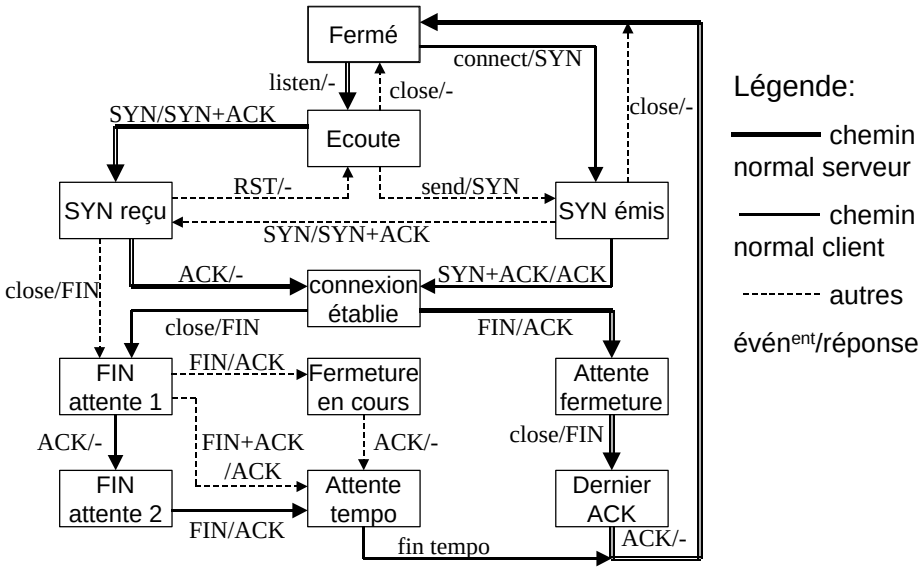
- Libération en 3 temps modifiés:



- Les 2 flux étant indépendants, la libération doit fermer chaque sens

R. CHALON Protocoles TCP/IP 45

Automate à nombre d'états finis



R. CHALON Protocoles TCP/IP 46

Comparaison TCP/TP4

- Comparaison de différents points:

Spécifications	*TP4 OSI*	*TCP*
Différents types de PDU	9	1
Qualité de service (QoS)	négociable	optionnel
Données dans une CR	autorisé	possible ?
Nature du flux	messages	octets
Données spéciales	Données exprès	Données urgentes
Données en retour	non	oui
Régulation de flux explicite	toujours	oui
Relation d'ordre sur les ACK	autorisé	interdit
Libération	brutale (laissé à couche session)	négociée
Taille maximale d'un segment	8 Ko	64 Ko

R. CHALON Protocoles TCP/IP 47

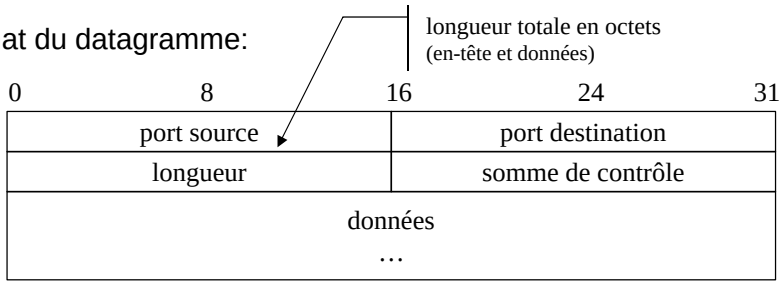
Protocole UDP

- UDP [User Datagram Protocol] fournit un service de transport de datagrammes, basiquement le même que IP
- Caractéristiques :
  - mode **non-connecté**
  - transfert **non fiable** des données (la fiabilité des réseaux traversés)
  - taille maximale d'un datagramme= 64 Ko
- Il ajoute seulement à IP le multiplexage grâce à l'utilisation des ports (Cf. TCP):
  - ➡ le port source est facultatif (=0 si non utilisé): il identifie un port pour la réponse
- Il est défini par la RFC 768 (STD 6)

R. CHALON Protocoles TCP/IP 48

datagramme UDP

- Format du datagramme:



- Somme de contrôle:
  - facultative (=0 si non utilisé)
  - calculée avec un pseudo-en-tête qui contient les adresses IP source et destination (Cf. TCP)
- Quelques exemples d'applications utilisant UDP:
  - NFS: partage de fichiers
  - DNS: service de nommage
  - RTP [Real-Time Protocol]: applications temps-réel

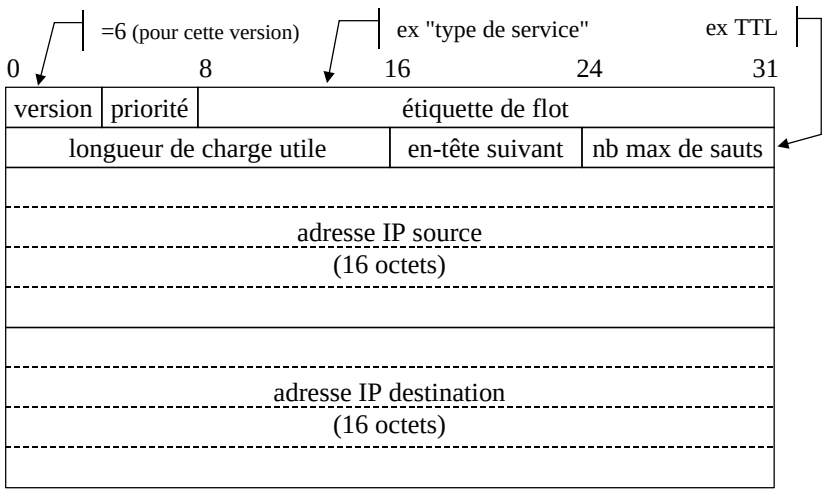
5ème partie: IPv6

- Objectifs de ce nouveau protocole:
  - résoudre le problème de l'épuisement des adresses IPv4 (prévu vers 2008 à +/- 3 ans)
  - réduire la taille des tables de routage grâce à l'organisation hiérarchique des adresses
  - simplifier le protocole ==> rapidité de traitement
  - fournir une meilleure sécurité: authentification et chiffrement
  - gérer la qualité de service en particulier pour le temps réel
  - gérer la diffusion multicast en standard
  - gérer la mobilité des ordinateurs
  - permettre l'évolution future du protocole
- Mais il faut assurer la coexistence des 2 versions pendant la période transitoire (au minimum 10 ans, peut-être toujours !)

Adresses IPv6

- Adresses de 128 bits (16 octets):
  - 340.10^{36} équipements adressables (soit 10^{23} adresses par m² !)
  - seul 1/4 des adresses est alloué
- Adressage hiérarchique: mais plan d'adressage contreversé
- Notation:
  - 8 groupes de 4 chiffres hexadécimaux séparés par ":"
  - exemple: 8000:0000:0000:0000:0123:4567:89AB:CDEF
    qui peut s'abréger en: 8000::123:4567:89AB:CDEF
  - compatibilité avec adresses IPv4 en mettant le début à zéro
    exemple: 156.18.22.3 devient ::156.18.22.3
- 3 catégories:
  - Unicast
  - Multicast (remarque: le broadcast est supprimé, utilise le multicast)
  - Anycast (adressage au premier vu)

En-tête IPv6 (1/3)



En-tête IPv6 (2/3)

- Priorité:
  - permet de classer la nature des flux
  - utile aux routeurs en cas de congestion
  - il est suggéré: 1 pour *news*, 4 pour *ftp*, 6 pour *telnet*
- Étiquette de flot:
  - permet de définir des pseudo-circuits virtuels
- En-tête suivant:
  - donne:
    - soit le type d'en-tête d'option qui suit,
    - soit le type de protocole de niveau supérieur (TCP, UDP, …)
- champ "somme de contrôle" n'existe plus:
  - calcul trop "coûteux"
  - les réseaux sont de plus en plus fiables
  - possibilité de la calculer au niveau 2 (liaison de données)

R. CHALON Protocoles TCP/IP 53

En-tête IPv6 (3/3)

- Plus de champs pour la fragmentation:
  - datagrammes de 576 octets doivent être supportés
  - si paquet trop grand:
    - le routeur renvoie un code d'erreur ICMP
    - et possibilité d'utiliser l'option de fragmentation à la source
- 6 types d'en-tête d'options:
  - pas-à-pas: option traitée par chaque routeur,
    permet d'avoir des datagrammes > 64 Ko (jumbogrammes)
  - routage: strict ou lâche (seuls quelques routeurs sont précisés)
  - fragmentation: similaire à IPv4 mais seul l'ordinateur source fragmente
  - authentification: signature des datagrammes (par défaut MD5)
  - charge utile chiffrée: permet la confidentialité, seul le destinataire peut lire les données (par défaut utilise chiffrement DES)
  - option de destination: non utilisée

R. CHALON Protocoles TCP/IP 54

Annexe: Bibliographie

- Livres:
  - D. Comer, "TCP/IP Architecture, protocoles, applications", InterEditions, Masson, 3ème édition, 1998.
  - A. Tanenbaum, "Réseaux", InterEditions/Prentice Hall, 3ème édition, 1997.
- Sites Internet:
  - Cours de l'UREC: www.urec.cnrs.fr/cours/
  - RFC: www.pasteur.fr/other/computer/RFC/