

TCP/IP

Fabien Chhel

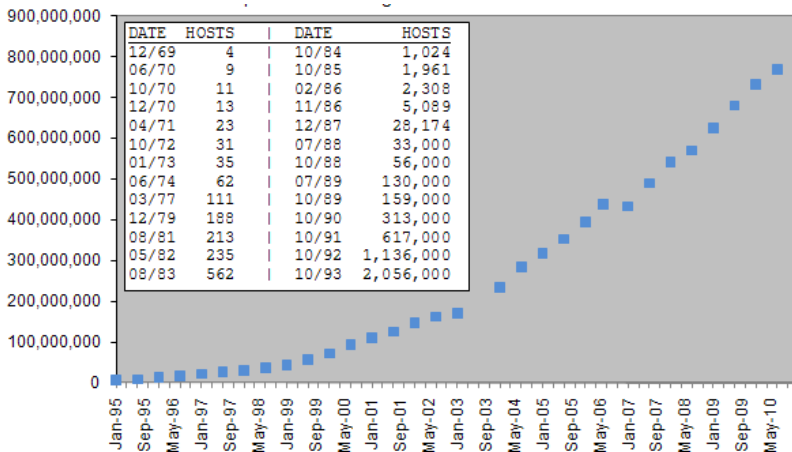
UFR Sciences Angers

2013-2014

Historique d'Internet

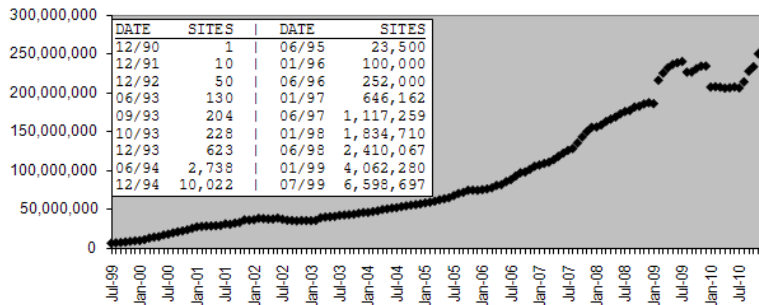
- *internet* : connexion de réseaux différents (*internetworking*)
- *Internet* : l'ensemble des *internets* suivant les protocoles TCP/IP
- Premiers développements sur l'intenet (année 70)
- de la DARPA (*Defense Advanced Research Project Agency*) naît :
 - ARPANET
 - Réseaux reliant (point-à-point) des sites de recherche pour
 - échanger des données et du courrier
 - partager des ressources
 - résistant aux attaques militaires
 - sans centre névralgique
 - sans connection
 - « au mieux »
- <http://www.internetworldstats.com/>

Nombre de machines connectées à Internet

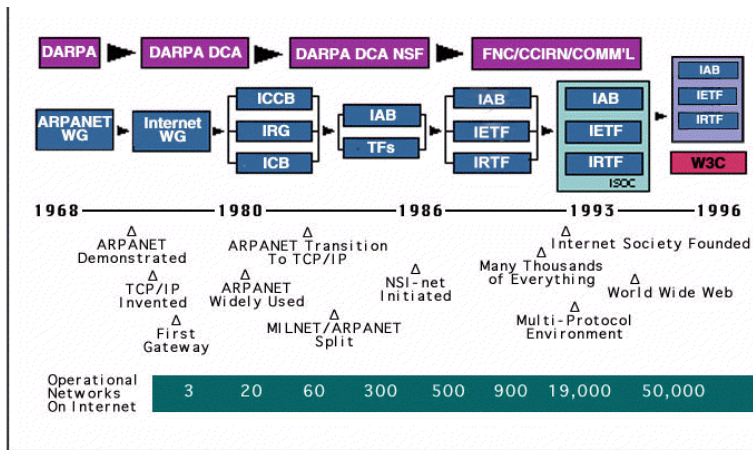


source <http://www.zrakon.org/robert/internet>

Nombre de sites web



source <http://www.zrakon.org/robert/internet>



source <http://www.zrakon.org/robert/internet>

Alors vint TCP/IP

- Premiers développements de réseaux à *commutation de paquets* (années 70)
- de la DARPA (*Defense Advanced Research Project Agency*)
 - autour des réseaux radio et de la communication satellite
 - autour des protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*)
- création de l'IRG (*Internet Research Group*) groupe de travail autour de TCP/IP
- TCP/IP est intégré dans le système UNIX de Berkeley
- création de l'ICCB (*Internet Configuration Control Board*) en 1979
- TCP/IP devient le standard dans ARPANET (Janvier 1983)
- la DCA (*Defense Communication Agency*) scinde ARPANET en deux
 - ARPANET pour la recherche (l'Internet actuel)
 - MILNET (*Military network*)

Dompté la croissance

- création de l'IAB (*Internet Architecture Board*) qui coordonne et standardise les protocoles autour de TCP/IP.
- l'IAB est scindée en 4 entités :
 - IAB
 - IETF (*Internet Engineering Task Force*)
 - IESG (*Internet Engineering Steering Group*) l'état major de l'IETF
 - IRTF (*Internet Research Task Force*) regroupant les recherches sur le futur de l'Internet
- création de l'ISOC (*Internet Society*) en 1991 regroupant
 - l'IAB, l'IETF, l'IESG, l'IRTF
 - l'ICANN (*Internet Corporation for Assigned Names and Numbers*) qui gère l'adressage et les noms de domaine
 - le W3C (*World Wide Web Consortium*)

The goal of the IETF is to make Internet work better

- l'IETF :
 - groupes de travail créés pour traiter des sujets spécifiques
 - définition des solutions techniques
- Les RFC (*Request For Comments*)
 - documents techniques définissant les standards de l'Internet
 - créé à partir d'*Internet Draft*, documents de travail des groupes d'IETF
 - publiés

Les services Internet

- Niveau application
 - *World Wide Web* (WWW)
 - Courrier électronique
 - Transferts de fichiers
 - Connexion et bureau à distance
- Niveau réseau
 - Service de transport de flux fiable
 - Indépendance vis-à-vis de la technologie de réseau
 - Interconnexion universelle
 - Accusés de réception de bout en bout
 - Standards de protocole d'application
 - Service de transmission de paquets sans connexion

Besoins des applications

	Perte de données	Débit (Contrainte de temps)
Transfert de données informatiques	Interdite	Au mieux (non)
Courrier	Interdite	Au mieux (non)
Web	Interdite	Au mieux (non)
Audio/Vidéo enregistrés	Acceptable	Au mieux (non)
Audio/Vidéo temps réel	Acceptable	$10Kbit/s < audio < 1Mbit/s$ $100Kbit/s < video < 5Mbit/s$
Messagerie instantanée	Interdite	Au mieux (faible)
Peer 2 Peer	Interdite	Au mieux (non)

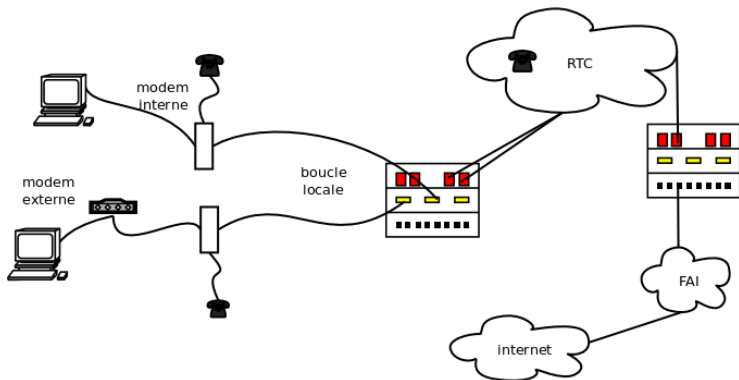
Connexion à Internet

- se connecter à Internet nécessite
 - un moyen physique : un raccordement (ligne téléphonique, câble, liaison satellite)
 - un moyen logique :
 - une adresse IP fournie par un Fournisseur d'accès internet (FAI)
 - un Système de noms de domaine (DNS)
- offre un débit
 - descendant (ou *download*) nombre de bits/sec de données téléchargeables sur l'internet
 - montant (ou *upload*) nombre de bits/sec de données expédiables sur l'internet

Réseau Téléphonique Commuté (RTC)

- modem V90 ou V92 rattaché à une ligne téléphonique
- débit descendant maximum : 56 kbit/sec
- débit montant maximum : 48 kbit/sec
- « Internet à bas débit »
- ligne téléphonique inutilisable pendant la connexion à internet
- intérêt : il suffit d'une ligne téléphonique

Réseau Téléphonique Commuté (RTC)



source Pr. Pascal Nicolas

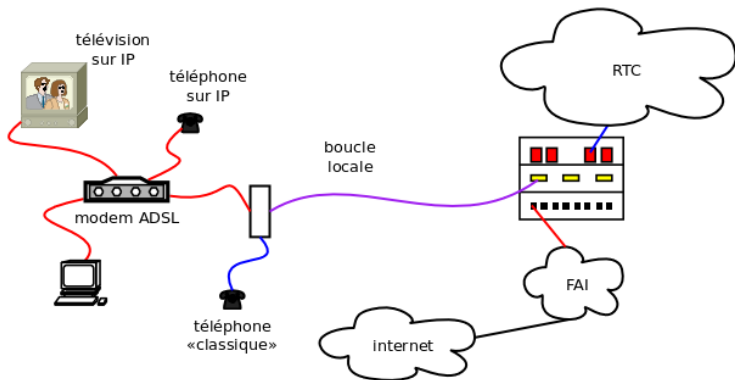
Numéris - Réseau Numérique à Intégration de Services (RNIS)

- adaptateur Numéris rattaché à une ligne téléphonique
- débit garanti : 64 kbit/sec (ou 128 kbit/sec avec 2 canaux)
- plusieurs canaux de communication (voix, fax, images, données, etc)
- intérêt : il suffit d'une ligne téléphonique pouvant accueillir numéris

ADSL

- Réseau de Raccordement Numérique Asymétrique (*Asymmetric Digital Subscriber Line*)
- modem ADSL (i.e. une « box ») rattaché à une ligne téléphonique
- « Internet à haut débit »
- débit descendant minimum : 512 kbit/sec
- débit montant minimum : 128 kbit/sec
- débits non garantis et dépendant de la distance au centre téléphonique
- ligne téléphonique utilisable pendant la connexion à internet
- possibilité de recevoir la télévision et le téléphone IP
- évolution en VDSL2 et ADSL2+

ADSL

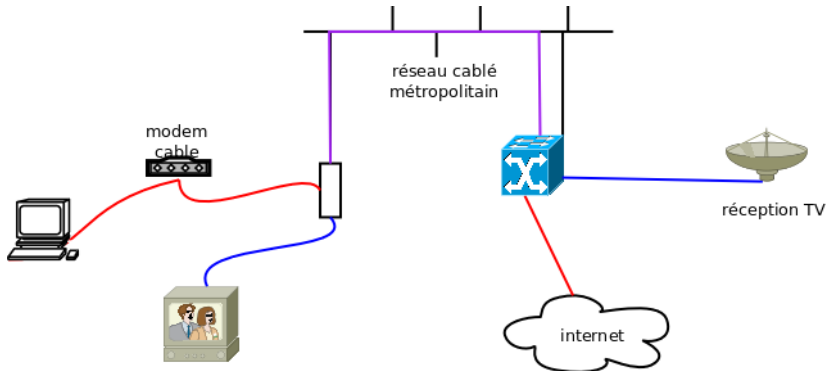


source Pr. Pascal Nicolas

Câble

- réseau métropolitain câblé de télévision
- modem câble
- « Internet à haut débit »
- débit descendant minimum : 20 Mbit/sec
- débit montant minimum : 512 kbit/sec

Câble

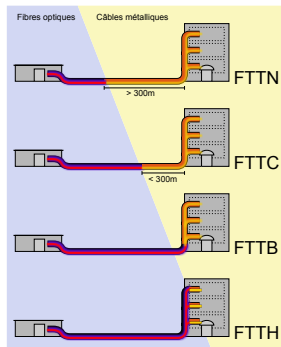


source Pr. Pascal Nicolas

Fibre

- réseau (métropolitain) voir international (backbone)
- modem fibre/adsl ou liaison ethernet
- « Internet à très haut débit »
- débit montant/descendant minimum : 2 Gbit/sec
- PON : Passive Optical Network ou Point à Multipoint Passif
- P2P : Point à Point Passif

Fibre

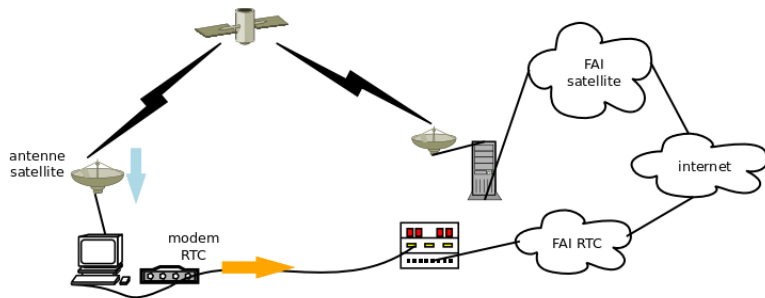


source Wikipédia

Satellite (en monodirectionnel)

- réception (*download*) par satellite
- parabole de réception
- expédition (*upload*) via une liaison RTC
- modem rattaché à une ligne téléphonique
- temps de latence élevé dû à l'éloignement du satellite géostationnaire (36000km)

Satellite (en monodirectionnel)

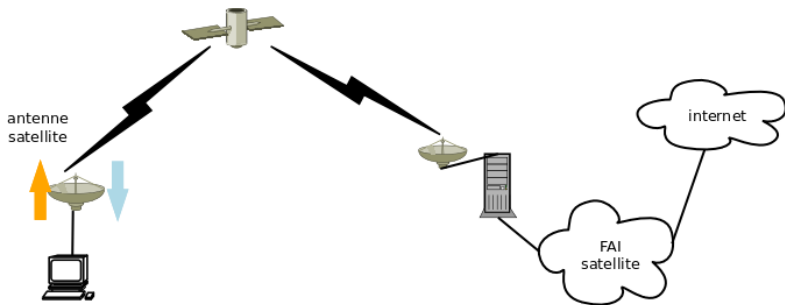


source Pr. Pascal Nicolas

Satellite (en bidirectionnel)

- réception (*download*) par satellite
- parabole de réception
- expédition (*upload*) par satellite
- antenne d'émission
- temps de latence élevé dû à l'éloignement du satellite géostationnaire (36000km)
- coût très important

Satellite (en bidirectionnel)



source Pr. Pascal Nicolas

Liaison spécialisée

- Liaison loué
- liaison permanente
- débit disponible garanti
- adresse IP fixe
- hébergement de services professionnels

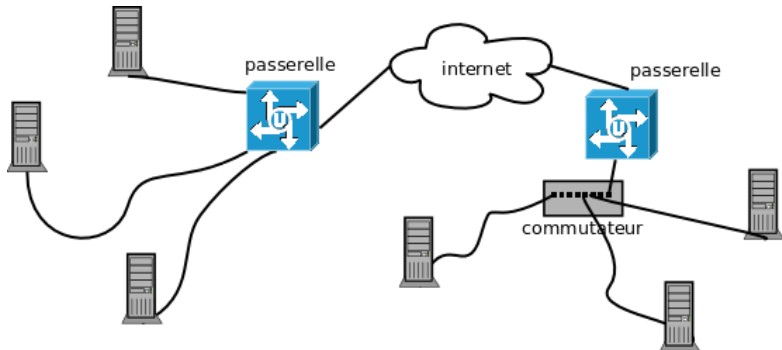
Partage d'un accès Internet

- partage sur un « petit » réseau de l'accès à Internet
- passerelle possédant une adresse IP (publique)
- autres éléments (les « hôtes ») du réseau avec adresses IP privées
- 3 grands types de partage :
 - via de l'Ethernet filaire
 - via du WiFi
 - via du CPL
 - ou une combinaison des 3.

Ethernet filaire

- chaque hôte dispose d'une carte Ethernet (10 ou 100 Mbit/sec)
- passerelle reliée (via de la connection RJ45)
 - directement à chaque hôte
 - indirectement via un commutateur (*switch*) (ou un concentrateur (*hub*))

Ethernet filaire

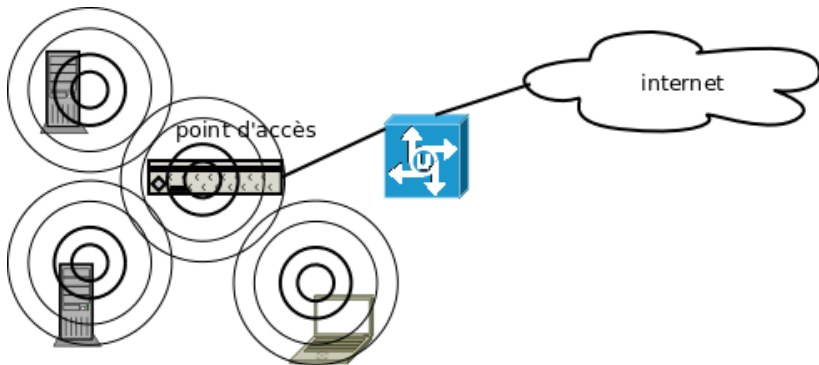


source Pr. Pascal Nicolas

WiFi

- point d'accès et passerelle
- carte WiFi pour chaque hôte
- accès sécurisés
 - identification lors de la connexion
 - chiffrement des échanges
- débits : 11 Mbit/sec (802.11b) ou 54 Mbit/sec (802.11g)
- simplicité à l'installation
- fiabilité et performance en fonction des conditions d'utilisation

WiFi

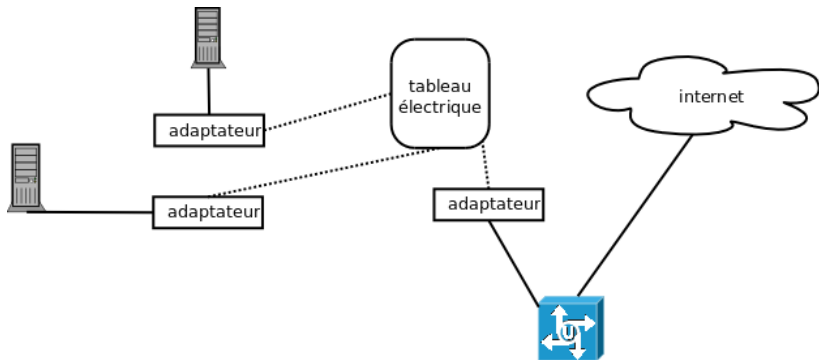


source Pr. Pascal Nicolas

Courant porteur en ligne (CPL)

- utilisation du réseau électrique « indoor »
- réseau Ethernet sur le réseau électrique
- carte réseau Ethernet pour chaque hôte reliée via un adaptateur sur une prise de courant
- passerelle reliée via un adaptateur à une prise de courant
- utilisation d'un réseau préexistant

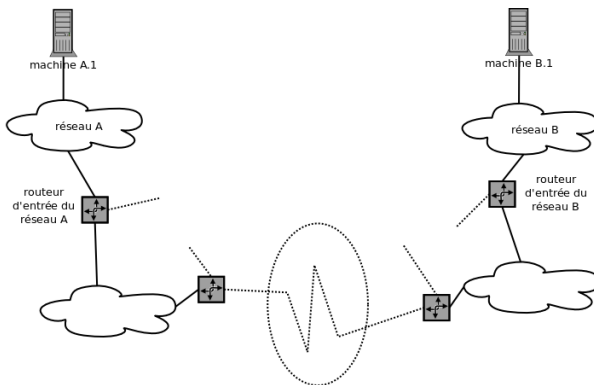
Courant porteur en ligne (CPL)



source Pr. Pascal Nicolas

Objectif des protocoles TCP/IP

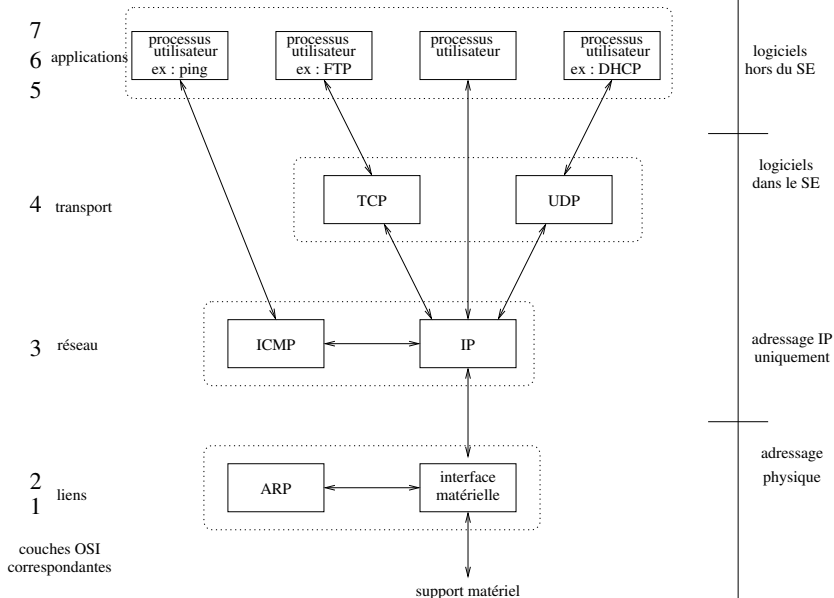
- Assurer la transmission d'informations entre deux entités situées dans des réseaux locaux possiblement distincts.



source Pr. Pascal Nicolas

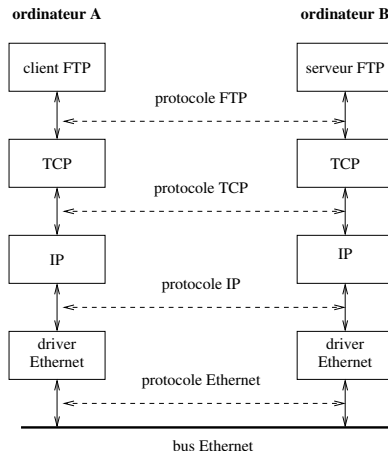
Les 4 couches de TCP/IP

- couche application (les programmes utilisateurs)
- couche transport
 - TCP
 - UDP (*User Datagram Protocol*)
- couche réseau
 - IP
 - ICMP (*Internet Control Message Protocol*)
- couche de liens d'interface avec le matériel
 - pilote (*driver*) du système d'exploitation
 - carte d'interface entre l'hôte et le réseau
- Les couches « réseau » et « de liens » sont présentes sur tous les équipements tandis que les couches « application » et « transport » ne sont présentes que sur les hôtes (de « bout en bout »).



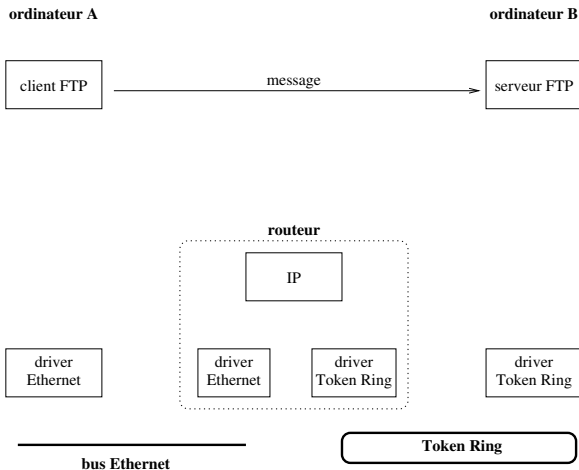
Transmission d'informations en local

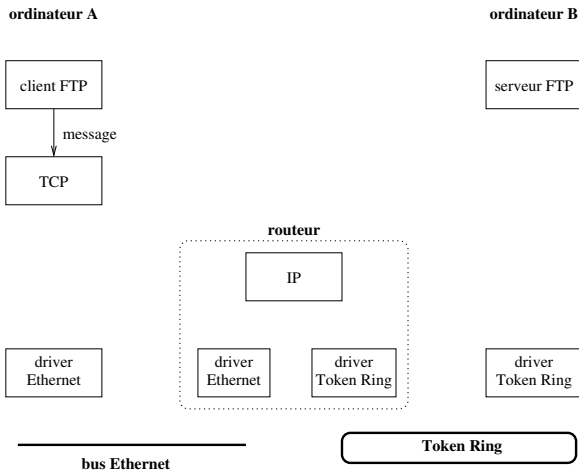
Un ordinateur A (client) interroge un ordinateur B (serveur) via l'application FTP (*File Transfert Protocol*)

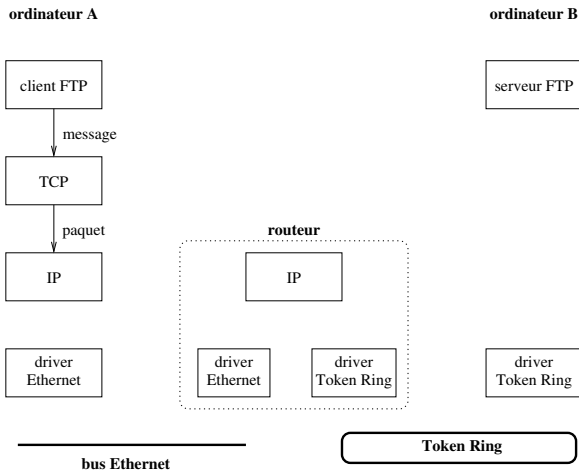


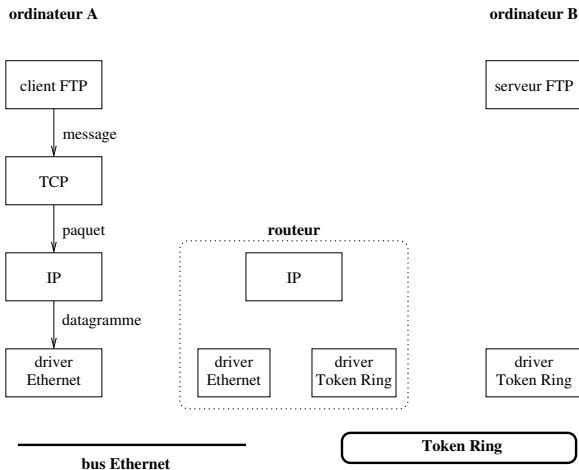
Interconnexion de réseaux hétérogènes

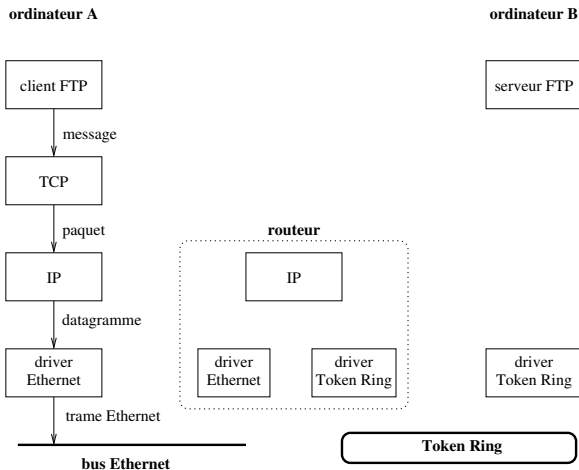
- Deux systèmes terminaux A et B
- A sur un réseau de type « bus Ethernet »
- B sur un réseau de type « Token Ring »
- un routeur entre A et B disposant
 - d'une carte et driver Ethernet
 - d'une carte et driver Token Ring
- une trame Ethernet et une trame Token Ring
- messages identiques (niveau applications)
- paquets identiques (niveau transport)
- datagrammes identiques dans le cas d'un seul routeur (niveau réseau)
- datagrammes possiblement différents dans le cas général

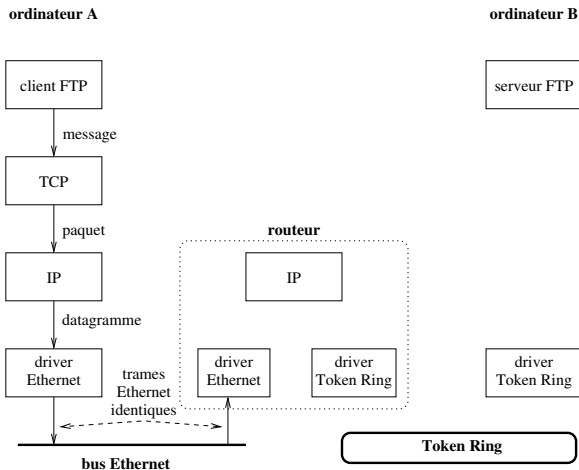




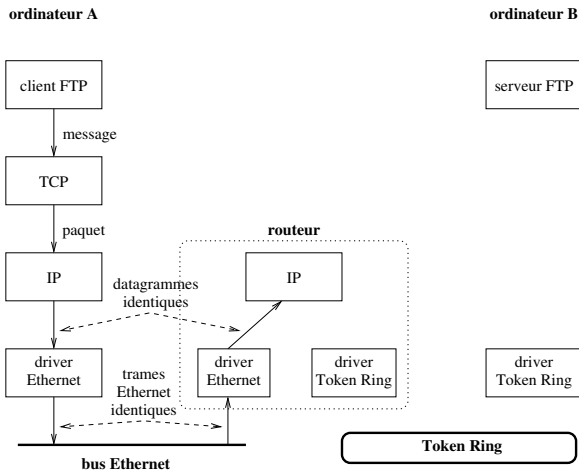


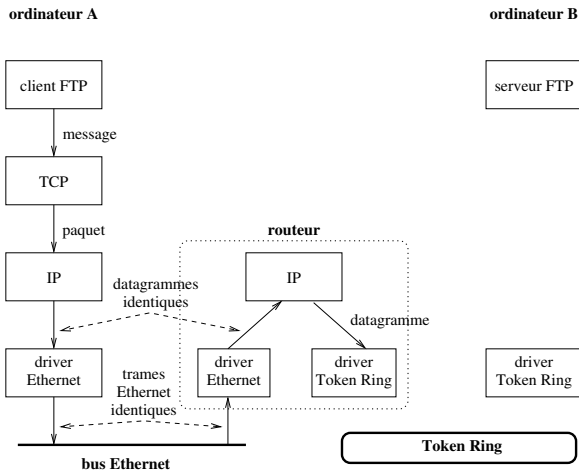


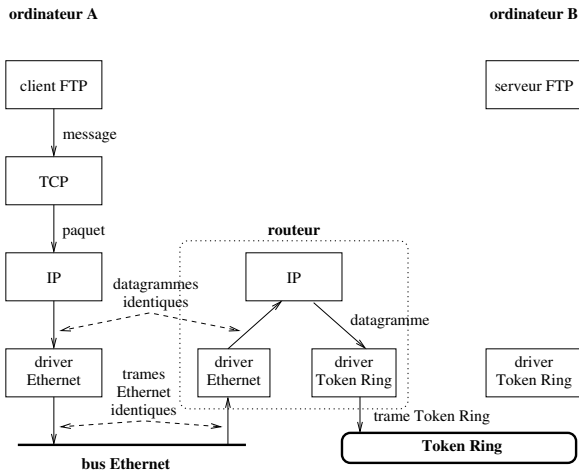


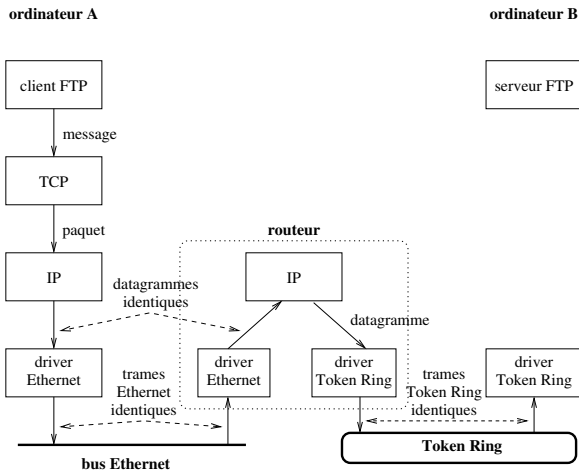


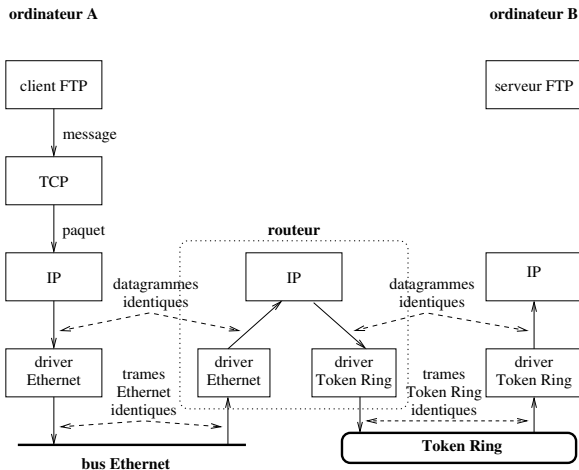
« routeur » : machine permettant l'acheminement d'un réseau à un autre réseau.

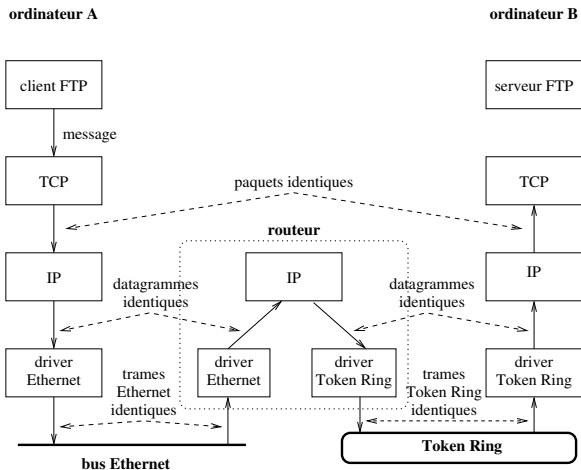


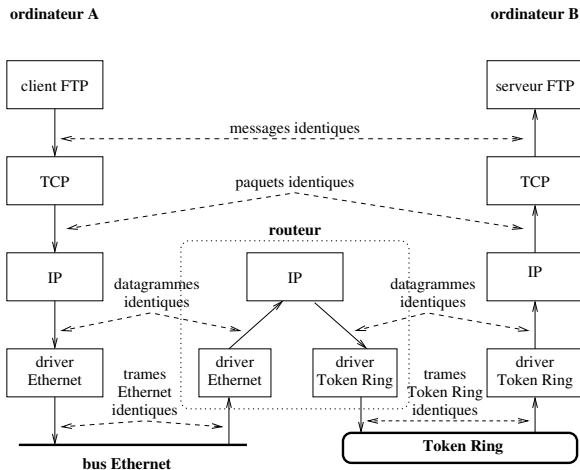


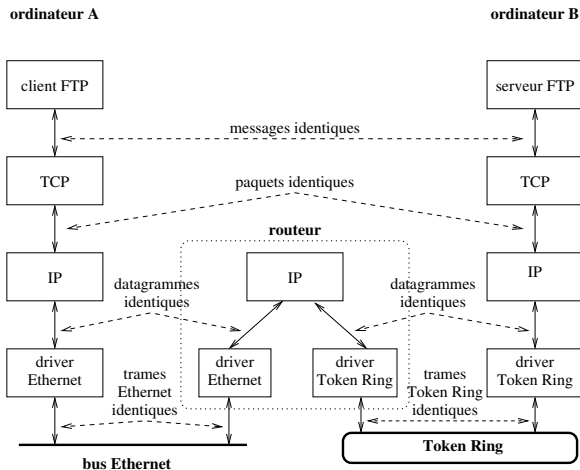






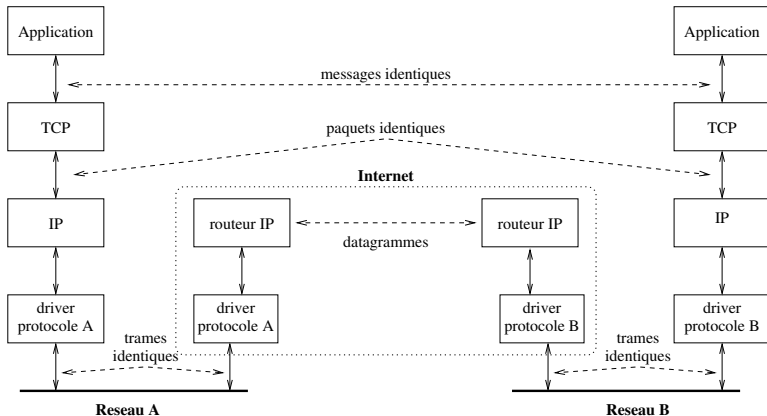






ordinateur A

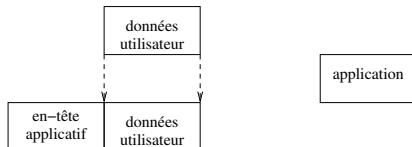
ordinateur B



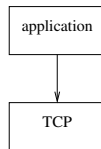
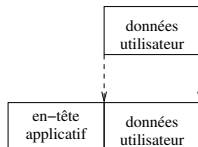
Encapsulation de la pile de protocoles TCP/IP

données
utilisateur

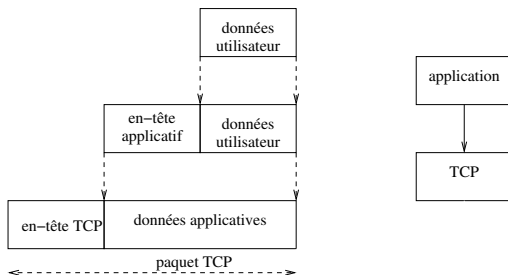
Encapsulation de la pile de protocoles TCP/IP



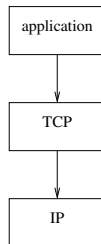
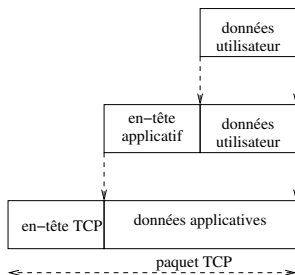
Encapsulation de la pile de protocoles TCP/IP



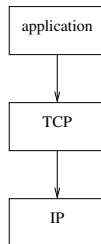
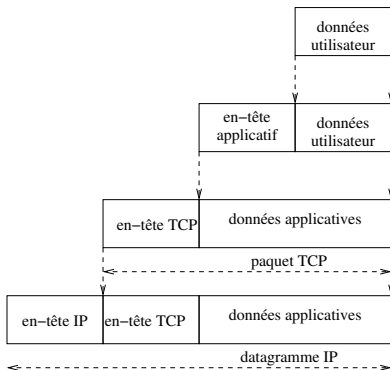
Encapsulation de la pile de protocoles TCP/IP



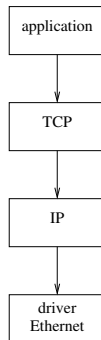
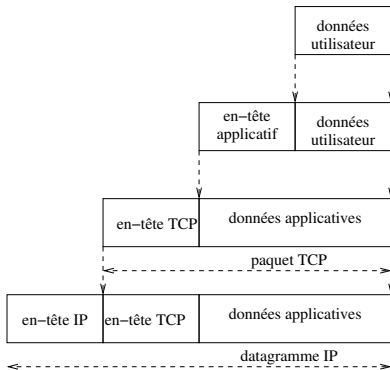
Encapsulation de la pile de protocoles TCP/IP



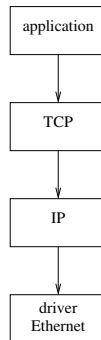
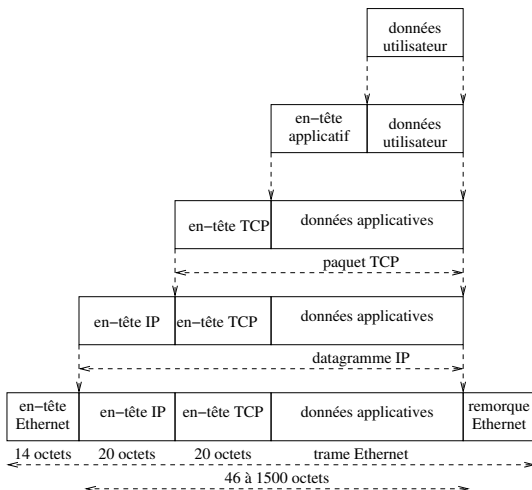
Encapsulation de la pile de protocoles TCP/IP



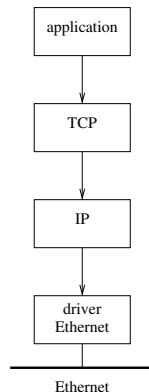
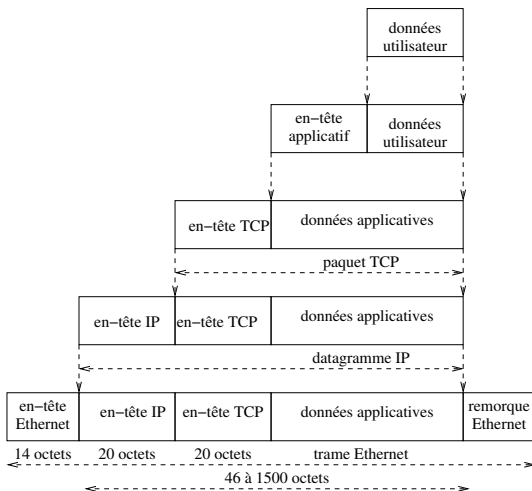
Encapsulation de la pile de protocoles TCP/IP



Encapsulation de la pile de protocoles TCP/IP



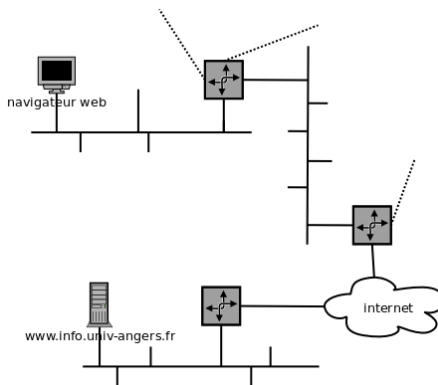
Encapsulation de la pile de protocoles TCP/IP



Un exemple

Accéder à la page web

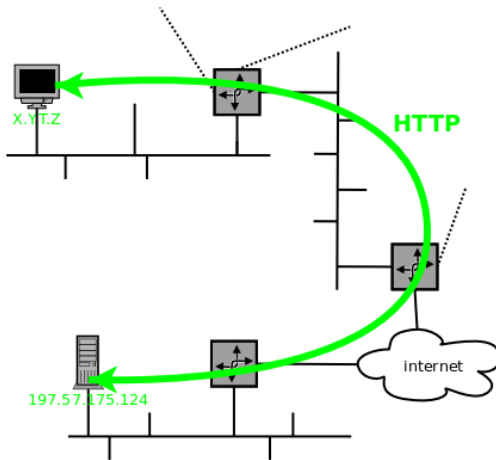
`http://www.info.univ-angers.fr/~chhel/index.html`



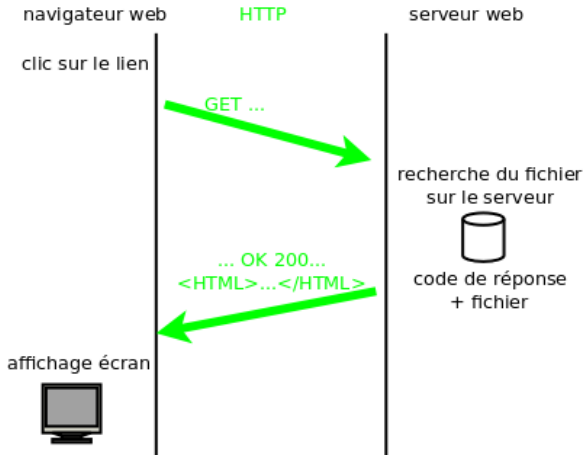
Niveau HTTP

- le navigateur demande au DNS l'adresse IP du serveur
`www.info.univ-angers.fr`
- le DNS retourne `194.57.175.124`
- le navigateur envoie la requête HTTP
`GET /~ chhel/index.html HTTP/1.1`
`Host: www.info.univ-angers.fr`
`User-Agent : ...`
- le serveur web répond
`HTTP/1.1 200 OK`
`Date: Wed, 31 Aug 2011 15:28:46 GMT`
`Server: Apache/2.2.14 (Ubuntu)`
`...`
`<HTML>`
`...`
`</HTML>`

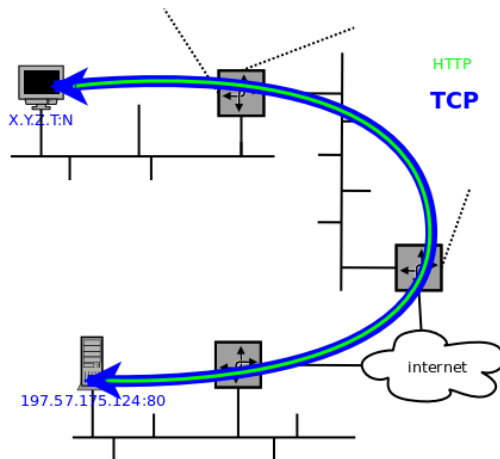
Niveau HTTP



Échange de messages HTTP



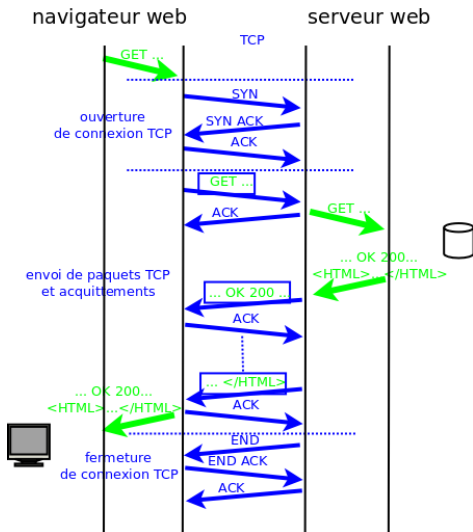
Niveau TCP (et HTTP)



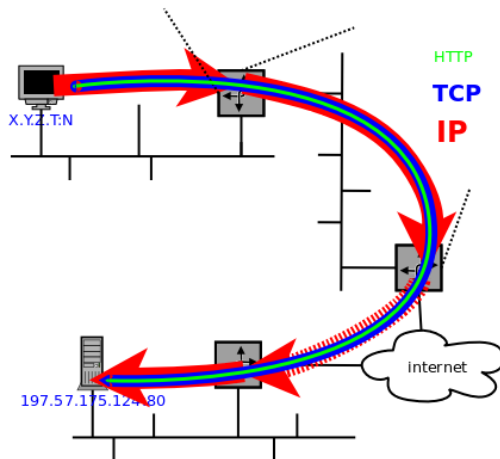
Niveau TCP

- Canal de communication *socket* (X.Y.Z.T :N, 194.57.175.124 :80)
- port 80 pour le serveur
- port N libre pour le client
- dialogue HTTP s'appuyant sur une connexion TCP
 - établissement de la connexion TCP
 - envoi du navigateur client au serveur de la requête HTTP (1 seul paquet suffit)
 - envoi du serveur au navigateur client de la réponse HTTP (plusieurs paquets)
 - fermeture de la connexion TCP

Échange de paquets TCP (et de messages HTTP)



Niveau IP (et TCP (et HTTP))



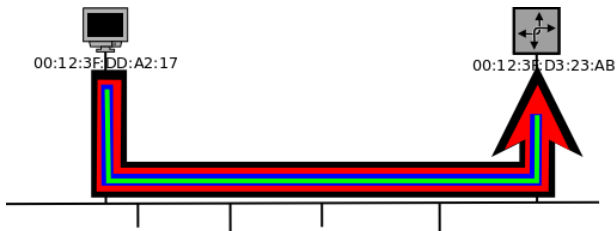
Niveau IP

- Chaque paquet TCP est encapsulé dans un datagramme IP
- chaque datagramme IP contient (en autres)
 - l'adresse IP de l'émetteur du datagramme IP
 - l'adresse IP du destinataire final du datagramme IP
- chaque datagramme IP va de routeur en routeur jusqu'à sa destination
- à chaque routeur, la table de routage indique
 - l'adresse IP du prochain routeur nécessaire connecté au même réseau que le routeur effectuant le routage
 - l'interface de sortie

Niveau liens

Dans le cas d'une connexion entre un client et un serveur sur le même réseau Ethernet

- Chaque datagramme IP est placé dans autant de trames Ethernet que nécessaires (par fragmentation)
- chaque trame Ethernet contient les adresses MAC (*Medium Access Control*) des cartes réseaux de l'émetteur et du destinataire



HTTP

TCP

IP

Ethernet

Couche de liens d'Internet

- réseau à commutation de circuit
 - mode connecté
 - une connection pour un circuit
 - débit garanti
 - réseau téléphonique
- réseau à commutation de paquets
 - mode non connecté
 - fragmentation des données et multiplexage
 - nombreuses communications sur une même ligne
 - pas de débit garanti
 - la plus grande part du réseau Internet

Distance versus débit

- réseaux étendus
 - WAN (*Wide Area Network*)
 - longue distance
 - faible débit (1,5Mbit/s à 2,4Gbit/s)
 - mise-en-œuvre de routeurs
- réseaux locaux
 - LAN (*Local Area Network*)
 - petite distance
 - haut débit (100Mbit/s à 10Gbit/s)
 - La technologie Ethernet
- Taille maximale pour une trame ou MTU (*Maximum Transfert Unit*)

Caractéristiques des topologies de réseaux

Topologie	Équipement critique	Insertion/retrait d'hôtes	Localisation des pannes	Mode de transmission
Bus	Aucun	Avec coupure	Difficile	Diffusion
Étoile	Équipement central	Sans coupure	Directe	Diffusion (hub) Point à point (commutateur)
Anneau	Tous les hôtes	Avec coupure	Directe	Diffusion

Accès au support physique

- Centralisé (un hôte règle le « temps de parole ») / distribué
- Statique (intervalles réservés \rightsquigarrow gaspillage) / dynamique
- Déterministe (\rightsquigarrow temps réel) / aléatoire
- Équitable / prioritaire
- Avec / sans contentions (collisions)

Les réseaux Ethernet

- Position hégémonique
- Xerox au début des années 1970
- Normalisé par l'IEEE vers 1980
- Premières et secondes générations : câble coaxial
- Générations suivantes :
 - câble type paire torsadée
 - 10Base-T (10Mbit/s)
 - 100Base-T (*Fast Ethernet*, 100Mbit/s)
 - 1000Base-T (*Ethernet GigaBit*, 1Gbit/s)

Caractéristiques de l'Ethernet

- « Bus partagé » simulé sur une topologie en étoile
- « remise au mieux » : sans garanti de réception
- « diffusion » : tous les hôtes reçoivent l'ensemble des trames
- filtrage sur l'adresse Ethernet incluse dans la trame
- pas d'autorité de contrôle au bus : risque de collisions
- CSMA/CD (*Carrier Sense Multiple Acces with Collision Detection*) :
 - accès simultanément au réseau
 - test d'activité par détection d'« onde porteuse » (*carrier wave*)
 - possibilité de transmissions simultanées
 - détection de collision par écoute d'éventuelles interférences
 - interruption de la transmission puis réémission aléatoire selon des fenêtres croissantes ($\times 2$)

Adresses physiques Ethernet

- notation hexadécimale doublement pointée de 6 mots de 8 bits
- adressage sur 48 bits ($6 \times 2 \times 4$ bits)
- adresse MAC (*Media ACcess*)
- adresse associée à une interface réseau
- espace des adresses MAC =

$$\left\{ \begin{array}{l} U : V : W : X : Y : Z \mid \\ 0 \leq U, V, W, X, Y, Z \leq FF \end{array} \right\}$$

- trois types d'adressage
 - *unicast* : désigne un interface unique
 - *broadcast* : désigne tous les interfaces (FF:FF:FF:FF:FF:FF)
 - *multicast* : désigne un groupe d'interfaces

Trame Ethernet

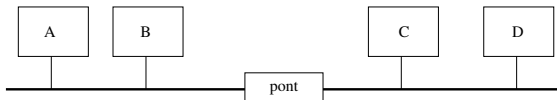
adresse de destination	adresse source	type	données	CRC
6 octets	6 octets	2 octets	46–1500 octets	4 octets

- CRC (*Cyclic Redundancy Check*) : code de redondance pour le contrôle des données
- La trame est acceptée si le CRC est correct par rapport aux données.
- Le type différencie les trames :
 - datagramme IP
 - requête ou réponse ARP
 - protocole expérimental
 - etc.

Équipements matériels d'un réseau Ethernet

- « Répéteur » : retransmission et amplification du signal
- « Concentrateur » (*hub*) : retransmission multiports
- « Pont » (*bridge*) : extension d'un réseau
- « Commutateur » (*switch*) : pont multiports

Pont et Commutateur



- Accès transparent pour les hôtes
- Filtre les trames
 - interdit le passage des trames non valides
 - définit deux segments : AB et CD
 - autorise le passage de trames d'un segment à l'autre
 - bloque les trames internes à AB qui sont alors visibles ni de C ni de D
- Améliore le débit du réseau
- Renforce la confidentialité
- Le « tout commuté » : chaque hôte est relié directement à un port d'un commutateur ne recevant que les trames qui lui sont destinées

WiFi

- *Wireless Fidelity*
- mode « infrastructure » : un point d'accès (antenne émettrice/réceptrice) connecté à un réseau filaire
- mode « ad-hoc » : sans point d'accès (d'hôte à hôte)
- CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*)
- Deux stations peuvent être trop loin l'une de l'autre pour s'entendre : possibilité de collisions
- Si une station veut émettre un petit message :
 - 1. elle explore le spectre des fréquences
 - 2. si une activité est détectée, elle attend
 - 3. sinon elle expédie les données et attend l'acquittement
 - 4. le récepteur reçoit les données et envoie un acquittement
 - 5. si elle reçoit l'acquittement, elle clôt la transmission sinon elle réémet

WiFi

- Si une station veut émettre un volumineux message :
 - 1. elle explore le spectre des fréquences
 - 2. si une activité est détectée, elle attend
 - 3. sinon elle expédie un message RTS (*Ready to Send*) qui contient le volume de données et la vitesse de transmission
 - 4. le récepteur expédie un message CTS (*Clear to Send*)
 - (les autres stations vont être silencieuses pendant le temps de la transmission)
 - 5. elle expédie les données et attend un acquittement
 - 6. le récepteur reçoit les données et envoie un acquittement
 - 7. si elle reçoit l'acquittement, elle clôt la transmission sinon elle recommence le processus

La couche réseau

- Protocole IP (*Internet Protocol*)
- sans connexion (chaque datagramme est traité indépendamment des autres)
- non fiable (perte, inversion, duplication)
- remise « au mieux » (pas de perte sans nécessité)
- norme initiale IPv4
- « nouvelle » norme IPv6
- définition du protocole IP :
 - définition de l'adressage
 - définition du format du datagramme
 - définition de l'acheminement
 - définition de la gestion de la remise non fiable

Adressage IP

- Réseau virtuel homogène masquant les réseaux physiques interconnectés
- identifiants universels pour communication universelle
- adressage logique : identification et localisation
- chaque interface réseau d'un matériel dispose d'une adresse IP (dynamique ou non)
- les routeurs ont une adresse IP pour chaque interface réseau

(IPv4) Adressage IPv4

- Notation décimale pointée de 4 nombres (4 octets)
- adressage sur 32 bits
- espace des adresses IPv4 = $\{X.Y.Z.T | 0 \leq X, Y, Z, T \leq 255\}$
- l'adresse IP du serveur web du département informatique :
194.57.175.124
- paire identifiant réseau/identifiant hôte

(IPv4) Adressage avec classes

	7 bits		24 bits	
classe A	0	id. de réseau	id. d'interface	
	14 bits		16 bits	
classe B	1	0	id. de réseau	id. d'interface
	21 bits		8 bits	
classe C	1	1	0	id. d'interface
	28 bits			
classe D	1	1	1	0
	27 bits			
classe E	1	1	1	1

- Seules les classes A, B et C fournissent des adresses IP
- les bits de point fort détermine la classe
- grande efficacité pour le routage

(IPv4) Adressage avec classes

classe	adresses
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255

- Au plus 127 réseaux de classe A (plus de 2^{16} hôtes)
- 2^{14} réseaux de classe B (entre 2^8 et 2^{16} hôtes)
- 2^{21} réseaux de classe C (entre 1 et 256 hôtes)

(IPv4) Adresses réservées

- 0.0.0.0 (par exemple, pour qu'un hôte demande son adresse)
- <id réseau nul>.<id d'hôte> (par exemple, pour qu'un hôte demande son adresse)
- <id réseau>.<id d'hôte nul> réseau lui-même
- <id réseau>.<id d'hôte avec tous les bits à 1> adresse de diffusion sur le réseau
- 255.255.255.255 adresse de diffusion sur le réseau (sans connaître l'identifiant du réseau)
- 127.Y.Z.T communication inter-processus sur un même hôte
- réseaux privés *intranet*
 - 10.0.0.0 à 10.255.255.255 (classe A)
 - 172.16.0.0 à 172.31.255.255 (classe B)
 - 192.168.0.0 à 192.168.255.255 (classe C)

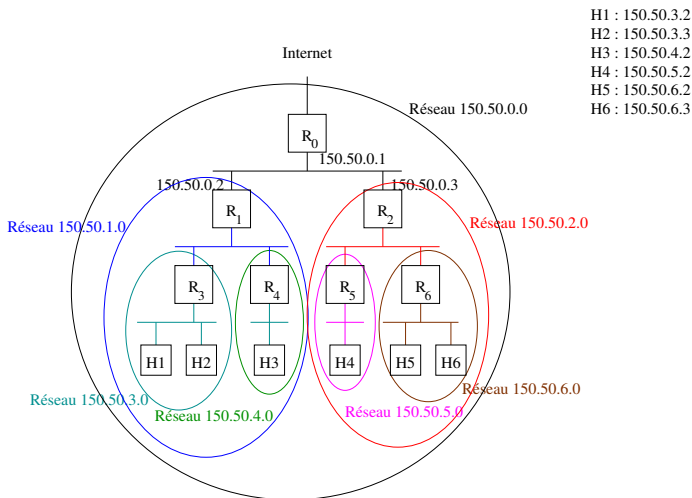
(IPv4) Les faiblesses de l'adressage IPv4 avec classes

- Pas pensé pour la croissance d'Internet
- plus assez d'identifiants réseau
- pénurie des adresses de classe B
- pas adapté aux réseaux de taille moyenne
 - pour un réseau de 500 hôtes
 - classe C trop petite
 - gaspillage en classe B
- avant de passer à IPv6
 - adressage en sous-réseaux
 - CIDR

(IPv4) Adressage en sous-réseaux

- Augmenter le nombre de préfixes réseaux
- l'identifiant hôte devient un identifiant local
- l'identifiant local comprend
 - des identifiants sous-réseaux
 - un identifiant hôte
- hiérarchie locale de réseaux

(IPv4) Exemple d'adressage en sous-réseaux



(IPv4) Adressage en sous-réseaux par masques

- accès aux sous-réseaux et identifiant hôte par masques
- les bits à 1 désigne l'identifiant réseau
- les bits à 0 désigne l'identifiant local
- un ET logique binaire les calculent

adresse IP de classe B

150.50.215.200	10010110.00110010.11010111.11001000
----------------	-------------------------------------

masque (21 premiers bits à 1)

255.255.248.0	11111111.11111111.11111000.00000000
---------------	-------------------------------------

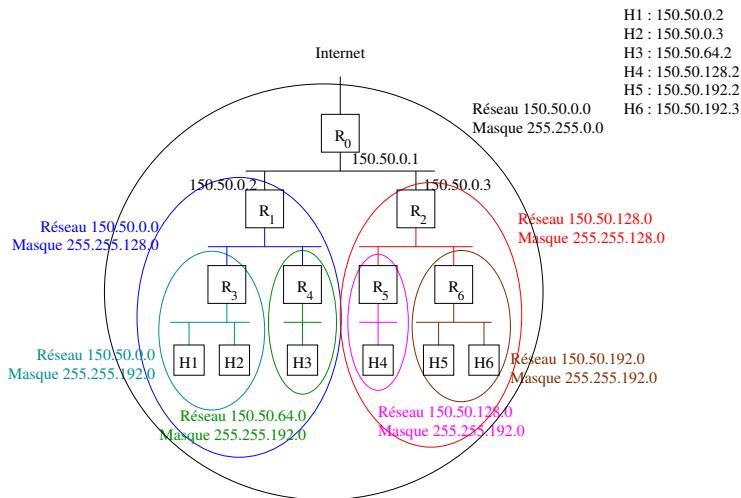
identifiant réseau

150.50.208.0	10010110.00110010.11010	000.00000000
--------------	-------------------------	--------------

identifiant local

0.0.7.200	00000000.00000000.00000	111.11001000
-----------	-------------------------	--------------

(IPv4) Exemple d'adressage en sous-réseaux par masques



(IPv4) Exemple d'adressage en sous-réseaux par masques

adresse IP de classe B

150.50.64.2	10010110.00110010.01000000.00000010
-------------	-------------------------------------

masque (18 premiers bits à 1)

255.255.192.0	11111111.11111111.11000000.00000000
---------------	-------------------------------------

identifiant réseau

150.50.64.0	10010110.00110010.01	000000.00000000
-------------	----------------------	-----------------

identifiant local

0.0.0.2	00000000.00000000.00	000000.00000010
---------	----------------------	-----------------

(IPv4) CIDR

- *Classless Inter Domain Routing*
- Routage interdomaine sans classe
- adresse CIDR : $X.Y.Z.T/m$ où m est un masque entier
- le masque désigne le nombre de bits constituant l'identifiant réseau
- la valeur du masque m fixe les m premiers bits à 1 et les $32-m$ derniers bits à 0
- avantages :
 - découper librement des blocs d'adresses sans classe
 - agréger des blocs d'adresses pour simplifier le routage
 - agréger des classes C pour pallier à la pénurie de classes B
- pour un réseau de n hôtes,
 - $2^{32-m} \geq n$, m masque d'une classe suffisamment grande
 - des réseaux de classe insuffisamment grande mais de masques contigus (le sur-adressage)

(IPv4) Exemple d'adressage sans classe

- Fournisseur d'accès dispose d'un bloc CIDR 150.50.0.0/17
- $2^{32-17} - 2 = 32766$ adresses possibles

150.50.0.0/17

150.50.0.0	10010110.00110010.00000000.00000000
------------	-------------------------------------

masque (17 premiers bits à 1)

255.255.128.0	11111111.11111111.10000000.00000000
---------------	-------------------------------------

adresse minimale attribuable

150.50.0.1	10010110.00110010.0	00000000.00000001
------------	---------------------	-------------------

adresse maximale attribuable

150.50.127.254	10010110.00110010.0	11111111.11111110
----------------	---------------------	-------------------

(IPv4) Exemple d'adressage sans classe

- Client de 2000 hôtes
- bloc CIDR 150.50.8*x.0/21
- $2^{32-21} - 2 = 2^{11} - 2 = 2046$ adresses disponibles pour le client
- au choix : $0 \leq x \leq 15 = 2^{32-(17+11)} - 1 = 2^4 - 1$

Réseau client

150.50.8*x.0	10010110.00110010.0????	000.00000000
masque (21 premiers bits à 1)		
255.255.248.0	11111111.11111111.11111000	00000000
adresse minimale attribuable		
150.50.8*x.1	10010110.00110010.0????	000.00000001
adresse maximale attribuable		
150.50.8*x+7.254	10010110.00110010.0????	111.11111110

(IPv4) Exemple d'adressage sans classe

- Client de 2000 hôtes
- bloc CIDR **150.50.0.0/21**
- $2^{32-21} - 2 = 2046$ adresses disponibles pour le client
- **x = 0**

Réseau client

150.50.0.0	10010110.00110010.00000	000.00000000
masque (21 premiers bits à 1)		
255.255.248.0	11111111.11111111.11111000	00000000
adresse minimale attribuable		
150.50.0.1	10010110.00110010.00000	000.00000001
adresse maximale attribuable		
150.50.7.254	10010110.00110010.00000	111.11111110

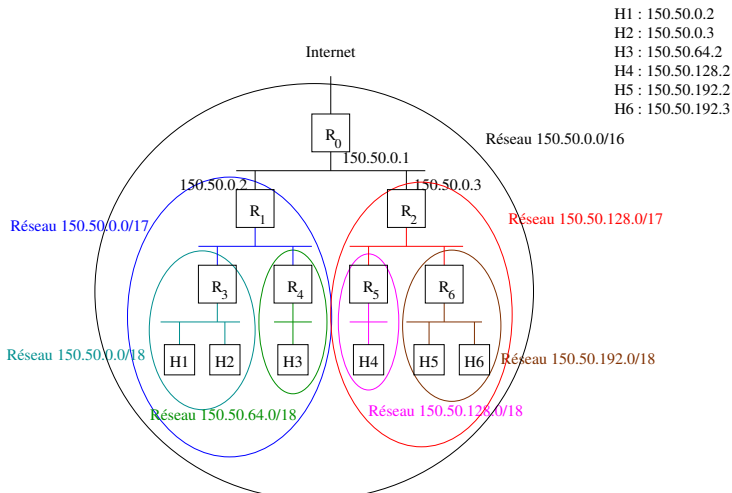
(IPv4) Exemple d'adressage sans classe

- Client de 2000 hôtes
- bloc CIDR **150.50.120.0/21**
- $2^{32-21} - 2 = 2046$ adresses disponibles pour le client
- **$x = 15$**

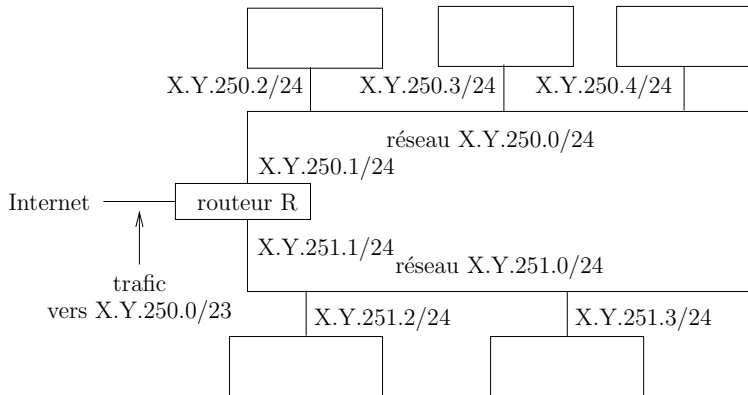
Réseau client

150.50.120.0	10010110.00110010.0 1111	000.00000000
masque (21 premiers bits à 1)		
255.255.248.0	11111111.11111111.11111000	00000000
adresse minimale attribuable		
150.50.120.1	10010110.00110010.0 1111	000.00000001
adresse maximale attribuable		
150.50.127.254	10010110.00110010.0 1111	111.11111110

(IPv4) Exemple d'adressage en sous-réseaux par masques CIDR



(IPv4) Réseaux de classe C agrégés



Le 24^{ème} bit distingue les deux sous-réseaux.

(IPv4) Traduction d'adresse réseau

- NAT (*Network Address Translation*)
- Accès transparent à Internet au niveau IP pour réseaux privés
- Traduction des adresses IP privées en adresses IP routables sur Internet
- Seuls les interfaces nécessitant une connexion avec Internet sont traduites
- Diminution du besoin d'adresses IP
- Seul le « routeur » NAT est connu d'Internet
- Table de traduction (statique ou dynamique) identifiant l'adresse IP du destinataire sur Internet à l'adresse IP source sur le réseau privé
- NAT multidomicilié pour accès concurrents
- Problème avec les protocoles manipulant les adresses IP

(IPv4) Traduction d'adresse réseau avec traduction de port

- NAPT (*Network Address Port Translation*)
- Accès au même service sur un même serveur d'Internet par deux interfaces d'un réseau privé
- multiplexage sur le numéro du port
- Table pour le NAT

Adresse Privée	Port Privé	Port NAT	Adresse Serveur	Port Serveur
-------------------	---------------	-------------	--------------------	-----------------

(IPv4) Traduction d'adresse réseau avec traduction de port

- Deux machines d'adresses privées 10.0.0.1 et 10.0.0.2 désirent par le même port privé P communiquer, via un NAT d'adresse G , avec un serveur web (port 80) d'adresse 197.57.175.124
- Pour les hôtes : (10.0.0.1 : P , 197.57.175.124 : 80) et (10.0.0.2 : P , 197.57.175.124 : 80)
- remplacement par le NAT : (G : P , 197.57.175.124 : 80) et (G : P , 197.57.175.124 : 80)
- remplacement par le NAPT : (G : P_1 , 197.57.175.124 : 80) et (G : P_2 , 197.57.175.124 : 80)
- Table pour le NAPT

Adresse Privée	Port Privé	Port NAPT	Adresse Serveur	Port Serveur
10.0.0.1	P	P_1	197.57.175.124	80
10.0.0.2	P	P_2	197.57.175.124	80

(IPv6) Adressage IPv6

- Notation hexadécimale doublement pointée de 8 mots de 16 bits
- Adressage sur 128 bits ($8 \times 4 \times 4$ bits)
- Espace des adresses IPv6 =

$$\left\{ [S : T : U : V : W : X : Y : Z] \mid \begin{array}{l} 0 \leq S, T, U, V, W, X, Y, Z \leq FFFF \end{array} \right\}$$

- :: que des 0
- Trois types d'adressage
 - *unicast* : désigne une interface unique
 - *multicast* : désigne un groupe d'interfaces
 - *anycast* : désigne une interface parmi un groupe d'interfaces
- Adressage hiérarchique
- Pour une interface, possibilité de plusieurs adresses IPv6
- Adresse à durée de vie limitée

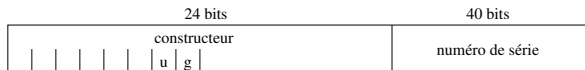
(IPv6) Adressage unicast

3 bits			13 bits	8 bits	24 bits	16 bits	64 bits
0	0	1	TLA	réservé	NLA	id. de site	id. d'interface

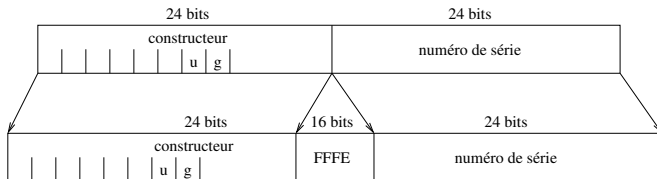
- identifiant public (48 bits)
 - [2000 ::]/3 identifiant les « adresses unicast globales de type plan agrégé »
 - unité d'agrégation haute (TLA : *Top Level Aggregator*)
 - partie réservée sur 8 bits réallouable entre TLA et NLA
 - unité d'agrégation basse (NLA : *Next Level Aggregator*)
- identifiant de site (SLA : *Site Level Aggregator*, 16 bits)
- identifiant d'interface (64 bits)

(IPv6) Identifiant d'interface

- Identifiant interface à partir d'un identificateur IEEE EUI-64

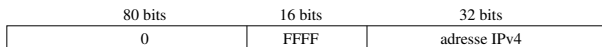


- Identifiant interface à partir d'une adresse MAC IEEE 802

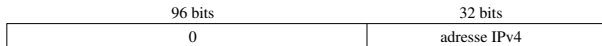


(IPv6) Autres adresses unicast

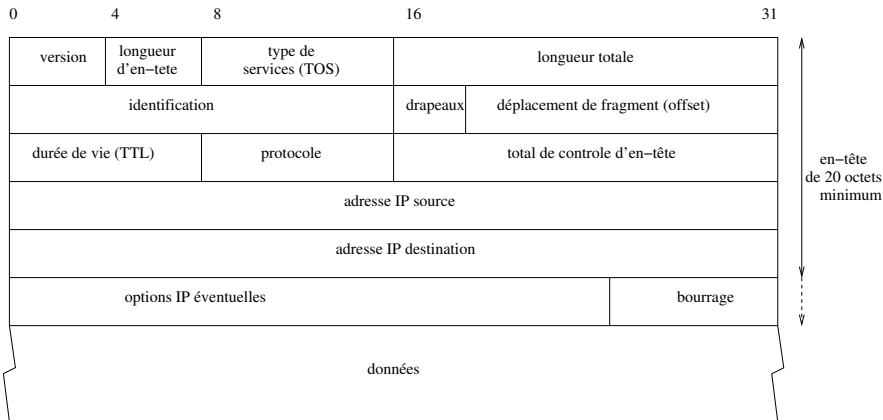
- Adresse IPv4 mappée (de IPv4 à IPv4)



- Adresse IPv4 compatible (de IPv6 à IPv6)



(IPv4) Datagramme IPv4



(IPv4) En-tête d'un datagramme

- longueur d'en-tête sur 4 bits en nombre de mots de 32 bits (au minimum 5 pour 20 octets)
- type de service ou TOS (*Type Of Service*)
- longueur totale du datagramme en octets sur 16 bits
- identification, drapeaux et déplacement de fragment pour la fragmentation des datagrammes
- durée de vie ou TTL (*Time To Live*) indique le nombre maximum de routeurs que le datagramme peut traverser
- protocole identifie le protocole d'un niveau supérieur qui utilise le datagramme (6 pour TCP et 17 pour UDP)
- total de contrôle d'en-tête calculé à partir de l'entête permet d'en assurer son intégrité
- options (d'une taille quelconque) complétée jusqu'à 32 bits par du bourrage

(IPv4) Fragmentation des datagrammes

- Réseaux à taille de trames différentes
- Datagramme trop volumineux pour une seule trame
- Fragmentation au routeur d'entrée sur un réseau de capacité moindre
- Défragmentation uniquement à destination
- Taille maximale pour une trame ou MTU (*Maximum Transfert Unit*)
- Taille des fragments la plus grande possible en restant multiple de 8 octets
- Chaque fragment est routé séparément

(IPv4) En-tête d'un datagramme

- **identification** : numéro unique attribué à chaque datagramme initial
- **offset** : déplacement en multiple de 8 octets dans les données du datagramme initial
- **drapeaux** :
 - 1 bit (à 1) pour interdire de fragmenter
 - 1 bit « à suivre » pour indiquer que c'est un fragment mais pas le dernier (à 0 s'il est le dernier)

(IPv4) Exemple pour un datagramme de 1300 octets



en-tête du datagramme : num=N	données1 600 octets	données2 600 octets	données3 100 octets
----------------------------------	------------------------	------------------------	------------------------

fragment1	en-tête du fragment1 : num=N, déplacement=0, à suivre=1	données1 600 octets
-----------	--	------------------------

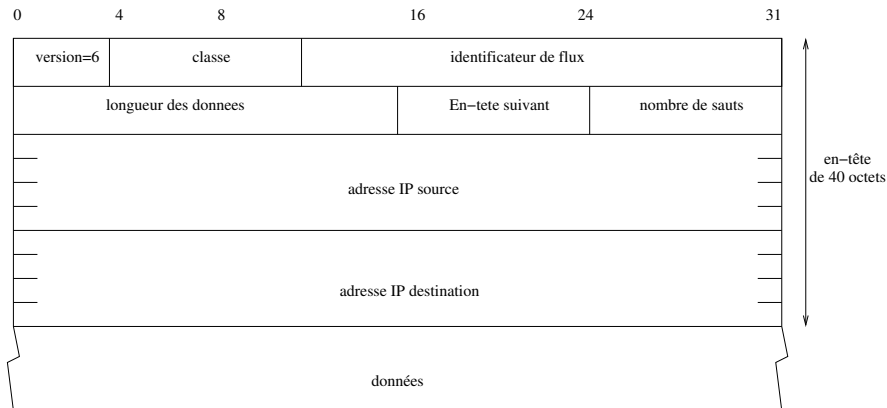
fragment2	en-tête du fragment2 : num=N, déplacement=75, à suivre = 1	données2 600 octets
-----------	---	------------------------

fragment3	en-tête du fragment3 : num=N, déplacement=150, à suivre=0	données3 100 octets
-----------	--	------------------------

(IPv6) Datagramme IPv6

- Champs alignés sur 64 bits
- Contrôle de somme effectué par le protocole de niveau transport
- Taille minimale des MTU de 1280 octets
- Options de IPv4 remplacées par des extensions en début des données
- Fragmentation par la source selon la découverte du plus petit MTU

(IPv6) Datagramme



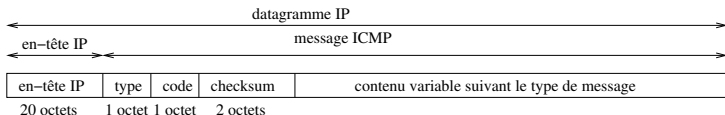
(IPv6) En-tête Datagramme

- version sur 4 bits
- classe sur 8 bits :
 - DSCP (*DiffServ Code Point*) sur 6 bits
 - 2 bits non utilisés
- identificateur de flux : numéro de contexte pour le routage unique et généré par la source
- longueur des données : longueur des données (sans l'en-tête) en octets sur 16 bits (0 si supérieure à 65535)
- En-tête suivant sur 1 octet : identifie le protocole d'un niveau supérieur qui utilise le datagramme ou la première des extensions
- Nombre de sauts : indique le nombre maximum de routeurs que le datagramme peut traverser

Gestion des erreurs : le protocole ICMP

- *Internet Control Message Protocol*
- Requis dans tous les routeurs
- Encapsulé dans un message IP
- Couche réseau
- Fournir des erreurs (et non fiabiliser IP) à
 - une couche IP d'un hôte
 - un protocole de la couche transport (TCP ou UDP)
 - un protocole applicatif
- Pas de message d'erreur en cas d'une erreur sur un message ICMP (éviter une « avalanche »)
- Fournir des informations sur l'état du réseau

(IPv4) Message ICMP IPv4

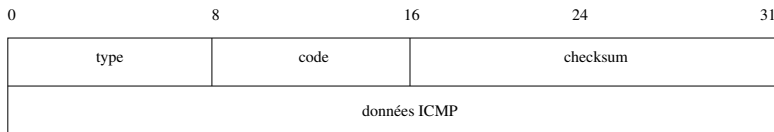


- **type** : nature du message envoyé
 - 8/0 : demande et réponse d'information
 - 3 : inaccessibilité
 - 4 : demande de régulation
 - 5 : modification de route (non optimale)
- **code** : contexte d'émission du message
- Début du datagramme ayant entraîné l'erreur

(IPv6) ICMP IPv6

- Détection des erreurs
- Tests d'accessibilité
- Configuration automatique des hôtes
- Remplace le protocole ARP
- Gestion des groupes multicast
- Message limité à 1028 octets

(IPv6) Message ICMP IPv6



- type :
 - ≤ 127 : message d'erreur
 - > 127 : message d'information
- code : contexte d'émission du message

(IPv6) Gestion des erreurs

- type = 1 : Destination inaccessible, code =
 - 0 : Aucune route vers la destination
 - 1 : La communication avec la destination est administrativement interdite
 - 2 : Hors de portée de l'adresse source
 - 3 : Adresse inaccessible
 - 4 : Numéro de port inaccessible
- type = 2 : Paquet trop volumineux
- type = 3 : Temps dépassé, code =
 - 0 : Limite du nombre de sauts atteinte
 - 1 : Temps de réassemblage dépassé
- type = 4 : Erreur de paramètre, code =
 - 0 : Champ d'en-tête erroné
 - 1 : Champ d'en-tête suivant non reconnu
 - 2 : Option non reconnue

(IPv6) Informations sur le réseau

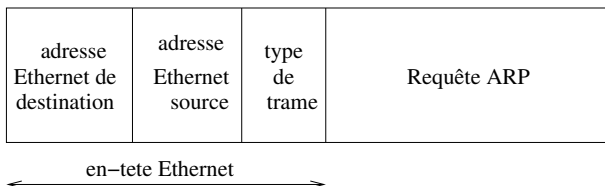
- 128 : Demande d'écho
- 129 : Réponse d'écho
- Découverte des voisins :
 - 133 : Sollicitation du routeur
 - 134 : Annonce du routeur
 - 135 : Sollicitation d'un voisin
 - 136 : Annonce d'un voisin
 - 137 : Redirection

Mise en correspondance des adresses

- À partir de l'adresse IP obtenir une adresse physique
 - coder l'adresse physique dans l'adresse IP (IPv6)
 - rechercher dynamiquement par diffusion
- Délivrer un message pour un hôte ne connaissant que l'adresse IP d'un autre hôte sur un même réseau physique
- Une solution pour la recherche dynamique :
 - les protocoles ARP et RARP (IPv4)
 - ICMP (IPv6)

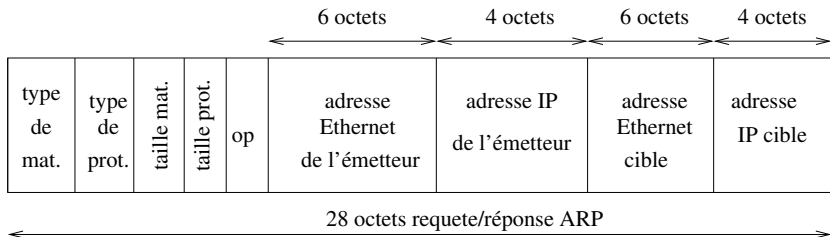
(IPv4) Protocole ARP

- *Address Resolution Protocol*
- Protocole adapté à différentes technologies réseaux
- Exemple dans le cas d'Ethernet et d'adresses IP



- type de trame : 0806 indiquant le protocole ARP
- adresse Ethernet de destination :
FF:FF:FF:FF:FF:FF pour la diffusion sur le réseau

(IPv4) Protocole ARP pour Ethernet/IP



- type de materiel : 1 indiquant un interface Ethernet
- type de protocole : 0800 indiquant le protocole IP
- taille mat. : 6 octets des adresses Ethernet
- taille prot. : 4 octets des adresses IP
- op : 1 pour une requête ARP et 2 pour une réponse ARP

La recherche de l'adresse physique par diffusion

- L'hôte A recherche l'adresse physique d'un hôte B sur un même réseau physique à partir de l'adresse IP de B
 - ① A émet une requête en diffusion contenant son adresse physique et son adresse IP ainsi que l'adresse IP de B
 - ② Tous les hôtes du réseau (sauf A) mettent à jour leurs câches pour A
 - ③ B reconnaît son adresse IP et renvoie la trame Ethernet vers A avec son adresse physique
 - ④ Tous les hôtes du réseau (sauf B) mettent à jour leurs câches pour B
- Le câche des associations d'adresses physiques et IP met en œuvre des temporisateurs pour conserver la validité des données

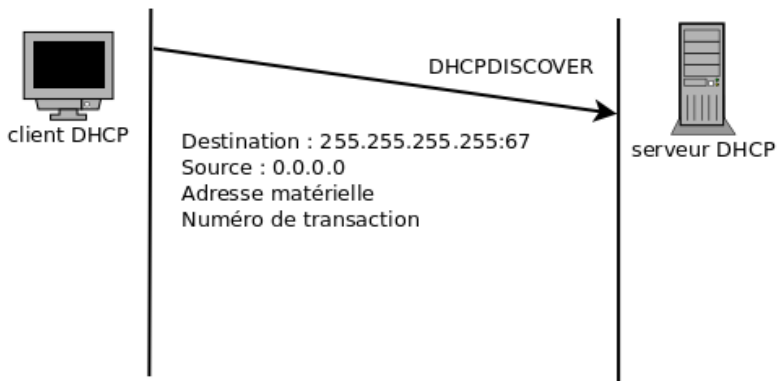
Autoamorçage et autoconfiguration

- RARP (*Reverse Address Resolution Protocol*)
 - protocole niveau liens
 - obtenir une adresse IP à partir d'une adresse matérielle
 - obtenir une adresse IP à partir d'un serveur
 - en diffusion sur le réseau
- BOOTP (*BOOTstrap Protocol*)
 - protocole niveau applicatif
 - obtenir une adresse IP à partir d'une adresse matérielle
 - obtenir une adresse IP statique à partir d'un serveur
 - maintien d'un fichier de correspondance entre les adresses matérielles et les adresses IP
 - démarrage des terminaux sans mémoire locale
 - basé sur le protocole UDP en diffusion
- DHCP (*Dynamic Host Configuration Protocol*)

(IPv4) DHCP

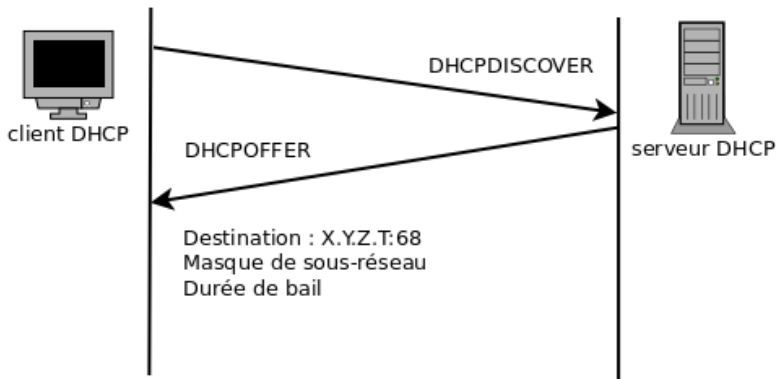
- protocole niveau applicatif
- obtenir une adresse IP dynamique à partir d'un serveur DHCP
- obtenir des adresses de serveurs de noms de domaines
- basé sur le protocole UDP en diffusion
- adapté aux connections ponctuelles et nomades
 - allocation fixée lors de la première connexion
 - allocation à durée limitée avec bail

(IPv4) Acquisition DHCP d'une adresse IP avec bail



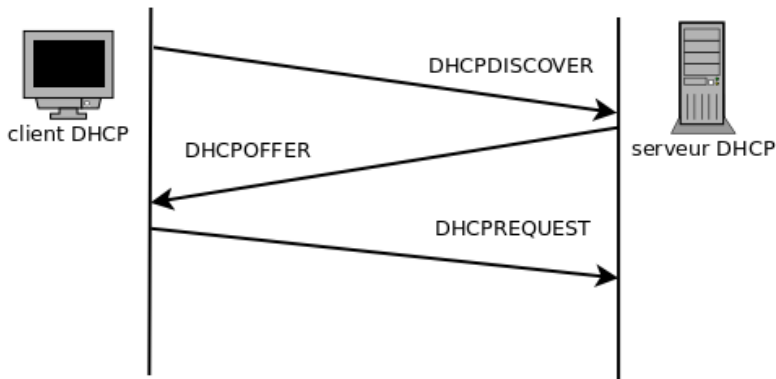
- 67 : port UDP du serveur

(IPv4) Acquisition DHCP d'une adresse IP avec bail



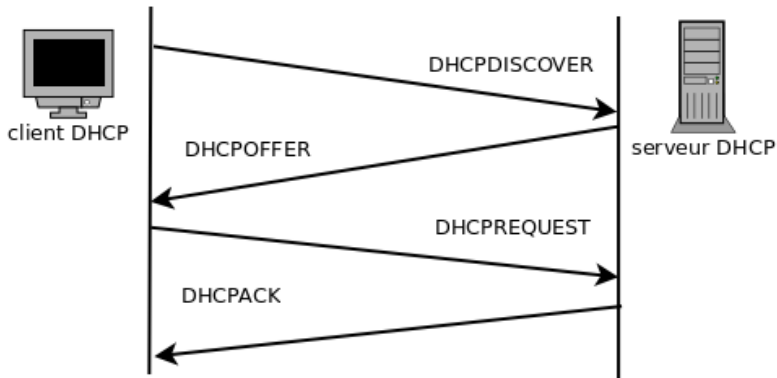
- 68 : port UDP du client

(IPv4) Acquisition DHCP d'une adresse IP avec bail



- Acceptation de la proposition par le client

(IPv4) Acquisition DHCP d'une adresse IP avec bail

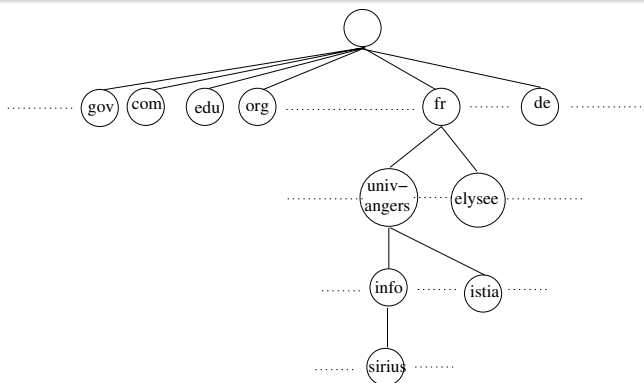


- Confirmation du bail par le serveur au client
- Réserve par le serveur de l'adresse IP pour le temps du bail

Système de noms de domaines

- Nommage plus mnémotechnique que des adresses IP
- DNS (*Domain Name System*)
- correspondance entre nom de machine et numéro IP
- Espace de noms hiérarchisé (arborescent)
 - racine de nom vide
 - nom de chaque nœud de 63 caractères maximum
 - majuscules et minuscules indifférenciées
- une zone est un sous-arbre
- un nom de domaine est la concaténation du nom du nœud avec celui de ses ancêtres
- pas de sémantique nécessairement géographique

Système de noms de domaines

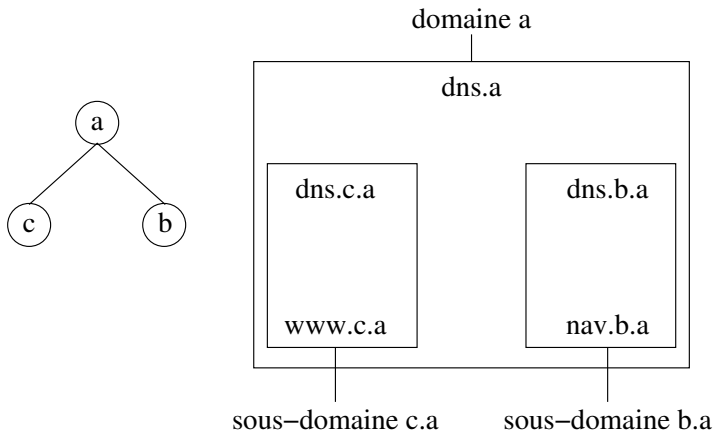


- l'ICANN (*Internet Corporation for Assigned Names and Numbers*) qui gère l'adressage et les noms de domaine
- l'AFNIC (Association Française pour le Nommage Internet) assure la gestion pour le .fr

Résolution de nom

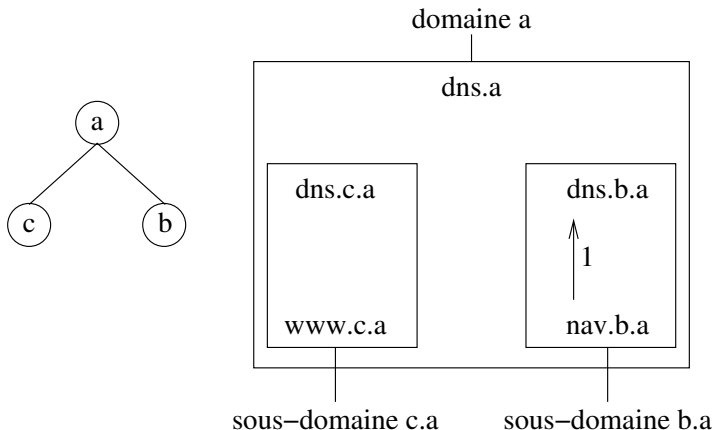
- Résolution de nom : mise en correspondance d'un nom avec une adresse IP
- Base de donnée distribuée sur les serveurs de noms
 - un serveur primaire
 - des serveurs secondaires en cas de panne
- serveur en mode non récursif ou itératif
 - renvoie l'adresse IP si le nom appartient au sous-domaine qu'il gère
 - renvoie l'adresse IP si le nom appartient à son cache
 - sinon le serveur indique au client un autre serveur de noms.
- serveur en mode récursif ou complet
 - renvoie l'adresse IP si le nom appartient au sous-domaine qu'il gère
 - renvoie l'adresse IP si le nom appartient à son cache
 - sinon le serveur interroge d'autres serveurs de noms et retransmettra la réponse

Résolution de nom en mode non récursif



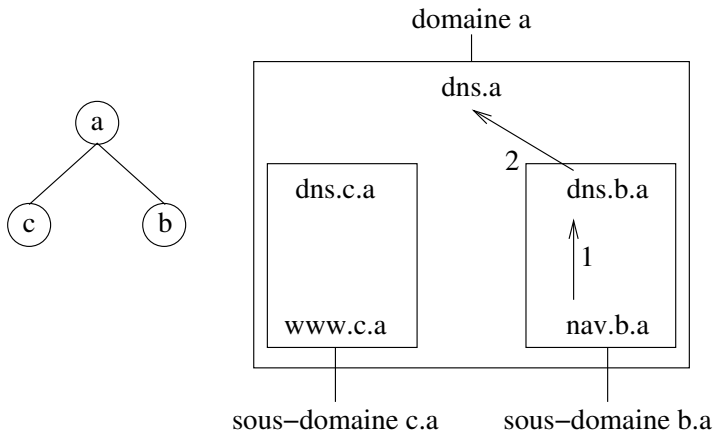
Le navigateur sur machine *nav.b.a* cherche à se connecter au serveur web *www.c.a*.

Résolution de nom en mode non récursif



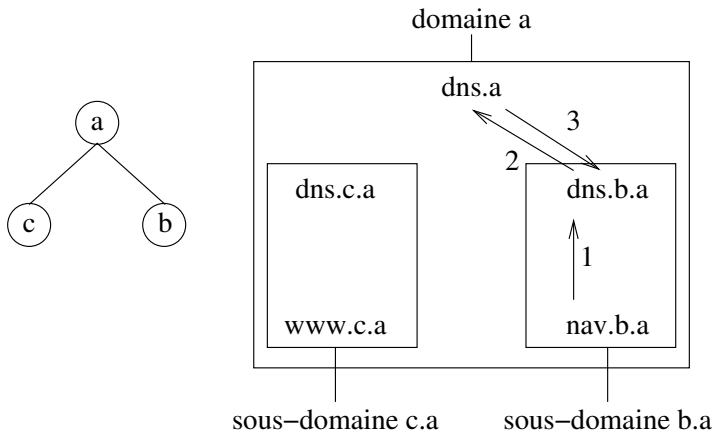
Le navigateur transmet à son DNS *dns.b.a* une requête de résolution du nom *www.c.a*.

Résolution de nom en mode non récursif



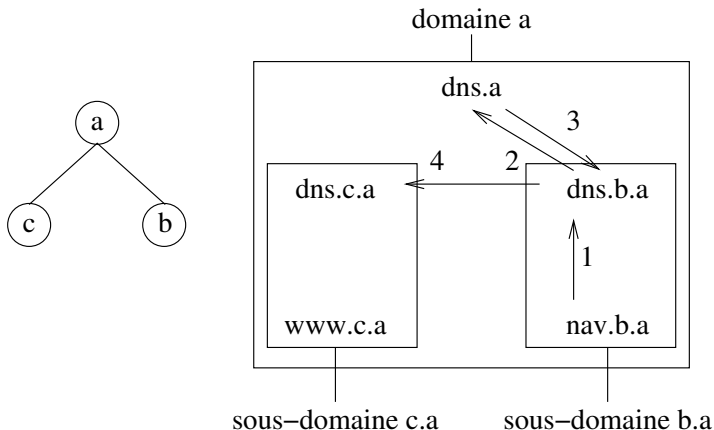
Le DNS *dns.b.a* ne connaissant pas *www.c.a* transmet la requête au DNS *dns.a*.

Résolution de nom en mode non récursif



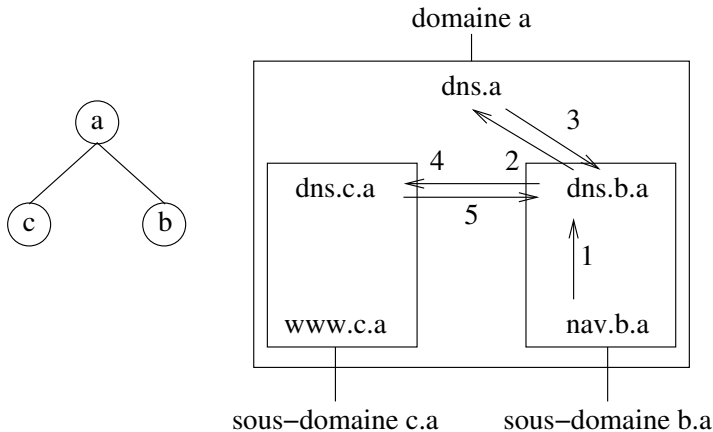
Le DNS *dns.a* ne connaissant pas *www.c.a* transmet au DNS *dns.b.a* l'adresse du DNS *dns.c.a*.

Résolution de nom en mode non récursif



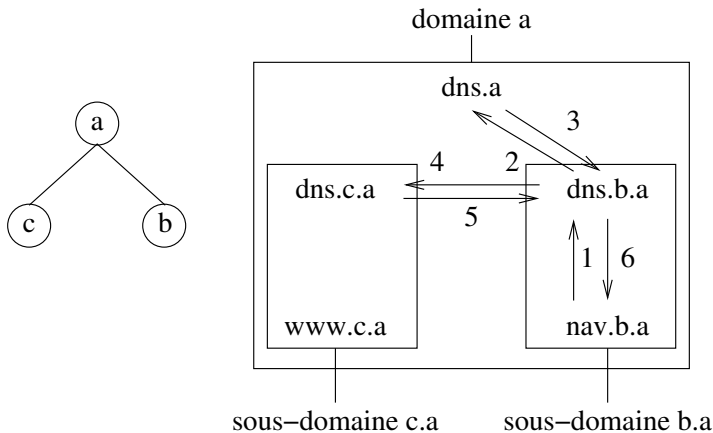
Le DNS *dns.b.a* transmet au DNS *dns.c.a* une requête de résolution du nom *www.c.a*.

Résolution de nom en mode non récursif



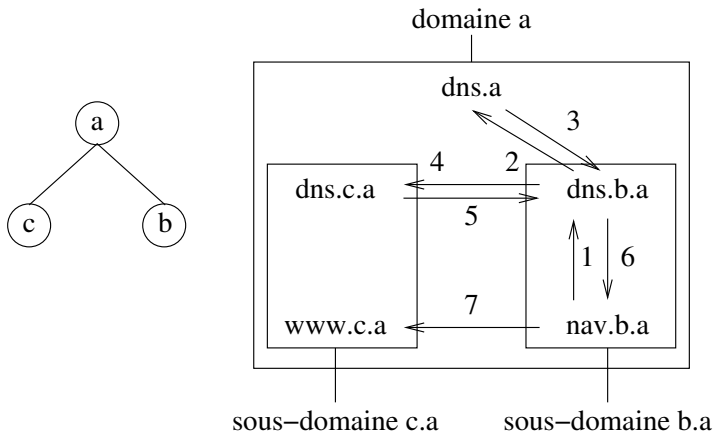
Le DNS *dns.c.a* reconnaît le nom *www.c.a*, mémorise l'adresse IP et le nom dans son cache et transmet l'adresse IP de *www.c.a* au DNS *dns.b.a*.

Résolution de nom en mode non récursif



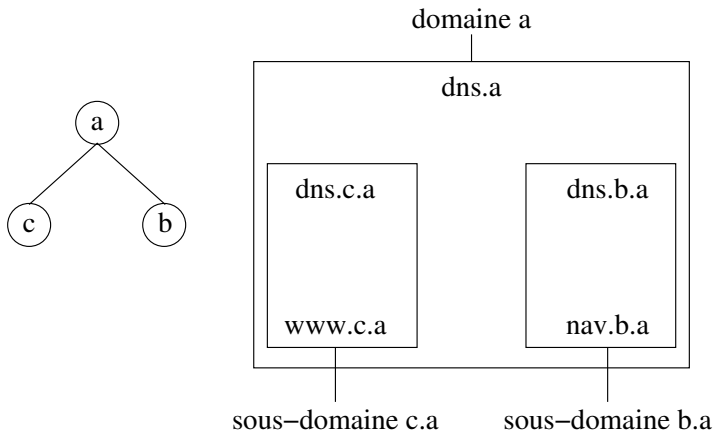
Le DNS *dns.b.a* mémorise l'adresse IP et le nom dans son cache et transmet l'adresse IP au navigateur de la machine *nav.b.a*.

Résolution de nom en mode non récursif



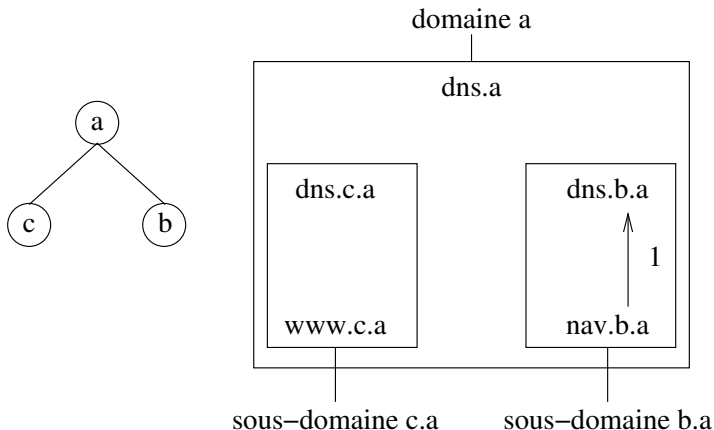
La machine *nav.b.a* se connecte au serveur *www.c.a*.

Résolution de nom en mode récursif



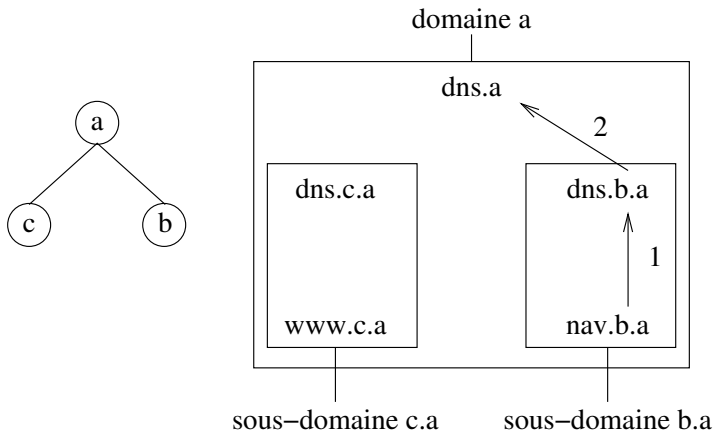
Le navigateur sur la machine *nav.b.a* cherche à se connecter au serveur web *www.c.a*.

Résolution de nom en mode récursif



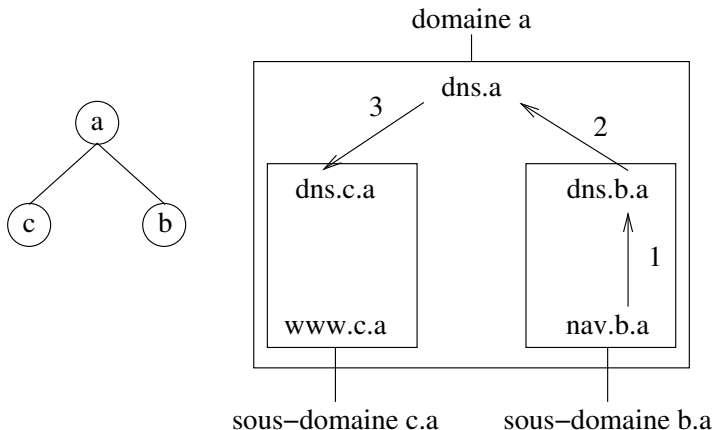
Le navigateur transmet à son DNS *dns.b.a* une requête de résolution du nom *www.c.a*.

Résolution de nom en mode récursif



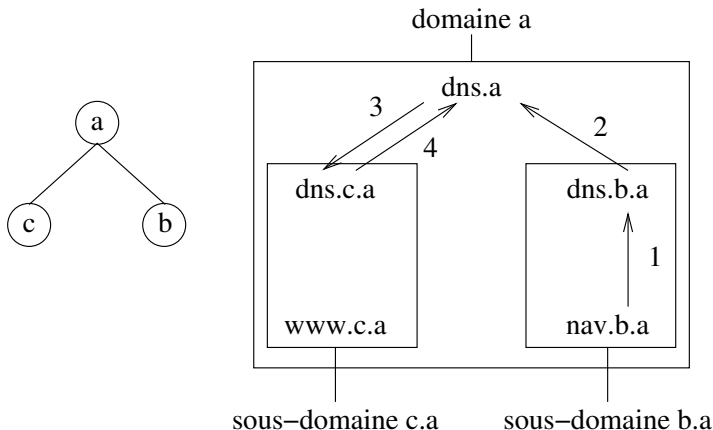
Le DNS *dns.b.a* ne connaissant pas *www.c.a* transmet la requête au DNS *dns.a*.

Résolution de nom en mode récursif



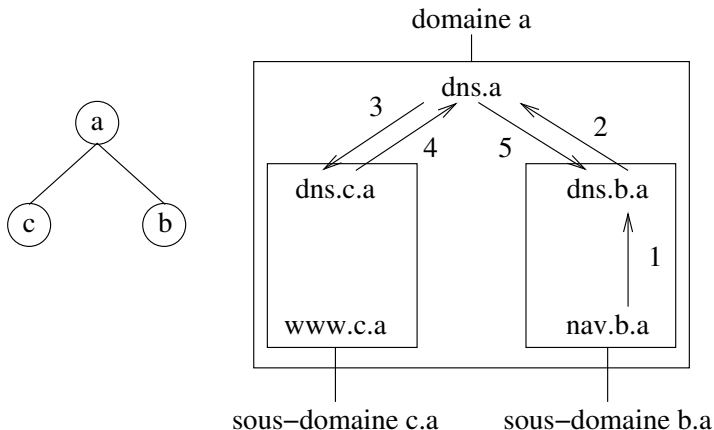
Le DNS *dns.a* ne connaissant pas *www.c.a* transmet la requête au DNS *dns.c.a*.

Résolution de nom en mode récursif



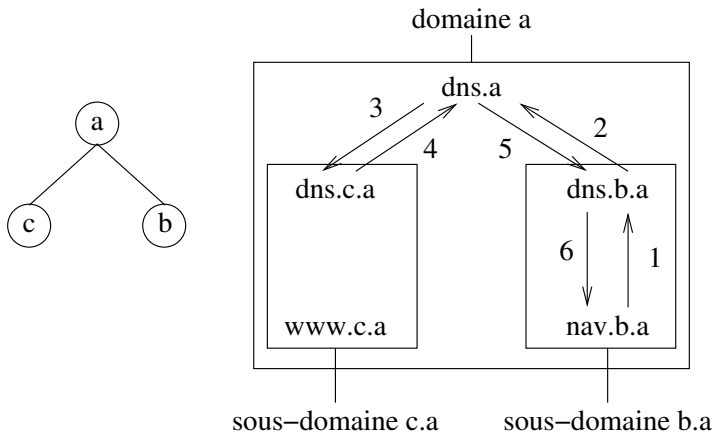
Le DNS *dns.c.a* reconnaît le nom *www.c.a*, mémorise l'adresse IP et le nom dans son cache et transmet l'adresse IP au DNS *dns.a*.

Résolution de nom en mode récursif



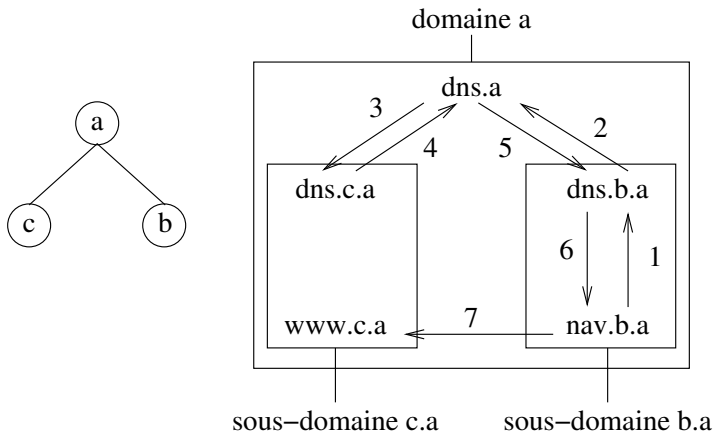
Le DNS *dns.a* mémorise l'adresse IP et le nom dans son cache et transmet l'adresse IP au DNS *dns.b.a*.

Résolution de nom en mode récursif



Le DNS *dns.b.a* mémorise l'adresse IP et le nom dans son cache et transmet l'adresse IP au navigateur de la machine *nav.b.a*.

Résolution de nom en mode récursif



La machine *nav.b.a* se connecte au serveur *www.c.a*.

Acheminement ou routage

- Choisir la manière de transmettre les datagrammes IP à travers divers réseaux interconnectés
 - Routeur : ordinateur dédié à l'acheminement connecté à au moins deux réseaux
 - Router : réémettre des datagrammes reçus par une interface vers une autre interface
 - Table de routages : liste de quadruplets (*Destination*, *Passerelle*, *Masque*, *Interface*) :
 - *Destination* : identifiant d'un réseau (ou adresse IP d'un hôte)
 - *Passerelle* : adresse IP du prochain routeur
 - *Masque* : masque associé au réseau destination
 - *Interface* : interface (physique) de sortie
- + un quadruplet par défaut

« Routage par sauts successifs » (*next-hop routing*)

- Conservation des données relatives aux réseaux :
 - Peu volumineux
 - Très efficace
- Une source de difficultés :
 - Ensemble d'un trafic pour une même direction emprunte (sauf incident) le même chemin
 - Seul le dernier routeur a connaissance de l'existence effective de l'hôte destination
 - Existence effectivement d'un chemin retour pour des communications bidirectionnelles
- Pas de modification de l'entête du datagramme (sauf pour le TTL et le checksum)

La remise d'un datagramme

- remise directe : d'un interface du réseau à l'interface final destinataire d'un même réseau
- remise indirecte : via (au moins) un routeur
- remise directe en Ethernet :
 - Mettre en correspondance l'adresse IP avec l'adresse physique
 - Encapsuler le datagramme dans une trame Ethernet
 - Emettre la trame sur le réseau
- Détection de la présence de deux hôtes sur un même réseau par comparaison des adresses IP (et des masques d'identifiants de réseau)
- Pour deux hôtes sur deux réseaux distincts : passage via un routeur

Établissement d'une table de routage

- Statique
 - Configuration par défaut
 - Grâce à une redirection ICMP
- Dynamique
 - Protocoles entre routeurs
 - IGP (*Interior Gateway Protocol*) à l'intérieur des systèmes autonomes
 - RIP
 - SPF (*Shortest Path First*) : par état de liens
 - BGP (*Border Gate Protocol*) entre systèmes autonomes

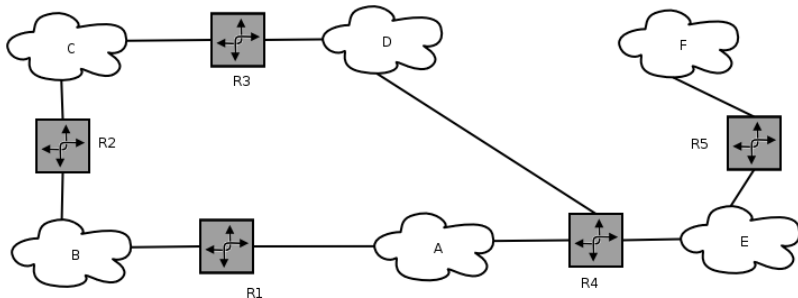
RIP

- *Routing Information Protocol*
- Protocole à vecteur de distance (des distances entre routeurs et destinations)
- Métrique : nombre de sauts (entre 1 et 15, 16 pour l'infini)
- Encapsulation UDP
- À l'initialisation : requête en broadcast via tous les interfaces de l'hôte demandant les tables de routage des voisins
- Annonces régulières et pour une modification d'une métrique
- Une annonce :
 - adresse de destination
 - nouvelle métrique
 - prochain routeur
 - des informations de temporisation

Bellman-Ford de plus court chemin

- Entrée inexistante dans la table et métrique finie alors entrée nouvelle :
 - adresse de destination
 - adresse du prochain routeur
 - métrique
 - temporisation armée
- Entrée présente mais ancienne métrique supérieure alors modification :
 - nouvelle métrique
 - adresse du nouveau prochain routeur
 - réinitialisation de la temporisation
- Entrée présente et émetteur de la réponse identique au prochain routeur alors modification :
 - nouvelle métrique
 - réinitialisation de la temporisation

Exemple avec RIP pour le routeur R1



destination	passerelle	métrique
A	direct	1
B	direct	1
C	R2	2
D	R2	3
E	R2	4

Exemple avec RIP pour le routeur R1

- Annonces de R4

destination	passerelle	métrique
C	R3	2
D	direct	1
E	direct	1
F	R5	2

- Nouvelle table pour R1

destination	passerelle	métrique
A	direct	1
B	direct	1
C	R2	2
D	R4	2
E	R4	2
F	R4	3

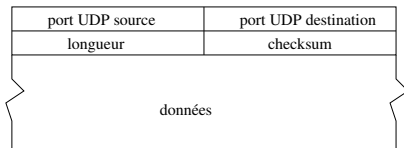
Les protocoles UDP et TCP

- Couche transport
- Utilisent la couche réseau IP
- UDP (*User Datagram Protocol*) : transport non fiable
- TCP (*Transmission Control Protocol*) : transport fiable

Protocole UDP

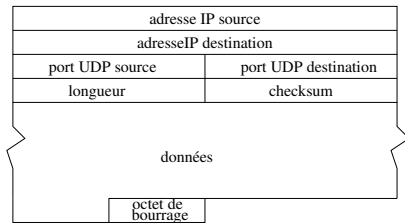
- UDP (*User Datagram Protocol*)
- Couche transport
- Utilise la couche réseau IP
- Transport non fiable
 - Pas d'accusé de réception
 - Pas de gestion des pertes, duplications, inversions, retards
 - Pas de contrôle de flux
 - Pas de contrôle d'erreurs obligatoire
- Introduction des « ports » : chaque application utilisant UDP le fait via un port qui identifie l'application

Datagramme UDP



- port UDP source sur 2 octets : identifie l'application source
- port UDP destination sur 2 octets : identifie l'application destinataire
- longueur sur 2 octets : taille de l'en-tête et des données
- checksum sur 2 octets : contrôle d'erreur (0 si non calculé)

Pseudo-entête et données pour le contrôle d'erreurs

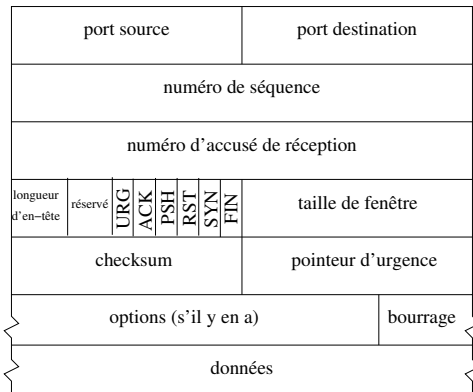


- Inutile sur un réseau très fiable
- Rajout des adresses IP de la source et de la destination en une pseudo en-tête (dialogue avec la couche IP)
- 1 octet de bourrage éventuel pour atteindre un alignement sur 16 bits

Protocole TCP

- TCP (*Transmission Control Protocol*)
- Couche transport
- Utilise la couche réseau IP
- Transport fiable
- Données non interprétées par TCP
- Service de flux d'octets « orienté connexion » :
 - Relation client/serveur
 - Établissement d'une connexion avant tout dialogue
 - Connexion bidirectionnelle simultanée (*full duplex*)
- Les 3 missions de TCP :
 - Établir une connexion
 - Transférer les données
 - Libérer une connexion

Paquet TCP



En-tête paquet TCP

- port TCP source sur 2 octets : identifie l'application source
- port TCP destination sur 2 octets : identifie l'application destinataire
- numéro de séquence : position dans le flux d'octets du premier octet de données du paquet
- numéro d'accusé de réception : position dans le flux d'octets du premier octet de données du prochain paquet attendu

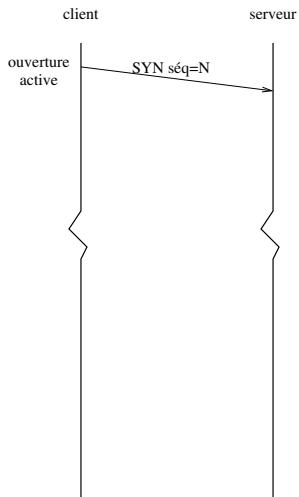
En-tête paquet TCP

- longueur d'en-tête sur 16 bits en multiples de 4 octets
- réservé : 6 bits réservés à un usage ultérieur
- bits de code :
 - URG : le pointeur d'urgence est valide
 - ACK : le numéro d'accusé de réception est valide
 - PSH : le paquet requiert un envoie immédiat
 - RST : réinitialiser la connexion
 - SYN : synchroniser les numéros de séquence pour initialiser la connexion
 - FIN : l'émetteur a atteint la fin de son flot de données

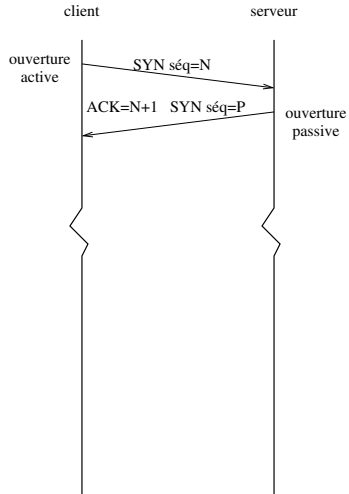
En-tête paquet TCP

- taille de fenêtre : nombre d'octets que le récepteur est prêt à accepter
- checksum sur 2 octets : contrôle d'erreurs obligatoire avec pseudo en-tête
- pointeur d'urgence : décalage ajouté au numéro de séquence pour indiquer le dernier octet de données urgentes
- options
- bourrage : pour aligner sur 32 bits

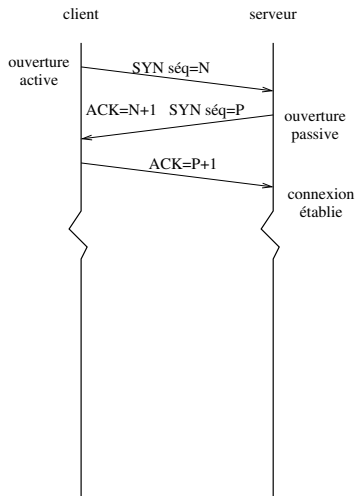
Connexion TCP



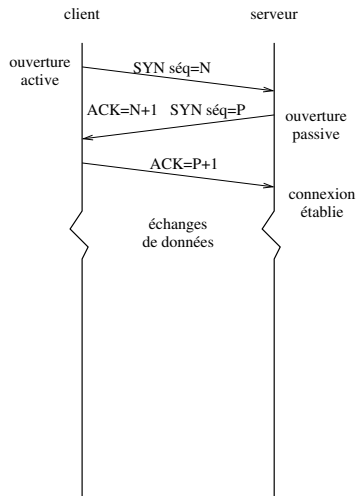
Connexion TCP



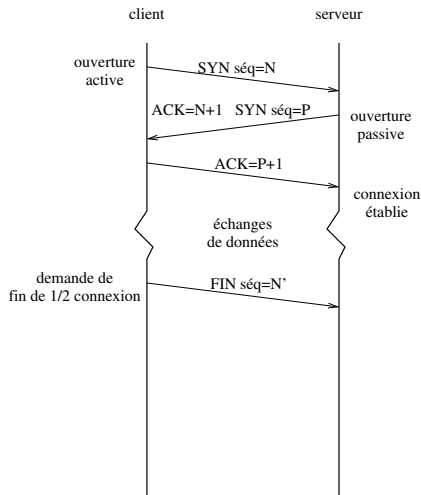
Connexion TCP



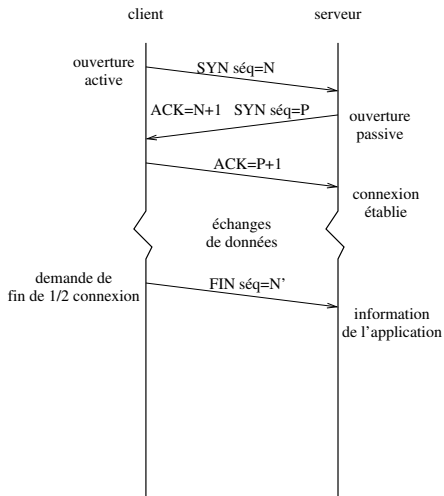
Connexion TCP



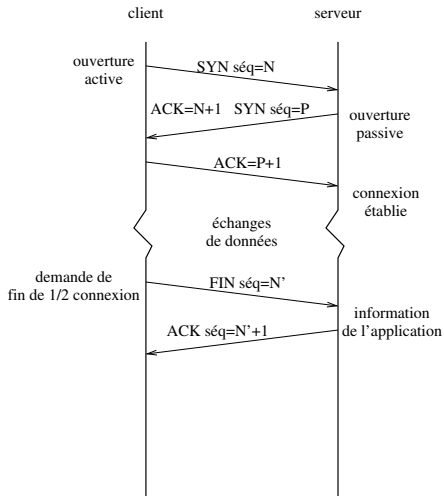
Connexion TCP



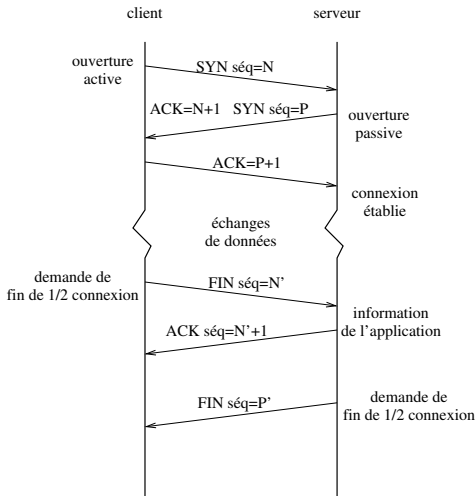
Connexion TCP



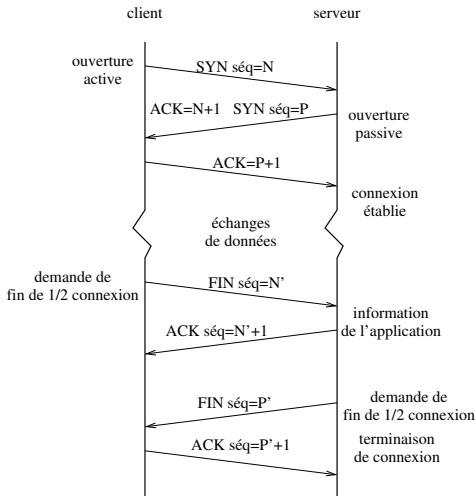
Connexion TCP



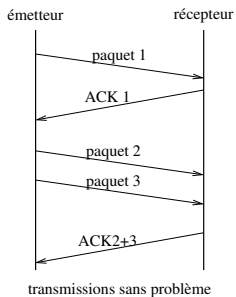
Connexion TCP



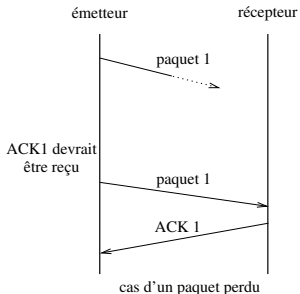
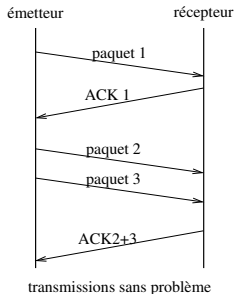
Connexion TCP



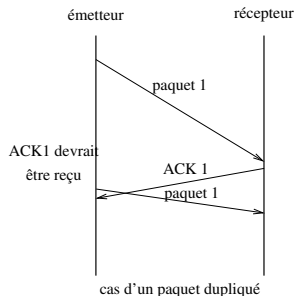
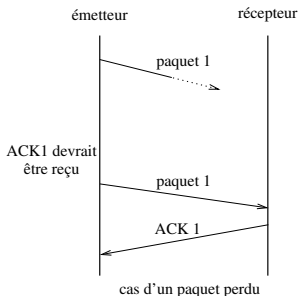
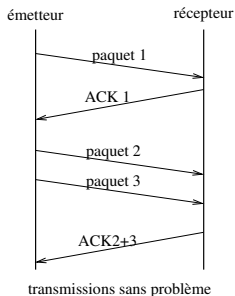
Fiabilité par accusé de réception



Fiabilité par accusé de réception



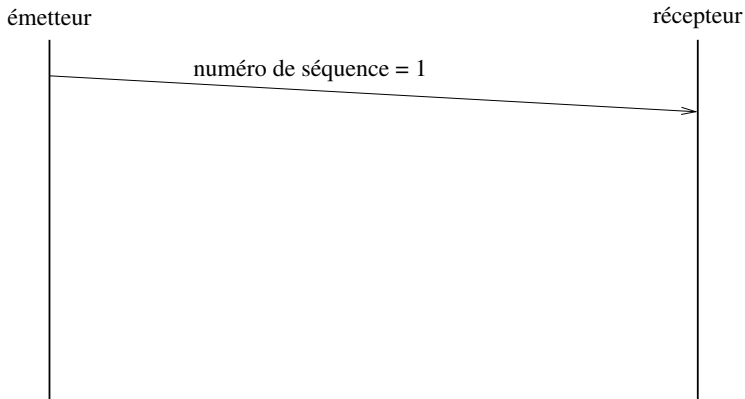
Fiabilité par accusé de réception



- Temporisateur pour réémettre les paquets
 - perdus
 - dont l'acquittement n'arrive pas (ou après expiration du temporisateur)

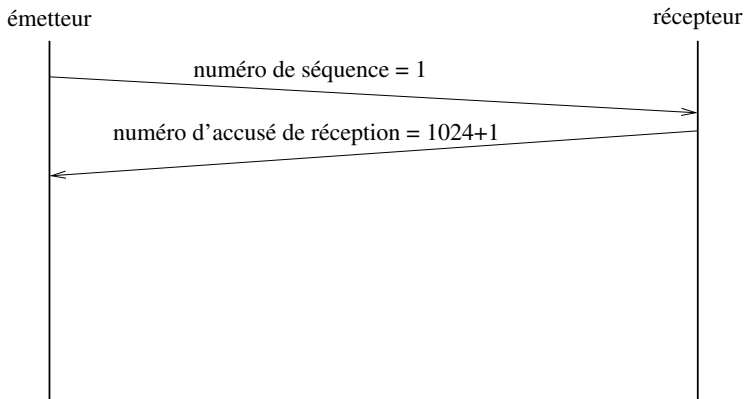
Acquittement par ensemble du flot de données

taille des données = 1024 octets



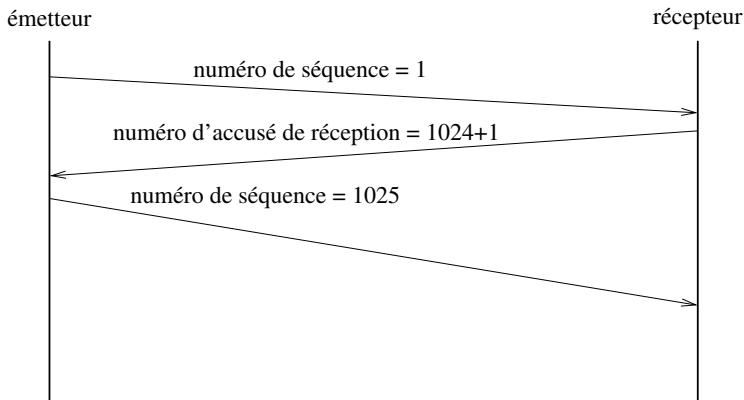
Acquittement par ensemble du flot de données

taille des données = 1024 octets



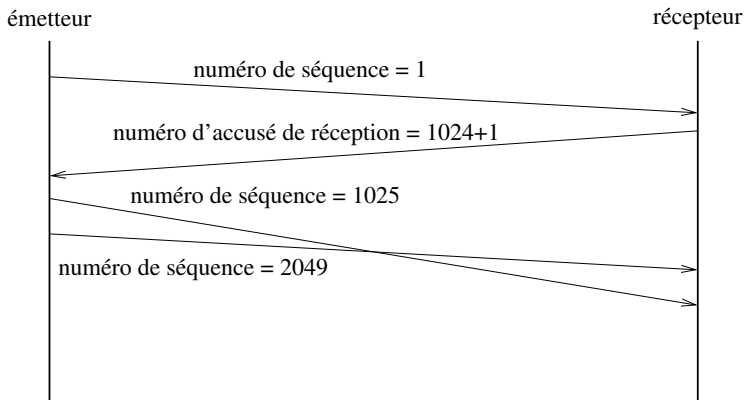
Acquittement par ensemble du flot de données

taille des données = 1024 octets



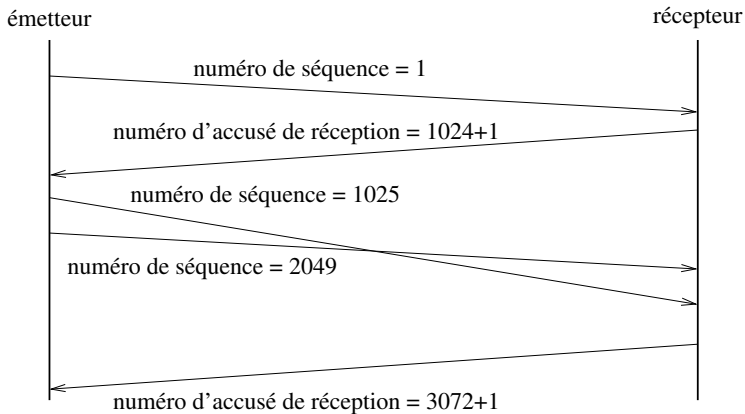
Acquittement par ensemble du flot de données

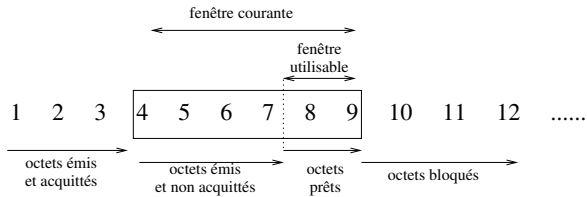
taille des données = 1024 octets



Acquittement par ensemble du flot de données

taille des données = 1024 octets





Fenêtre glissante

