



## Partie 7 : Internet et l'architecture TCP/IP

Olivier GLÜCK

Université LYON 1 / Département Informatique

Olivier.Gluck@univ-lyon1.fr

<http://perso.univ-lyon1.fr/olivier.gluck>

### Copyright

- Copyright © 2021 Olivier Glück; all rights reserved
- Ce support de cours est soumis aux droits d'auteur et n'est donc pas dans le domaine public. Sa reproduction est cependant autorisée à condition de respecter les conditions suivantes :
  - Si ce document est reproduit pour les besoins personnels du réproducteur, toute forme de reproduction (totale ou partielle) est autorisée à la condition de citer l'auteur.
  - Si ce document est reproduit dans le but d'être distribué à des tierces personnes, il devra être reproduit dans son intégralité sans aucune modification. Cette notice de copyright devra donc être présente. De plus, il ne devra pas être vendu.
  - Cependant, dans le seul cas d'un enseignement gratuit, une participation aux frais de reproduction pourra être demandée, mais elle ne pourra être supérieure au prix du papier et de l'encre composant le document.
  - Toute reproduction sortant du cadre précisé ci-dessus est interdite sans accord préalable écrit de l'auteur.

Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux

2

### Remerciements

- Certains transparents sont basés sur des supports de cours de :
  - Danièle DROMARD (PARIS 6)
  - Andrzej DUDA (INP Grenoble/ENSIMAG)
  - Shivkumar KALYANARAMAN (RPI/ECSE)
  - Alain MILLE (LYON 1)
  - CongDuc PHAM (LYON 1)
  - Michel RIVEILL (Université de Nice/ESSI)
  - L'Institut National des Télécommunications (INT)
  - Cisco Networking Academy
- Des figures sont issues des livres cités en bibliographie

Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux

3

### Bibliographie

- « Réseaux », 4ième édition, Andrew Tanenbaum, Pearson Education, ISBN 2-7440-7001-7
- « Réseaux et Télécoms », Claude Servin, Dunod, ISBN 2-10-007986-7
- « Analyse structurée des réseaux », 2ième édition, J. Kurose et K. Ross, Pearson Education, ISBN 2-7440-7000-9
- « TCP/IP Illustrated Volume 1, The Protocols », W. R. Stevens, Addison Wesley, ISBN 0-201-63346-9
- « TCP/IP, Architecture, protocoles, applications », 4ième édition, D. Comer, Dunod, ISBN 2-10-008181-0
- « An Engineering Approach to Computer Networking », Addison-Wesley, ISBN 0-201-63442-6
- Internet...
  - <http://www.guill.net/>
  - <http://www.courseforge.org/courses/>
  - <http://www.commentcamarache.net/ccm/doc/>
  - <http://www.rfc-editor.org/> (documents normatifs dans TCP/IP)

### Bibliographie

- « Réseaux », 4ième édition, Andrew Tanenbaum, Pearson Education, ISBN 2-7440-7001-7
- « Réseaux et Télécoms », Claude Servin, Dunod, ISBN 2-10-007986-7
- « Réseaux locaux et Internet, des protocoles à l'interconnexion », 3ième édition, Laurent Toutain, Hermès Science, ISBN 2-7462-0670-6
- « An Engineering Approach to Computer Networking », Addison-Wesley, ISBN 0-201-63442-6
- Internet...
  - <http://www.guill.net/>
  - <http://www.courseforge.org/courses/>
  - <http://www.commentcamarache.net/ccm/doc/>
  - <http://www.protocols.com/>
  - [http://dir.yahoo.com/Computers\\_and\\_Internet/](http://dir.yahoo.com/Computers_and_Internet/)
  - <http://www.rfc-editor.org/> (documents normatifs dans TCP/IP)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

5

### Plan de la partie 7

- Description générale
- Adressage dans l'Internet (IPv4)
- Le protocole IP (IPv4)
- Les protocoles de routage de l'Internet
- Protocoles de contrôle de l'Internet et les utilitaires réseaux
- Le protocole IPv6
- Les protocoles de transport
- Exemples de connexion à Internet

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

6

## Description générale

Visage de l'Internet  
 Architecture TCP/IP  
 Protocoles et applications  
 Identification des protocoles et applications

## Historique et acronymes

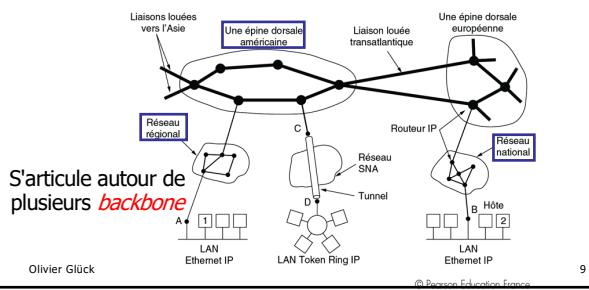
- Architecture développée par la DARPA (*Defence Advanced Research Project Adgency*), milieu des années 1970
- IP : *Internet Protocol* - résout les problèmes d'interconnexion en milieu hétérogène (1974)
- TCP : *Transmission Control Protocol* - protocole de transport de l'Internet (de bout en bout)
- TCP/IP est intégré à Unix BSD 4 (Berkeley) en 1980
- TCP/IP est intégré à ARPANET en 1983
- Aujourd'hui, TCP/IP est devenu le standard d'Internet (*Internet pour Inter-Networking*)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

8

## Le visage de l'Internet (1)

- Un ensemble de sous-réseaux indépendants (*Autonomous System*) et hétérogènes qui sont interconnectés (organisation hiérarchique)



## Le visage de l'Internet (2)

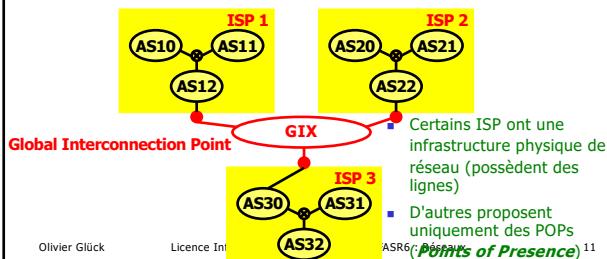
- Trois types de systèmes autonomes
  - les AS de transit (*backbone*) (réseaux régionaux, nationaux, ...) qui acceptent de faire transiter des paquets d'autres AS
    - parfois avec certaines restrictions
    - souvent moyennant finance
  - les puits (*stubs*) : réseaux sans issue qui ne peuvent acheminer aucun trafic externe
  - les AS multi-connectés qui peuvent être utilisés pour du transit, sauf indication contraire (mais ce n'est pas leur rôle premier)
- **Peering** : accords de transit entre ISP -> points d'interconnexion privés

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

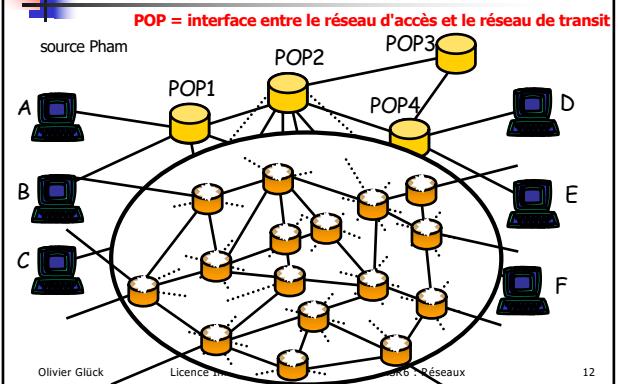
10

## Le visage de l'Internet (3)

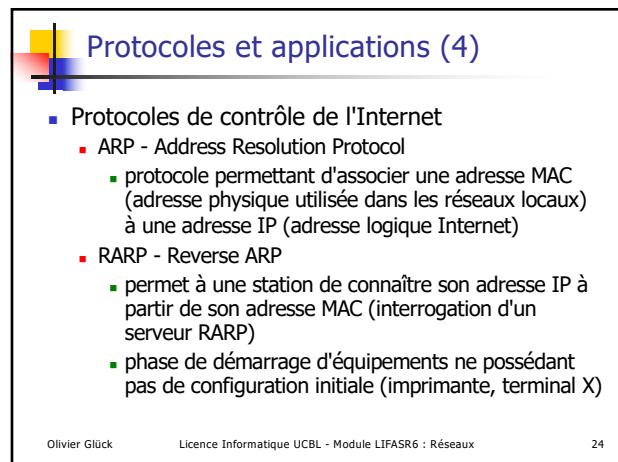
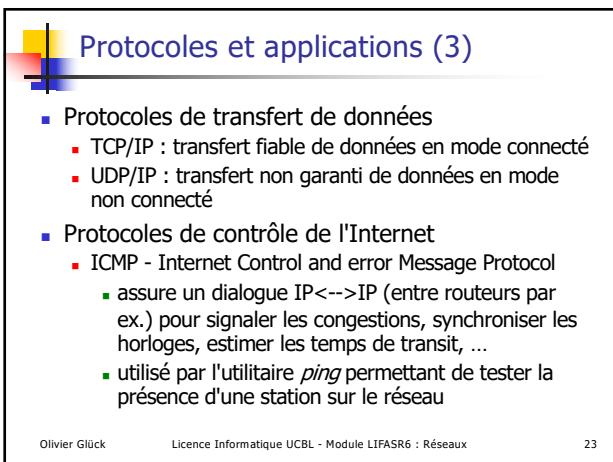
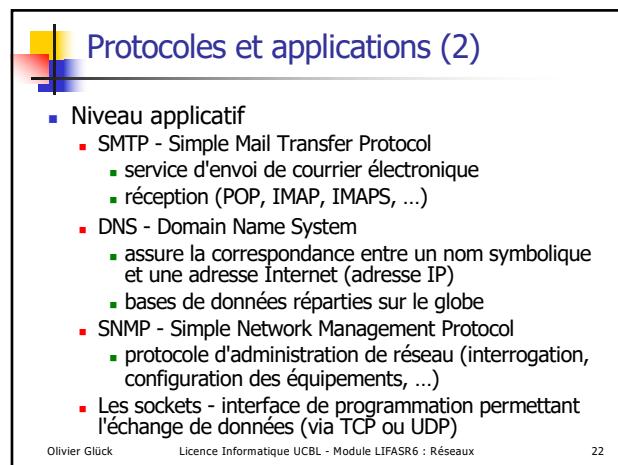
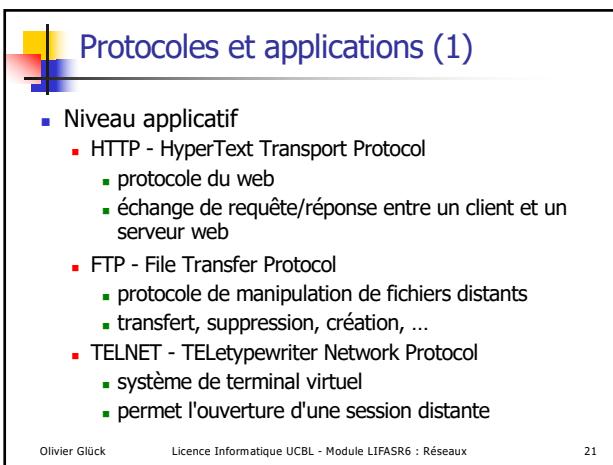
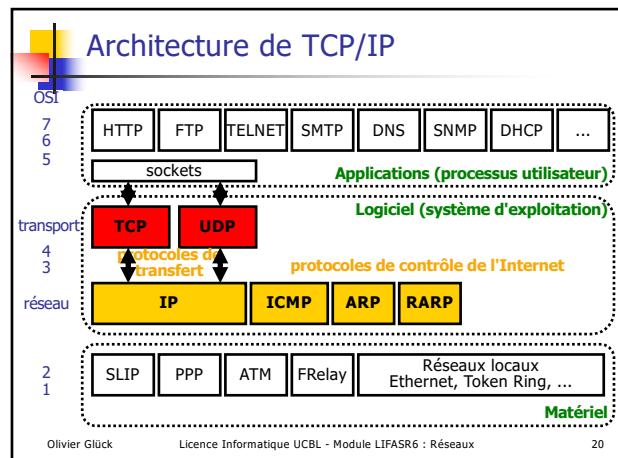
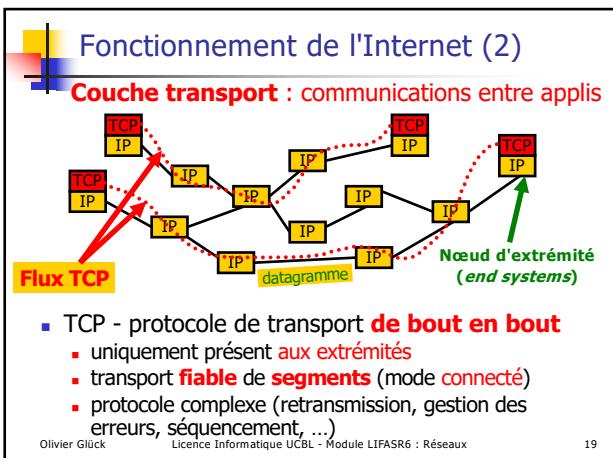
- ISP - Internet Service Provider
  - un ou plusieurs systèmes autonomes
  - un AS = ensemble de réseaux/routeurs sous la même autorité d'administration (entreprise, campus, ...)



## Le visage de l'Internet (4)







## Protocoles et applications (5)

- Protocoles de contrôle de l'Internet
  - BOOTP - Boot Protocol
    - permet à une station de connaître sa configuration réseau lors du démarrage par interrogation d'un serveur *bootp*
    - au-dessus d'UDP (ports 67 et 68)
  - DHCP - Dynamic Host Configuration Protocol
    - extension du protocole BOOTP
    - meilleure gestion du plan d'adressage IP avec attribution dynamique des adresses IP pour une certaine durée (bail ou *lease time*)
    - au-dessus d'UDP (ports 67 et 68)

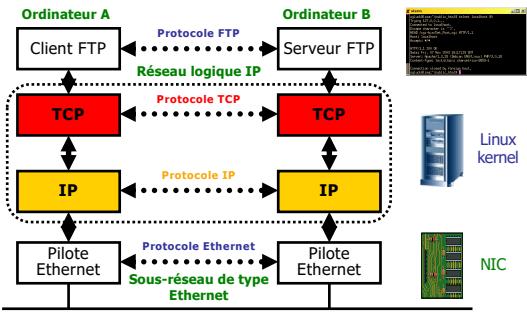
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

25

## Communications sans routeur

- Deux machines sur un même sous réseau



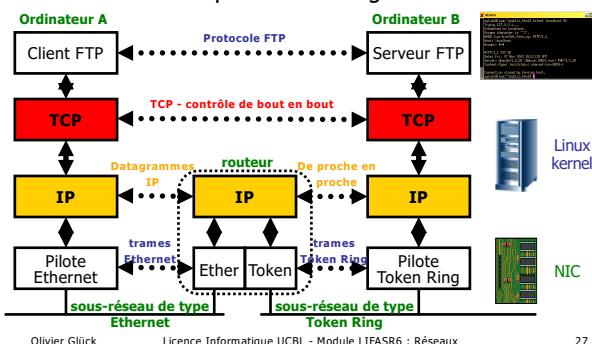
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

26

## Communications avec routeur(s)

- Prise en compte de l'hétérogénéité

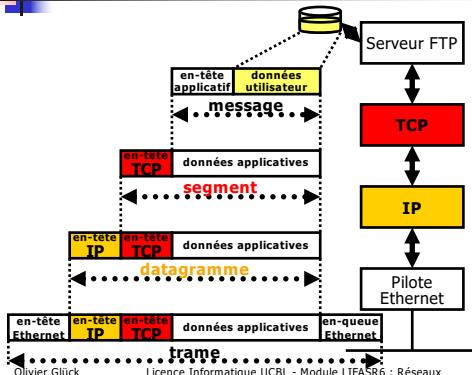


Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

27

## Encapsulation



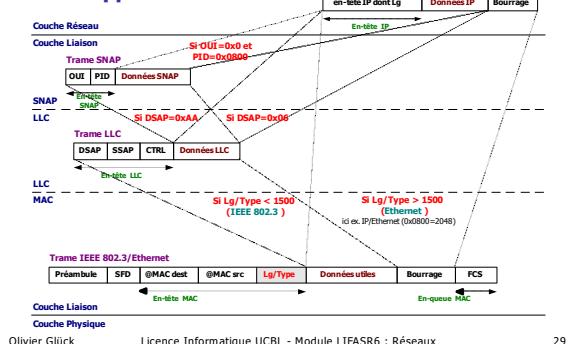
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

28

## Identification des protocoles (1)

### Rappel

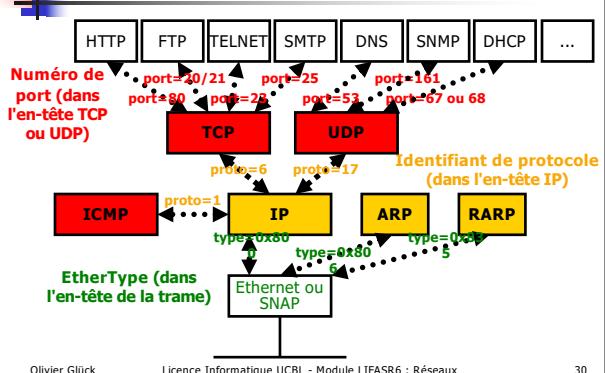


Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

29

## Identification des protocoles (2)



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

30

## Identification des protocoles (3)

- Une adresse de transport = une adresse IP + un numéro de port (16 bits) + TCP ou UDP -> adresse de socket
- Une connexion TCP s'établit entre une socket source et une socket destinataire -> une connexion = un quadruplé (@IPsrc, port src, @IPdest, port dest)
- Deux connexions peuvent aboutir à la même socket
- Les ports permettent un multiplexage ou démultiplexage de connexions au niveau transport
- Les ports inférieurs à 1024 sont appelés **ports réservés**

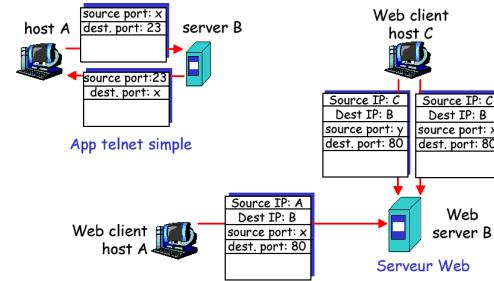
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

31

## Identification des protocoles (4)

### Multiplexage/démultiplexage: exemples



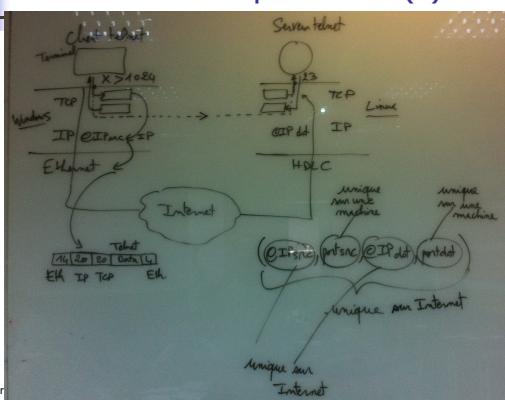
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

32

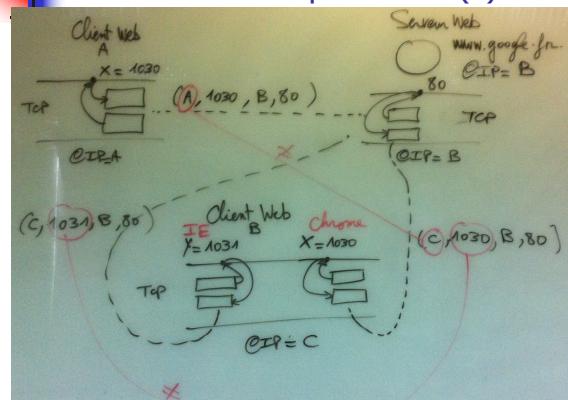
## Identification des protocoles (4)

Olivier Glück



33

## Identification des protocoles (4)



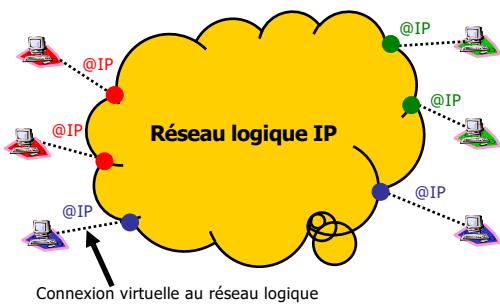
34

## Adressage dans l'Internet (IPv4)

- Format de l'adresse IPv4
- Les classes d'adressage
- Adresses IP particulières
- Adresses privées et NAT
- Les sous-réseaux
- Adressage géographique (CIDR)



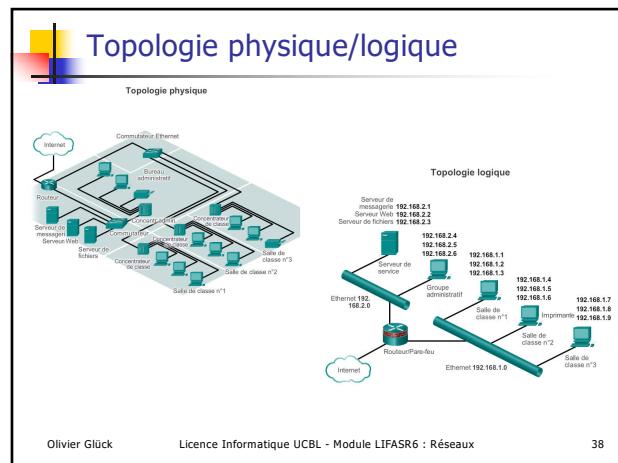
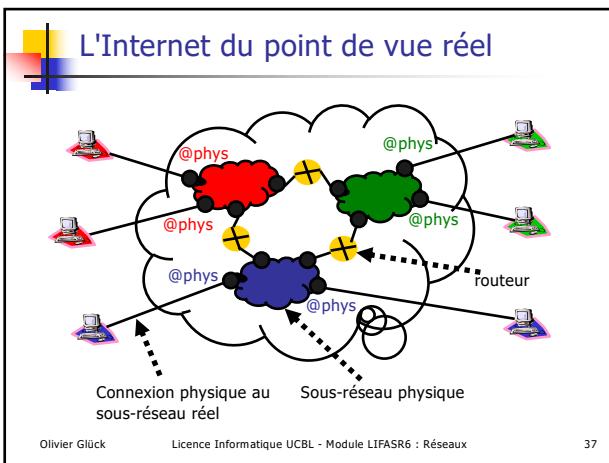
## L'Internet du point de vue utilisateur



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

36



- ## Format de l'adresse IP
- L'internet se décompose en plusieurs réseaux logiques IP
  - L'adresse IP est composée de deux champs
    - NET\_ID : identifiant du réseau IP (utilisé pour le routage)
    - HOST\_ID : identifiant de la machine dans le réseau IP
- NET ID    HOST ID**
- réseau logique IP ..... machine
- Adresse IP = 32 bits = 4 octets (représentée par 4 valeurs décimales [0-255] séparées par un .)
- Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      39

## Les classes d'adressage

Classe	Réseau	Hôte	Plage des adresses d'hôtes
A	0		1.0.0.0 à 127.255.255.255
B	10		128.0.0.0 à 191.255.255.255
C	110		192.0.0.0 à 223.255.255.255
D	1110	Adresse multicast	224.0.0.0 à 239.255.255.255
E	1111	Réserve pour une utilisation future	240.0.0.0 à 255.255.255.255

© Pearson Education France

- Les adresses réseaux sont distribuées par un organisme international à but non lucratif : ICANN (Internet Corporation for Assigned Names and Numbers) puis décentralisé au niveau de chaque pays

Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      40

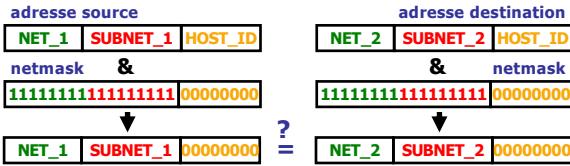
- ## Adresses IP particulières
- Diffusions locale et distante
    - 255.255.255.255 : adresse de broadcast sur le réseau IP local (ne passe pas le routeur, traduit en broadcast ARP)
    - <NET\_ID><111...111> : adresse de broadcast dirigée vers le réseau de numéro NET\_ID (exemple : 132.227.255.255 = diffusion dans le réseau 132.227.0.0 traduit en broadcast ARP par le routeur destination)
  - Rebouclage local (*loopback*) : 127.x.y.z
    - généralement 127.0.0.1 (*localhost*)
    - permet de tester la pile TCP/IP locale sans passer par une interface matérielle
  - l'adresse 0.0.0.0
    - utilisée par le protocole RARP (@IP de démarrage)
    - adresse de la route par défaut dans les routeurs
- Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      41

- ## Les adresses privées et le NAT (1)
- Adresses privées (RFC 1918)
    - des adresses qui ne seront jamais attribuées (adresses illégales) et qui ne sont pas routables sur l'Internet
    - classe A : de 10.0.0.0 à 10.255.255.255
    - classe B : de 172.16.0.0 à 172.31.255.255
    - classe C : de 192.168.0.0 à 192.168.255.255
  - Si une entreprise qui utilise des adresses privées souhaitent tout de même disposer d'une connexion à l'Internet, il faut
    - demander une adresse publique
    - faire des conversions adresse privée <--> adresse publique
- Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      42



## Les sous-réseaux (3)

- Détermination du sous-réseau : ET logique avec le netmask



- le netmask permet de savoir si la machine source et destination sont sur le même sous-réseau
- la classe d'adressage permet de savoir si elles sont sur le même réseau

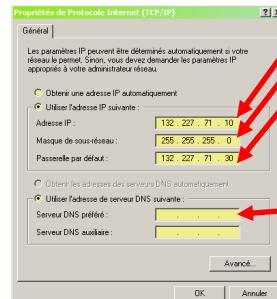
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

49

## Configuration réseau

- Pour une machine d'extrémité, il suffit d'indiquer



son adresse IP  
le masque de sous-réseau  
l'adresse IP du routeur par défaut (tous les paquets qui ne sont pas à destination du même sous-réseau sont envoyés vers ce routeur)  
éventuellement, un serveur de noms

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

50

## L'adressage géographique - CIDR (1)

- Routage inter-domaine sans classe - *Classless InterDomain Routing* - RFC 1519, 1466
  - pour répondre (partiellement) aux problèmes de pénurie d'adresses de classe B et d'explosion des tables de routage
  - idée : allouer les adresses IP restantes sous la forme de blocs de taille variable (sans considération de classe) en tenant compte de la localisation géographique
  - > évite le gaspillage : si un site a besoin de 2000 adresses, 2048 lui sont attribuées
  - > agrégation de routes (plusieurs réseaux peuvent être regroupés sous le même identifiant)
  - > les tables de routage doivent alors contenir un masque de sous-réseau pour l'acheminement (il n'y a pas de masque implicite indiqué par la classe)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

51

## L'adressage géographique - CIDR (2)

- Exemple d'agrégation de 2 adresses de classe C :
  - une entreprise a besoin de 510 adresses IP -> deux adresses de classe C
    - 193.127.32.0 netmask 255.255.255.0
    - 193.127.33.0 netmask 255.255.255.0
  - les réseaux 193.127.32.0 et 193.127.33.0 sont agrégés en 193.127.32.0 netmask 255.255.254.0
  - ce qui se note 193.127.32.0/24 + 193.127.33.0/24 = 193.127.32.0/23 (préfixe/nb\_bits du masque à 1)
  - dans une table de routage, cela représente les deux réseaux 193.127.32.0 et 193.127.33.0

193.127.32.0	11000001.01111111.00100000.00000000
193.127.33.0	11000001.01111111.00100001.00000000
193.127.32.0 / 23	11000001.01111111.00100000.00000000

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

52

## L'adressage géographique - CIDR (3)

- Allocation géographique des adresses restantes Europe (194-195), Amérique du nord (198-199), Amérique du sud (200-201), Pacifique (202-203), Afrique (99-?)  
-> 194 et 195 ont les 7 premiers bits identiques donc il suffit d'indiquer aux routeurs (hors Europe) : 194.0.0.0/7
- Autres exemples (source L. Toutain)

société	nb d'adresses	nb de classes C	adresse de début	adresse de fin	adresse de début	netmask	netmask en binaire	
A	< 2048	8	192.24.0	192.24.7	192.24.0	255.255.248.0	255.255.1111.1000.0	192.24.0.0/21
B	< 4096	16	192.24.16	192.24.31	192.24.16	255.255.240.0	255.255.1111.0000.0	192.24.16.0/20
C	< 1024	4	192.24.8	192.24.11	192.24.8	255.255.252.0	255.255.1111.1100.0	192.24.8.0/22
D	< 1024	4	192.24.12	192.24.15	192.24.12	255.255.252.0	255.255.1111.1100.0	192.24.12.0/22
E	< 512	2	192.24.32	192.24.33	192.24.32	255.255.254.0	255.255.1111.1110.0	192.24.32.0/23
F	< 512	2	192.24.34	192.24.35	192.24.34	255.255.254.0	255.255.1111.1110.0	

53

## L'adressage géographique - CIDR (4)

- Conclusions
  - il n'y a plus de notion de classes et de sous-réseaux
  - une plage d'adresses est désignée par
    - un "network-prefix" : des bits désignant le réseau
    - un "host-number" : des bits désignant la machine
  - > un réseau est désigné par une adresse IP et une longueur de préfixe réseau
    - 132.227.0.0 n'a pas de sens
    - 132.227.0.0/16 ou 132.227.0.0/23 ont un sens
  - une table de routage peut contenir les deux destinations précédentes : la route avec le préfixe le plus long ("the longest matching network prefix") est choisie si une destination correspond aux deux entrées (ici 132.227.0.0/23)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

54

## Numérotation des sous-réseaux

- Peut-on mettre dans SUBNET\_ID tous les bits à 1 ou tous les bits à 0 ?
  - exemple : 10.0.0.0 avec *netmask* 255.192.0.0 (2 bits pour numérotter les sous-réseaux)  
--> 10.0.0.0, 10.64.0.0, 10.128.0.0, 10.192.0.0
- La RFC 950 (1985 - définition des SR) dit que cela n'est pas conseillé car
  - 10.0.0.0 désigne t-il le réseau 10.0.0.0 ou le sous-réseau ?
  - 10.255.255.255 désigne t-il le *broadcast* sur le réseau 10.0.0.0 ou sur le sous-réseau 10.192.0.0 ?
- Il n'y a plus d'ambiguïté avec CIDR (RFC 1812 -1995)
  - 10.0.0.0/8 et 10.0.0.0/10 ne désignent pas la même chose
- En pratique, on peut utiliser 10.0.0.0 et 10.192.0.0 !

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

55



## Le protocole IP (IPv4)

Datagramme IPv4

Fragmentation dans IP

Routage dans IP

Routage statique

## L'Internet Protocol

- IP (RFC 791) : protocole d'interconnexion de l'Internet
  - conçu pour transporter des datagrammes d'une certaine source A vers une destination B
  - A et B peuvent être sur le même réseau ou séparés par d'autres réseaux de nature très différentes
  - livraison au mieux - **best-effort delivery** : aucune garantie quant au service d'acheminement (délai, taux de perte, ...), aucune variable d'état
  - IP n'accomplit que trois tâches élémentaires :
    - adaptation des datagrammes IP à la MTU du réseau physique traversé
    - acheminement dans le réseau logique
    - désignation des noeuds (adressage IP)

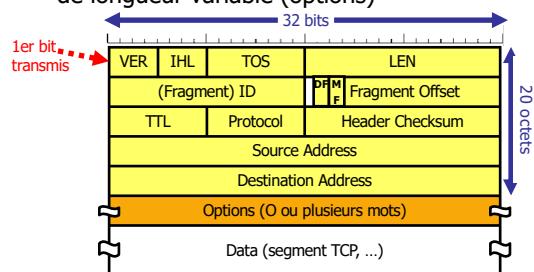
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

57

## Le datagramme IPv4 (1)

- Un en-tête de 20 octets + une partie facultative de longueur variable (options)



Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

58

## Le datagramme IPv4 (2)

- VER - Version - 4 bits
  - numéro de version d'IP (généralement 4 pour IPv4)
  - permet de faire cohabiter plusieurs versions (transition)
- IHL - Internet Head Length - 4 bits
  - longueur de l'en-tête du datagramme (en nombre de mots de 32 bits, 4 octets) -> 5 si pas d'option
  - valeur maximale = 15 -> 40 octets d'options maximum
- TOS - Type Of Service - 6+2 bits
  - pour distinguer différentes classes de services (niveaux de priorités) -> compromis entre fiabilité, délai et débit
  - champ ignoré par la plupart des routeurs

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

59

## Le datagramme IPv4 (3)

- LEN - total LENGTH field - 16 bits
  - longueur totale du datagramme en octets
  - au maximum 65535 octets
- ID - Identification - 16 bits
  - identifiant de datagramme (ou paquet)
  - tous les fragments d'un même paquet ont le même ID
- DF (1bit) et MF (1 bit)
  - DF - Don't Fragment : ordre au routeur de ne pas fragmenter (autre route ou destruction)
  - MF - More Fragment : indique qu'un fragment suit
- Fragment Offset - 13 bits
  - position du premier bit du fragment dans le datagramme d'origine, en multiple de 8 octets

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

60

## Le datagramme IPv4 (4)

- TTL - Time To Live - 8 bits
  - compteur qui sert à limiter la durée de vie du datagramme
  - 255 au départ puis décrémenté à chaque nouveau saut
  - datagramme éliminé s'il atteint zéro
  - évite les paquets perdus (erreurs de routage)
- Protocol - 8 bits
  - numéro du protocole destinataire (RFC 1700)
- Header Checksum - 16 bits
  - CRC sur l'en-tête uniquement
  - complément à 1 de la somme des demi-mots de 16 bits
  - doit être recalculé dès qu'une valeur change (ex. TTL) !

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

61

## Le datagramme IPv4 (5)

- Le champ Options
  - prévu pour des expérimentations mais peu utilisé dans la pratique
  - codé : <code option (1 octet)>, <longueur (1 octet)>, <données>
  - longueur variable, plusieurs options possibles
  - exemples d'options :
    - sécurité : degré de confidentialité du datagramme (route plus sécurisée que d'autres !)
    - routage strict par la source : suite d'@ IP décrivant le chemin pour atteindre la destination
    - enregistrement de route : les routeurs traversés insèrent chacun leur @IP

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

62

## La fragmentation des datagrammes IP

- Caractéristiques :
  - fragmentation non-transparente : réassemblage uniquement sur le destinataire
  - chaque fragment est acheminé de manière indépendante
  - temporisateur de réassemblage sur le destinataire quand le premier fragment arrive (décrémentation de TTL)
  - la perte d'un fragment IP provoque la retransmission de l'ensemble du datagramme

S'il y a une perte, elle ne sera détectée qu'au niveau TCP où la notion de fragments n'existe pas

Un routeur IP ne s'encombre pas de fragments qu'il ne peut réassembler

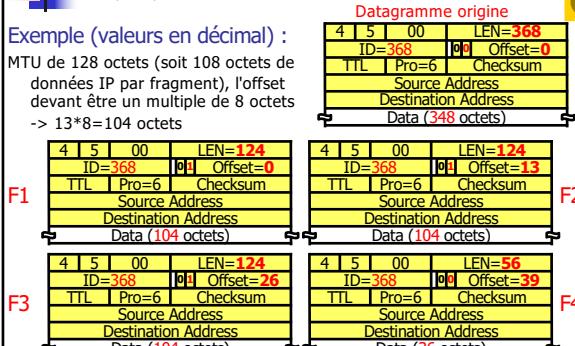
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

63

## La fragmentation des datagrammes IP

[http://wps.aw.com/aw\\_kurose\\_network\\_2/0,7240,227091-00.html](http://wps.aw.com/aw_kurose_network_2/0,7240,227091-00.html)



Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

64

## Le routage dans IP

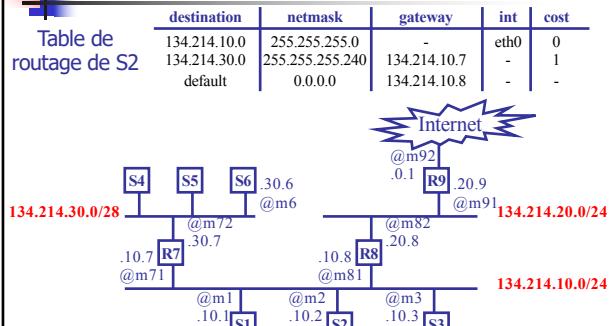
- Routeur :
  - passerelle entre sous-réseaux
  - une adresse IP par interface (par sous-réseau)
  - communications à l'intérieur d'un même sous-réseau sans passer par un routeur
  - acheminement à partir de l'@ destination (& logique avec le netmask de chaque entrée de la table de routage)
- Mise à jour de la table de routage :
  - Manuelle = **routage statique**
    - commande "route" des stations unix
    - langage de commande des routeurs (ip route ...)
  - Automatique = **routage dynamique**
    - processus sur les stations et les routeurs
    - échanges d'informations de routage : protocoles de routage

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

65

## Le routage dans IP - exemple



Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

66

## Routage statique

- La commande `ip route` permet d'indiquer une route :
  - vers un réseau (net) ou vers un équipement (host)
  - ou une route par défaut (default)
- Syntaxe :
 

```
ip route add [delete] [net|host]
           destination [default gateway metric]
```
- En général, sur les équipements non routeur, on définit uniquement une route par défaut

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

67

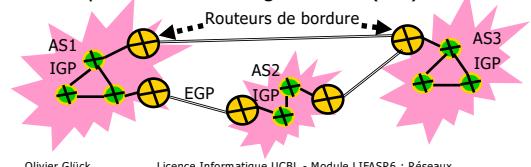


## Les protocoles de routage de l'Internet

Systèmes autonomes  
Routage interne : RIP et OSPF  
Routage externe : EGP et BGP

## Systèmes autonomes (rappels)

- Autonomous System (AS)
  - ensemble de réseaux et de routeurs sous une administration unique (entreprise, campus, réseau régional, cœur de réseau national, ...)
  - permet de limiter les échanges d'informations de routage
  - chaque AS se voit attribuer un numéro d'AS (16 bits)
  - > protocoles de routage internes (IGP) et externes (EGP)



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

70

## Protocoles de routage de l'Internet

- Protocoles de routage internes (intra-AS)
  - RIP** (RFC 1058), RIP-2 (RFC 1721 à 1724)
    - Routing Information Protocol
    - type vecteur de distance
  - OSPF** - Open Short Path First (RFC 2178)
    - type état de liens
- Protocoles de routage externes (inter-AS)
  - EGP** - Exterior Gateway Protocol (RFC 827)
    - premier protocole externe utilisé dans Internet
  - BGP** - Border Gateway Protocol (RFC 1771)
    - définit les échanges internes au domaine (iBGP) et externes (eBGP)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

71

## RIP - Principe

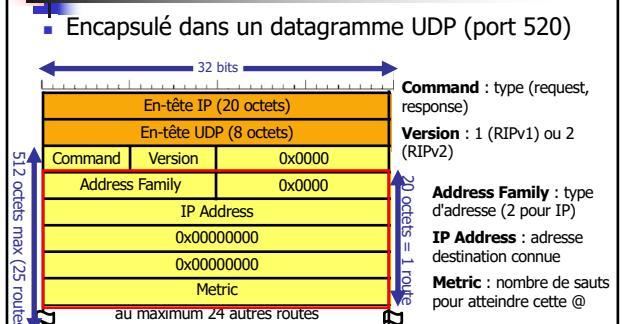
- Un nœud construit sa table de routage en fonction des vecteurs de distance reçus de ses voisins
- métrique = nombre de sauts (entre 1 et 15)
  - 16 = valeur maximum (représente l'infini)
  - utilisable uniquement à l'intérieur de domaines peu étendus
- Le routeur diffuse toutes les 30 secondes un message RIP à ses voisins contenant la liste des réseaux qu'il peut atteindre avec leur distance
  - si aucun message pendant 180s, route inaccessible (d=16)
- Implantation : démons *gated*, *routed*, *zebra* sous Unix ou matériel propriétaire (Cisco, ...)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

72

## RIP - Message RIPv1



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

73

## RIP - avantages/désavantages

- Avantages
  - très utilisé et très répandu sur tous les équipements
  - s'adapte automatiquement (panne, ajout de réseau, ...)
- Désavantages
  - la distance ne tient pas compte de la charge, du débit, du coût des lignes, ...
  - distance maximale = 15
  - trafic important (toutes les 30s) + temps de convergence
  - pas d'authentification des messages (attaques de routeurs en générant des "faux" messages RIP)
- Conclusion
  - utiliser RIP sur un petit réseau que l'on contrôle est très efficace mais pas adapté aux grands domaines

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

74

## RIP - RIPv2

- Remédie à certains inconvénients de RIPv1 en restant compatible (et en utilisant les champs 0x0)
  - permet le routage des sous-réseaux (véhicule le netmask dans le vecteur de distance)
  - diffusion multicast (224.0.0.9) : permet aux routeurs RIPv1 d'ignorer les messages RIPv2
  - possibilité d'authentification (cryptée ou non) des messages

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

75

## OSPF - Principe

- Routage à état des liens
  - chaque nœud
    - évalue le coût pour joindre ses voisins selon une certaine métrique (plusieurs métriques peuvent être utilisées simultanément)
    - construit un paquet contenant les infos relatives à chacun de ses liens (voisins)
    - le diffuse à tout le monde (par inondation)
    - calcule la route de moindre coût pour atteindre chaque entité du réseau
  - ensuite, les routeurs s'échangent uniquement les changements détectés dans la topologie
  - chaque nœud a une vision globale de la cartographie du réseau

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

76

## OSPF - Aires

- Le routage est hiérarchisé pour
  - limiter la diffusion (inondation)
  - réduire le temps de calcul des routes (*Dijkstra*)
- Un AS est divisé en aires (*area*) ou zones
  - une aire ne connaît que l'état des liaisons internes à l'aire
  - deux niveaux de routage : intra-area et inter-area
  - chaque aire est identifiée par un numéro sur 32 bits
- Ne pas confondre AS et aires
  - AS : un ou plusieurs réseaux sous une même autorité ; deux AS peuvent utiliser un protocole interne différent
  - Aire : toutes les aires OSPF utilisent le protocole OSPF

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

77

## OSPF - Hiérarchie des aires (1)

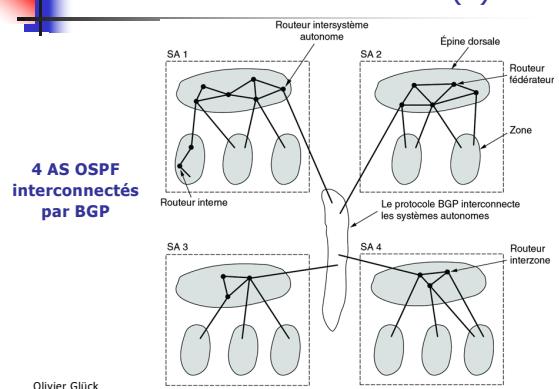
- Un AS contient une aire "épine dorsale" ou fédératrice (la zone 0.0.0.0) qui assure l'acheminement entre les autres aires
- Toutes les autres aires sont reliées à la zone *backbone* par au moins un routeur
- Chaque routeur qui est relié à deux zones ou plus fait partie de l'épine dorsale
- Trois catégories de routeurs
  - routeurs internes à une zone (50 max par zone)
  - routeurs fédérateurs ou inter-zones qui connectent au moins deux zones
  - routeurs inter-AS (routeurs de bordure) qui échangent les informations de routage entre les AS (BGP)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

78

## OSPF - Hiérarchie des aires (2)



Olivier Glück

© Pearson Education France

79

## OSPF - Hiérarchie des aires (3)

- Dans chaque zone, découverte de la topologie de la zone et calcul des plus courts chemins
- Les routeurs fédérateurs reçoivent les informations locales à leurs zones pour calculer la meilleure route pour atteindre chaque routeur de l'AS
- Cette information est ensuite communiquée à tous les routeurs inter-zones qui la répercutent au sein de leurs zones
- Si les réseaux et sous-réseaux d'une zone ont des adresses IP contigües, le routeur inter-zones ne signale qu'une seule route par agrégation

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

80

## OSPF - Types de messages

- 5 types de messages
  - message "Hello" : découvrir les voisins et déterminer le coût pour les joindre
  - message de "description de la base de données" : annonce les mises à jour dont le routeur dispose
  - message de "requête d'état de lien" : demande des informations à un routeur désigné
  - message de "mise à jour d'état de lien" : indique les coûts depuis le routeur émetteur vers ses voisins
  - message d'acquittement d'état de lien : acquittement d'une réception d'état de lien

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

81

## OSPF - Fonctionnement (1)

- A l'initialisation, avec des messages "Hello"
  - élection d'un **routeur désigné** dans chaque zone
    - chargé de la diffusion des informations dans la zone
    - permet de limiter les messages d'inondation
    - un routeur désigné de *backup* est également élu
    - chaque routeur envoie des messages "Hello" pour découvrir ses voisins
- Chaque routeur envoie ses états de liens au routeur désigné avec des messages "mise à jour d'état de lien"
  - après la découverte des voisins ou quand l'état d'un lien change
- Ces messages sont acquittés pour plus de fiabilité

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

82

## OSPF - Fonctionnement (2)

- Chaque message contient un numéro de séquence qui indique l'âge du message (permets de savoir quelle est l'information la plus récente)
- Les messages "description de base de données" contiennent les numéros de séquence de tous les états de lien connus du routeur émetteur du message
  - permet de savoir quel routeur détient l'information la plus récente
  - utilisés quand une liaison devient accessible
- Les messages "requête d'état de lien" permet à un routeur de demander au routeur désigné l'ensemble des états qu'il connaît

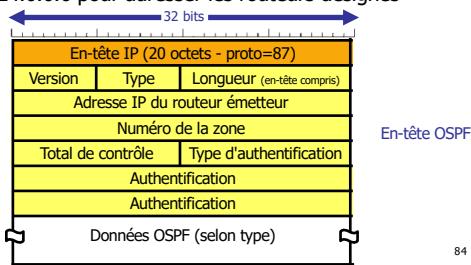
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

83

## OSPF - Message OSPF

- Directement au-dessus d'IP (proto=87)
- Adresses multicast
  - 224.0.0.5 pour adresser les routeurs de l'aire
  - 224.0.0.6 pour adresser les routeurs désignés



Olivier Glück

84

## OSPF - Conclusion

- Protocole complexe encore peu mis en œuvre mais
  - remède aux inconvénients de RIP
    - temps de convergence
    - OSPF adapté aux grands domaines
    - OSPF prend en compte plusieurs métriques
  - autres avantages d'OSPF
    - permet de router les sous-réseaux
    - peut assurer un routage différent selon le champ ToS IP (adapte le type de service demandé à la bonne métrique)
    - permet l'équilibrage de charge entre différentes routes de même coût
    - inclus un système d'authentification des messages

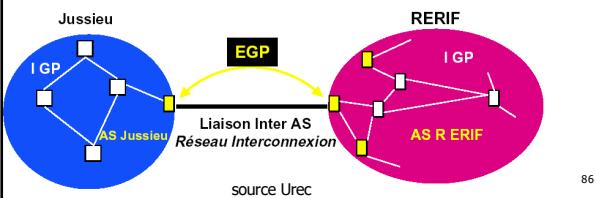
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

85

## EGP

- Premier protocole externe utilisé dans Internet (désormais remplacé par BGP)
- Echanges entre routeurs déclarés comme "pairs"
  - deux routeurs de bordure s'échangent à intervalles réguliers la liste des réseaux accessibles dans leur AS respective (pas de diffusion)
  - tout le trafic entre 2 AS passe par le même chemin physique



## BGP - Stratégies de routage

- Besoin de prendre en compte dans les stratégies de routage des considérations d'ordres
  - politique : certains AS peuvent refuser de faire transiter du trafic externe ou le trafic sortant de tel AS préfère transiter par tel AS que tel autre...
  - de sécurité : du trafic en provenance de tel AS ne doit pas transiter par tel AS
  - économique : la traversée d'une AS peut être payante...
- La prise en compte de ces stratégies ne fait pas partie du protocole (configuration manuelle des routeurs à l'aide de scripts)

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux

87

## BGP - Principe (1)

- Deux routeurs BGP établissent une connexion TCP pour s'échanger des infos de routage :
  - numéro de l'AS
  - liste des sous-réseaux de l'AS
  - distance relative vers chacun des sous-réseaux de l'AS
  - adresse IP du routeur (interne) d'accès à ces réseaux
- Quatre types de messages :
  - messages d'ouverture : ouverture d'une session BGP entre deux routeurs
  - messages de mise à jour : signaler à un *peer router* le changement d'état d'une route interne à l'AS
  - messages de notification : clore une session BGP
  - message "Hello" : message signalant que tout va bien au routeur voisin (*Keep Alive*)

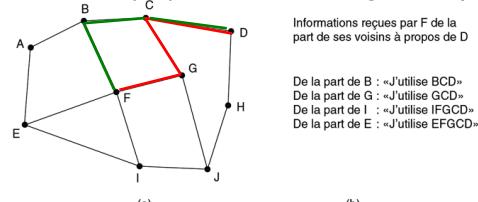
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

88

## BGP - Principe (2)

- Type vecteur de distance mais les paires s'échangent le chemin complet correspondant à chaque destination (pas uniquement le coût)
- Exemple : pour la destination D, F utilise actuellement FGCD et apprend d'autres routes de ses voisins (il peut alors choisir celle qu'il préfère selon la stratégie choisie)



Olivier Glück

© Pearson Education France 89

## Protocoles de contrôle de l'Internet et utilitaires réseaux



### ICMP

ping et traceroute

ARP et RARP

BOOTP et DHCP

Fichiers de config. et commandes UNIX

## ICMP - Internet Control Message Protocol

RFC 792

- Protocole de messages de contrôle de l'Internet
  - échange de messages entre routeurs : signaler une erreur réseau, demande d'information d'état, tests
  - utilisé par des utilitaires (*ping*, *traceroute*, *Network Time Protocol*)
  - permet de pallier au manque de service d'IP

Le champ **Code** : code d'erreur (fonction du type)

32 bits

En-tête IP (20 octets - proto=1)

Type Code Total de contrôle

Paramètres (optionnel)

Informations (en-tête datagramme IP en erreur + 64 1er bits du champ data)

Le champ **Type** :

0 : réponse d'Echo

3 : destination inconnue

4 : limitation du débit par la source

5 : redirection (ICMP redirect)

8 : demande d'Echo

11 : expiration de délai (TTL=0)

12 : en-tête IP invalide

13/14 : requête/réponse d'horodatage

17/18 : requête/réponse de netmask

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

91

## ICMP - Types de message

- réponse/demande d'Echo : utilisé par *ping*
- réponse/demande d'horodate : idem mais heures incluses pour mesures de performances
- destination inconnue : un routeur ne parvient pas à localiser la destination, problème de fragmentation (bit DF=1), ...
- délai expiré : paquet éliminé car TTL a atteint 0 (boucle, congestion, ...)
- en-tête IP invalide : la valeur d'un champ IP a une valeur illégale
- ICMP redirect : envoyé par un routeur à un nœud d'extrémité pour signaler une meilleure route (évite la mise à jour manuelle de toutes les tables de routage quand ajout d'un routeur...)
- ralentissement de la source : contrôle de congestion (mais quasiment plus utilisé car génération du trafic supplémentaire -> congestion au niveau TCP)
- autres messages : [www.iana.org/assignments/icmp-parameters](http://www.iana.org/assignments/icmp-parameters)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

92

## L'utilitaire ping

- Ping : envoi d'un écho, attente de réponse, mesure du temps aller-retour
  - teste l'accessibilité d'une destination **de bout en bout**
  - évaluation de performances
  - la réponse doit parvenir avant 20 secondes
- Exemples :
  - ping 127.0.0.1 : permet de tester la pile TCP/IP locale (en loopback)
  - ping mon@IP : permet de vérifier la configuration réseau locale de la station
  - ping @default-routeur : permet de tester la configuration du sous-réseau et de la passerelle
  - ping @dest : permet de tester un chemin de bout en bout

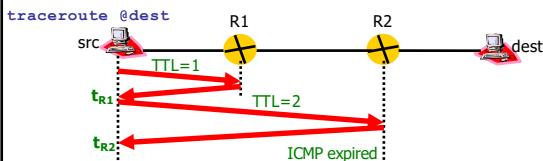
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

93

## L'utilitaire traceroute

- Permet de trouver pas à pas le chemin pour atteindre une destination
  - envoi d'un paquet IP avec TTL=1
  - attend ICMP délai expiré
  - envoi d'un paquet IP avec TTL=2, ...



Olivier Glück

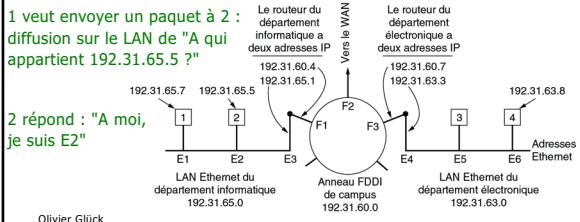
Licence Informatique UCBL - Module LIFASR6 : Réseaux

94

## ARP - Address Resolution Protocol

RFC 826

- Problème : les équipements de liaison (cartes réseau...) ne comprennent pas les adresses IP mais utilisent des adresses physiques (MAC)
- Besoin d'associer @MAC <-> @IP



Olivier Glück

© Pearson Education France

95

## ARP - Fonctionnement (1)

- Si la machine source et destinataire sont sur le même réseau (par ex. de 1 vers 2)
  - 1 - requête ARP (broadcast MAC)
  - 2 - réponse ARP (le destinataire a reçu le broadcast et s'est reconnu, il envoie son @MAC)
  - 3 - la source peut envoyer ses données vers le destinataire (adresse MAC destination connue)
- Si elles ne sont pas sur le même réseau (par ex. de 1 vers 4)
  - la diffusion ne passe pas le routeur
  - résolution de proche en proche : 1 envoie les données à 192.31.65.1 (ARP pour trouver E3), le routeur info envoie les données à 192.31.60.7 (ARP pour trouver F3), le routeur élec envoie les données à 4 (ARP pour E6)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

96

## ARP - Fonctionnement (2)

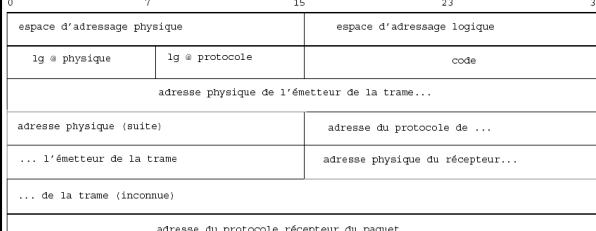
- Optimisations
  - Cache ARP : le résultat de chaque résolution est conservé localement pour les émissions suivantes
  - la correspondance (@IP, @MAC) de l'émetteur sont inclus dans la requête ARP pour que le récepteur, voire toutes les machines qui reçoivent le broadcast, mettent à jour leur cache
- Proxy ARP : une machine qui répond à une requête à la place du destinataire (qui ne reçoit pas le broadcast)
  - nécessaire si la route (adresse de la passerelle) pour atteindre le destinataire n'est pas connue

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

97

## ARP - Format du paquet

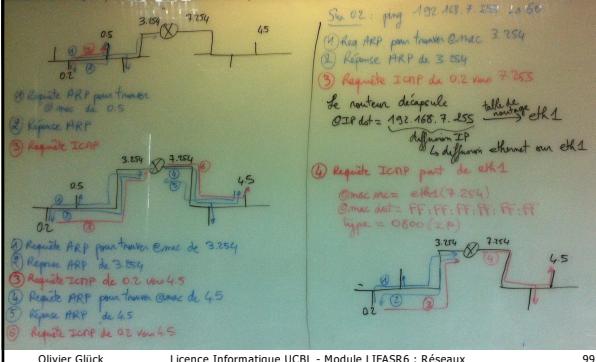


Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

98

## ARP - ICMP

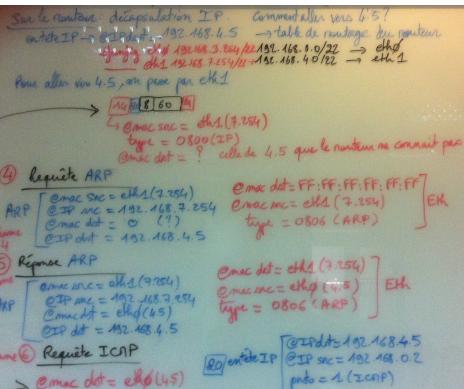


Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

99

## ARP - ICMP



100

## RARP - Reverse ARP

RFC 903

- ARP : @IP->@MAC RARP : @MAC->@IP
- "Mon @MAC est xx:xx:xx:xx:xx:xx. Quelqu'un connaît-il mon @IP ?"
- permet à un hôte de récupérer son @IP au démarrage par interrogation d'un serveur RARP
  - stations sans disque
  - imprimantes,...
- Même fonctionnement, même format de paquet
- Obsolète car désormais remplacé par BOOTP ou DHCP qui peuvent rendre le même service et ne nécessite pas un serveur RARP sur chaque réseau (*broadcast MAC limité*)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

101

## BOOTP (bootstrap) - Principe

RFC 951, 1048, 1084

- Protocole d'amorçage du réseau au dessus de UDP (les diffusions passent les routeurs)
- le serveur informe la machine qui démarre de
  - son @IP, @IP du serveur de fichiers qui contient son image disque, @IP du routeur par défaut, masque de sous-réseau
- Inconvénient : les tables de correspondances sont statiques (configurées manuellement)
- Pour y remédier, BOOTP est devenu DHCP : *Dynamic Host Configuration Protocol*

Olivier Glück

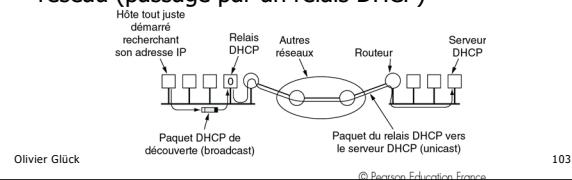
Licence Informatique UCBL - Module LIFASR6 : Réseaux

102

## DHCP - Principe

RFC 2131, 2132

- Configuration manuelle ou assignation dynamique des adresses IP
- Un serveur spécifique s'occupe d'assigner des configurations réseaux aux hôtes qui en font la demande
- Le serveur n'est pas nécessairement sur le même réseau (passage par un relais DHCP)



Olivier Glück

© Pearson Education France

103

## DHCP - Fonctionnement

- DHCP - économie d'adresses IP : quand un hôte quitte le réseau, il restitue son adresse
- Les messages DHCP (au dessus d'UDP)
  - **DHCPDiscover** : diffusion du client pour que les serveurs DHCP actifs répondent en fournissant une @IP
  - **DHCPOffer** : offre des serveurs (réponse à DHCPDiscover)
  - **DHCPRequest** : après avoir sélectionné une offre, le client émet une requête d'affectation d'@ au serveur élu
  - **DCHPAck** : le serveur renvoie une config. Réseau et une durée de validité (*lease time*)
  - **DCHPNACK** : refus d'un renouvellement par le serveur
  - **DCHPRelease** : résiliation du bail avant échéance par le client

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

104

## Quelques fichiers de config. UNIX

- **/etc/hosts** : association locale nom/@IP
- **/etc/resolv.conf** : @ des serveurs de noms, noms de domaines
- **/etc/protocols** : association nom de protocole, numéro de protocole, liste d'alias
  - icmp 1 ICMP
  - tcp 6 TCP
- **/etc/services** : association nom de service, numéro de port/protocole, liste d'alias
  - ftp 21/tcp FTP
  - ssh 22/UDP
- **/etc/inetd.conf** : association entre nom de service et exécutable réalisant le service

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

105

## Quelques commandes UNIX

- ping : teste l'accessibilité d'une destination
- traceroute : renvoie la route prise par les paquets pour atteindre une destination
- arp : visualiser/modifier le cache ARP
- host : interroger un serveur de noms
- netstat : obtenir des statistiques sur le nombre de paquets, les erreurs, les collisions, une interface, une table de routage, les sockets ouvertes, ...
- tcpdump : visualiser des informations qui passent par l'interface réseau d'une machine

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

106



## Le protocole IPv6

## Pourquoi IPv6 ?

- La fin d'IPv4 est proche
  - pénurie d'adresses IP et explosion des tables de routage
  - prolongement de quelques années grâce au routage CIDR et au NAT (solutions transitoires)
  - besoin d'un nouveau protocole mais suppose de le déployer sur tous les noeuds de l'Internet actuel !
- L'IETF, en 1990, élabora les souhaits d'un nouveau protocole et fit un appel à propositions
- 1993 : IPv6 est née de propositions combinées (Deering et Francis) - RFC 2460 à 2466

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

108

## Un nouveau protocole IP

- IETF - 1990 - objectifs d'une nouvelle version d'IP
  - supporter des milliards d'hôtes
  - réduire la taille des tables de routage
  - simplifier encore le protocole pour routage plus rapide des paquets
  - offrir une meilleure sécurité
  - accorder plus d'importance à la QoS (trafic temps-réel)
  - améliorer la diffusion multicast
  - permettre la mobilité des hôtes sans changer d'@ IP
  - rendre le protocole plus évolutif
  - permettre au nouveau protocole et à l'ancien de coexister pendant quelques années

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

109

## IPv6 - Caractéristiques (1)

- IPv6 est compatible avec
  - non seulement IPv4
  - mais aussi TCP, UDP, ICMP, OSPF, BGP, DNS, ... (ou quelques modifications mineures)
- Supporte un format d'adresses plus longues
  - 16 octets au lieu de 4 (quasiment inépuisable)
- Simplification de l'en-tête
  - 7 champs au lieu de 13 (accélère le traitement dans les routeurs)
  - meilleure gestion des options avec une taille fixe (accélère le temps de traitement des paquets)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

110

## IPv6 - Caractéristiques (2)

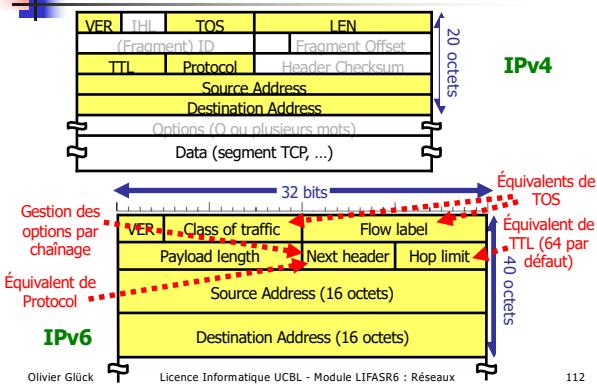
- Sécurité accrue
  - intégrité des données
  - mécanismes d'autentification et de cryptographie
- Plus de fragmentation dans les nœuds intermédiaires
  - mécanisme de découverte du MTU optimal (envoi de paquets ICMP en diminuant la taille jusqu'à recevoir une réponse)
  - fragmentation par la source uniquement
- Plus de champ *checksum*
  - allège considérablement le travail des routeurs
- Amélioration des aspects de diffusion (multicast)

Olivier Glück

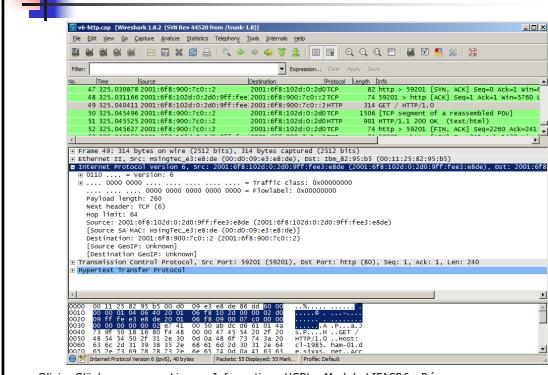
Licence Informatique UCBL - Module LIFASR6 : Réseaux

111

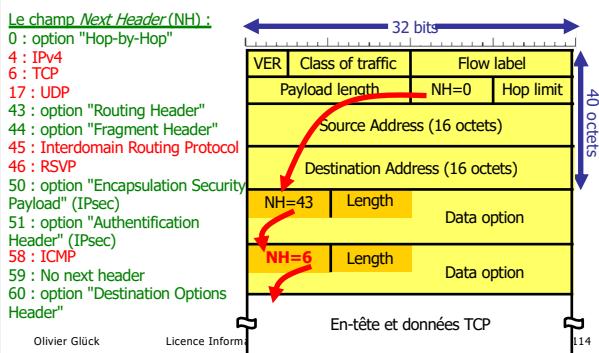
## Le datagramme IPv6



## Exemple d'en-tête IPv6



## Le chaînage des options



## Exemples d'options

- Hop by Hop
  - la seule qui doit être traitée par tous les routeurs traversés (les autres extensions sont traitées comme un protocole de niveau 4 !)
  - transport d'informations <type d'option, longueur, valeur> dont on sait qu'elle sera examinée par tous les routeurs (par ex. support de datagramme de taille supérieure à 64Ko : *jumbogram*)
- Routing Header
  - liste de routeurs à traverser obligatoirement
- Fragmentation Header
  - pour permettre au destinataire de réassembler les fragments (reprend les champs de IPv4)
- Destination Options Header
  - informations additionnelles pour la destination

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

115

## L'adressage (1)

- Adressage hiérarchique pour alléger les tables de routage

Public	Site	Interface_ID
--------	------	--------------

- un préfixe de localisation - public - 48 bits
- un champ de topologie locale (subnet) - 16 bits
- un identifiant de désignation de l'interface (basé sur l'@MAC) sur 64 bits (équivalent HOST\_ID) qui garantie l'unicité de l'adresse

- Notation : groupes de 4 chiffres hexadécimaux séparés par :

- ex : 8000:0000:0000:0000:0123:4567:89AB:CDEF
- :: représente un ou plusieurs groupes de 0000
- ex : 8000::123:4567:89AB:CDEF

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

116

## L'adressage (2)

- Trois types

- adresses unicast : désigne une interface
- adresses multicast (FF00::/8) : désigne un ensemble d'interfaces (localisées n'importe où)
- adresses anycast :

  - restriction du multicast
  - désigne un ensemble d'interfaces partageant un même préfixe réseau
  - n'est délivré qu'à une interface du groupe (celle dont la métrique est la plus proche du nœud source)

- plus d'adresses de broadcast, remplacée par FF02::1

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

117

## L'adressage (3)

- Adresses particulières

- :: (unspecified address) : équivalent de 0.0.0.0, interface en cours d'initialisation
  - ::1 (loopback address) : équivalent de 127.0.0.1
  - adresses de site local (adresses privées) : commençant par FD00::
  - adresses de lien : commençant par FE80::
- Construction de Interface\_ID  
@ MAC 00:A0:24:E3:FA:4B  
Interface\_ID 02A0:24FF:FEE3:FA4B (U/L=1, I/G=0)
  - Adressage agrégé
    - la partie publique est découpée en différents sous-champs ; un sous-champ est attribué par l'organisme qui s'est vu affecter le champ précédent (assignation hiérarchique)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

118



## Les protocoles de transport : UDP et TCP

### Le protocole UDP

- UDP (RFC 768) - User Datagram Protocol
  - protocole de transport le plus simple
  - service de type best-effort (comme IP)
    - les segments UDP peuvent être perdus
    - les segments UDP peuvent arriver dans le désordre
  - mode non connecté : chaque segment UDP est traité indépendamment des autres
- Pourquoi un service non fiable sans connexion ?
  - simple donc rapide (pas de délai de connexion, pas d'état entre émetteur/récepteur)
  - petit en-tête donc économie de bande passante
  - sans contrôle de congestion donc UDP peut émettre aussi rapidement qu'il le souhaite

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

120

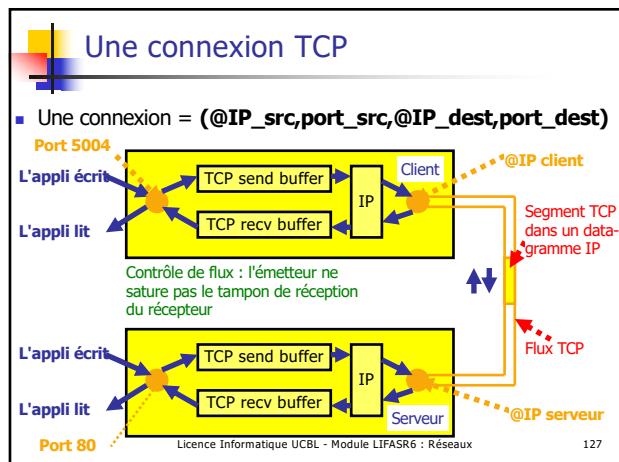
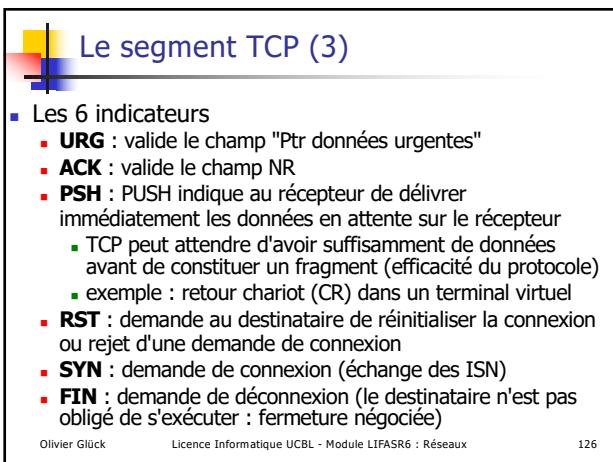
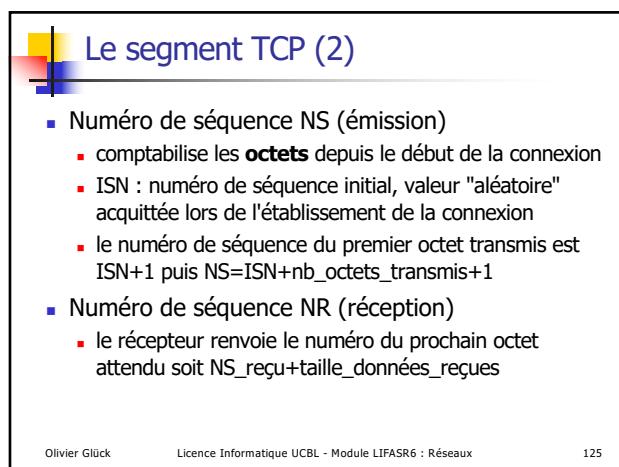
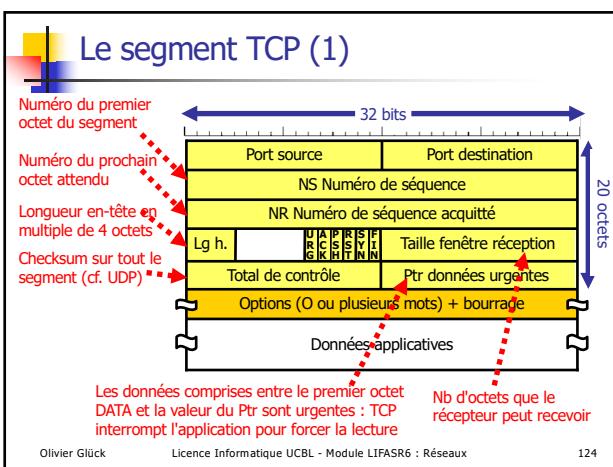
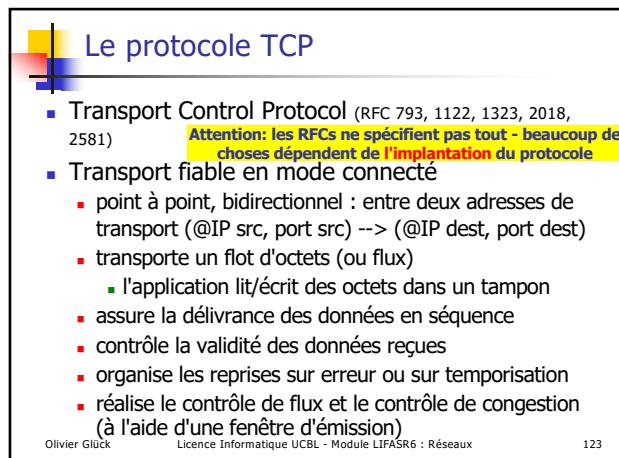
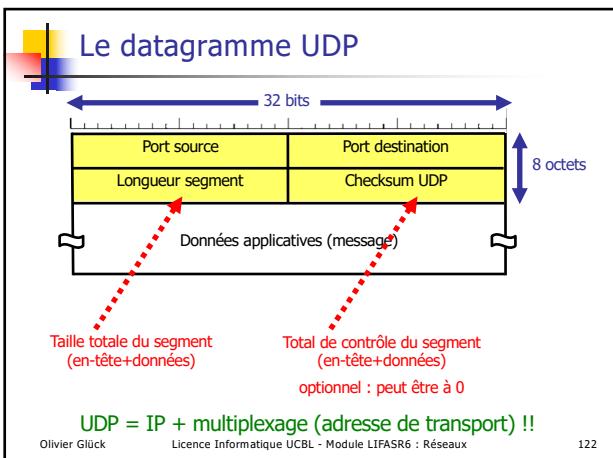
### Les utilisations d'UDP

- Performance sans garantie de délivrance
- Souvent utilisé pour les applications multimédias
  - tolérantes aux pertes
  - sensibles au débit
- Autres utilisations d'UDP
  - applications qui envoient peu de données et qui ne nécessitent pas un service fiable
  - exemples : DNS, SNMP, BOOTP/DHCP
- Transfert fiable sur UDP
  - ajouter des mécanismes de compensation de pertes (reprise sur erreur) au niveau applicatif
  - mécanismes adaptés à l'application

Olivier Glück

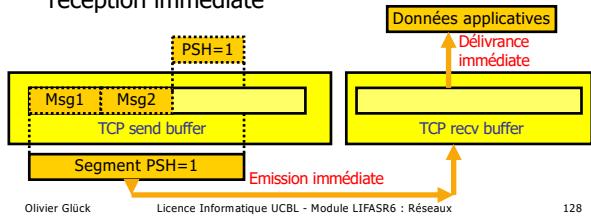
Licence Informatique UCBL - Module LIFASR6 : Réseaux

121



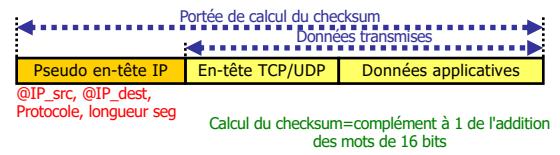
## Le bit PUSH

- Pour optimiser la transmission, par défaut TCP attend que le tampon d'émission soit plein pour constituer un segment (groupage de messages)
- Le bit PUSH sert à demander la transmission et réception immédiate



## Le contrôle d'erreur dans UDP et TCP

- Deux objectifs
  - vérifier que les données transmises n'ont pas été altérées
  - garantir que les données sont transmises au bon destinataire --> rajout d'un pseudo en-tête IP pour le calcul du checksum (qui est non transmis)



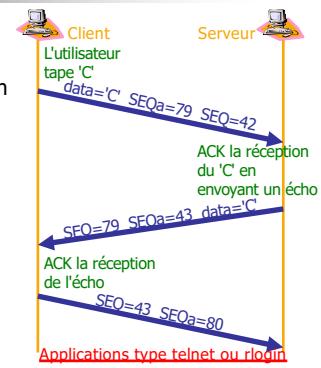
## Exemple de calcul de checksum

- Calcul du checksum par additions des mots de 16 bits complémentées à 1
- Exemple : checksum sur 3 mots de 16 bits
  - 0110011001100110
  - 0101010101010101
  - 0000111000011111
- Somme des deux premiers mots
  - 1011101110111011
- Addition du troisième mot
  - 1100101011001010
- Complément à 1
  - 0011010100110101 (= le champ checksum)
- Si pas d'erreur, la somme de tous les mots de 16 bits reçus doit faire 1111111111111111

Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      130

## Numéro de séquence et ACK

- Principe du *piggybacking* : un segment peut contenir des données et acquitter un segment précédent
- SEQ=numéro du premier octet dans le segment depuis l'ouverture de la connexion
- SEQa=numéro du prochain octet attendu
- L'acquittement d'un octet acquitte tous les octets précédents



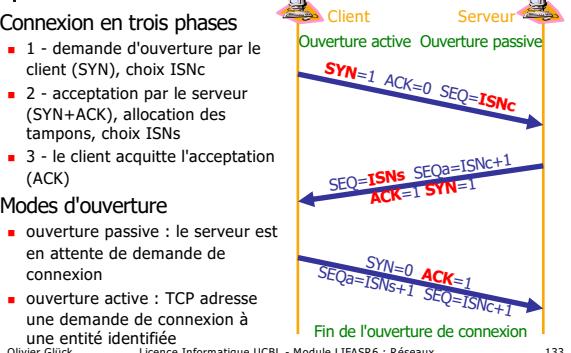
## Le numéro de séquence initial (ISN)

- Chaque entité communique son ISN à l'autre à l'ouverture de la connexion
- Il permet de distinguer les octets de deux connexions successives utilisant les mêmes adresses de transport
  - ouverture de la connexion (@IP1,p1,@IP2,p2)
  - échanges de segments
  - fermeture de la connexion (@IP1,p1,@IP2,p2)
  - ouverture de la connexion (@IP1,p1,@IP2,p2)
  - ...
- Un même ISN est tiré toutes les 4h30 environ

Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      132

## Etablissement d'une connexion TCP

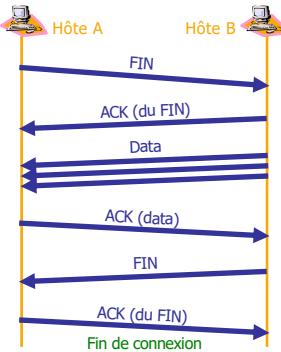
- Connexion en trois phases
  - 1 - demande d'ouverture par le client (SYN), choix ISNc
  - 2 - acceptation par le serveur (SYN+ACK), allocation des tampons, choix ISNs
  - 3 - le client acquitte l'acceptation (ACK)
- Modes d'ouverture
  - ouverture passive : le serveur est en attente de demande de connexion
  - ouverture active : TCP adresse une demande de connexion à une entité identifiée



## Fermeture d'une connexion TCP

### Fermeture négociée

- 1 - demande de fin de connexion (FIN) par une des extrémités
- 2 - acquittement du FIN (ACK) mais mise en attente de la demande (B a encore des données non transmises)
- 3 - B envoie ses données en attente
- 4 - A acquitte les données (ACK)
- 5 - acceptation de la fin de connexion par B (FIN)
- 6 - acquittement de la fin de connexion (ACK)



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

134

## Taille des segments TCP

### Souplesse de TCP :

- l'application lit/écrit dans un tampon
- TCP décide quand envoyer/restituer un segment (si PSH n'est pas positionné)

### Idée :

- TCP a intérêt d'envoyer des segments de taille maximale (limitation de l'overhead lié à la taille de l'en-tête)
- fragmentation IP coûteuse --> éviter la fragmentation
- la taille max. d'un segment TCP est de 64Ko (à cause d'IP)

### MSS : Maximum Segment Size (sans en-tête)

- à l'ouverture de la connexion, chaque entité peut annoncer (option TCP) son MSS à l'autre, en fonction de la MTU de son réseau (MSS=MTU-40) (20, IP+20, TCP)
- par défaut, MSS=536 octets

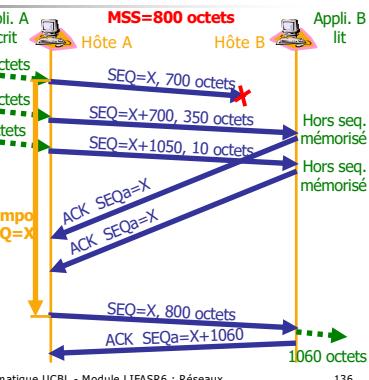
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

135

## Politique de retransmissions

- Les pertes de segment sont détectées par absence d'ack positif à expiration d'un temporisateur sur l'émetteur
- 1 tempo. par seg.
- Toutes les données reçues hors séquence sont mémorisées par le destinataire



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

136

## Envoi des ACK (RFC 1122, 2581)

- Idée : essayer de ne pas envoyer d'ACK sans données, faire des acquittements cumulés

### Événement sur le récepteur

Arrivée d'un segment, dans l'ordre (sans trou), les octets précédents ayant été acquis

Action du récepteur

ACK mis en attente. Envoi de l'ACK au bout de 500ms s'il n'y a pas eu de données à envoyer entre temps

Arrivée d'un segment, dans l'ordre (sans trou), un ACK d'un segment précédent est déjà en attente

Envoi immédiat d'un ACK qui acquitte l'ensemble (ACK cumulé)

Arrivée d'un segment, dans le désordre (avec un numéro de séquence supérieur à celui attendu : création d'un trou)

Envoi d'un ACK dupliqué : si le récepteur attendait 120, il renvoie un ACK avec SEQa=120

Arrivée d'un segment qui remplit partiellement ou complètement un trou

Envoi immédiat d'un ACK

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

137

## Valeur du temporisateur RTO

- RTO : Retransmission Time Out
- Impact de cette valeur sur les performances
  - valeur trop petite : des retransmissions inutiles ont lieu
  - valeur trop grande : attente trop importante entre deux retransmissions
- TCP fait une estimation du RTT (temps aller/retour) et ajuste **dynamiquement** la valeur du temporisateur en fonction de cette estimation
  - utilisation d'une option TCP :
    - l'émetteur met la valeur de son horloge dans l'option
    - le récepteur fait écho de cette valeur dans l'ACK
    - l'émetteur fait la différence entre son horloge et cette valeur à la réception de l'ACK

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

138

## Retransmissions rapides (Fast Retransmit)

- Idée : il est de toute façon pénalisant d'attendre l'expiration du RTO pour retransmettre
  - quand le récepteur reçoit des données hors-séquence, il renvoie immédiatement un ACK indiquant les données qu'il attend
  - si l'émetteur a reçu 3 ACK dupliqués (4 ACK avec le même numéro de séquence attendu), il retransmet sans attendre l'expiration du RTO
- Suppositions de cas de perte :
  - expiration du RTO --> pas d'ACK dupliqués, congestion dans le réseau (plusieurs segments sont perdus)
  - ACK dupliqués --> peu de segments sont perdus (un ACK dupliqué signifie la réception d'un segment)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

139

## Algorithme de Nagle

- Idée : il est pénalisant d'envoyer des segments contenant 1 seul octet de données (par ex. terminal virtuel)
- principe de Nagle : si l'appli. écrit octet par octet
  - envoi du premier octet dans un segment
  - accumulation dans le tampon des octets suivants tant que le premier octet n'est pas acquitté
  - envoi des octets accumulés dans un seul segment
  - attente de l'acquittement pour envoyer le segment suivant...
- Peut être désactivé dans certains cas (X-Window : mouvements de souris saccadés)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

140

## Gestion de la fenêtre

### Contrôle de flux TCP :

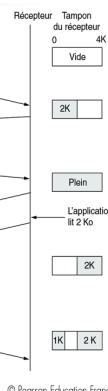
- l'émetteur ne doit pas en envoyer de données si le tampon de réception n'a pas l'espace libre correspondant

### Quand l'émetteur est bloqué, il peut :

- envoyer des données urgentes (interruption de l'application réceptrice)
- envoyer des segments de 1 octet pour obliger le récepteur à envoyer SEQ<sub>a</sub> et WIN et maintenir l'état actif de la connexion

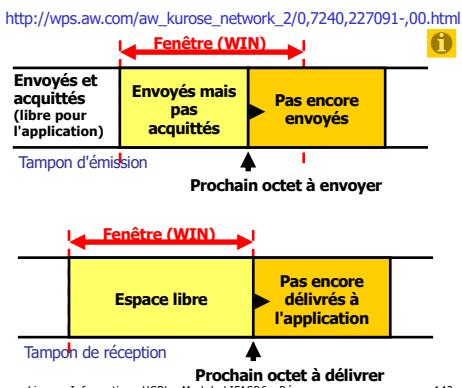
Olivier Glück

Licence Infor



© Pearson Education France

## Contrôle de flux TCP



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

142

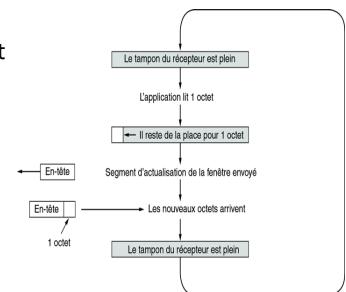
## Syndrome de la fenêtre stupide

### Problème lié au fait que l'application réceptrice lit (vide le tampon) octet par octet

- l'émetteur ne peut alors envoyer que des petits segments

### Solution de Clark :

- le récepteur n'annonce la réouverture de la fenêtre que lorsqu'une taille suffisante est disponible  
--> minimum entre MSS et taille\_tampon/2



© Pearson Education France

## Contrôle de congestion dans TCP

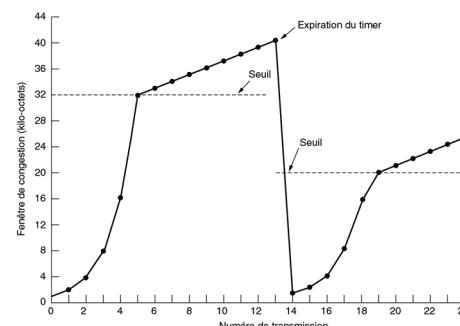
- Congwin* : taille de la fenêtre de congestion
- Recvwin* : taille de la fenêtre de réception
- La fenêtre d'émission (quantité d'octets que l'émetteur peut envoyer) est  $\min(Recvwin, Congwin)$
- Threshold* : seuil d'évitement de congestion qui définit la limite entre les deux phases suivantes
  - slow start* : *Congwin* augmente exponentiellement tant que *Threshold* n'est pas atteint
    - une perte se produit
  - congestion avoidance* : *Congwin* augmente linéairement tant que pas de perte
- au départ, *Threshold*=64Ko et *Congwin*=1\*MSS

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

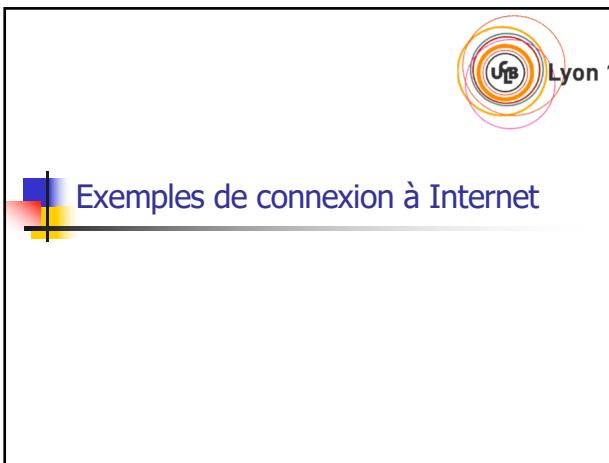
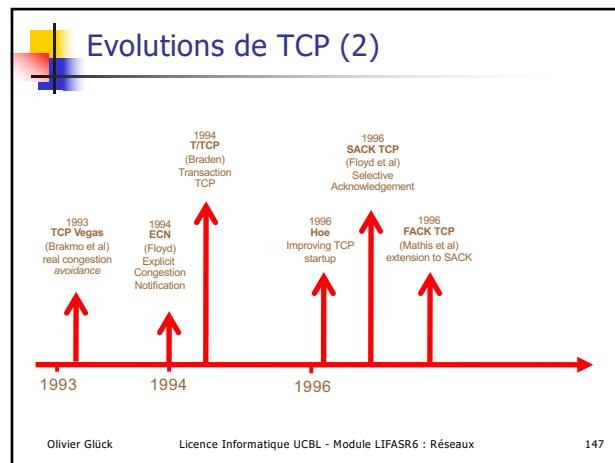
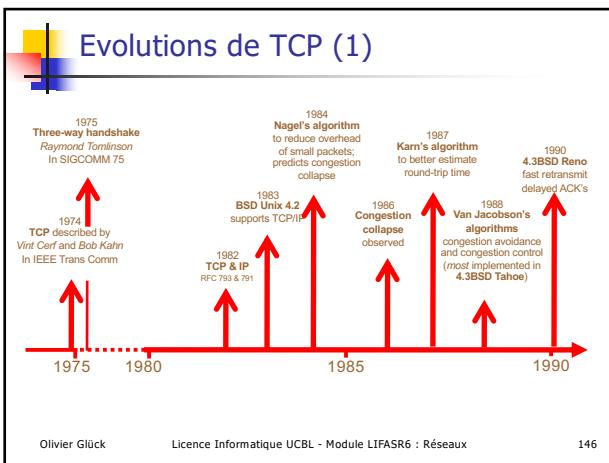
144

## Contrôle de congestion dans TCP

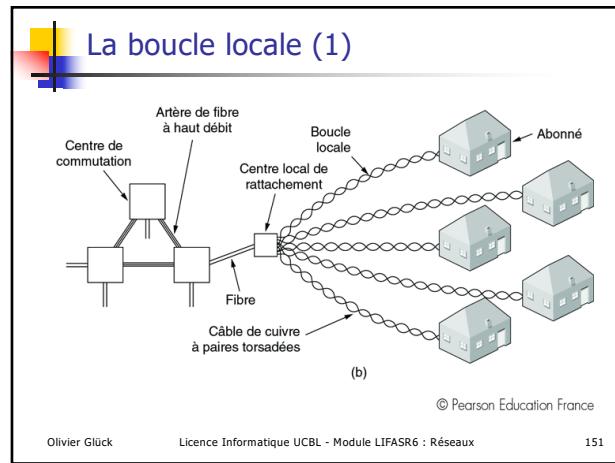
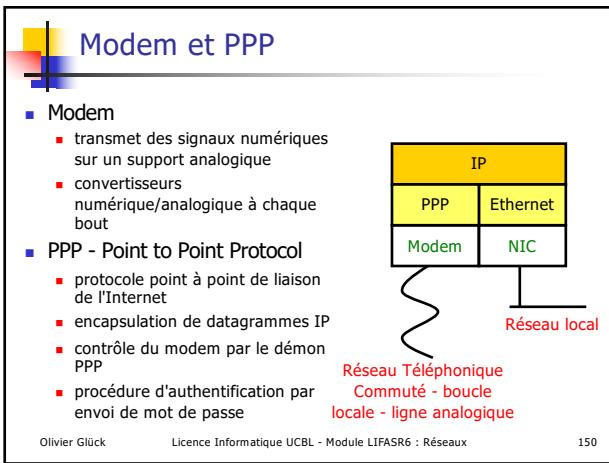


Olivier Glück

© Pearson Education France



- ## Depuis quel réseau ?
- Depuis un réseau local (LAN)
    - Ethernet 10/100/1000 Mbps
    - ATM 155 Mbps
  - Depuis un réseau distant (WAN)
    - RTC : 56 Kbps descendant (*download* vers l'abonné) et 36 Kbps remontant (*upload* depuis l'abonné)
    - RNIS : 128 Kbps
    - xDSL sur ligne téléphonique : y Mbps souvent asymétrique (ADSL)
    - câble TV : y Mbps souvent asymétrique
    - satellite : souvent sens descendant
    - liaisons louées (X25, ATM, ...) (par ex. Transpac)
    - téléphones portables : GSM (9600 bit/s), UMTS, ...
- Olivier Glück      Licence Informatique UCBL - Module LIFASR6 : Réseaux      149



## La boucle locale (2)

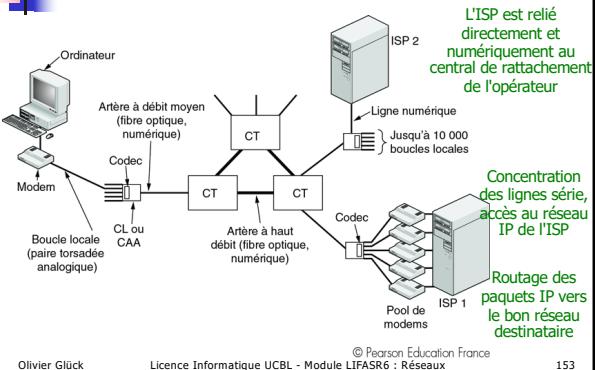
- Lien entre l'abonné au réseau téléphonique et le central de rattachement de l'opérateur
- Paire de cuivre
  - transmission analogique dans la gamme de fréquences 350Hz-3750Hz
  - économique
- Bandes passantes limitées à 4KHz par des filtres mis en place par les opérateurs
  - suffisant pour le transport de la voix
  - sans les filtres, la bande passante peut atteindre le MHz
  - > ADSL : division de la bande de fréquences en environ 250 canaux d'environ 4KHz chacun

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

152

## Principe d'une connexion par RTC



© Pearson Education France

153

## Les technologies xDSL (1)

- DSL : Digital Subscriber Line**
- Multiplexage en fréquences**
  - voix : bande de fréquences de 3.3KHz
  - utilisation des fréquences dans le MHz pour transporter de la donnée
    - l'atténuation augmente avec la fréquence et la longueur du lien, elle dépend aussi de la qualité du lien
    - > pour un débit donné, la distance abonné-réseau doit être respectée
- Idée : faire transiter sur une ligne téléphonique d'usager (paire de cuivre) des informations**
  - à un débit de l'ordre du mégabit par seconde
  - en limitant la longueur de la ligne à quelques km

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

154

## Les technologies xDSL (2)

Technologie	Mode de transmission	Débit opérateur vers utilisateur (Mbit/s)	Débit utilisateur vers opérateur (Mbit/s)	Distance maximale (km)
HDSL	symétrique (2B1Q/CAP)	1,54	1,54	3,6
SDSL	symétrique (2B1Q/CAP)	768 Kbit/s	768 Kbit/s	3,6
<b>ADSL</b>	<b>Asymétrique (DMT)</b>	<b>1,54 à 8,2</b>	<b>16 Kbit/s à 640 Kbit/s</b>	<b>5,4 (à 1,5 Mbit/s)</b>
RADSL	Asymétrique (CAP)	600 Kbit/s à 7 Mbit/s	128 Kbit/s à 1 Mbit/s	5,4 (à 1,5 Mbit/s)
DSL	symétrique (DMT/CAP)	160 Kbit/s	160 Kbit/s	5,4
IDSL	symétrique (2B1Q)	128 Kbit/s	128 Kbit/s	3,6
VDSL	Asymétrique (CAP/DMT ...)	13 à 53	1.544 à 2.3	1.5 (à 13 Mbit/s)

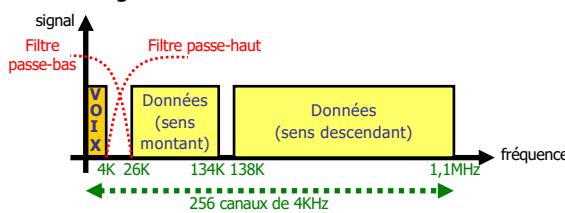
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

155

## L'ADSL - fonctionnement

- Asymétrique : débit descendant très supérieur au débit montant
  - > applications type client/serveur
- La ligne téléphonique reste disponible quand l'usager est connecté à Internet

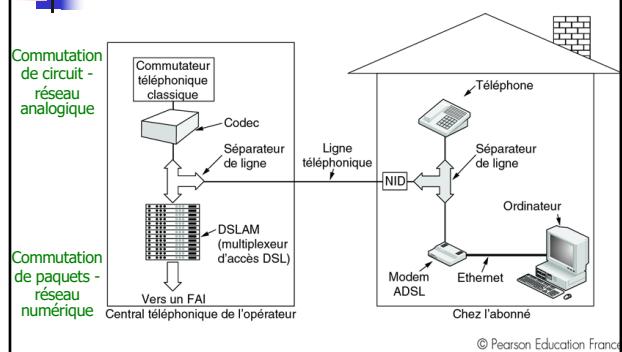


Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

156

## L'ADSL - installation



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

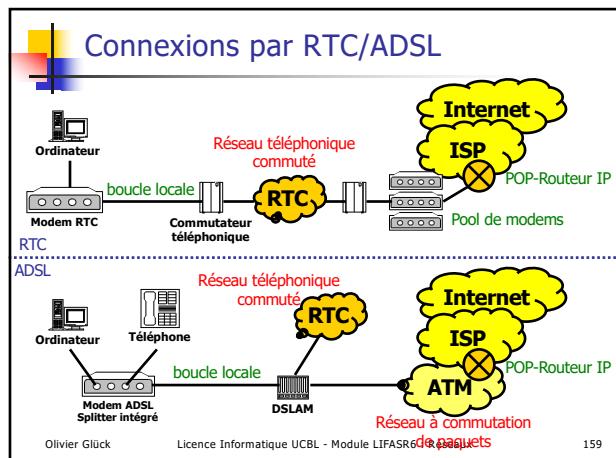
157

## L'ADSL - équipements

- Splitter :**
  - séparateur de ligne ou séparateur de fréquences (filtre passe-bas/passe-haut)
- Modem ADSL :**
  - convertit signaux numériques/analogiques
  - peut intégrer le séparateur de ligne
- DSLAM : DSL Access Multiplexer**
  - multiplexeur d'accès ADSL
  - modems et *splitters* intégrés
  - donne accès à un réseau à commutation de paquets



Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 158



## L'ADSL - 3 options définies par l'ART

- Option 5 : de loin la plus répandue actuellement**
  - FT a en charge l'accès et la collecte DSL des internautes / interneute / FT / FAI
- Option 3 : peu répandu car FT plus compétitif**
  - la collecte est laissée à un opérateur tiers qui achète ce service à FT (FT garde la maîtrise de la boucle locale) / internaute / FT / opérateur de collecte / FAI
- Option 1 : très récent, réduction des coûts FAI->FT**
  - dégroupage total : un opérateur tiers a la maîtrise de bout en bout du trafic ADSL (FT n'intervient plus)
  - dégroupage partiel : la bande de fréquence basse de la paire de cuivre reste gérée par FT (voix)
    - l'abonnement FT reste nécessaire pour l'utilisateur
    - la partage de la bande passante est gérée par le FAI qui met son DSLAM dans le central FT
  - internaute / opérateur de dégroupage / FAI

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 160

## L'ADSL - conclusions

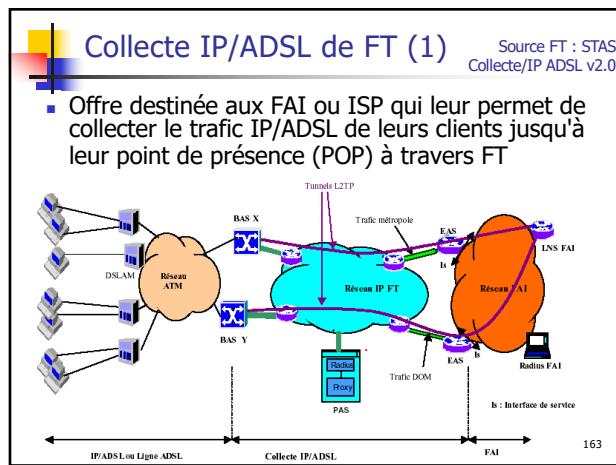
- Deux conditions d'utilisation de l'ADSL**
  - être à moins de 5,4km du central de rattachement (80% des lignes - certaines parties du territoire ne seront jamais couvertes)
  - l'opérateur a pu mettre en place le séparateur de ligne et le DSLAM dans le central de rattachement
- Avantages**
  - séparation voix/données dès le central de rattachement : les données d'une connexion Internet n'encombrent plus les circuits de transport de la voix (cf. RTC)
  - plus de facturation à la minute --> connexion illimitée
  - la ligne téléphonique reste libre durant la connexion Internet
  - débits plus élevés

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 161

## L'ADSL - conclusions

- Couverture actuelle**
  - réservé aux villes importantes (équipements dans le central de rattachement coûteux)
  - près de 18 000 communes couvertes actuellement par FT, 79% de la population (objectif 2005 : 90%)
- Offres ADSL actuelles**
  - entre 128/64Kbps et 2048/256Kbps (généralement 1024/256 ou 512/128)
- Marché encore à ces débuts**
- Les sondages récents montrent que les clients sont satisfaits du service**

Olivier Glück Licence Informatique UCBL - Module LIFASR6 : Réseaux 162



## Collecte IP/ADSL de FT (2)

- L'utilisateur ADSL souscrit le contrat d'un FAI
- FT crée un circuit virtuel permanent entre l'utilisateur et le FAI (transporte le flux IP dans une session PPP)
- Le FAI (ou le transporteur du FAI) doit avoir souscrit un contrat Collecte IP/ADSL auprès de FT pour acheminer le trafic IP de ses clients vers son point de présence (PoP)
- Le FAI est facturé au débit (nb paquets transportés)
- Deux types de flux sont transportés
  - le flux Radius : trafic d'authentification entre FT et le FAI qui identifie le tunnel L2TP dans lequel les sessions PPP sont acheminées
  - le flux utilisateur (montant et descendant)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

164

## Collecte IP/ADSL de FT (3)

- BAS - Broadband Access Server**
  - concentration de plusieurs DSLAM via ATM
- EAS - Equipement d'Accès au Service**
  - situé chez le FAI mais installé, configuré, exploité par FT
  - adaptation des flux du FAI au support le reliant au réseau IP FT
  - interface côté FAI : Fast Ethernet ou 1000BaseSX (FO multimode)
  - routeur IP qui doit connaître les adresses des BAS (FT), du PAS (FT), des LNS (FAI) et des serveurs RADIUS (FAI)
  - session BGP entre le réseau IP de FT et le routeur IP du FAI (EAS)
  - le FAI doit posséder un numéro d'AS public

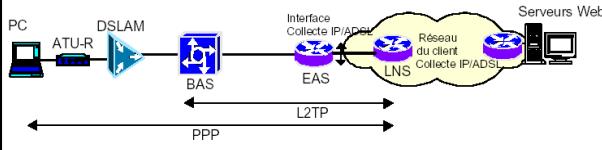
Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

165

## Collecte IP/ADSL de FT (4)

- L2TP - Layer Two Tunneling Protocol (RFC 2661)
  - protocole qui permet la création de tunnels et la gestion de VPN (réseau privé virtuel)
  - le tunnel L2TP ne fait que prolonger la session PPP de l'utilisateur à travers le réseau IP de FT jusqu'au FAI



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

166

## Collecte IP/ADSL de FT (5)

- Etablissement du tunnel L2TP
  - demande de connexion de l'utilisateur (PPP transporte l'identifiant et le mot de passe jusqu'au DSLAM)
  - le BAS envoie (via le PAS - Proxy Access Server) un message RADIUS *access-request* au serveur RADIUS du FAI contenant les identifiants utilisateur, l'@IP du BAS...
  - le serveur RADIUS contient les coordonnées du tunnel (@IP du LNS=L2TP Network Server, ...)
  - ces coordonnées sont transmises au PAS qui les relaie vers le BAS dans un message RADIUS *access-accept*
  - une fois le tunnel L2TP établi, la session PPP est établie de bout en bout dans le tunnel L2TP
  - le FAI authentifie le client, lui attribue une @IP...

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

167

## Connexion par câble/CATV (1)

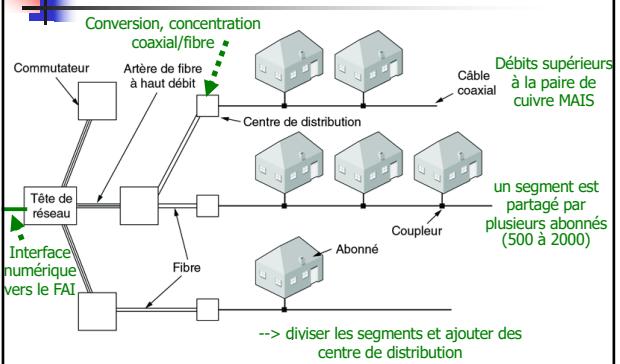
- CATV - Community Antenna TeleVision
- Les câblo-opérateurs :
  - bénéficie d'un réseau existant pour une offre de télévision (à l'origine unidirectionnel)
  - ajout d'une offre de téléphonie classique et d'une offre Internet (mise à jour du réseau pour être duplex : amplificateurs bidirectionnels)
  - câble coaxial : supporte des débits plus élevés que la paire de cuivre torsadée
    - débit descendant : environ 30Mbps
    - débit montant : environ 1Mbps
  - problème : débits partagés entre les utilisateurs

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

168

## Connexion par câble (2)



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

169

## Connexion par câble (3)

- Multiplexage en fréquence (cf. ADSL)



- Modem-câble

- connexion permanente établie - attribution d'un canal montant et d'un canal descendant
- les câblo-opérateurs ne facturent pas le temps de connexion
- coaxial = support partagé --> méthode d'accès ALOHA + chiffrement des données

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

170

## Câble ou ADSL ?

- Quel langage ou quel OS est le meilleur ?!

- Similitudes

- cœur de réseau en fibre optique large bande

- Avantages câble - inconvénients ADSL

- bande passante du coaxial 100 fois supérieure à la paire torsadée mais la TV consomme une grande partie de la BP
- la distance par rapport à la tête de réseau n'entre pas en jeu avec le câble : l'usager est câblé ou il ne l'est pas !

- Avantages ADSL - inconvénients câble

- le débit de l'utilisateur du câble dépend des autres utilisateurs du segment (caractère imprévisible)
- ADSL : chaque utilisateur dispose d'une sorte de connexion dédiée
- ADSL : pas de problème de sécurité (support non partagé)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

171

## Renater

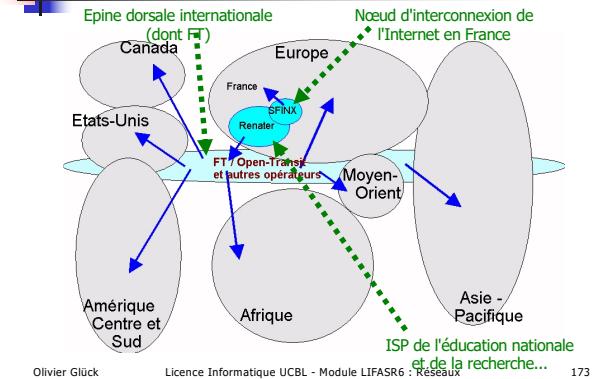
- Renater est un ISP - prestataire de services Internet
  - interconnecte plus de 600 sites français ayant une activité dans les domaines de la recherche, la technologie, l'enseignement et la culture
  - pas d'infrastructure physique (liaisons louées actuellement à FT ou Télécom Développement)
- liaisons louées métropolitaines et internationales à haut débit
  - réseaux de collecte régionaux
  - RENATER 3 - épine dorsale nationale de Renater - jusqu'à 80 Gbit/s
  - lien à 1 Gbit/s vers le noeud d'échange SFINX (accès à Internet France)
  - 2 liens à 2,5 Gbit/s vers l'épine dorsale de l'Internet mondiale : Open Transit

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

172

## Renater dans l'Internet



Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

173

## SFINX : Internet en France

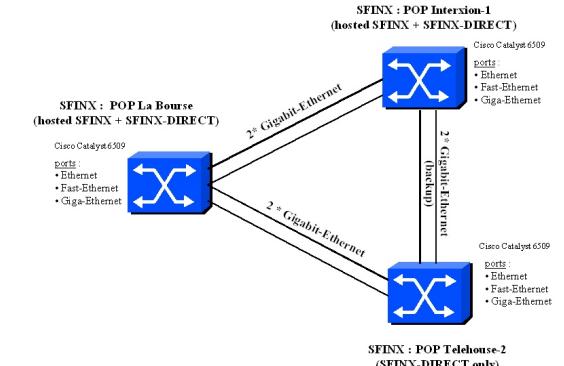
- SFINX : Service for French Internet eXchange
  - le GIX (Global Internet eXchange) français
  - noeud d'interconnexion qui permet aux ISP et opérateurs français connectés sur un POP SFINX d'échanger du trafic national
  - 3 POPs sur lesquels les ISP se connectent (= 3 gros routeurs interconnectés par des liens 2 Gbit-Ethernet)
- créé par le GIP Renater en 1995
  - GIP : Groupement d'Intérêt Public
  - contribuer au développement d'Internet en France sans finalité commerciale (à but non lucratif)

Olivier Glück

Licence Informatique UCBL - Module LIFASR6 : Réseaux

174

## Architecture de SFINX



SFINX : POP Interxion-1  
(hosted SFINX + SFINX-DIRECT)

Cisco Catalyst 6509  
ports:  
• Ethernet  
• Fast-Ethernet  
• Giga-Ethernet

SFINX : POP La Bourse  
(hosted SFINX + SFINX-DIRECT)

Cisco Catalyst 6509

ports:  
• Ethernet  
• Fast-Ethernet  
• Giga-Ethernet

SFINX : POP Telephone-2  
(SFINX-DIRECT only)

175