

Protocoles Internet

IFT 6802
Par Laurent Magnin

Introduction

Internet : réseau de réseaux...

- « Internet » a pour but l'interconnexion de réseaux informatiques sur une base planétaire
- Technologie issue des années 1970, de projets DARPA (*Department of Defense* américain)
 - Robustesse
 - Hétérogénéité
 - « Service publique »
- Croissance exponentielle

Universalité

- Adaptation de la technologie IP (*Internet Protocol*) à la plupart des interfaces matérielles (micro, station, super-calculateur et équipements de réseaux)
- Ces services de base sont indépendants du support de transmission (Ethernet, T.R., X25, FR, FDDI, etc.) ; adaptables à toute sorte de media depuis les réseaux locaux jusqu'aux réseaux longue distance
- Technologie publique et largement diffusée au travers de RFC's (*Requests for Comments*).
- Largement validée depuis de nombreuses années dans un monde hétérogène

Interconnexion « égalitaire »

- Interconnexion universelle : les machines ont une adresse unique sur l'Internet. Deux machines reliées au réseau, communiquent grâce aux autres noeuds du réseau qui routent de manière coopérative sur la base de l'adresse destinataire
- Interconnexion d'égal à égal (*peer to peer systems*) : il n'y a pas de machines prioritaires (en opposition à une structure hiérarchique)
- Dans le cadre du transport sécurisé, les acquittements sont effectués entre les systèmes finaux (source et destinataire) plutôt que continuellement entre chaque noeud relayant les messages

Couches réseau

- La technologie est constituée par des protocoles de base (IP, TCP/IP, etc.) qui offrent les services de transfert des données :
 - transport de datagrammes : service élémentaire de la commutation de paquets.
 - transport de messages sécurisés : service orienté connexion permettant d'acheminer des données en garantissant leur intégrité
- Applications standards bâties sur ces technologies de base : courrier électronique, transfert de fichier, émulation terminal, etc.

Adresses Internet

Adresses Internet

Université de Montréal

L'adressage Internet

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

Université de Montréal Cours IFT 6802, tous droits réservés / 8

L'adressage Internet

- **Solution : adressage binaire compact assurant un routage efficace**
- **Adressage « à plat » par opposition à un adressage hiérarchisé permettant la mise en œuvre de l'interconnexion d'égal à égal**
- **Utilisation de noms pour identifier des machines (réalisée à un autre niveau que les protocoles de base. Cf. les serveurs DNS)**

Université de Montréal Cours IFT 6802, tous droits réservés / 9

L'adressage Internet (notation décimale)

- **L'interface utilisateur concernant les adresses IP consiste en la notation de quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP :**
 - 10000000 00001010 00000010 00011110
 - est écrit : 128.10.2.30

Université de Montréal Cours IFT 6802, tous droits réservés / 10

Les classes d'adressage

- **Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (netid, hostid) où netid identifie un réseau et hostid identifie une machine sur ce réseau.**
- **Cette paire est structurée de manière à définir cinq classes d'adresse**
 - Class A - supporte 16 million d'adresses pour chacun des 126 réseaux
 - Class B - supporte 65 000 adresses pour chacun des 16 000 réseaux
 - Class C - supporte 254 adresses pour chacun des 2 millions de réseaux

Université de Montréal Cours IFT 6802, tous droits réservés / 11

L'adressage Internet (suite)

Université de Montréal Cours IFT 6802, tous droits réservés / 12

Adresses particulières

- **Adresses réseau** : adresse IP dont la partie hostid ne comprend que des zéros; => la valeur zéro ne peut être attribuée à une machine réelle : 192.20.0.0 désigne le réseau de classe B 192.20.
- **Adresse machine locale** : adresse IP dont le champ réseau (netid) ne contient que des zéros;
- **IP Adresses de diffusion** : la partie hostid ne contient que des 1

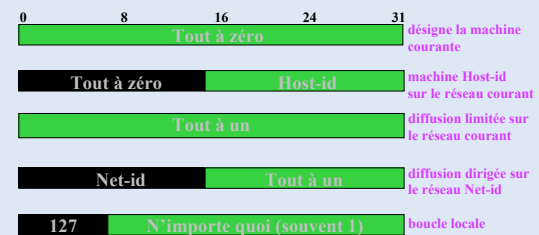
Adresses particulières (suite)

- **Adresse de diffusion limitée** : netid ne contient que des 1 : l'adresse constituée concerne uniquement le réseau physique associé
- **L'adresse de diffusion dirigée** : netid est une adresse réseau spécifique => la diffusion concerne toutes les machines situées sur le réseau spécifié : 192.20.255.255 désigne toutes les machines du réseau 192.20.
 - En conséquence, une adresse IP dont la valeur hostid ne comprend que des 1 ne peut être attribuée à une machine réelle.

Adresses particulières (suite)

- **Adresse de boucle locale** : l'adresse réseau 127.x.x.x est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Une adresse réseau 127 ne doit, en conséquence, jamais être véhiculée sur un réseau et un routeur ne doit jamais router un datagramme pour le réseau 127.

Adresses particulières (résumé)



Domain Name System (DNS)

- Les adresses IP numériques sont difficiles à mémoriser
- Les serveurs DNS servent à convertir des adresses alphabétiques en adresses numériques
 - « www.iro.umontreal.ca » donne « 132.204.24.128 »
- Si un serveur DNS ne sait traduire une adresse, il interroge un autre serveur, et ainsi de suite jusqu'à ce que l'adresse soit traduite correctement
- « Localhost » donne « 127.0.0.1 » (machine locale)
- Adresses dynamiques : <http://www.dyndns.org/>

Internet Corporation For Assigned Names and Numbers

- organisation de droit privé à but non lucratif
- est chargée d'allouer l'espace des adresses de protocole Internet (IP), d'attribuer les identificateurs de protocole, de gérer le système de nom de domaine de premier niveau pour les codes génériques (gTLD) et les codes nationaux (ccTLD), et d'assurer les fonctions de gestion du système de serveurs racines.
- dans le cadre d'un contrat avec le gouvernement fédéral américain, remplace l'Internet Assigned Numbers Authority (IANA) et d'autres organismes
- <http://www.icann.org/>

Enregistrement d'un nom de domaine

- Se fait auprès d'un organisme accrédité par l'ICANN
- <http://www.icann.org/registrars/accredited-list.html> (.aero, .biz, .com, .coop, .info, .museum, .name, .net, .org, .pro)
- **Autorité canadienne pour les enregistrements Internet (ACEI)**
 - Gère les adresses en « .ca »
 - <http://www.cira.ca/>

Informations sur un nom de domaine ?

- « Whois » permet de retrouver des informations sur le propriétaire d'un nom de domaine
- Exemple : <http://www.internic.net/whois.html>
- **Domain Name: SUN.COM**
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: <http://www.networksolutions.com>
Name Server: NS8.SUN.COM
...
Status: ACTIVE
Updated Date: 17-dec-2002
Creation Date: 19-mar-1986
Expiration Date: 20-mar-2010

Le sous-adressage

- **Le sous-adressage est une extension du plan d'adressage initial**
- **Devant la croissance du nombre de réseaux de l'Internet, il a été introduit afin de limiter la consommation d'adresses IP qui permet également de diminuer :**
 - la gestion administrative des adresses IP,
 - la taille des tables de routage des passerelles,
 - la taille des informations de routage,
 - le traitement effectué au niveau des passerelles.

Le sous-adressage (suite)

- **Principes**
 - A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.
 - On dit alors que ces réseaux physiques sont des sous-réseaux (*subnet*) du réseau d'adresse IP.
- <http://www.freenix.fr/unix/linux/HOWTO/mini/IP-Subnetworking-6.html>

Adresses physiques, logiques et connexions réseau

- Une adresse (logique) IP => une interface physique => une connexion réseau
- S'applique particulièrement aux « routeurs » qui possèdent par définition plusieurs connexions à des réseaux différents

Attribution des adresses IP

- **À chaque interface réseau physique doit être attribuée une adresse IP**
- **Numéro IP statique**
 - Définit comme paramètre de l'OS
 - Attribué en fonction de l'adresse « Mac » de la carte Ethernet
 - Service payant des fournisseurs d'accès Internet (FAI)
- **Numéro IP dynamique**
 - Au sein d'un réseau local : serveur *Dynamic Host Configuration Protocol* (DHCP) - <http://www.dhcp.org/>
 - FAI : protocoles PPP (modem) ou PPPoE (ADSL)

ARP: Address Resolution Protocol

- **Le besoin**
 - La communication entre machines ne peut s'effectuer qu'à travers l'interface physique
 - Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
- **La solution : ARP**
 - Mise en place dans IP d'un protocole de bas niveau appelé *Address Resolution Protocol (ARP)*
 - Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de son adresse IP

Identification du service : les ports

- **les adresses IP désignent les machines entre lesquelles les communications sont établies**
- **Lorsqu'un processus désire entrer en communication avec un autre processus, il doit adresser le processus s'exécutant cette machine.**

Les ports (suite)

- **L'adressage de ce processus est effectué selon un concept abstrait indépendant du système d'exploitation des machines car :**
 - les processus sont créés et détruits dynamiquement sur les machines,
 - il faut pouvoir remplacer un processus par un autre (exemple *reboot*) sans que l'application distante ne s'en aperçoive,
 - il faut identifier les destinations selon les services offerts, sans connaître les processus qui les mettent en oeuvre,
 - un processus doit pouvoir assurer plusieurs services.

Les ports (suite)

- **Ces destinations abstraites permettant d'adresser un service applicatif s'appellent des ports de protocole.**
- **L'émission d'un message se fait sur la base d'un port source et un port destinataire.**
- **Les processus disposent d'une interface système leur permettant de spécifier un port ou d'y accéder (socket, TLI, ...).**
- **Les accès aux ports sont généralement synchrones, les opérations sur les ports sont tamponnés (files d'attente).**

Le cheminement des paquets

Le protocole IP

Concepts de l'interconnexion

- **Point de départ : les réseaux interconnectés sont de nature diverse**
- **Les différences entre tous ces réseaux ne doivent pas apparaître à l'utilisateur de l'interconnexion.**
- **Abstraction à chaque niveau de fonctionnalité (couches de protocoles) qui encapsule les fonctionnalités de niveau inférieur**
- **Affranchit l'utilisateur des détails relatifs aux couches inférieures et finalement au réseau lui-même (couche physique)**

Concepts de l'interconnexion (suite)

- **Les premiers systèmes d'interconnexion ont traité le problème au niveau applicatif : messagerie relayant le message de nœud en nœud. Cette solution présente plusieurs inconvénients :**
 - si les applications interfacent elles-mêmes le réseau (aspects physiques), elles sont victimes de toute modification de celui-ci,
 - plusieurs applications différentes sur une même machine dupliquent l'accès au réseau,
 - lorsque le réseau devient important, il est impossible de mettre en œuvre toutes les applications nécessaires à l'interconnexion sur tous les nœuds des réseaux.

Concepts de l'interconnexion (suite)

- **Alternative à cette solution : mise en œuvre de l'interconnexion au niveau des protocoles gérant la couche réseau de ces systèmes**
- **Avantage considérable : les données sont routées par les nœuds intermédiaires sans que ces nœuds aient la moindre connaissance des applications responsables des ces données**

Concepts de l'interconnexion (suite)

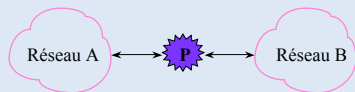
- **Autres avantages :**
 - la commutation est effectuée sur la base de paquets de petite taille plutôt que sur la totalité de fichiers pouvant être de taille très importante,
 - le système est flexible puisque l'on peut facilement introduire de nouvelles interfaces physiques en adaptant la couche réseau alors que les applications demeurent inchangées,
 - les protocoles peuvent être modifiés sans que les applications soient affectées.

Concepts de l'interconnexion (suite)

- **Le concept d'interconnexion ou d'Internet repose sur la mise en œuvre d'une couche réseau masquant les détails de la communication physique du réseau et détachant les applications des problèmes de routage.**
- **L'interconnexion : faire transiter des informations depuis un réseau vers un autre réseau par des nœuds spécialisés appelés routeurs (router)**
 - À noter que « routeur » remplace le terme plus générique de passerelle (*gateway*)

Concepts de l'interconnexion (suite)

- **Les routeurs possèdent une connexion sur chacun des réseaux:**



- **Le routeur P interconnecte les réseaux A et B.**
- **Le rôle du routeur P est de transférer sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B et inversement.**

Concepts de l'interconnexion (suite)

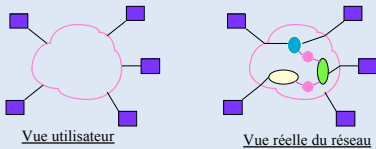
- **P1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C**



- **P1 doit avoir connaissance de la topologie du réseau; à savoir que C est accessible depuis le réseau B.**
- **Le routage n'est pas effectué sur la base de la machine destinataire mais sur la base du réseau destinataire**

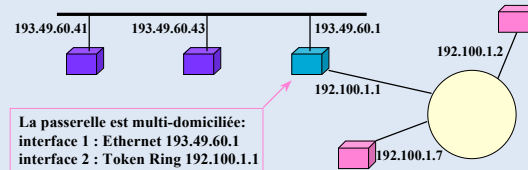
Concepts de l'interconnexion (suite)

- A l'intérieur de chaque réseau, les nœuds utilisent la technologie spécifique de leur réseau (Ethernet, X25, etc)
- Le logiciel d'interconnexion (couche réseau) encapsule ces spécificités et offre un service commun à tous les applicatifs, faisant apparaître l'ensemble de ces réseaux disparates comme un seul et unique réseau.



Machine multi-domiciliée

- A une machine, est associé un certain nombre N d'adresses IP.
- Si $N > 1$ la machine (ou passerelle) est multi-domiciliée.



La passerelle est multi-domiciliée:
interface 1 : Ethernet 193.49.60.1
interface 2 : Token Ring 192.100.1.1

Adresse LAN ou WAN ?

- **LAN (Local-Area Network) est un réseau local**
 - À la maison (p. ex. 192.1.1.101), au sein d'une entreprise...
- **WAN (Wide-Area Network) est un regroupement de réseaux, i.e. Internet**
 - Connexion obtenue auprès d'un fournisseur d'accès (p.ex. 131.204.25.134)
 - <http://www.whatismyip.com/>

IP : Internet Protocol

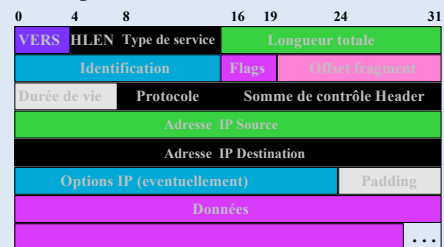
- Réalise les fonctionnalités de la couche réseau d'Internet
- Le service offert par le protocole IP est dit **non fiable** :
 - remise de paquets non garantie,
 - sans connexion (paquets traités indépendamment les uns des autres),
 - pour le mieux (best effort, les paquets ne sont pas éliminés sans raison).

IP : Internet Protocol (suite)

- **Le protocole IP définit :**
 - l'unité de donnée transférée dans les interconnexions (datagramme),
 - la fonction de routage,
 - les règles qui mettent en œuvre la remise de paquets en mode non connecté

IP : Internet Protocol (le datagramme)

- L'unité de transfert de base dans un réseau Internet est le datagramme :



Routage des datagrammes

- Le routage est le processus permettant à un datagramme d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme

Routage des datagrammes (suite)

- **Machines et routeurs participent au routage :**
 - les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées (routage direct) ou bien si le datagramme doit être acheminé vers une passerelle ; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée
 - les passerelles effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

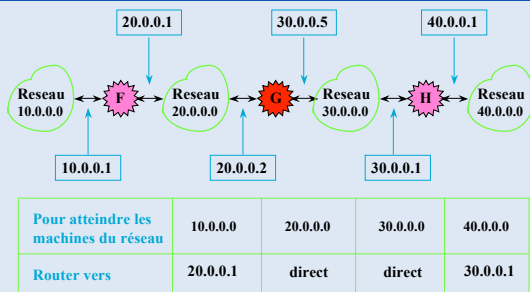
Routage des datagrammes (suite)

- Le routage indirect repose sur une table de routage IP, présente sur toute machine et passerelle, indiquant la manière d'atteindre un ensemble de destinations
- Les tables de routage IP, pour des raisons évidentes d'encombrement, renseignent seulement les adresses réseaux et non pas les adresses machines

Routage des datagrammes (suite)

- Typiquement, une table de routage contient des couples (R, P) où R est l'adresse IP d'un réseau destination et P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire
- La passerelle ne connaît pas le chemin complet pour atteindre la destination

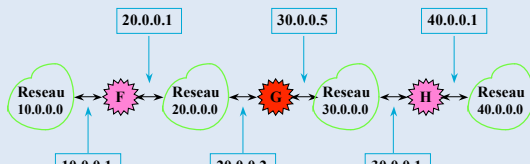
Routage des datagrammes (suite)



Routage des datagrammes (suite)

- Après exécution de l'algorithme de routage, IP transmet le datagramme ainsi que l'adresse IP déterminée, à l'interface réseau vers lequel le datagramme doit être acheminé
- L'interface physique détermine alors l'adresse physique associée à l'adresse IP et achemine le datagramme sans l'avoir modifié (l'adresse IP du prochain saut n'est sauvegardée nulle part)
- Si le datagramme est acheminé vers une autre passerelle, il est à nouveau géré de la même manière, et ainsi de suite jusqu'à sa destination finale

Routage des datagrammes (exemple)



• **Un datagramme arrivant sur F à destination du réseau 40.0.0.2 :**

- F le transmet à G
- G le transmet à H
- H le transmet à la machine locale 40.0.0.2

Le Protocole ICMP

- Le protocole ICMP (*Internet Control Message Protocol*) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles.
- Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet :
 - machine destination déconnectée,
 - durée de vie du datagramme expirée,
 - congestion de passerelles intermédiaires.

Le Protocole ICMP (suite)

- Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.
- Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'Internet.
- Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP (évite l'effet cumulatif).

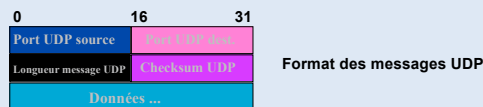
Le protocole UDP

UDP : User Datagram Protocol

- Émission de messages applicatifs sans établissement de connexion au préalable
- L'arrivée des messages ainsi que l'ordonnancement ne sont pas garantis
- Les messages UDP sont également appelés des datagrammes UDP

UDP : format des messages

- Ils contiennent deux parties : un en-tête UDP et les données UDP



- Les ports source et destination contiennent les numéros de port utilisés par UDP pour démultiplexer les datagrammes destinés aux processus en attente de les recevoir. Le port source est facultatif (égal à zéro si non utilisé).

UDP : les ports standards

- **Certains ports sont réservés :**

No port	Mot-clé	Description
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESERVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management prot.

- **D'autres numéros de port (non réservés) peuvent être assignés dynamiquement aux applications**

Le protocole TCP

TCP : *Transmission Control Protocol*

- **Transport fiable de la technologie TCP/IP.**
 - fiabilité = illusion assurée par le service
 - transferts tamponés : découpage en segments
 - connexions bidirectionnelles et simultanées
- **Service en mode connecté**
- **Garantie de non perte de messages ainsi que de l'ordonnancement**

TCP : La connexion

- **Une connexion de type circuit virtuel est établie avant que les données ne soient échangées : appel + négociation + transferts**
- **Une connexion = une paire d'extrémités de connexion**
- **Une extrémité de connexion = couple (adresse IP, port)**
- **Exemple de connexion : ((124.32.12.1, 1034), (19.24.67.2, 21))**

TCP : La connexion (suite)

- **Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)**
- **La mise en oeuvre de la connexion se fait en deux étapes :**
 - une application (extrémité) effectue une ouverture passive en indiquant qu'elle accepte une connexion entrante,
 - une autre application (extrémité) effectue une ouverture active pour demander l'établissement de la connexion.

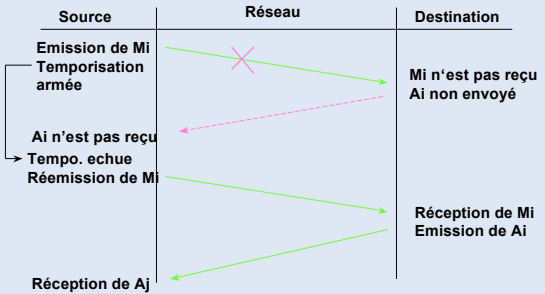
TCP : Segmentation , contrôle de flux

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

Acquittement de messages

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

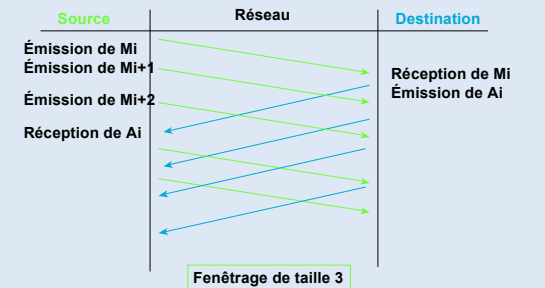
TCP : Acquittements



TCP : le fenêtrage

- La technique d'acquittement simple pénalise les performances puisqu'il faut attendre un acquittement avant d'émettre un nouveau message. Le fenêtrage améliore le rendement des réseaux.
- La technique du fenêtrage : une fenêtre de taille T, permet l'émission d'au plus T messages "non acquittés" avant de ne plus pouvoir émettre.

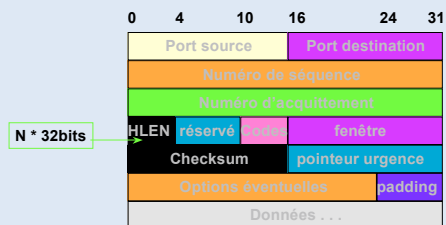
TCP : le Fenêtrage



TCP : Segments

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

TCP : Segments (suite)



TCP : ports standards

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

Routage basé sur TCP-IP

- La technologie TCP-IP est de type «bout en bout» en opposition aux technologies «point à point» (Cf X25),
- L'acheminement des paquets est réalisé par routage plutôt que par commutation :

- IP est dit «sans états»
- X25/X75 maintiennent des états associés au circuit virtuel (adresse du prochain relais, nombre de paquets restant à transmettre, contrôle de flux, etc.); si un de ces états est perdu, la communication est rompue.

Routage basé sur TCP-IP (suite)

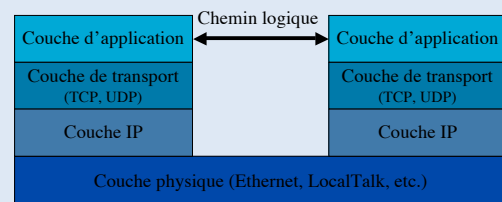
- les services nécessaires à la communication (Contrôle de flux, gestion des d'erreurs, congestion, etc.) sont réalisés de bout en bout à un autre niveau (Cf. TCP).
- Paradoxalement le mode «bout en bout» est le plus robuste que le mode point à point connecté; si un relais tombe en panne :
 - les voisins du relais IP recalculent les tables de routage, et acheminent les paquets suivants par une nouvelle route.
 - dans la technologie «point à point», le circuit est rompu et la connexion avortée.

Conclusion

Avenir d'Internet ? Pour tout, partout...

- Pour tout produits (Voice Over IP, inventaires, etc.)
 - Problèmes lié au nombre d'adresses IPv4 disponibles
 - IPv6
 - <http://www.ipv6.org/> ,
 - <http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html>
 - Codage des adresses IP sur 128 bits (au lieu de 32)
 - Soit 340 282 366 920 938 463 463 374 607 431 768 211 456 IPs
 - Soit 665 570 793 348 866 943 898 599 IPs / m² sur terre...
- Partout (connexions sans-fil)
 - Bluetooth - courte distance, débit faible, faible consommation
 - 802.11 (WiFi - HotSpot) - distance moyenne, débit plus élevé

Récapitulatif : les couches réseaux



Références

- Ce cours est largement inspiré de celui du site <http://www.centralweb.fr/download/index.html>
- Définition des termes liés à Internet (en anglais) : <http://www.webopedia.com/>