

Utilisation des Systèmes et Réseaux : TCP/IP

Licence 3 Pro 2012/13

David Lesaint

david.lesaint@info.univ-angers.fr
H104 LERIA Université d'Angers

Novembre 2012

● Planning

- 5 semaines : semaine 37 à 41
- 2 x 2h par semaine : 3 cours, 3 TD et 4 TP

● Contrôles

- 1 contrôle continu de 2h lors du dernier TP
- 1 contrôle continu commun de 1h en semaine 42
- Coefficients : CC=1/3 et CCC=2/3

- 1 Introduction
- 2 Les Réseaux et l'Internet
- 3 Les Services
- 4 Le Transport des Données
- 5 L'Adressage et le Routage
- 6 Sécurité sur Internet

1 Introduction

- Qu'est ce qu'un réseau ?
- La représentation de l'information
- La transmission en série
- Notion de protocole

2 Les Réseaux et l'Internet

3 Les Services

4 Le Transport des Données

5 L'Adressage et le Routage

6 Sécurité sur Internet

1

Introduction

- Qu'est ce qu'un réseau ?
- La représentation de l'information
- La transmission en série
- Notion de protocole

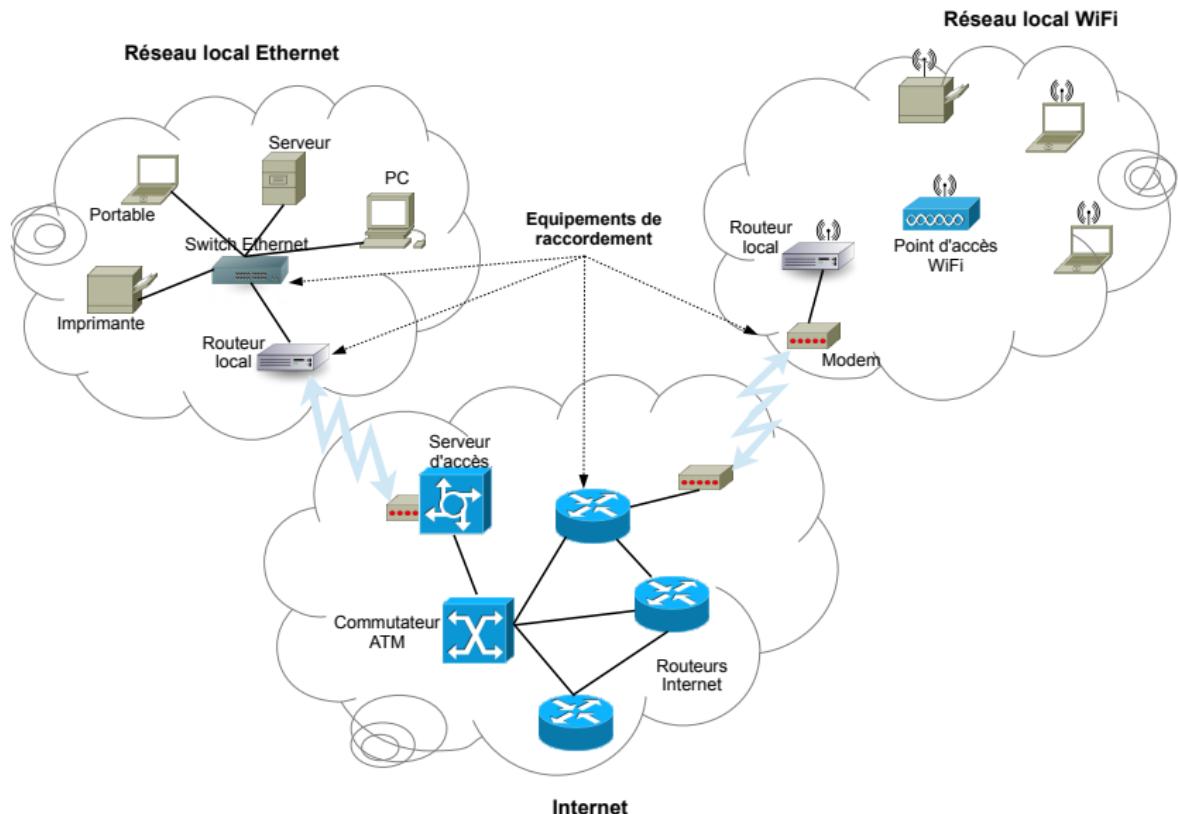
Qu'est ce qu'un réseau ?

- Réseau informatique = Système de communication (ensemble matériel + logiciel) permettant l'échange d'information entre différentes unités informatiques
- Différents types d'unités :
 - ordinateurs
 - tablettes
 - téléphones
 - smartphones
 - terminaux de paiement
 - capteurs ...
- Les informations (données) échangées sont représentées et exploitées dans un langage machine : le codage binaire

Qu'est ce qu'un réseau ?

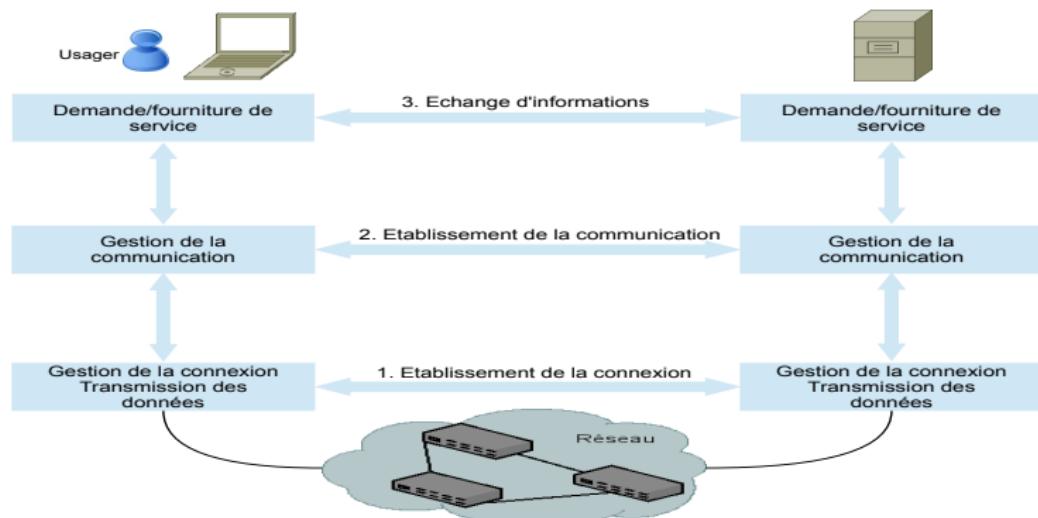
- Un réseau permet de :
 - partager des fichiers
 - partager des applications
 - partager des périphériques : imprimantes ...
 - communiquer entre personnes : courrier électronique, la discussion en direct ...
 - communiquer entre processus : logiciels d'entreprise ...
 - garantir l'unicité de l'information : bases de données ...
- Il faut une infrastructure de réseau fiable, rapide et sécurisée comprenant
 - machines d'extrémité
 - équipements de raccordement
 - supports physiques

Architecture générale d'un réseau



Principe de la communication en réseau

- Usagers (services, applications) à l'origine de la procédure de communication
- Etablissement de la communication entre systèmes informatiques à partir du réseau



1

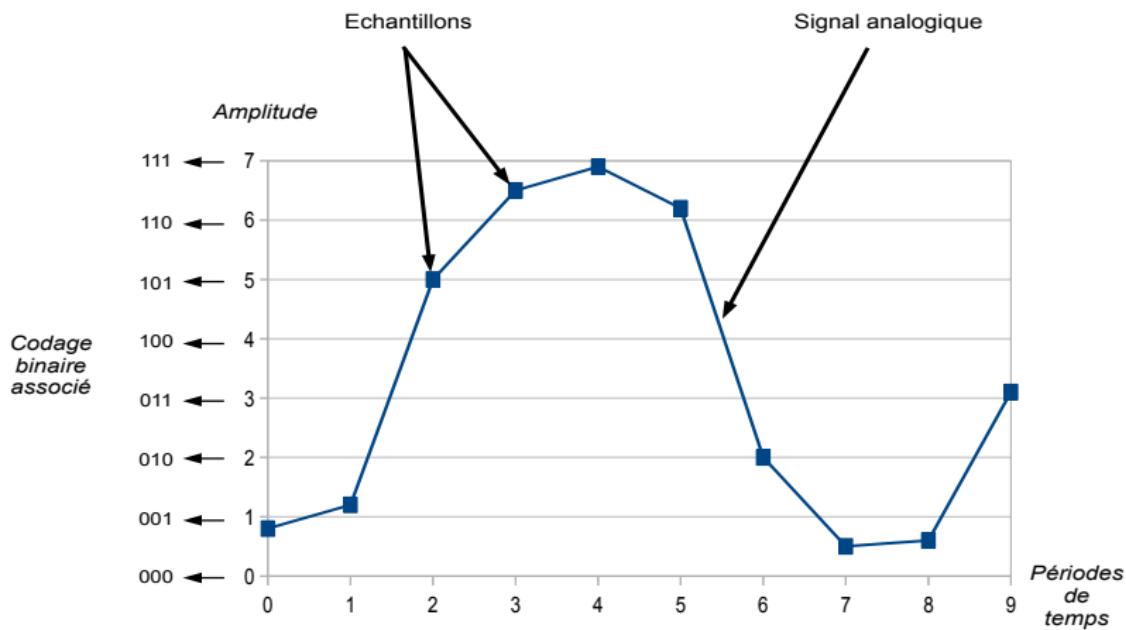
Introduction

- Qu'est ce qu'un réseau ?
- **La représentation de l'information**
- La transmission en série
- Notion de protocole

- Deux types de données :
 - numériques : suite d'éléments indépendants (ex. texte)
 - analogiques : signaux de type continu (ex. voix, son)
- Les données manipulées par les ordinateurs sont codées en binaire
 - base 2 : des "0" et des "1" (*bits*)
 - regroupement des bits en octets : 1 octet (*byte*) = 8 bits
 - alternative : base hexadécimale ($16=2^4$)
- Exemples
 - codage ASCII des caractères alphanumériques sur 8 bits
 - codage hexadécimal des couleurs utilisées dans les pages Web

Numérisation des données analogiques

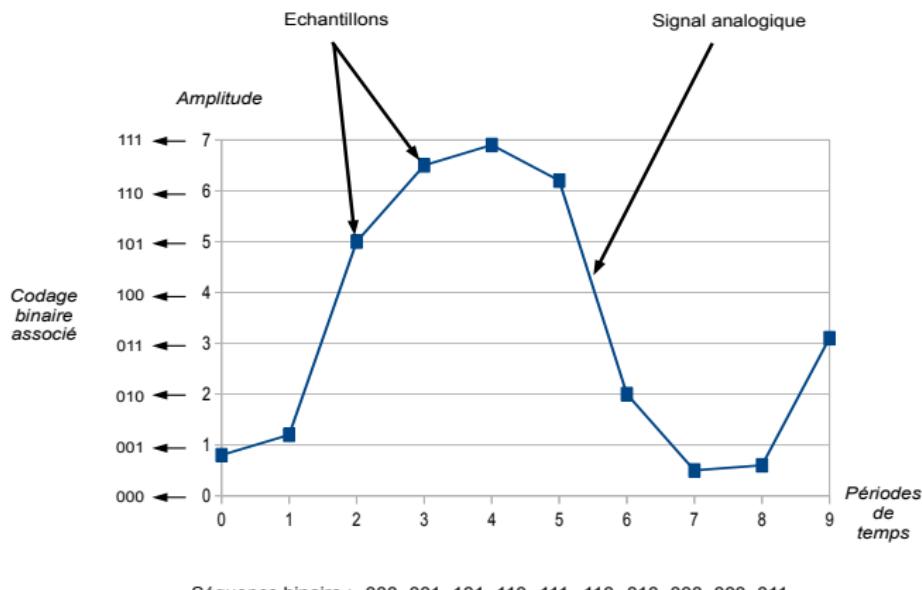
- Par échantillonnage et codage pour transmission via paquets IP : microphone, webcam ...



Séquence binaire : 000 001 101 110 111 110 010 000 000 011

Numérisation des données analogiques

- La fidélité dépend de la fréquence d'échantillonnage et de la profondeur du codage
 - qualité CD : fréquence de 44,1kHz et 16 bits par voie stéréo
 - qualité téléphonique : 8 kHz et 8 bits



1

Introduction

- Qu'est ce qu'un réseau ?
- La représentation de l'information
- La transmission en série**
- Notion de protocole

- Transmission sur le support physique sous forme
 - analogique : ex. liaison par modem ADSL
 - numérique : ex. réseaux locaux Ethernet
- Transmission série
 - éléments binaires transmis les uns à la suite des autres sur des distances relativement longues



- Débit = nombre de bits transmis par unité de temps
- Unités de mesure
 - le bit par seconde (*bit/s* ou *bps*)
 - ne pas confondre avec *baud* = nombre de symboles transmissibles par unité de temps
 - 1 kbit/s = 1000 bit/s
 - 1 Mbit/s = 1 000 000 bit/s
 - 1 kilooctet (Ko) = 1000 bits
 - 1 kibioctet (Kio) = 2^{10} bits
- En 2010

Type de réseau	Débit maximum
WAN	40 Gbit/s
MAN	10 Gbit/s
LAN	1Mbit/s - 100Gbit/s

- On distingue
 - débit descendant (*download*) : données en bit/s que l'on peut télécharger depuis l'Internet
 - débit montant (*upload*) : données en bit/s que l'on peut expédier sur l'Internet
- Ne pas oublier que le débit d'une chaîne (le chemin entre 2 ordinateurs connectés à l'Internet) est égal au débit du maillon le plus faible

- Logo de la page d'accueil de Google

- www.google.fr/intl/fr_fr/images/logo.gif
- image de 8866 octets = 70928 bits
- estimation faite sans compter les informations additionnelles qui sont expédiées par le serveur web

débit	temps de téléchargement
10 kbit/s	7 sec
100 kbit/s	0.7 sec

- Page d'accueil de TF1

- www.tf1.fr
- environ 800ko = $800 \times 1024 \times 8 = 6,5$ Mbits

débit	temps de téléchargement
10 kbit/s	11 min
100 kbit/s	1 min 5 sec
1 Mbit/s	6 à 7 sec

1

Introduction

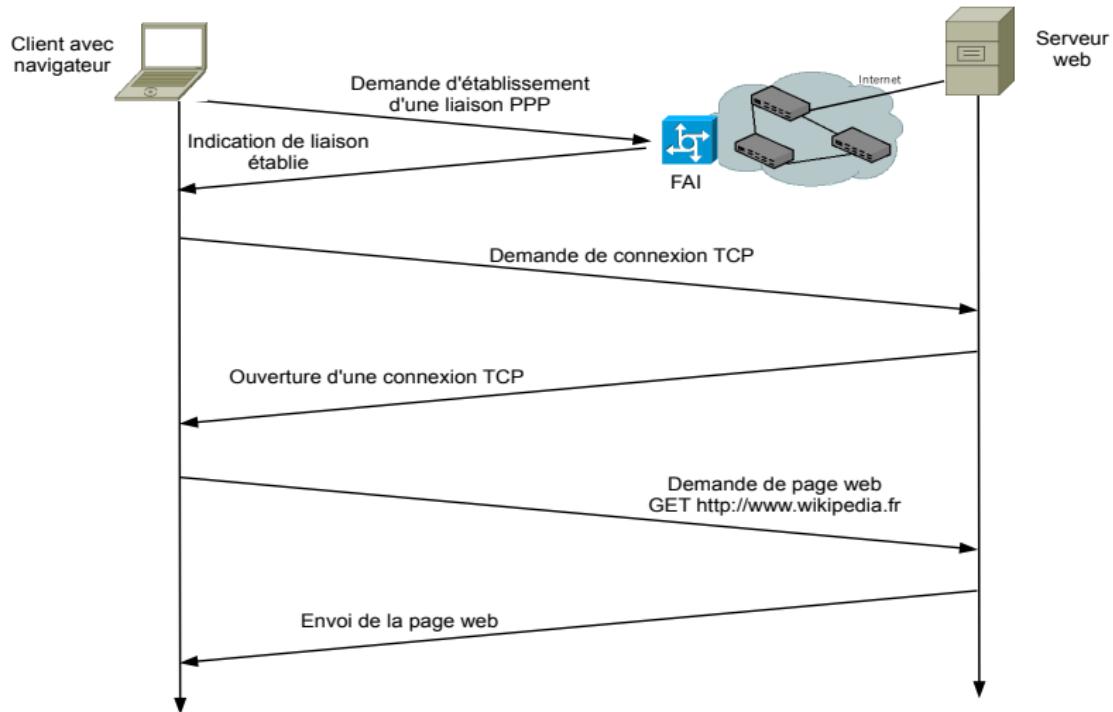
- Qu'est ce qu'un réseau ?
- La représentation de l'information
- La transmission en série
- Notion de protocole

Notion de protocole

- Un protocole = ensemble de règles suivies par les équipements dans le but d'échanger des informations
 - les formats des informations font partie du protocole
- Internet associe des protocoles à différentes couches

COUCHES	PROTOCOLES	SERVICES
services	HTTP SMTP, POP, IMAP SOAP	Web courriel services web
acheminement des données	TCP IP RIP	transport adressage routage
établissement de liaison	PPP ATM	liaison modem usager et FAI liaisons au coeur d'Internet

Exemple simplifié d'utilisation de protocoles à différents niveaux



1 Introduction

2 Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI
- Le cœur de réseau
- Délais, pertes et QoS
- Architecture des réseaux

3 Les Services

4 Le Transport des Données

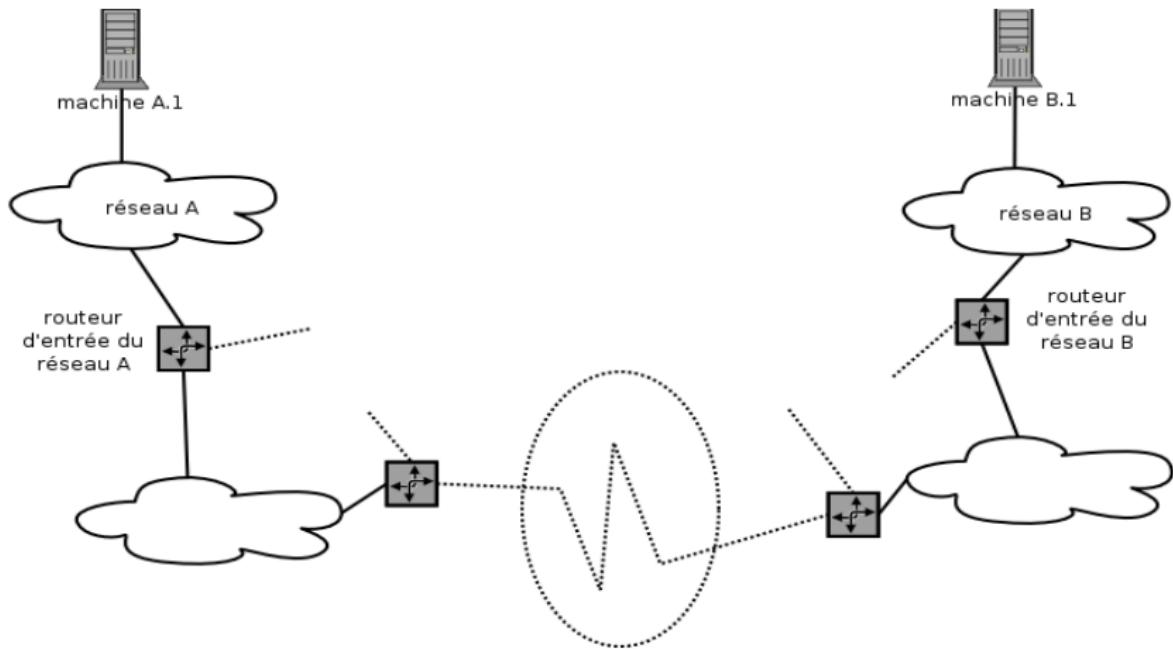
5 L'Adressage et le Routage

6 Sécurité sur Internet

2 Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI
- Le cœur de réseau
- Délais, pertes et QoS
- Architecture des réseaux

- **INTER**connected **NET**works : réseaux interconnectés



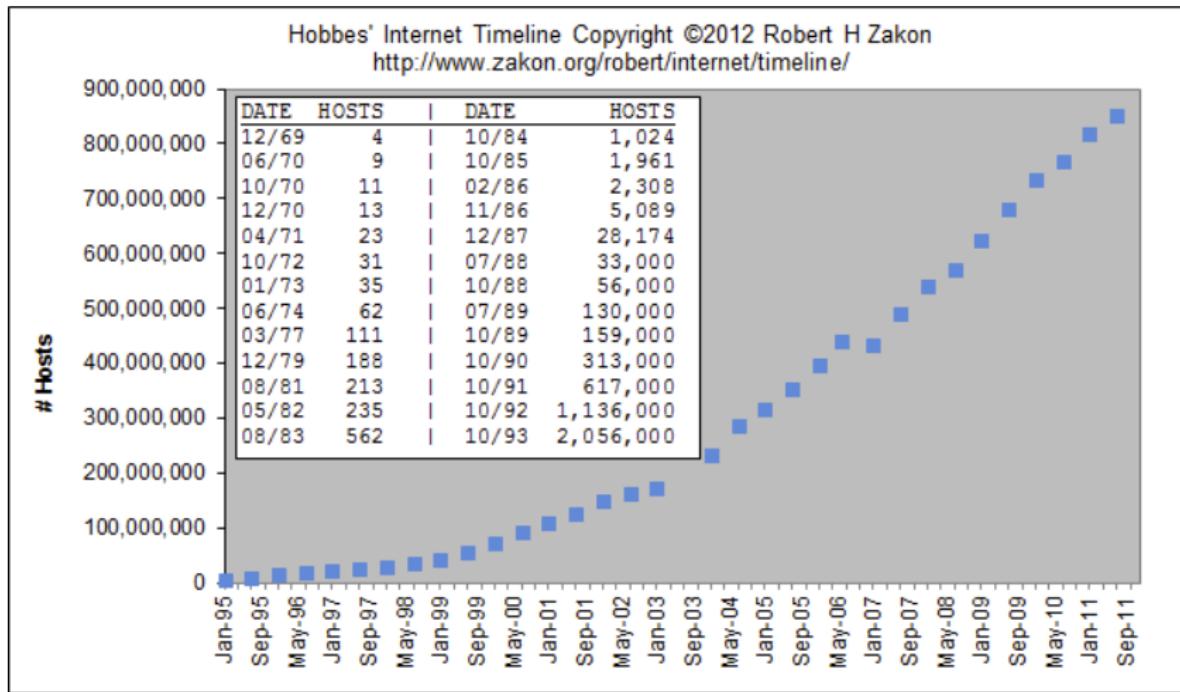
- **INTER**connected **NET**works : réseaux interconnectés
- Réseau de réseaux d'ordinateurs répartis sur le monde entier ... ou presque !
- Basé sur la famille de protocoles TCP/IP (Transmission Control Protocol / Internet Protocol)
- Ensemble de serveurs offrant des services à des clients
- Fonctionnement "autogéré"
- Financement "mutualisé"

- **INTER**connected **NET**works : réseaux interconnectés
- Réseau de réseaux d'ordinateurs répartis sur le monde entier ... ou presque !
- Basé sur la famille de protocoles TCP/IP (Transmission Control Protocol / Internet Protocol)
- Ensemble de serveurs offrant des services à des clients
- Fonctionnement "autogéré"
- Financement "mutualisé"

Ne pas confondre Internet et Web !

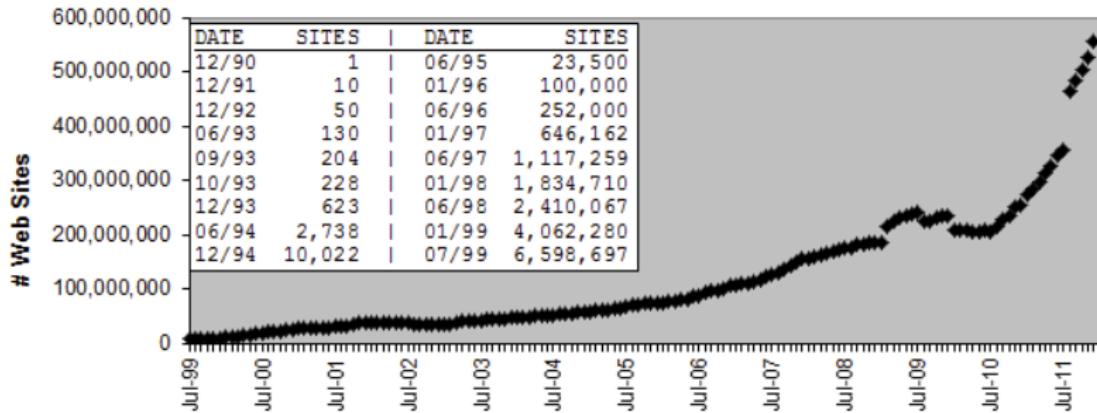
Le Web est l'**un** des services disponibles par Internet

Quelques chiffres : les ordinateurs connectés



Quelques chiffres : les sites web

Hobbes' Internet Timeline Copyright ©2012 Robert H Zakon
<http://www.zakon.org/robert/internet/timeline/>

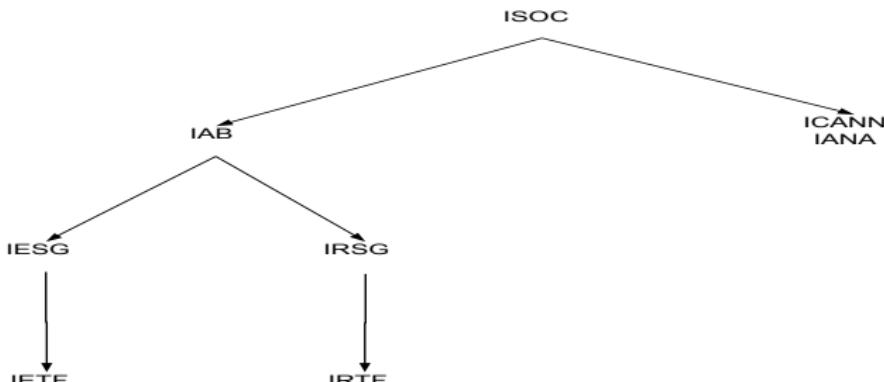


2 Les Réseaux et l'Internet

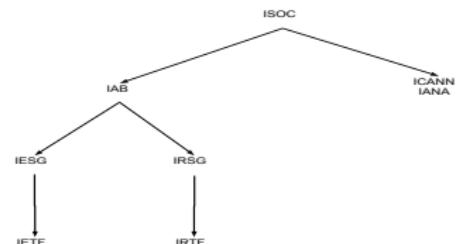
- Généralités
- **Organisation de l'Internet**
- Les réseaux d'accès et les FAI
- Le cœur de réseau
- Délais, pertes et QoS
- Architecture des réseaux

L'Administration d'Internet

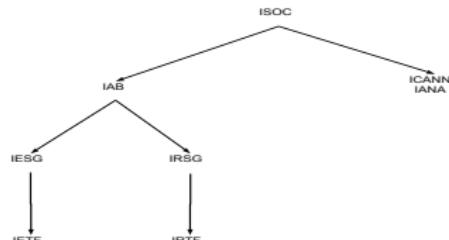
ACRONYME	ORGANISATION	SITE WEB
ISOC	Internet Society	www.isoc.org
ICANN	Internet Corp. for Assigned Names and Numbers	www.icann.org
IANA	Internet Assigned Numbers Authority	
IAB	Internet Architecture Board	www.iab.org
IESG	Internet Engineering Steering Group	
IETF	Internet Engineering Task Force	www.ietf.org
IRSG	Internet Research Steering Group	
IRTF	Internet Research Task Force	www.irtf.org



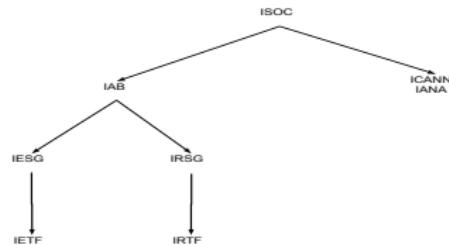
L'Administration d'Internet



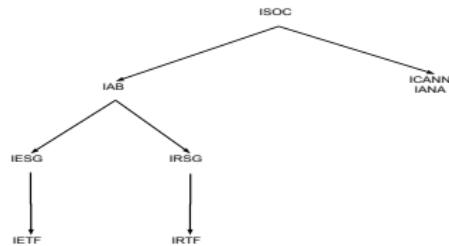
- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN



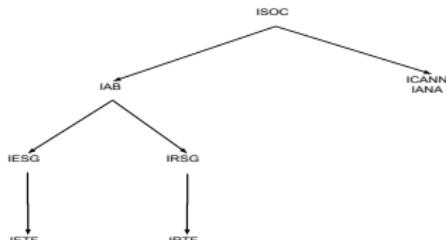
- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP



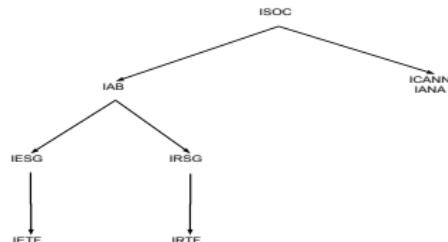
- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP
- L'**ICANN** gère la distribution des adresses IP, des noms de domaine de haut niveau (.com, .org, .fr ...), des numéros identifiant les protocoles de l'Internet et maintient les serveurs DNS de la racine



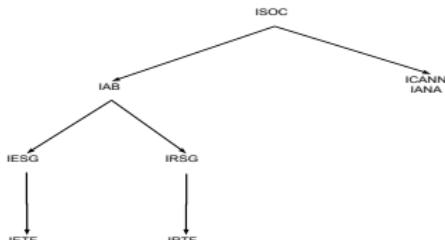
- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP
- L'**ICANN** gère la distribution des adresses IP, des noms de domaine de haut niveau (.com, .org, .fr ...), des numéros identifiant les protocoles de l'Internet et maintient les serveurs DNS de la racine
- L'**IESG** supervise l'IETF



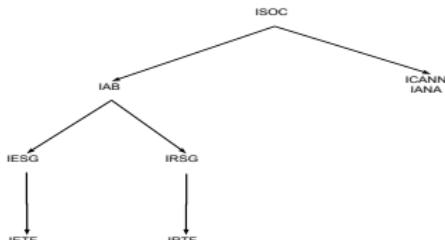
- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP
- L'**ICANN** gère la distribution des adresses IP, des noms de domaine de haut niveau (.com, .org, .fr ...), des numéros identifiant les protocoles de l'Internet et maintient les serveurs DNS de la racine
- L'**IESG** supervise l'IETF
- L'**IETF** établit les spécifications, réalise les premières implantations des nouveaux protocoles du modèle TCP/IP, produit les normes de l'Internet appelées *Request For Comments (RFC)*



- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP
- L'**ICANN** gère la distribution des adresses IP, des noms de domaine de haut niveau (.com, .org, .fr ...), des numéros identifiant les protocoles de l'Internet et maintient les serveurs DNS de la racine
- L'**IESG** supervise l'IETF
- L'**IETF** établit les spécifications, réalise les premières implantations des nouveaux protocoles du modèle TCP/IP, produit les normes de l'Internet appelées *Request For Comments (RFC)*
- L'**IRSG** supervise l'IRTF



- L'**ISOC** supervise le développement de l'Internet et exerce une autorité morale et technique sur l'IAB et l'ICANN
- L'**IAB** suit l'évolution des protocoles du modèle TCP/IP
- L'**ICANN** gère la distribution des adresses IP, des noms de domaine de haut niveau (.com, .org, .fr ...), des numéros identifiant les protocoles de l'Internet et maintient les serveurs DNS de la racine
- L'**IESG** supervise l'IETF
- L'**IETF** établit les spécifications, réalise les premières implantations des nouveaux protocoles du modèle TCP/IP, produit les normes de l'Internet appelées *Request For Comments (RFC)*
- L'**IRSG** supervise l'IRTF
- L'**IRTF** prévoit l'évolution des protocoles, architectures et technologies de l'Internet sur le long terme et prépare les travaux futurs de l'IETF



- Organisation internationale à but non lucratif
 - créée en 1992
 - supervise le développement de l'Internet
 - veille à ce qu'il reste un modèle ouvert
 - environ 170 organisations membres dans 180 pays, près de 30 000 membres (personnes physiques)
 - chapitre français (ISOC France - www.isoc.fr) est une association loi 1901 créée en mars 1996
- Espace de décision pour choisir les évolutions techniques, économiques et politiques
- Mission : assurer l'essor, l'évolution et l'utilisation de l'internet pour le bienfait de toutes et tous à travers le monde

- ➊ Facilite le développement accessible (ouvert) de normes et de protocoles, l'administration et les structures techniques de l'internet
- ➋ Soutient la formation dans les pays en développement et où le besoin existe
- ➌ Soutient le développement professionnel et encourage les occasions de contacts avec les chefs de file de l'internet
- ➍ Fournit des informations fiables sur l'internet

- ⑤ Organise des forum de discussions sur des questions touchant à l'évolution, au développement et à l'utilisation de l'internet (aux plans technique, commercial , social . . .)
- ⑥ Développe un environnement favorable à la coopération internationale, à la communauté et une culture qui rend possible l'autogestion
- ⑦ Sert de point focal pour les efforts communs de promotion de l'internet en tant qu'outil fiable pour tous les peuples du monde
- ⑧ Donne la direction et permet la coordination des efforts sur les plans humanitaire, éducatif, sociaux . . .

- Organisation de droit privé à but non lucratif issue de l'IANA
- Alloue les adresses IP de manière décentralisée et hiérarchique
 - le **RIPE Network Coordination Centre** s'en charge pour l'Europe (www.ripe.net)
- Attribue les identificateurs de protocole
- Gère le système de nom de domaine de premier niveau pour les codes génériques (tels que .com, .info ...) et les codes nationaux (.fr, .uk ...)
- Assure les fonctions de gestion du système de serveurs de noms racines

Request For Comments

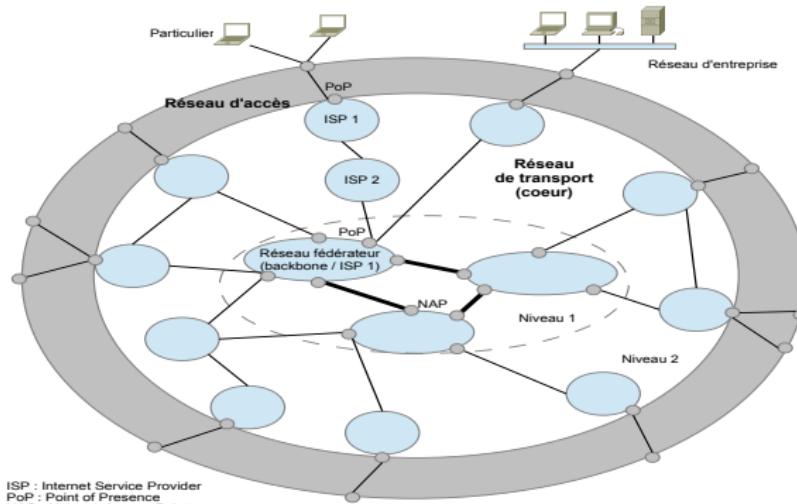
- Les RFC sont numérotés et accessibles
 - www.ietf.org/rfc.html
 - www.ietf.org/rfc/rfcNNNN.txt où NNNN est le numéro de RFC recherché
 - www.rfc-editor.org
- Les RFC sont au format texte
- Les RFC sont catégorisés
 - standard-tracks : normes officielles
 - *proposed standard*
⇒
draft standard
⇒
Internet standard
 - best current practices
 - informational, experimental
 - historique

Le W3C (www.w3.org) est un organisme international

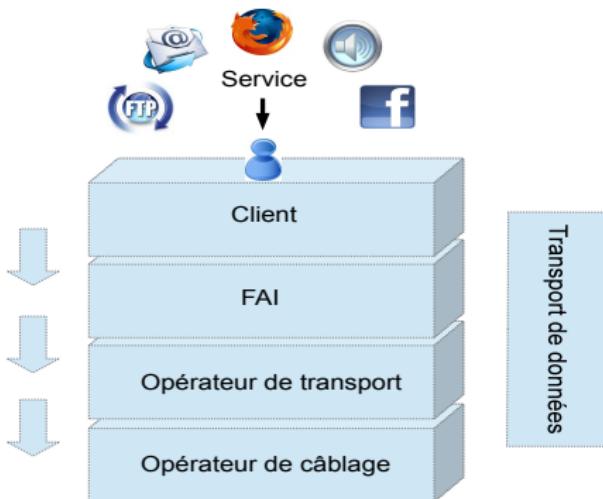
- chargé de la standardisation du web
- dirigé par Tim Berners-Lee l'inventeur du web
- “a pour but de mener le web à sa pleine capacité en développant les protocoles et les recommandations qui assurent sa croissance à long terme”

Structure de l'Internet

- Trois niveaux physiques
 - équipements d'extrême situés chez le particulier ou l'entreprise (PC, serveurs ...)
 - réseau d'accès (boucle locale, répartiteurs ...) connecte le particulier ou l'entreprise au réseau cœur
 - réseau cœur (routeurs, liaisons haut débit ...) achemine les données



- Quatre niveaux fonctionnels
 - les services et protocoles associés
 - les clients et leurs outils logiciels
 - les fournisseur d'accès (FAI)
 - les opérateurs de transport et de câblage du réseau



2 Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI**
- Le cœur de réseau
- Délais, pertes et QoS
- Architecture des réseaux

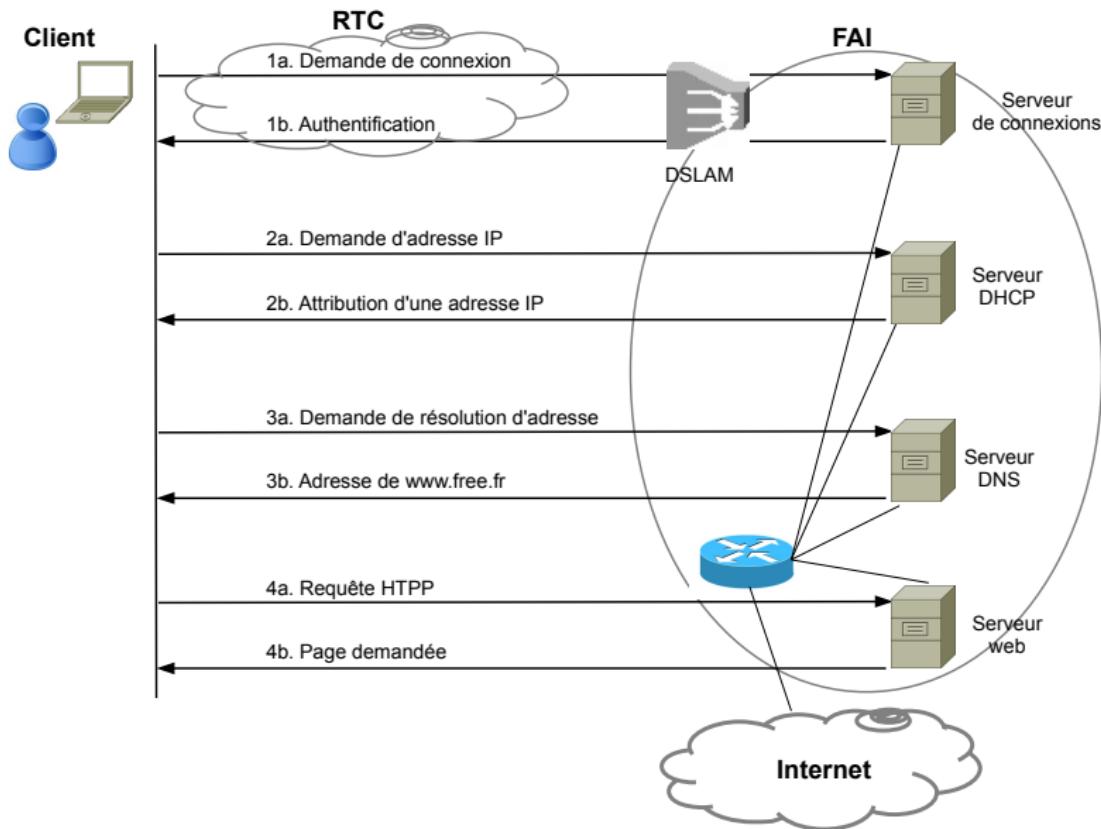
- Les réseaux d'accès (ou de distribution) relient les réseaux de particuliers et d'entreprises aux réseaux d'opérateurs
- Les FAI fournissent
 - des services de connexion et les équipements nécessaires
 - RTC, RNIS, ADSL, câble, fibre optique, WiMax
 - modem, DSLAM, serveur de connexion, serveur d'authentification, pare-feu ...
 - des adresses IP aux particuliers ou PME/PMI
 - des services : messagerie, connexion aux serveurs web ...
- Et éventuellement
 - des serveur DNS et DHCP
 - un serveur de messagerie et un portail Web
 - un serveur "proxy"

Pour connecter un ordinateur à l'internet il faut :

- un moyen physique : un raccordement (ligne téléphone, câble, liaison satellite ...)
- un moyen logique : une adresse IP fournie par un fournisseur d'accès Internet (FAI) qui fournit également l'adresse d'un ou plusieurs DNS
- Quand on a un raccordement et un abonnement, établir la connexion se décompose en 3 étapes :
 - ① l'ordinateur personnel établit un 1^{er} contact avec un ordinateur de son FAI
 - ② L'ordinateur personnel s'authentifie auprès de son FAI via un identifiant et un mot de passe
 - ③ Le FAI envoie une adresse IP et les adresses IP de un ou plusieurs DNS que l'ordinateur personnel utilise pour sa configuration

Les protocoles utilisés sont PPP, PPPOE ou DHCP selon les types de connexion

Exemple de communication entre un client et son FAI



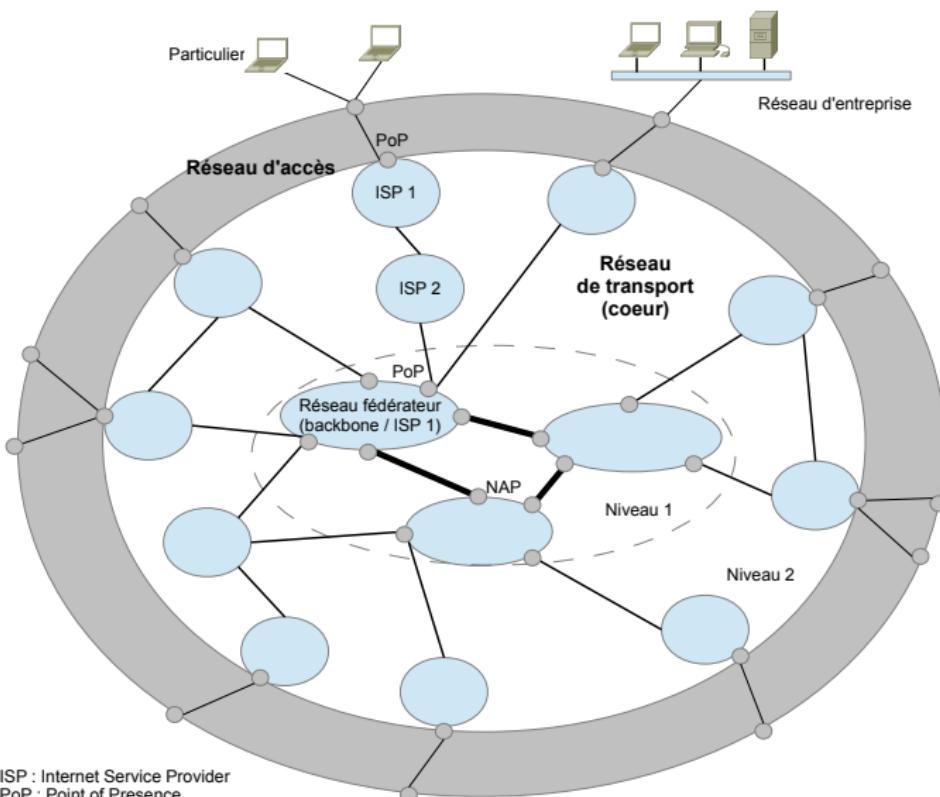
- L'accès permanent ou non ⇒ héberger ou non des serveurs sur son poste, faire du P2P ...
- Le débit (descendant et montant) plus ou moins élevé ⇒ navigation sur le web + ou - rapide, téléchargement et envois de mails avec fichiers attachés + ou - rapide
- La réactivité du réseau ou temps de latence (temps pour faire un aller-retour entre les 2 ordinateurs, testé par la commande ping) ⇒ jeux en réseaux + ou - réactifs, flux vidéo + ou - fluide
- La quantité de données téléchargées limitée ou non
- Le service (débit, connectivité ...) garanti ou minimum garanti,
- Le prix, le support (hotline) ...

2

Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI
- Le cœur de réseau**
- Délais, pertes et QoS
- Architecture des réseaux

Réseaux de transport

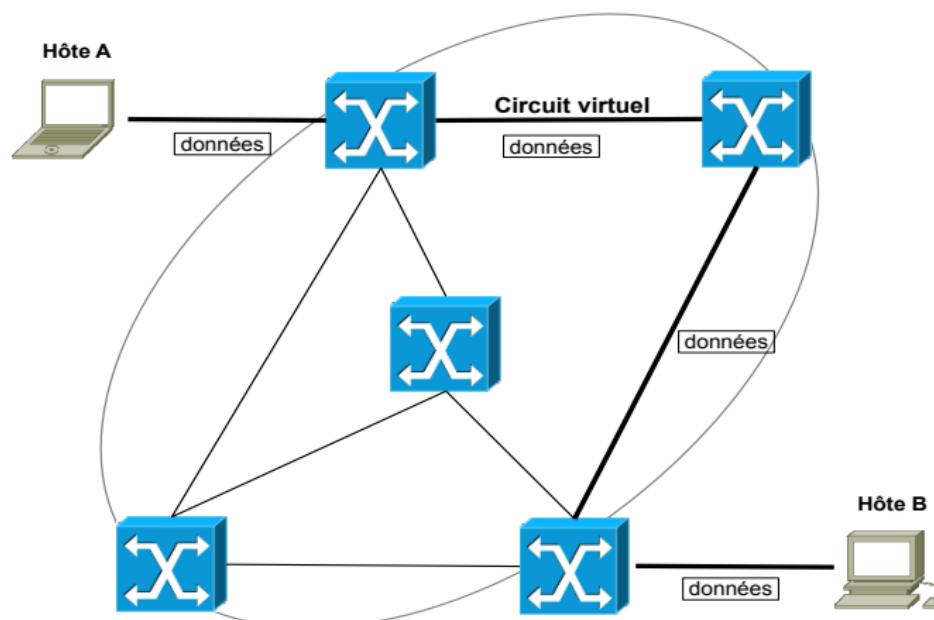


- Les réseaux fédérateurs (*backbone ISP* ou ISP de niveau 1) ont une couverture internationale
 - reliés entre eux par des *Network Access Point* (NAP)
 - le débit de ces liaisons peut atteindre 40Gbit/s
- Les ISP de niveau 2 ou 3 ont une couverture nationale ou régionale
 - reliés aux ISP 1 par des *Point of Presence* (POP)
 - débit de l'ordre du Gbit/s
 - exemple : RENATER est un ISP 2 reliant les universités et centres de recherche en France

- Commutation de circuits
 - exemple : le réseau téléphonique commuté (RTC)
 - le lien physique ou logique est établi durant tout échange entre émetteur et récepteur
 - garantit la largeur de bande
 - multiplexage fréquentiel et temporel pour faire passer plusieurs communications sur une même ligne
- Commutation de paquets
 - pour l'échange de données numérisées
 - messages découpés en paquets de longueur fixe
 - paquets transmis de commutateur en commutateur
- Commutation de cellules
 - exemple : réseau ATM (*Asynchronous Transfer Mode*)
 - pour garantir des délais de transmission acceptables pour la voix et la vidéo
 - cellules émises à intervalles de temps constant

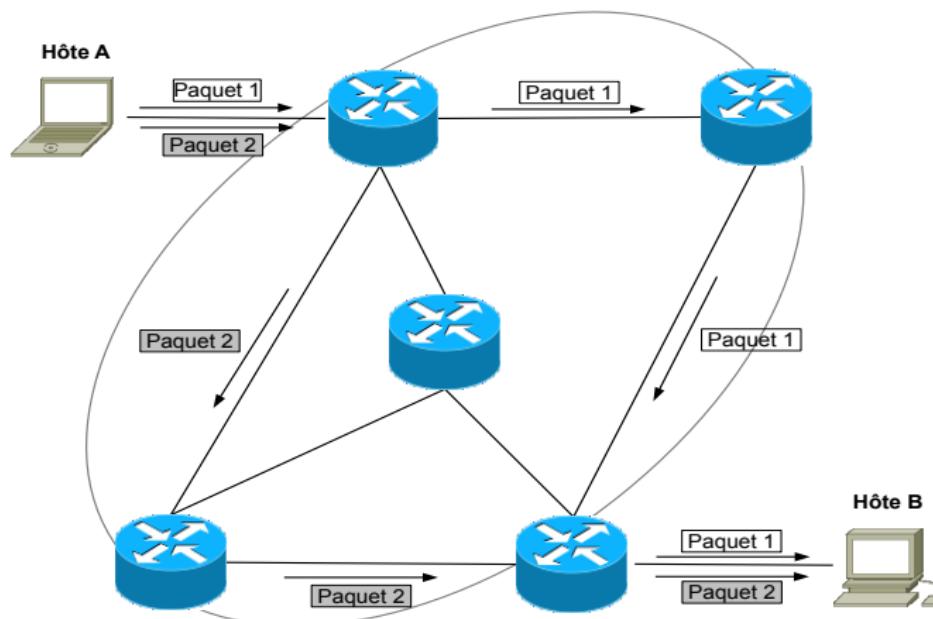
Réseaux à commutation de paquets

- La transmission des données s'effectue en mode connecté
 - les données suivent le même chemin pendant toute la session



Réseaux à routage de paquets

- La transmission des données s'effectue en mode datagramme
 - les paquets peuvent suivre des chemins différents
 - cas de l'Internet

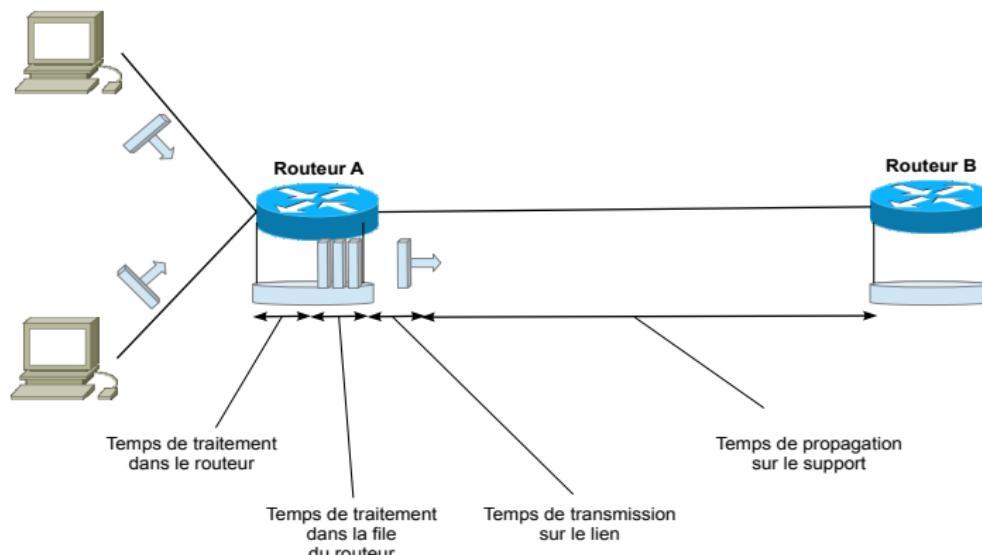


2 Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI
- Le cœur de réseau
- **Délais, pertes et QoS**
- Architecture des réseaux

Délais dans les réseaux IP

- Les réseaux de l'Internet sont de type *best-effort*
 - aucune garantie sur le délais et taux de pertes
 - en général, temps de transmission $>>$ temps de propagation



- Temps de traitement dans le routeur
 - durée pour la lecture et l'analyse d'en-têtes de paquets, durée du routage, temps de contrôle des erreurs
 - ordre de la μs
- Temps d'attente dans la file du routeur
 - dépend du trafic (nombre de paquets) et durée de traitement de la file (politiques, priorités)
 - ordre de la μs à ms

- Temps de transmission sur le lien
 - délai entre début et fin de la transmission d'un message sur une ligne
 - = longueur du message / débit de la ligne

- Temps de propagation sur le support
 - temps pour qu'un signal parcourt un support d'un point à un autre
 - fonction du support, de la distance et la fréquence du signal

Support	Vitesse
satellite	$7\mu\text{s}/\text{km}$
réseau téléphonique à paires métal.	$10\text{-}40\mu\text{s}$
réseau Ethernet	$4\mu\text{s}/\text{km}$

- Les pertes proviennent des limites du support et de la charge du réseau
 - capacité du support = débit binaire maximal
 - capacité fonction de la bande passante et du rapport signal à bruit
- Congestion de réseau IP : le nombre de paquets perdus augmente avec l'intensité du trafic
 - les files d'attente des routeurs sont saturées
 - des mécanismes de détection de pertes et retransmission sont nécessaires
- Qualité de service (*QoS*)
 - ensemble des procédures mises en oeuvre pour maîtriser délais, débits et pertes
 - les réseaux IP n'offrent pas de QoS aux applications à l'inverse des réseaux de télécom (RTC, RNIS, ATM)

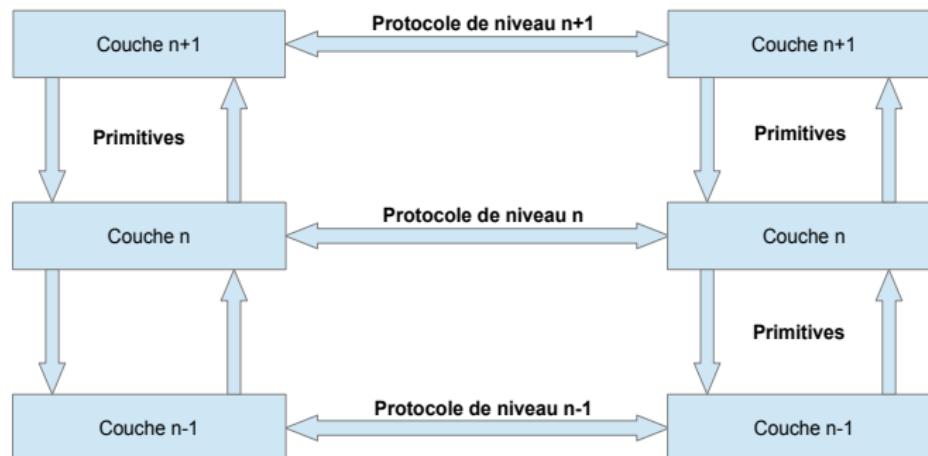
2 Les Réseaux et l'Internet

- Généralités
- Organisation de l'Internet
- Les réseaux d'accès et les FAI
- Le cœur de réseau
- Délais, pertes et QoS
- **Architecture des réseaux**

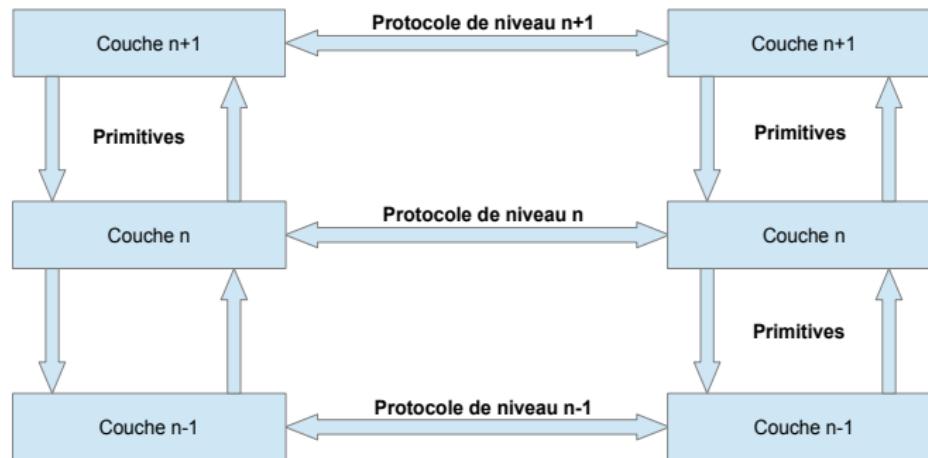
- Les architectures de réseaux sont structurés en couches
- Chaque couche gère un aspect spécifique de l'architecture :
 - caractéristiques physiques du réseau : nature du signal, type de support ...
 - méthode de communication : accusé de réception, envoi direct, détection d'erreurs ...
 - service rendu : transfert de fichiers, messagerie ...
- Deux équipements doivent suivre le même modèle pour pouvoir communiquer

Primitives de services

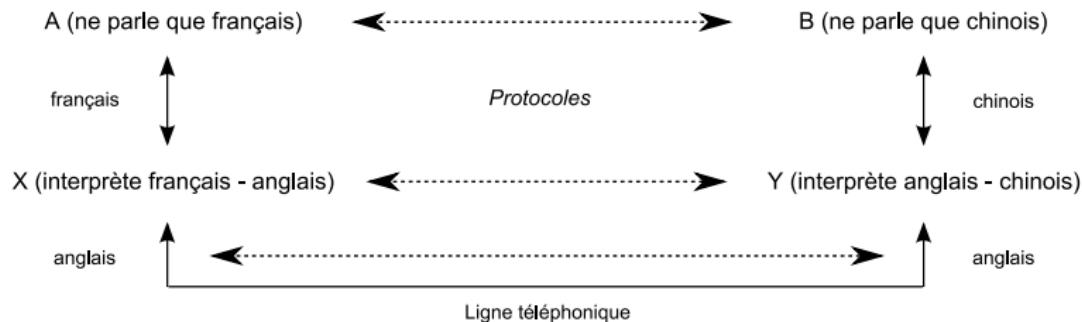
- Les couches adjacentes s'échangent des informations par le biais de primitives de service
 - chaque couche fournit des services à la couche au-dessus
 - chaque couche utilise les services de la couche en-dessous



- Les couches de même niveau communiquent en suivant un protocole

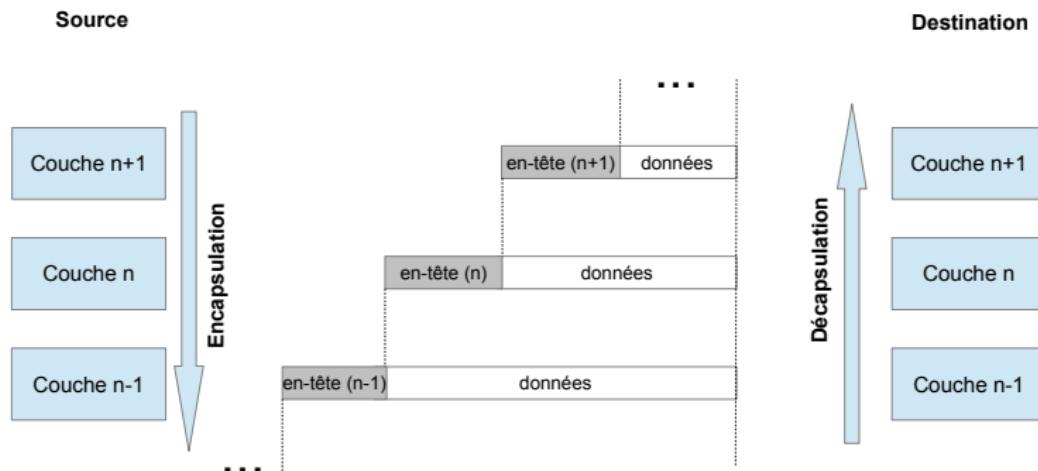


- Communication entre deux personnes ne parlant pas la même langue



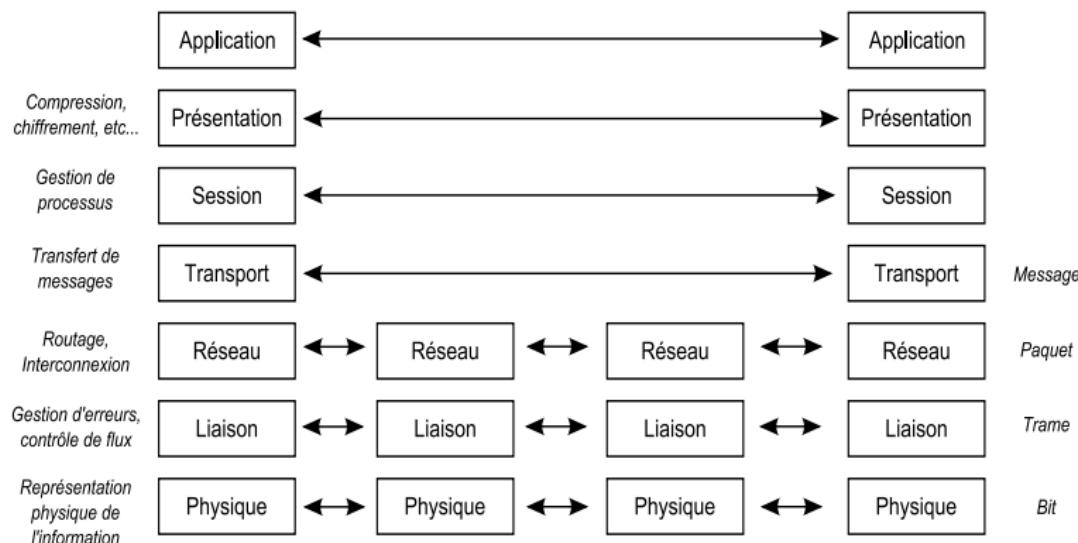
Encapsulation et décapsulation

- Encapsulation lors de l'émission de données
 - chaque couche encapsule les données venant de la couche supérieure en y ajoutant ses propres informations et remet le résultat à la couche inférieure
 - adresses des équipements, champs pour la correction d'erreurs, numéros de séquence ...
- Décapsulation à la réception



Modèle OSI

- Modèle théorique de référence (*Open Systems Interconnection*) créé en 1984 par l'ISO (*International Standards Organisation*)

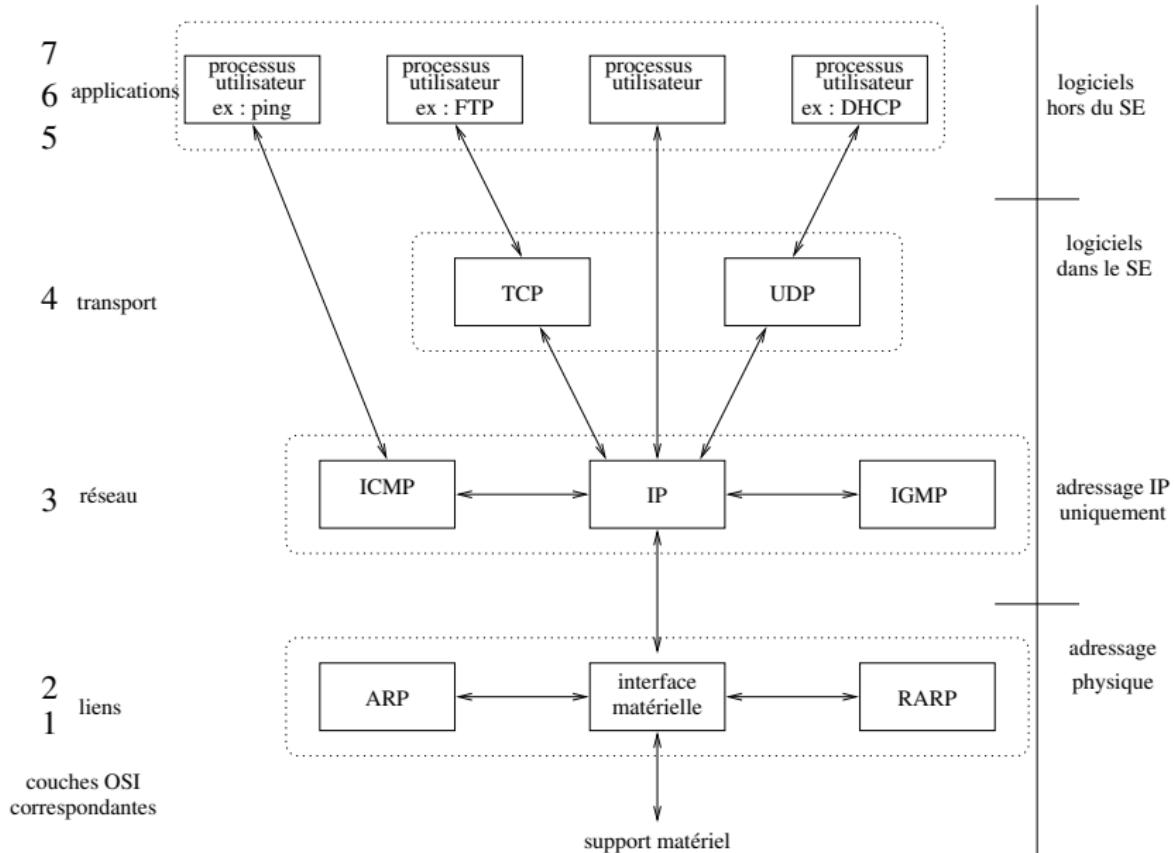


- Conçu par l'ARPANET puis normalisé par l'IETF
- Définit l'architecture des réseaux de l'Internet
 - TCP = Transport Control Protocol
 - IP = Internet Protocol
- Grands principes
 - fractionnement des messages en paquets
 - utilisation d'un système d'adresses
 - acheminement des données sur le réseau (routage)
 - contrôle des erreurs de transmission de données

Comparaison modèles OSI et TCP/IP

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application
	Couche Présentation
	Couche Session
Couche Transport	Couche Transport
Couche Réseau	Couche Réseau
Couche Liens	Couche Liaison
	Couche Physique

La pile TCP/IP



Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle

- La couche *accès réseau* (ou *liaison*) est l'interface avec le réseau et est constituée d'un pilote du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau
 - ARP (*Address Resolution Protocol*) : convertit une adresse IP en une adresse matérielle (MAC)
 - RARP (*Reverse ARP*) : convertit une adresse MAC en adresse IP

Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle

- La couche *Internet* (ou *réseau*) gère la circulation des paquets à travers le réseau en assurant leur routage
 - ICMP (*Internet Control Message Protocol*) : complète IP pour la gestion d'erreurs
 - IGMP (*Internet Group Management Protocol*) : complète IP pour la gestion de groupes

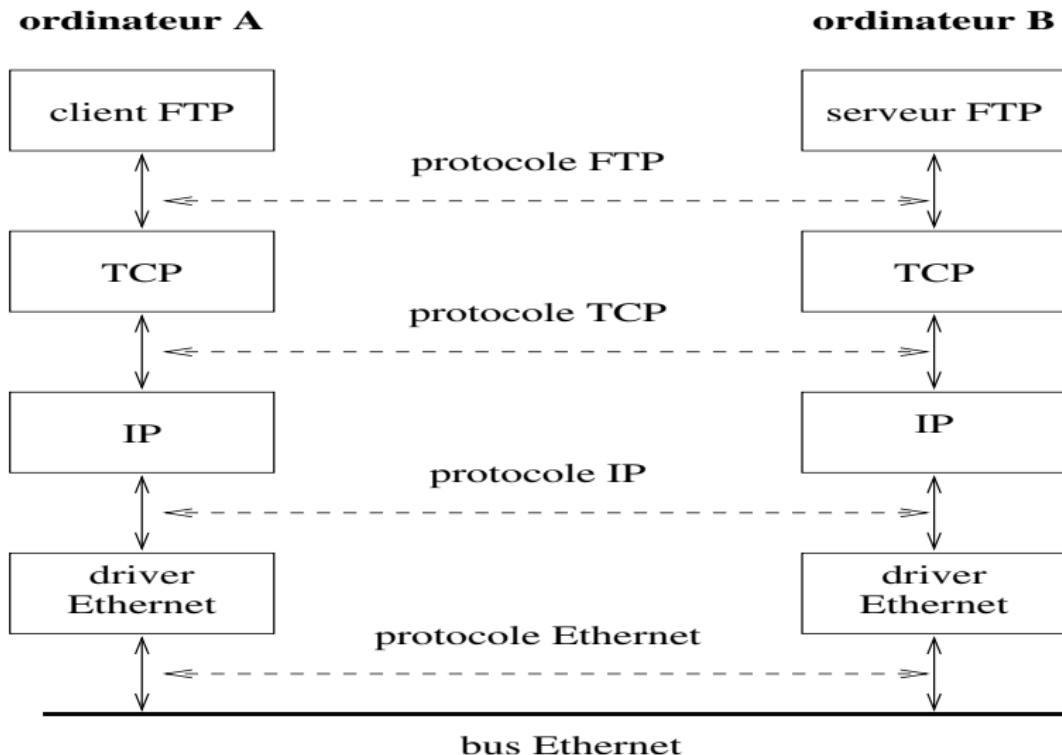
Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle

- La couche *transport* assure une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire
 - Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP
 - Le transport est non fiable dans le cas de UDP (*User Datagram Protocol*). Il n'est pas garanti qu'un paquet (appelé dans ce cas *datagramme*) arrive à bon port, c'est à la couche *application* de s'en assurer

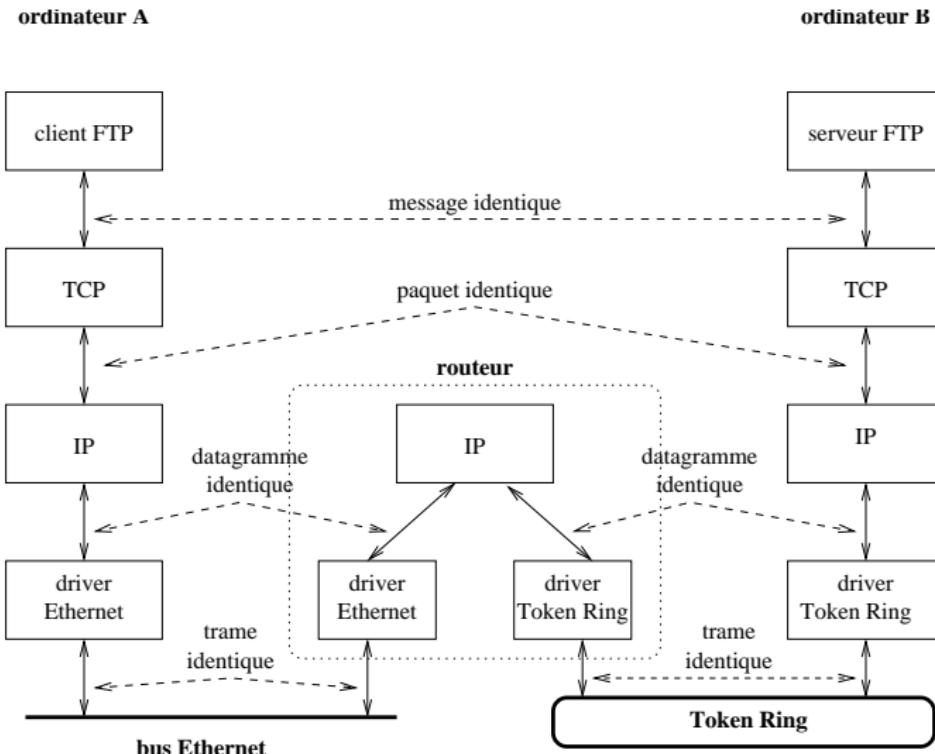
Les logiciels TCP/IP sont structurés en quatre couches de protocoles qui s'appuient sur une couche matérielle

- La couche *application* est celle des programmes utilisateurs comme les navigateurs et serveurs web, les clients et serveurs FTP, SMTP, POP, IMAP...

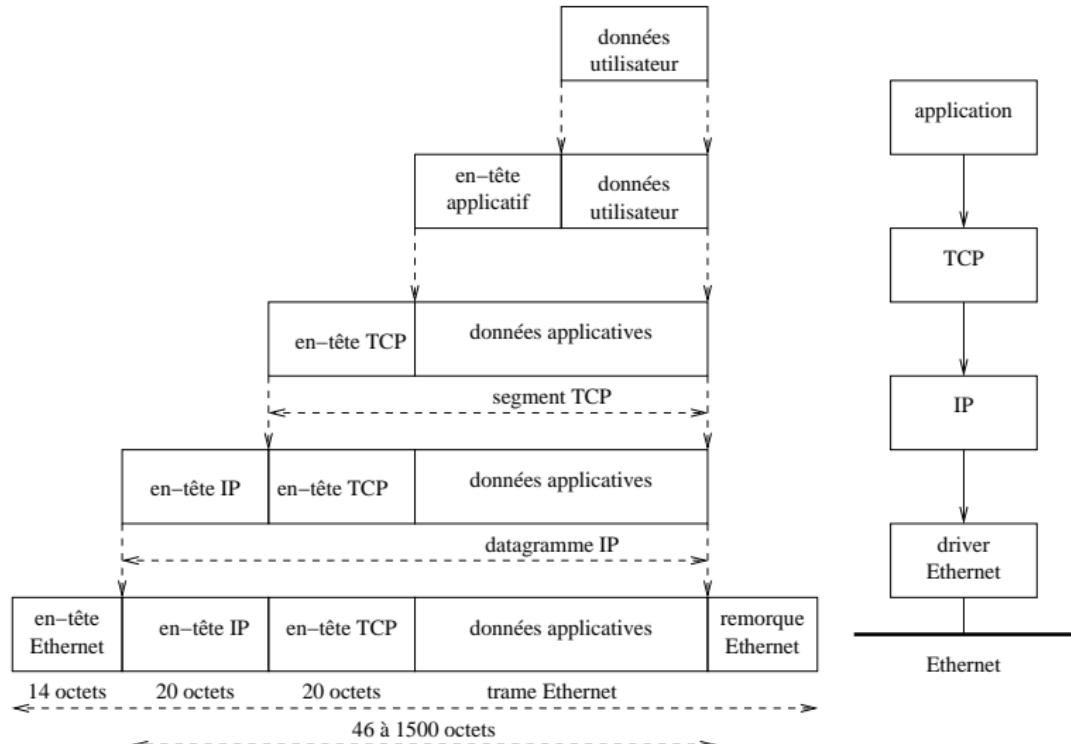
Communication entre 2 machines du même réseau



Interconnexion de 2 réseaux



Encapsulation des données par la pile TCP IP



1 Introduction

2 Les Réseaux et l'Internet

3 Les Services

- Les protocoles applicatifs
- Le nommage DNS
- Le Web
- La messagerie
- La messagerie instantanée
- Les forums de discussion
- Le transfert de fichiers

4 Le Transport des Données

5 L'Adressage et le Routage

6 Sécurité sur Internet

3

Les Services

- Les protocoles applicatifs
 - Le nommage DNS
 - Le Web
 - La messagerie
 - La messagerie instantanée
 - Les forums de discussion
 - Le transfert de fichiers

- Les services sont fournis grâce à des applications logicielles s'exécutant sur les clients et serveurs
- Un protocole applicatif permet la mise en oeuvre d'applications entre un client et un serveur en définissant
 - la séquence de messages échangés
 - le type de messages échangés (demande, réponse, confirmation, etc)
 - la syntaxe adoptée pour chaque type de message (champs et délimitations)
 - la sémantique des différents champs (le sens des informations contenues)
- Les protocoles des couches inférieures gèrent les connexions, les liaisons et à degré variable la qualité de service
 - les applications ont des exigences différentes en termes de pertes, débit et contraintes de temps

Besoins des applications

Application	Caractéristiques du multimédia			
	Débit	Sensible à		
	Délai	Gigue	Perte	
Voix sur IP	Faible	Important	Important	Moyen
Visioconférence	Important	Important	Important	Moyen
Streaming Vidéo à la demande	Important	Moyen	Moyen	Moyen
Streaming Audio	Faible	Moyen	Moyen	Important
Commerce Electronique	Moyen	Moyen	Faible	Important
Courier Electronique	Faible	Faible	Faible	Important
Transfert de fichiers	Moyen	Faible	Faible	Important

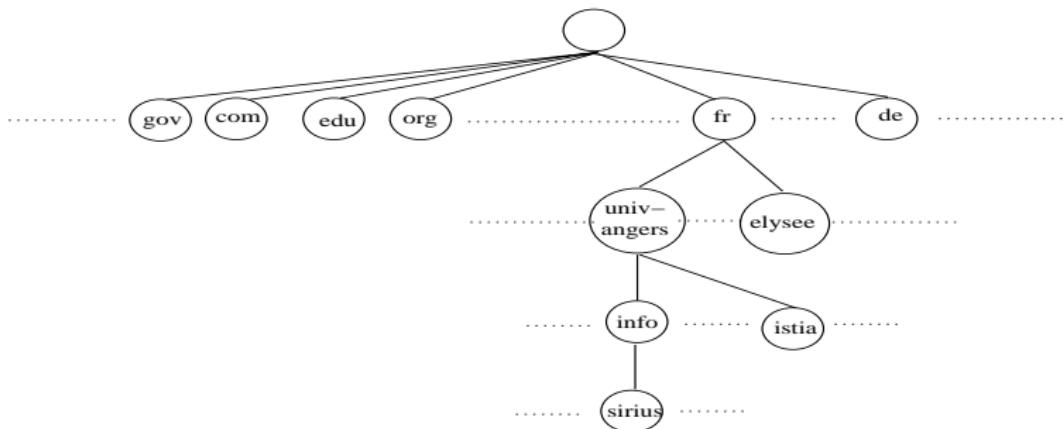
3

Les Services

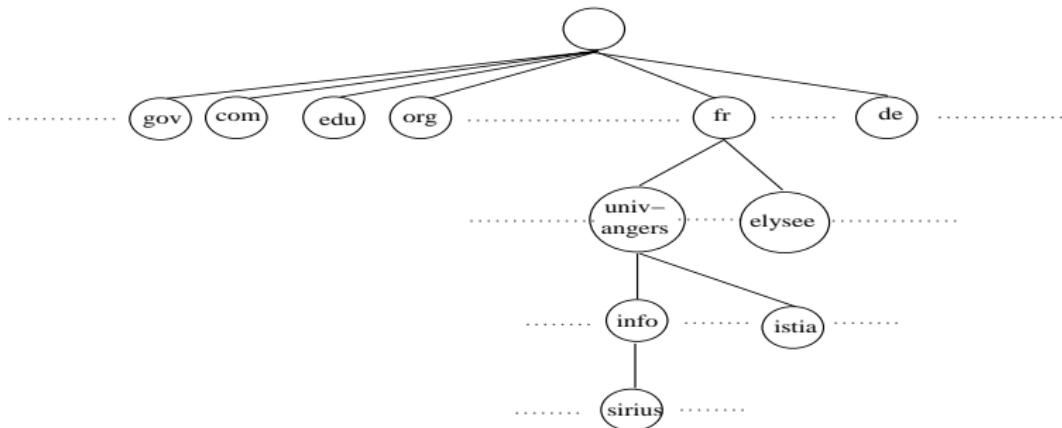
- Les protocoles applicatifs
- **Le nommage DNS**
- Le Web
- La messagerie
- La messagerie instantanée
- Les forums de discussion
- Le transfert de fichiers

- Chaque ordinateur directement connecté à Internet possède au moins une adresse IP propre
- Cependant, il n'est pas pratique de travailler avec des adresses numériques du genre 193.49.146.124
 - ⇒ on préfère généralement travailler avec des adresses URL du type *www.info.univ-angers.fr*
- Le DNS (Domain Name System) est un service qui effectue la correspondance entre les noms symboliques et les adresses IP
 - ⇒ à tout serveur identifié par son nom correspond une ou plusieurs adresses IP de machines hébergeant ce serveur
 - ⇒ à chaque fois que l'on appelle un service (un serveur) par son nom, le logiciel client doit d'abord "résoudre" le nom du service, cad. trouver l'adresse IP de la machine hébergeant ce service. Pour cela, il fait appel à un serveur DNS

Organisation des noms de domaines

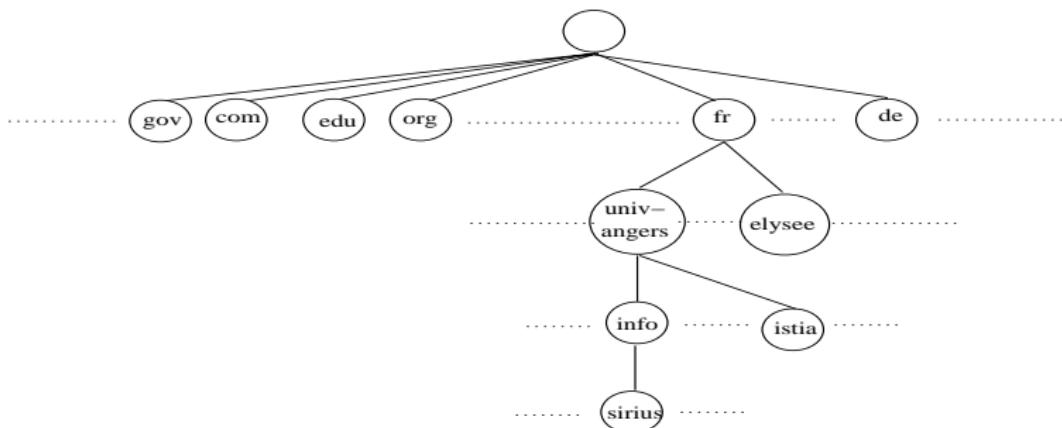


Organisation des noms de domaines



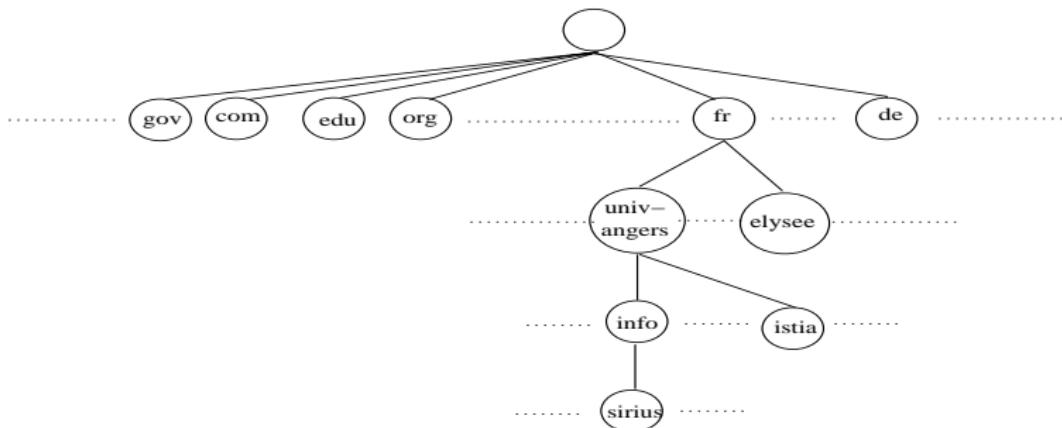
- C'est un espace de noms hiérarchisé
 - $\text{info.univ-angers.fr} \subset \text{univ-angers.fr} \subset \text{fr}$

Organisation des noms de domaines



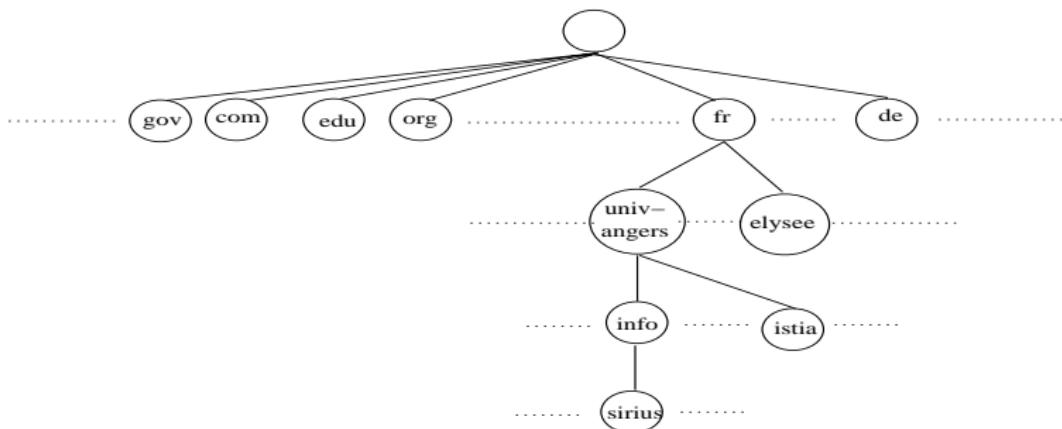
- C'est un espace de noms hiérarchisé
 - .fr, .com, ... sont des TLD (Top Level Domains)

Organisation des noms de domaines



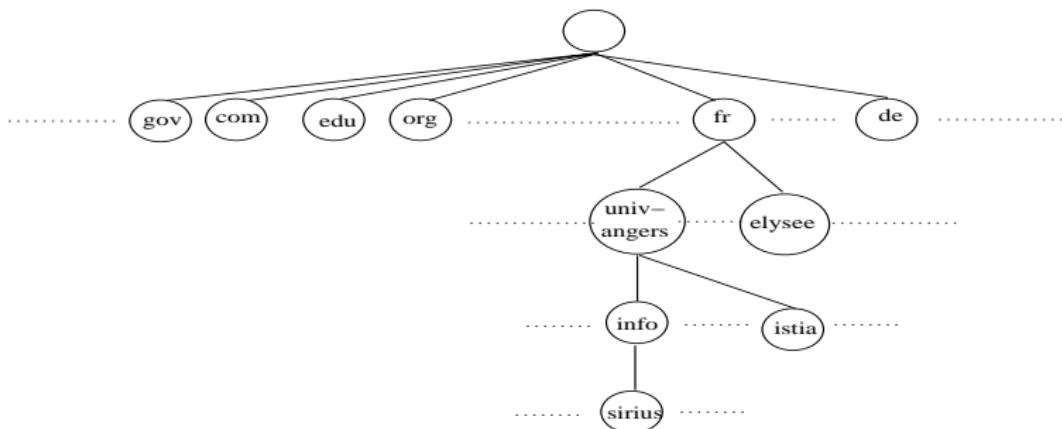
- Chaque niveau dépend du niveau supérieur
 - sirius : département informatique de l'université d'Angers

Organisation des noms de domaines



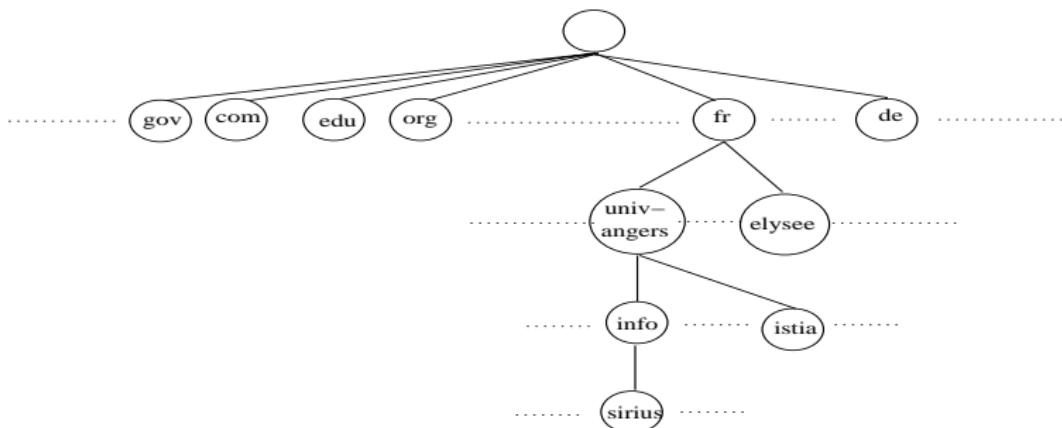
- Chaque niveau dépend du niveau supérieur
 - info : université d'Angers

Organisation des noms de domaines



- Chaque niveau dépend du niveau supérieur
 - univ-angers : AFNIC

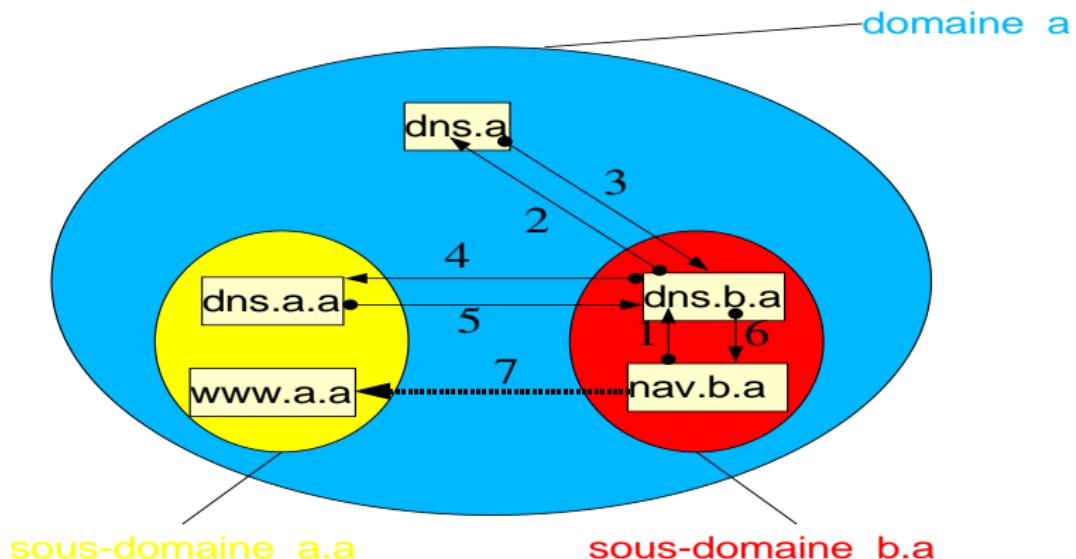
Organisation des noms de domaines



- Chaque niveau dépend du niveau supérieur
 - fr : ICANN

- La résolution d'un nom en une adresse IP est gérée par des serveurs de noms qui représentent une base de données distribuée des noms de domaine
- Quand une entité a reçu l'autorité de gérer une zone, elle doit maintenir au moins deux serveurs de noms : un primaire et un ou plusieurs secondaires
- Quand un serveur reçoit une question : quelle est l'adresse IP de `www.univ-angers.fr`?
 - soit il connaît la réponse (parce que cela concerne son domaine ou qu'il l'a mémorisée temporairement après une requête précédente identique) et il la retourne immédiatement
 - soit il interroge un autre serveur (mode récursif) et retournera la réponse quand il la recevra, soit il indique au demandeur quel serveur interroger (mode itératif) et le demandeur repose sa question à cet autre serveur

Résolution de noms de domaines



http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/dns/dns.html

3

Les Services

- Les protocoles applicatifs
- Le nommage DNS
- **Le Web**
- La messagerie
- La messagerie instantanée
- Les forums de discussion
- Le transfert de fichiers

- Collection de documents multimédia, hypertextes, répartis et plurithématisques appelés pages web
 - multimédia : textes, images (fixes ou animées), vidéos, sons
 - hypertexte : des liens permettent de naviguer (de passer) d'un document à l'autre
 - répartis : il n'y a pas une seule source, un document peut-être composé de différentes parties localisées en des lieux différents
 - plurithématisques : "on trouve de tout sur le web"

- C'est l'un des services de l'Internet, ce n'est pas tout l'Internet
- Il sert d'interface d'accès à d'autres services (courrier électronique, forum de discussions, ...)
- Inventé par Tim Berners-Lee au CERN à partir des années 90 et aujourd'hui le W3C <http://www.w3.org> gère son évolution
- Surf on the web : la lecture hypertextuelle ...

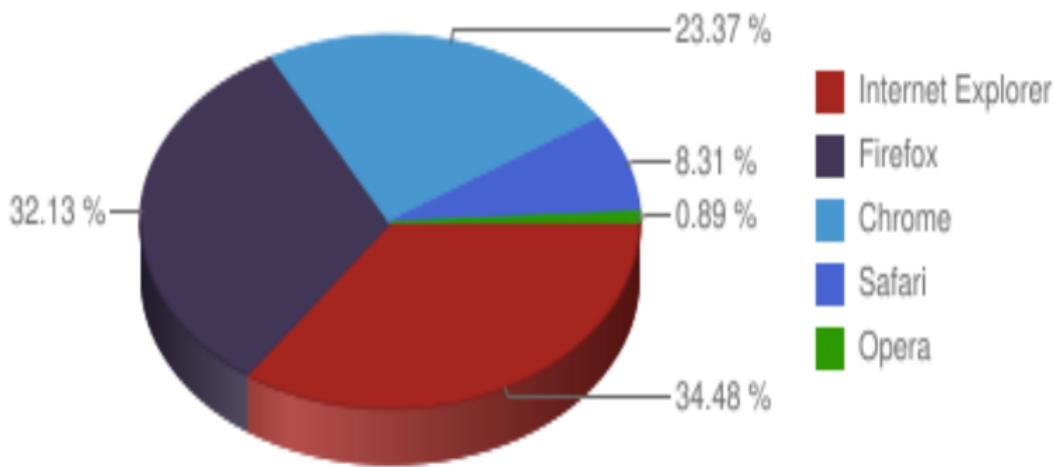
- Une URL (Uniform Resource Locator) est un format de nommage universel pour désigner une ressource sur Internet
 - ⇒ localisation d'un document sur la toile (adresse web)
 - ⇒ parcours du Web (liens hypertextes)

Protocole	Nom du serveur	Chemin d'accès à la ressource
http ://	www.univ-angers.fr	
http ://	www.univ-angers.fr	/accueilcomp.asp ?ID=11
http ://	www.info.univ-angers.fr	/pub/richer
ftp ://	sirius.info.univ-angers.fr	
telnet ://	sirius.info.univ-angers.fr	

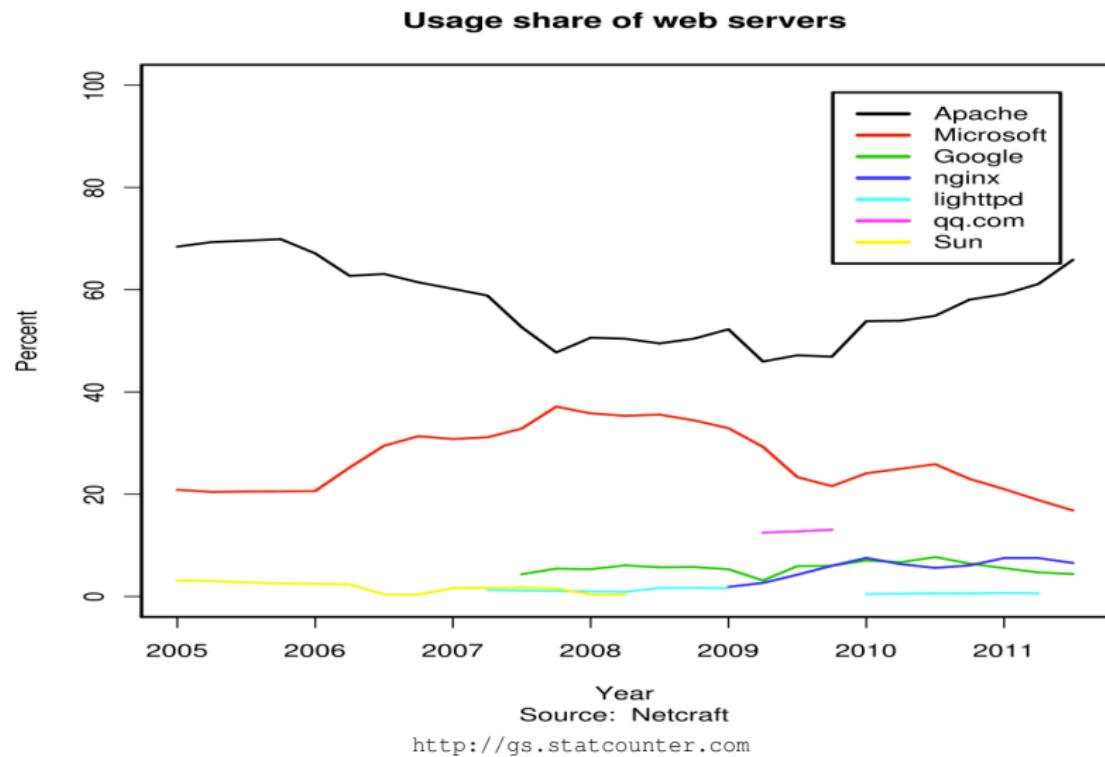
- Un site Internet est accessible par son nom mais aussi par son adresse IP
 - http ://www.univ-angers.fr identique à http ://193.49.144.40

- Un serveur web est un logiciel permettant la mise à disposition de données sur la toile
 - ⇒ par extension, l'ordinateur sur lequel il est exécuté est lui aussi considéré comme un serveur web, surtout si c'est son unique ou principale fonction
 - ⇒ Apache (logiciel libre, 50% des serveurs dans le monde, <http://www.apache.org>) et IIS (Microsoft), sont des exemples de logiciels serveurs web
- Un client web (ou navigateur) est un logiciel permettant d'afficher des pages web
 - ⇒ Firefox, Internet Explorer, Opera, ...

Parts de marché des navigateurs 2012



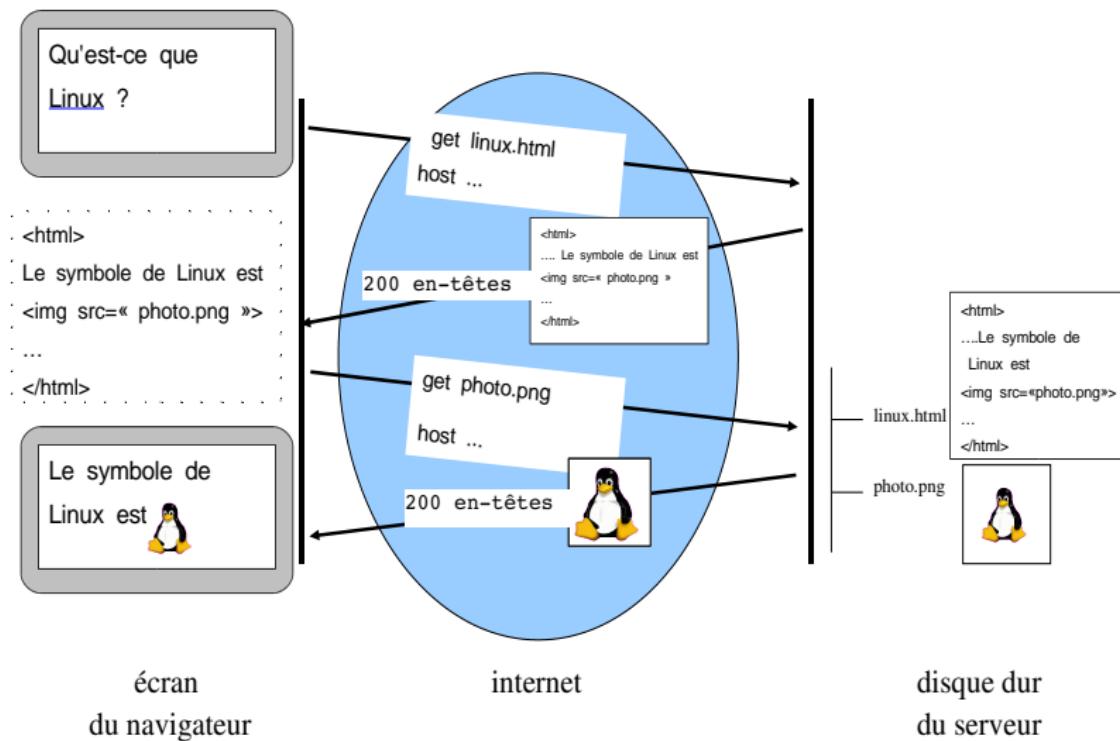
<http://blog.artenet.fr/2012/01/20/barometre-des-navigateurs-2012>



- Page web statique
 - contenu identique quelles que soient les conditions de sa consultation
 - document totalement enregistré sur le serveur
 - fichier (HTML, une image, ...) sur un disque dur
- Page web dynamique
 - contenu variable selon les conditions de sa consultation
 - document (textuel, image, ...) fabriqué à la volée (on the fly) au moment où il est consulté
 - résultat de l'exécution d'un programme ou script (PHP, ASP, servlets Java) côté serveur
- Page web animée
 - repose sur un document statique ou dynamique
 - le contenu est animé dans le navigateur
 - résultat de l'exécution d'un programme ou script (JavaScript, Flash, applet Java) côté navigateur (via un plugin)

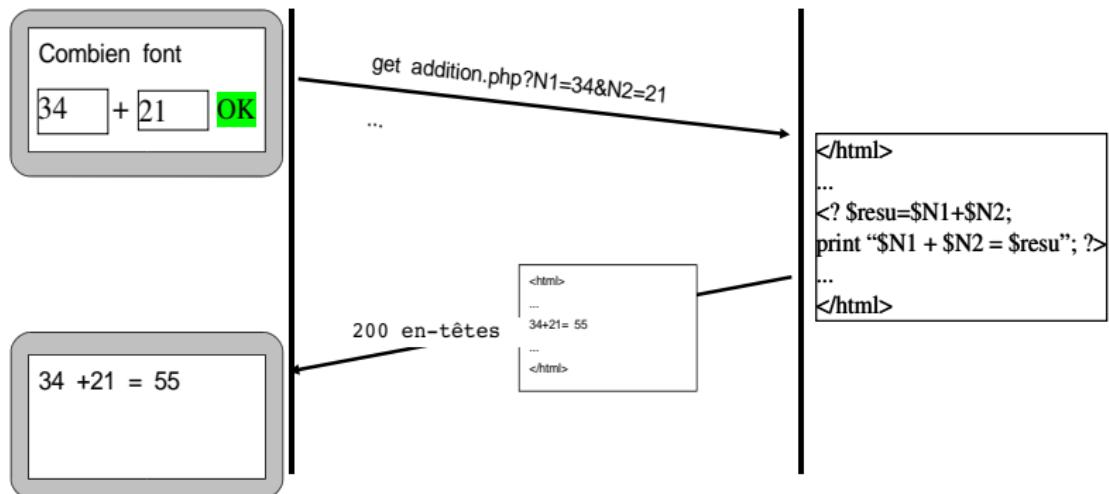
- Le serveur et le navigateur dialoguent selon le protocole HTTP (ou HTTPS pour des échanges sécurisés)
- Fonctionnement simplifié de HTTP :
 - 1 le client se connecte au serveur web
 - 2 il lui envoie une demande GET document ...
 - 3 le serveur envoie un code de réponse (ex : 200 tout va bien, 404 le document n'a pas été trouvé, 403 accès interdit...)
 - 4 le serveur envoie des informations sur le document : les en-têtes
 - 5 le serveur envoie le document et ferme (éventuellement) la connexion
 - 6 le client analyse le document reçu et affiche le document

Téléchargement d'une page web ...



- ➊ Lors de l'appel de la page web, des données sont transmises au serveur web
 - données saisies par l'utilisateur dans un formulaire
 - ou préalablement placées en fin d'URL
- ➋ Le programme est recherché sur le disque dur puis chargé en mémoire sur le serveur
- ➌ Les données sont transmises au programme qui est alors exécuté sur le serveur
- ➍ Le résultat (texte html, image, ...) est envoyé au navigateur, de manière identique au cas d'une page web statique

Téléchargement d'une page web dynamique . . .



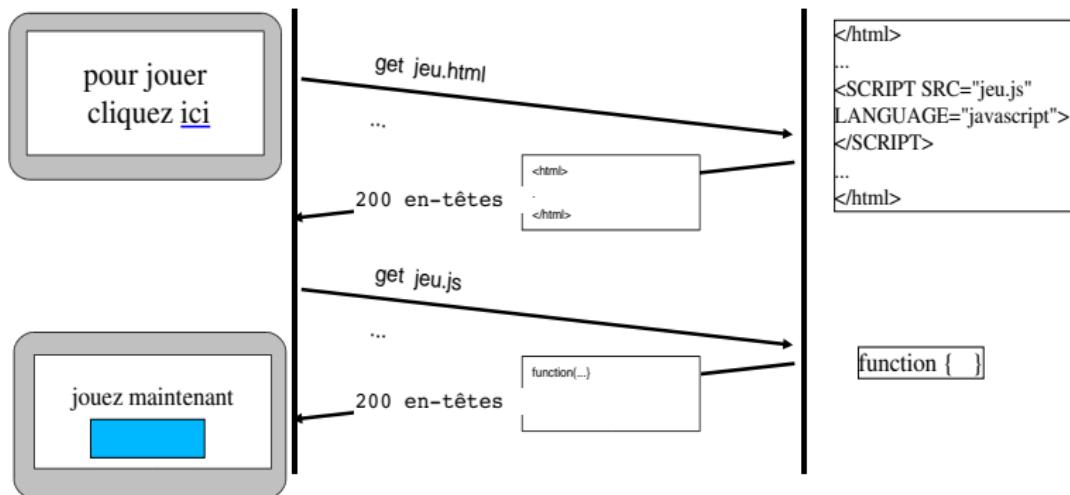
écran
du navigateur

internet

disque dur
et processeur
du serveur

- Fonctionnement
 - ① téléchargement d'une page HTML contenant une référence à un programme
 - ② téléchargement du programme
 - ③ exécution du programme dans le navigateur via un plugin
- Les principaux langages de programmation
 - Javascript (Netscape) : pour des petites animations (construction dynamique de menus par ex), des vérifications de saisie utilisateur, ...
 - Applet Java (Sun) : toute la puissance du langage Java, mise à disposition via le web de logiciels complexes sans intervention sur le poste
 - Flash (Adobe) : plus spécifiquement utilisé pour des animations graphiques (images, vidéos, jeux, pubs, ...)

Téléchargement d'une page web animée ...



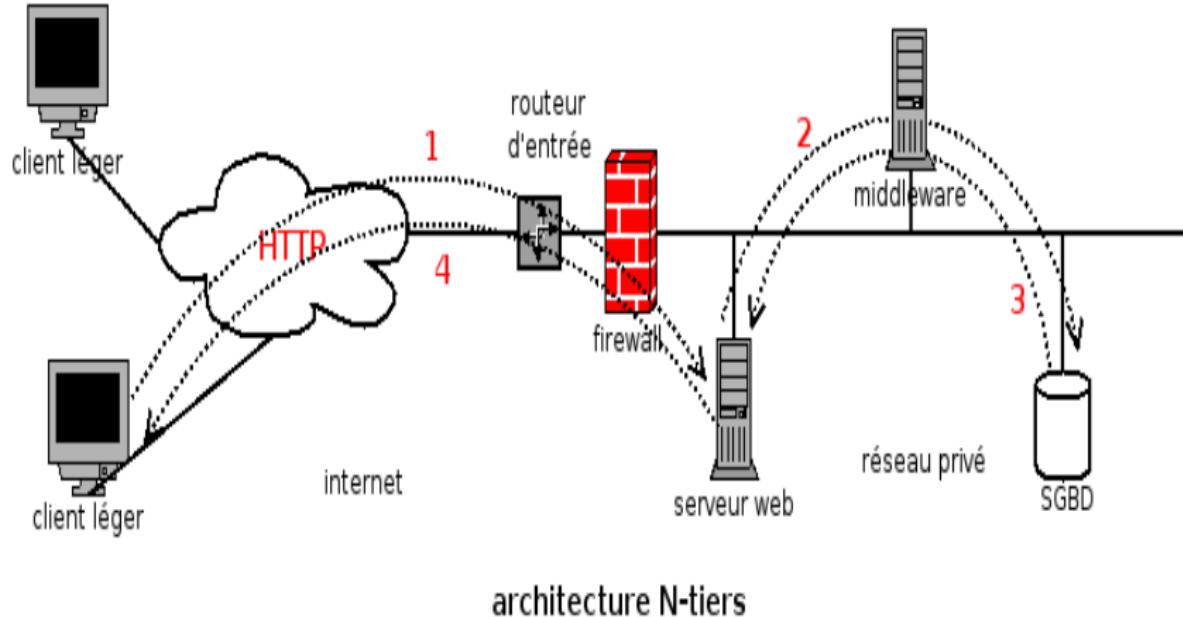
écran
du navigateur

internet

disque dur
du serveur

- Application client-serveur qui s'appuie sur HTTP
(ex. gestion de comptes bancaires par le web)
 - le logiciel serveur est un serveur web
 - le logiciel client (sur le poste de l'utilisateur) est un navigateur web qui présente une succession de pages web pour interagir avec l'application métier
 - la logique métier est située
 - sur le serveur web
 - ou sur une (ou plusieurs) machine intermédiaire : le middleware
- Déploiement rapide et uniforme, sans intervention sur les postes des utilisateurs
- Interface homme machine (IHM) limitée aux possibilités du navigateur web (HTML, Javascript, PHP,...)

Les applications web



- Services Web
 - généralisation des applications web où l'utilisateur humain n'est pas forcément requis
 - des applications dialoguent entre elles, par l'intermédiaire de messages transportés par le protocole HTTP
- Exemple : commande d'une entreprise à l'un de ses sous-traitants et en retour envoi de la facture

3

Les Services

- Les protocoles applicatifs
- Le nommage DNS
- Le Web
- La messagerie**
- La messagerie instantanée
- Les forums de discussion
- Le transfert de fichiers

- Échanges de messages entre utilisateurs
 - message simple : quelques lignes de texte brut
 - message enrichi : mis en forme grâce au langage HTML, agrémenté d'images, ...
- Il faut une adresse de courrier électronique
 - joe.dalton@far.west.us
 - destinataire at domaine

qui définit une boîte aux lettres
- Cette adresse n'est pas forcément chez son FAI (pratique en cas de changement de fournisseur)
- On peut disposer d'alias, cad. une adresse particulière qui renvoie vers une autre boîte aux lettres

- Des documents de toute nature peuvent être joints au message et transmis avec lui
 - Attention aux virus et à l'attachement de très gros fichiers
- Le même message peut être envoyé simultanément à plusieurs personnes
 - *To toto, titi* : toto et titi sont destinataires premiers du message, car ils sont concernés au même titre par le message. Si l'un répond au message, il placera l'autre dans les destinataires principaux de la réponse
 - *Cc toto* : toto recevra une copie du message, il n'est pas le destinataire principal, mais il est simplement tenu au courant de l'information. Si toto répond au message, il n'est pas obligé de répondre à tous les destinataires initiaux
 - *Bcc toto, titi* : toto et titi recevront une copie cachée (blind carbon copy) du message. Aucun des deux ne verra que l'autre a reçu le message

- Liste d'adresses permettant d'envoyer un même message à un ensemble de destinataires (publi-postage)
 - un message envoyé à la liste est redistribué à tous les abonnés
 - pour poster un message, il suffit de l'envoyer à l'adresse de la liste de type *nom-liste@lists.domaine.tld*
 - Exemples de listes :
 - info@info.univ-angers.fr
 - etudiants.sciences.0809@listes-etu.univ-angers.fr

- Listes de diffusion : quelques uns écrivent à beaucoup
 - Listes de discussion : des abonnés y échangent leurs points de vue
-
- Listes publiques : tout le monde y a accès
 - Listes privées : seuls les abonnés peuvent participer
-
- Listes non-modérées : on peut y écrire directement
 - Listes modérées : un modérateur décide quels messages pourront être diffusés
-
- Sympa est un logiciel serveur de listes de diffusion
 - offre un ensemble de fonctionnalités très riche
 - diffusé sous licence GPL par le Comité Réseau des Universités

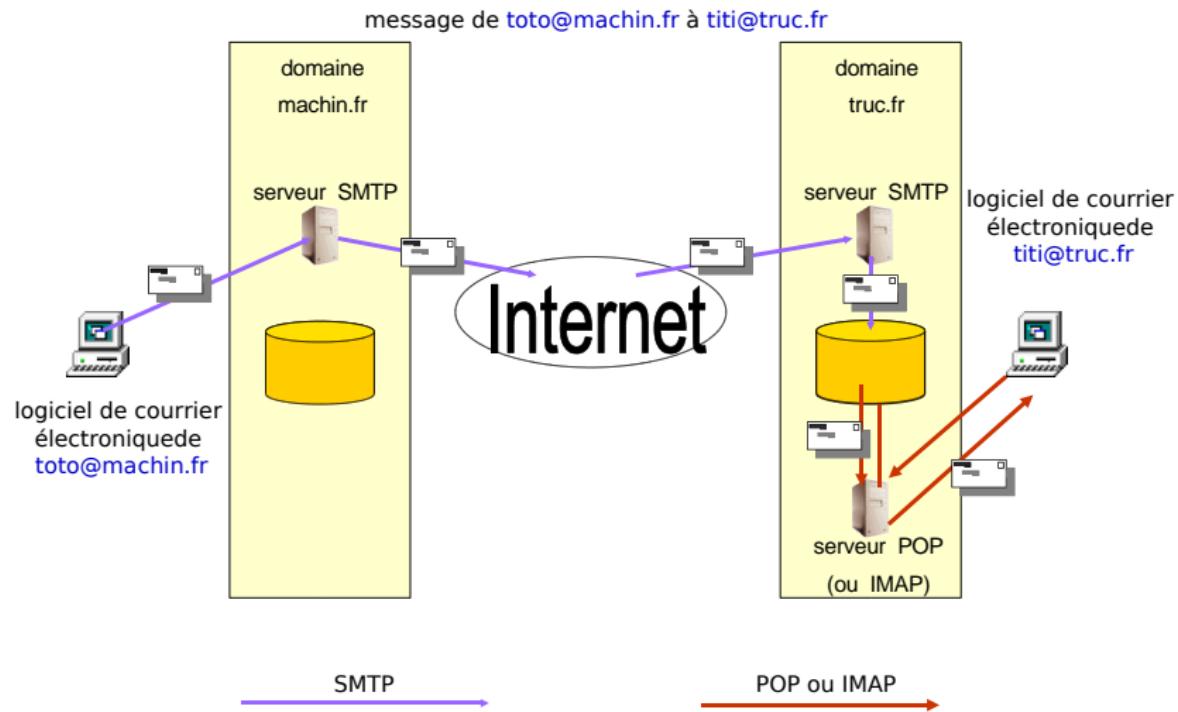
- SMTP (Simple Mail Transfert Protocol) achemine le courrier jusqu'à la boîte aux lettres et gère les messages d'erreurs
 - les logiciels qui implémentent ce protocole sont des MTA (Mail Transfert Agent)
 - logiciels libres (sendmail, postfix, ...) ou propriétaires (Microsoft Exchange)
- POP (Post Office Protocol) délivre le courrier à l'utilisateur final (ouvre la boîte aux lettres)
- IMAP (Internet Message Access Protocol) : POP en plus évolué

- ➊ On rédige le message avec un logiciel de courrier électronique appelé un MUA (Mail User Agent)
 - Thunderbird, Outlook, Eudora, ...
- ➋ On envoie le message via SMTP au serveur SMTP spécifié dans la configuration du logiciel
 - à priori celui de son FAI
 - le MUA et le PC de l'utilisateur n'interviennent plus
- ➌ Le serveur SMTP de l'expéditeur détermine, en fonction du domaine de l'adresse du destinataire et grâce à un DNS, le serveur SMTP qui gère le courrier du destinataire
- ➍ Le serveur SMTP de l'expéditeur transmet le message au serveur SMTP du destinataire
- ➎ Ce dernier stocke le courrier sur son disque dur dans la boîte aux lettres du destinataire

Réception d'un mail par logiciel de courrier électronique

- ➊ On relève la boîte aux lettres à l'aide d'un logiciel de courrier électronique
- ➋ Ce dernier se connecte au serveur POP ou IMAP gérant la boîte que l'on veut relever en envoyant l'identifiant de la boîte et un mot de passe pour l'authentification
- ➌ Le serveur POP envoie tous les messages au logiciel de courrier et les supprime de l'endroit où ils avaient été déposés par le serveur SMTP
- ➍ Le serveur IMAP offre plus de fonctionnalités
 - on peut laisser les messages dans la boîte aux lettres tout en en récupérant une copie dans le logiciel de courrier électronique
 - utile si l'on consulte son courrier depuis plusieurs postes

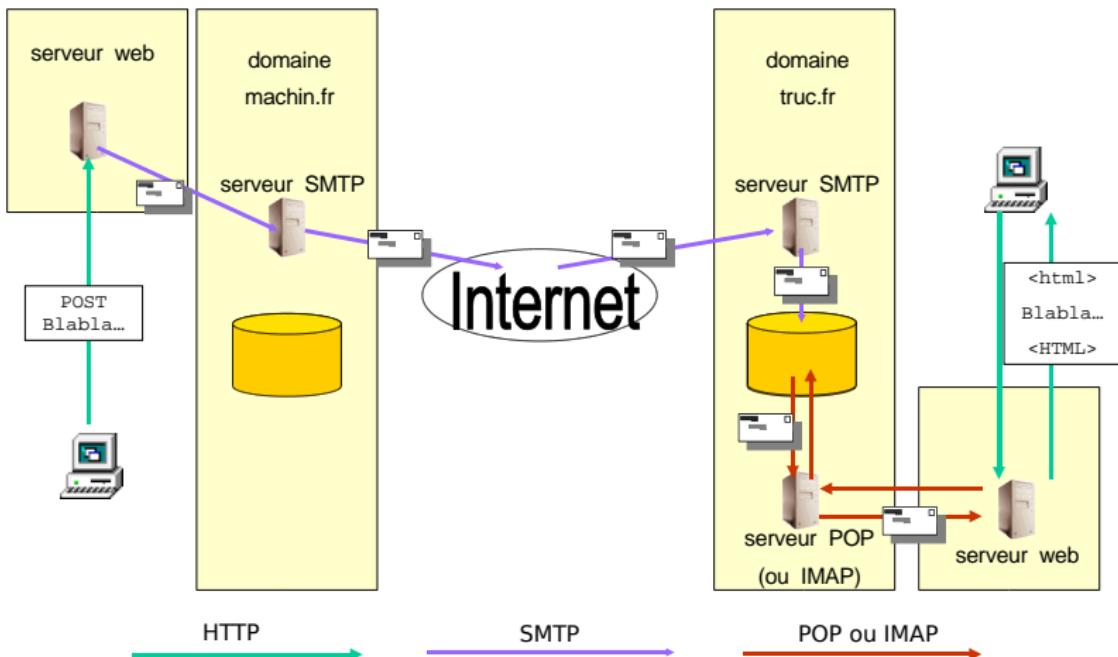
Envoi et réception d'un courriel par logiciel de courrier électronique



- L'utilisateur utilise une application web pour accéder à sa boîte aux lettres
 - tous les FAI le proposent et de nombreux autres sites sont disponibles (Gmail, Yahoo, La Poste, ...)
- Toutes les fonctionnalités d'un logiciel de courrier électronique sont reproduites au travers de l'interface web
- Rien n'est stocké sur le poste de l'utilisateur
 - pratique pour l'accès nomade
 - espace limité pour les archives
 - confidentialité et pérennité ne sont pas garanties
 - productivité plus faible qu'avec un logiciel de messagerie

Envoi et réception d'un mail par webmail

message de toto@machin.fr à titi@truc.fr



3

Les Services

- Les protocoles applicatifs
- Le nommage DNS
- Le Web
- La messagerie
- La messagerie instantanée**
- Les forums de discussion
- Le transfert de fichiers

- Une messagerie instantanée (IM : Instant Messaging) permet d'établir en temps réel des dialogues textuels ou audio-visuels entre plusieurs utilisateurs (chat)
- Historique
 - ① logiciel de *talk* sur les machines Unix multi-utilisateurs dès les années 80 pour échanger en direct des lignes de textes
 - ② IRC : Internet Relay Chat
 - ③ ICQ : I seek you
 - ④ messageries instantanées (MSN, Yahoo, AIM, ICQ, ...)

- Système de communication instantanée à travers Internet
- Discussions multi-utilisateurs à travers des canaux (channels) ou en direct entre 2 utilisateurs seulement
- Un réseau de serveurs interconnectés assure la diffusion des messages
 - ex. IRCNET
- Les clients se connectent à un serveur pour participer à une discussion
 - ex. Pidgin, Kopete, climm
- Chaque utilisateur choisit un pseudo (nickname) lorsqu'il veut participer à un canal

- Système de messagerie instantanée plus léger que IRC
- ICQ existe depuis 1996
- Chaque utilisateur possède un numéro ICQ (plus de 400 millions aujourd'hui) ce qui permet de constituer des annuaires
- Permet l'échange de messages et de fichiers à 2 ou plusieurs
- Protocole propriétaire mais de nombreux clients sont disponibles (Pidgin, Kopete, ...)

Messageries instantanées

- Rien de fondamentalement nouveau par rapport à IRC et ICQ
- Proposées à partir de 2000 par les fournisseurs de contenu (MSN, Yahoo, AOL, Google, ...)
- Intégration de la voix et de la vidéo grâce aux webcam
- Systèmes propriétaires forçant l'utilisation de logiciels clients spécifiques et permettant de garder captifs les utilisateurs et de proposer des contenus publicitaires
- Il existe des clients libres (Pidgin, ...) et le protocole XMPP (basé sur des échanges XML et utilisé dans Google Talk) permet d'envisager une interopérabilité des différents systèmes de messagerie

3

Les Services

- Les protocoles applicatifs
- Le nommage DNS
- Le Web
- La messagerie
- La messagerie instantanée
- Les forums de discussion**
- Le transfert de fichiers

- Les groupes de nouvelles (forums de news, de discussion)
 - constituent le réseau Usenet depuis 1979
 - sont régis par le protocole NNTP (Network News Transfer Protocol)
- Chaque client poste un message (analogique à courriel) dans un forum sur un serveur
- Le serveur met à disposition ce message pour tous les autres clients lecteurs de ce forum et le diffuse à d'autres serveurs de news auxquels il est connecté
 - le message sera visible sur tous les serveurs qui relaient ce forum
- Un utilisateur consultant un serveur de news choisit de consulter le contenu de certains forums en particulier

- Les forums sont accessibles via
 - un logiciel lecteur de news (Outlook, Thunderbird, ...)
 - une interface web, par ex :<http://groups.google.fr>
- Les noms des forums sont organisés en hiérarchie
 - fr.* groupes francophones
 - fr.lettres.*
 - fr.comp.*
 - ...
 - comp.* groupes relatifs à l'informatique
 - rec.* groupes relatifs aux loisirs
- Certains forums sont modérés

3

Les Services

- Les protocoles applicatifs
- Le nommage DNS
- Le Web
- La messagerie
- La messagerie instantanée
- Les forums de discussion
- Le transfert de fichiers**

- Permet l'échange de fichiers de toute nature d'un ordinateur vers un autre selon le protocole FTP (File Transfer Protocol), par ex.
 - téléchargement de documents, logiciels, ... depuis un serveur les mettant à disposition
 - mise à jour d'un site web
 - téléchargement vers le serveur web des nouvelles pages web que l'on a écrites sur son ordinateur personnel
 - suppression de certaines pages sur le serveur web
- La connexion au serveur FTP peut être contrôlée par un identifiant et un mot de passe ou être anonyme
 - (identifiant = anonymous ; mot de passe = adresse email) par convention
- Utilisation via un logiciel client FTP (Filezilla, ...) ou un navigateur web (URL débutant par `ftp://`)

- Système de partage de fichiers P2P (pair à pair, poste à poste, égal à égal)
- Réseau informatique où chaque nœud est à la fois client et serveur
- Chaque individu met à disposition sur son ordinateur tout ou partie de fichiers informatiques
 - musique (MP3, OGG, ...)
 - films (DIVX, MPEG, ...)
 - livres (PDF, ...)
 - logiciels, ...
- Premier système de ce type : Napster (1999-2002)
- Problème du droit de copie !

Pourquoi le P2P est-il répandu aujourd’hui ?

- Convergences de conditions économiques et techniques favorables
 - abonnement forfaitaire pour l'accès à Internet
⇒ on peut laisser sa connexion branchée tout le temps sans coût supplémentaire
 - internet haut débit (ADSL, câble)
⇒ le téléchargement d'un fichier volumineux est rapide
 - nouveaux formats de fichiers (MP3, DIVX, ...)
⇒ compression sans perte de qualité trop importante
⇒ réduction de la taille des fichiers
 - appareils de gravure (CD et DVD) et de lecture (MP3 DIVX) bon marché
⇒ l'utilisation du produit n'est plus limitée à l'ordinateur

- Réseaux Napster, eDonkey2000 (ed2k)
 - Logiciels eDonkey2000, eMule,...
 - Des serveurs particuliers servent d'annuaires pour localiser les fichiers recherchés
- Fonctionnement
 - ① le client se connecte à un serveur central pour y obtenir la localisation des différentes parties du fichier recherché (cad. sur quels ordinateurs se trouvent ces parties)
 - ② le client se connecte à ces différentes machines pour y télécharger chaque partie
 - ③ chaque demandeur est mis en file d'attente par le fournisseur
 - ④ dès qu'une partie est téléchargée par le client, le serveur central en est informé pour que le client puisse devenir le fournisseur de cette partie à d'autres clients
- Le téléchargement peut-être interrompu et repris n'importe quand

- Réseaux Gnutella et BitTorrent
 - pas de nœud particulier
 - chaque client démarre et se connecte à au moins un autre client dont l'adresse est dans un fichier de configuration ou obtenu de manière externe
 - chaque nœud échange avec les autres les adresses des nœuds qu'il connaît
 - quand un client cherche un fichier, il interroge les nœuds auxquels il est connecté et chacun va répercuter cette demande aux nœuds auxquels il est connecté
 - quand le fichier est localisé (en 1 ou plusieurs nœuds) le téléchargement peut commencer
- Impossible d'avoir une vue d'ensemble du réseau à tout instant
- Réseau résistant aux attaques car non centralisé

- ➊ Le logiciel doit posséder un *torrent*
 - fichier d'extension .torrent contenant les informations relatives au document recherché et notamment l'adresse d'un tracker qui est un nœud particulier, unique, responsable du fichier
 - le torrent se récupère via un site web, par mail, par IRC, ...
- ➋ Lorsqu'un client veut télécharger un fichier, il en informe le tracker qui lui retourne une liste de postes faisant de même
- ➌ Le client peut alors se connecter à ces postes pour commencer le téléchargement
- ➍ Tout au long du téléchargement, les clients dialoguent avec le tracker pour l'informer de l'avancée du téléchargement et recevoir des listes de nouveaux clients disposant de parties encore manquantes
- ➎ Un système d'équilibrage régule les échanges entre les clients
 - chaque client proposera plus de données aux clients qui en fournissent beaucoup

1 Introduction

2 Les Réseaux et l'Internet

3 Les Services

4 Le Transport des Données

- Introduction
- Le contrôle de flux
- Le protocole UDP
- Le protocole TCP

5 L'Adressage et le Routage

6 Sécurité sur Internet

4

Le Transport des Données

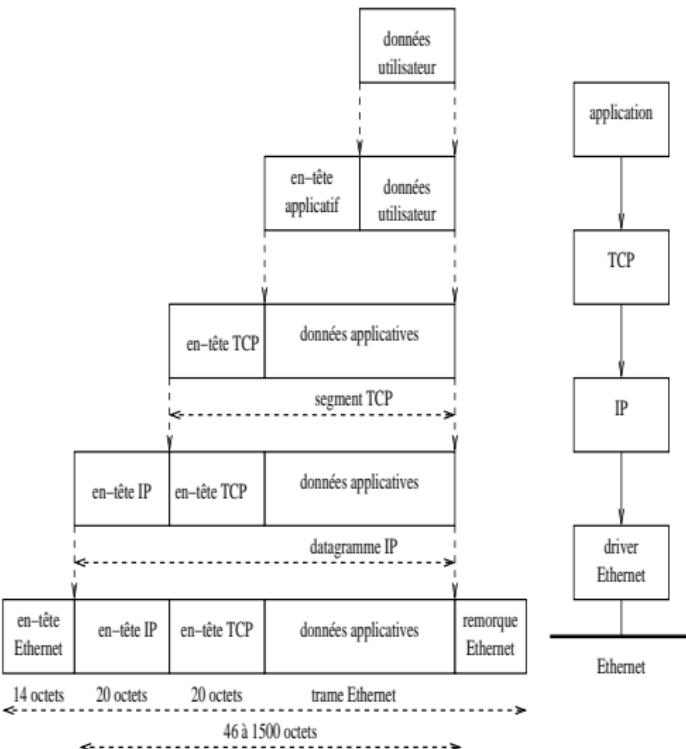
- Introduction
- Le contrôle de flux
- Le protocole UDP
- Le protocole TCP

- Un réseau “local” est un ensemble de machines qui peuvent communiquer entre elles sans avoir à passer par un routeur
- Transmettre des données d'une machine connectée au réseau *A* jusqu'à une machine connectée au réseau *B* à travers l'internet consiste à faire des “sauts” successifs de routeur en routeur en traversant à chaque fois un réseau particulier
- Illustration vidéo

<http://warriorsofthe.net/movie.html>

La couche Transport

- Couche 4 du modèle OSI
- Protocole TCP ou UDP encapsulent les données applicatives sous forme de segment
- Couche de bout en bout
- TCP assure la fiabilité des transmissions entre source et destination finale par numérotation des segments



4

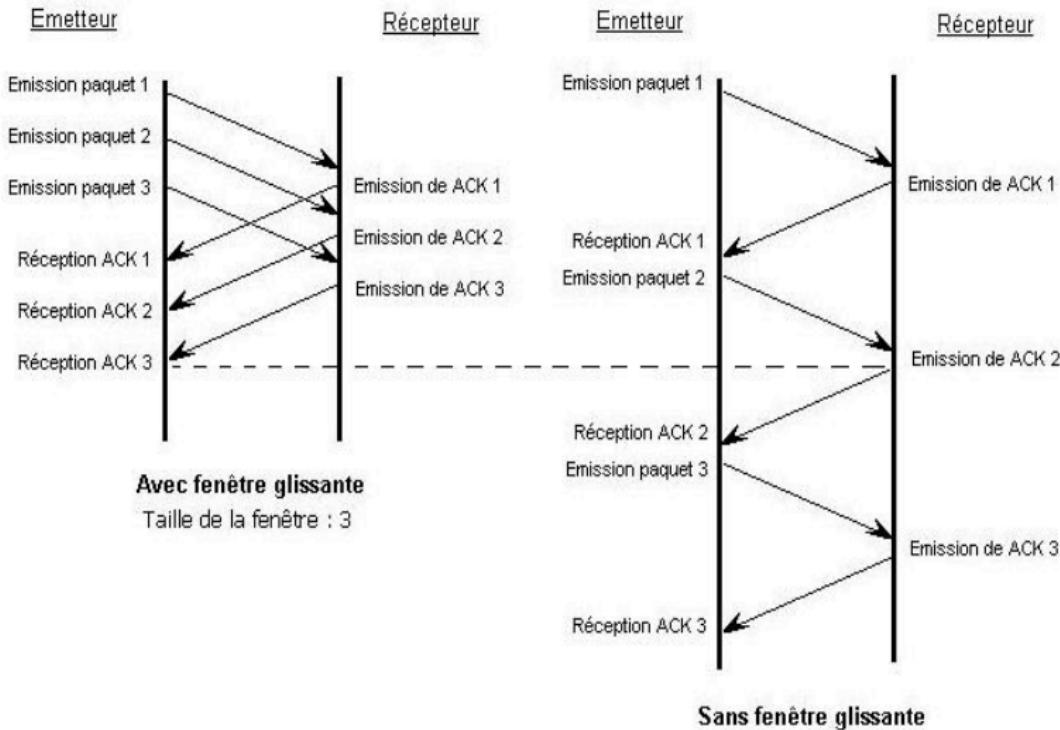
Le Transport des Données

- Introduction
- **Le contrôle de flux**
- Le protocole UDP
- Le protocole TCP

- Adapte le nombre de segments transmis par unité de temps entre un client et un serveur
 - les temps de traitement, ressources et débits diffèrent entre client et serveur
 - les temps de traitement et de transfert varient dans les équipements intermédiaires
- ⇒ Ralentir ou accélérer le débit de l'émetteur suivant la réaction du récepteur ou du réseau
 - à l'aide par ex. de segments d'acquittement

- Protocole "Envoyer et attendre"
 - l'émetteur attend un acquittement avant d'envoyer le segment suivant
 - ⇒ gestion simple des erreurs et pertes de segments
 - ⇒ plus le temps de propagation des supports traversés est grand par rapport à la transmission et au traitement des segments et acquittements, plus faible est l'efficacité
- Protocole à fenêtre d'émission
 - autoriser l'émission de plusieurs segments avant de s'arrêter pour attendre le premier segment
 - ⇒ efficacité maximum
 - ⇒ comment gérer les pertes ?

Comparaison



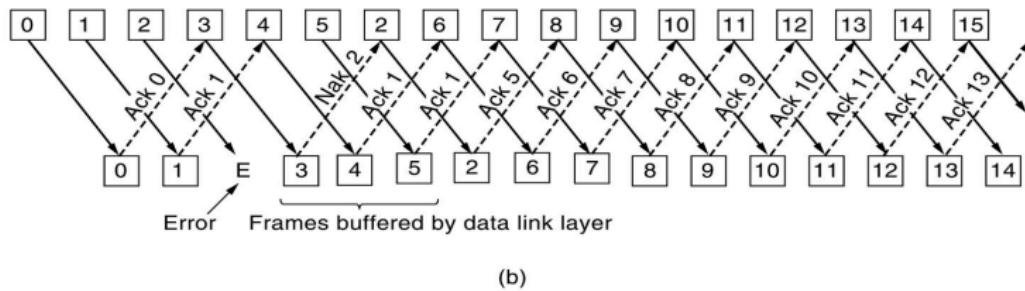
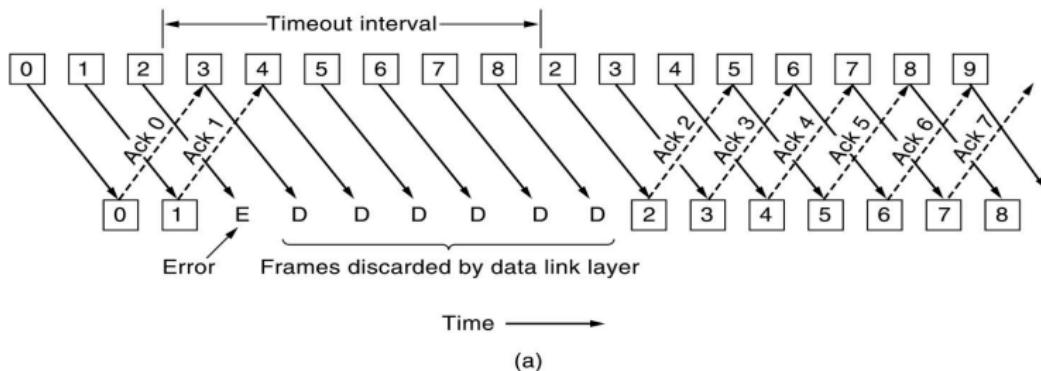
1 Rejet global

- un temporisateur (timeout) est déclenché à chaque segment émis
- retransmission du segment non acquitté à expiration du temporisateur
- le récepteur rejette tous les segments qui suivent une perte

2 Rejet sélectif

- le récepteur mémorise les segments reçus après une perte
- il émet un acquittement négatif pour accélérer la retransmission du segment par l'émetteur
- il acquitte en une seule fois tous les segments mémorisés une fois le segment manquant réceptionné et les transmet à la couche supérieure

Rejet global ou sélectif



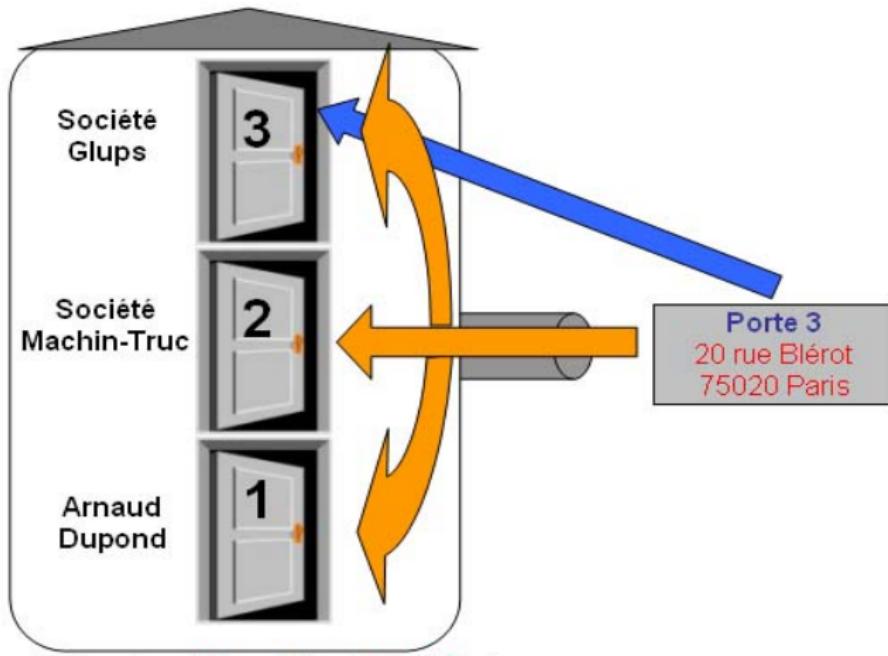
4

Le Transport des Données

- Introduction
- Le contrôle de flux
- **Le protocole UDP**
- Le protocole TCP

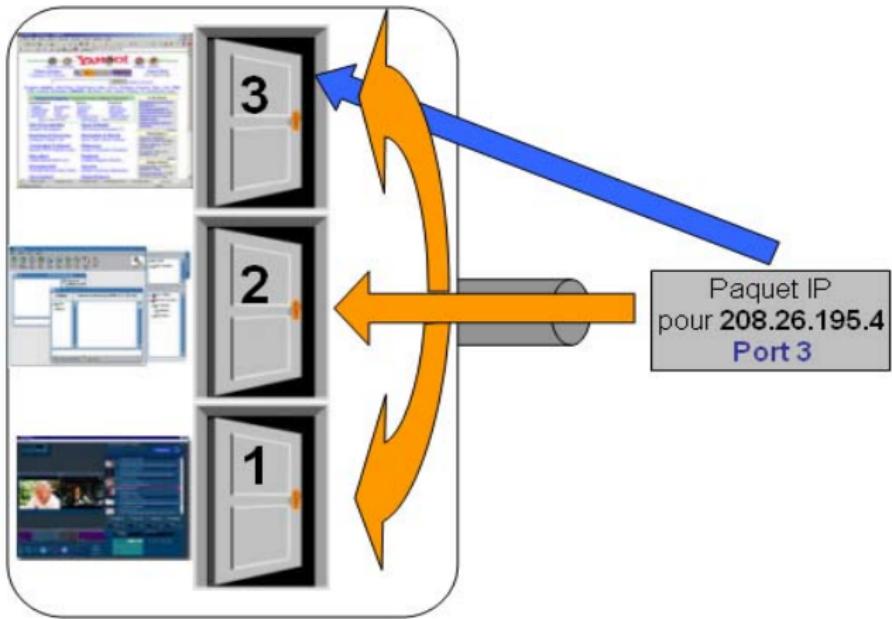
- Grâce à la couche IP, il est possible d'envoyer et recevoir des paquets de données d'un ordinateur à l'autre
- Imaginons que nous ayons plusieurs programmes qui fonctionnent en même temps sur le même ordinateur :
 - un navigateur Web
 - un logiciel de courriel
 - un logiciel pour écouter la radio sur Internet
- ⇒ Si l'ordinateur reçoit un paquet IP, comment savoir à quelle application donner ce paquet IP ?
 - chacun des programmes travaille avec un protocole spécifique, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données
 - ⇒ pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits : un numéro de port
 - ⇒ la combinaison adresse IP + port est appelée "socket"

Analogie : portes d'un immeuble



Avec la poste, à une même adresse, on peut s'adresser à différentes personnes en indiquant un numéro de porte.

Analogie : portes d'un immeuble



Votre ordinateur(adresse IP 208.26.195.4)

De même, à une même adresse IP, on peut s'adresser à différents logiciels en précisant le numéro du port (ici : 3).

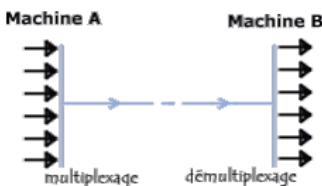
Les ports en TCP et UDP

Port	Service	Description
0		utilisé pour le DNS
20	Port de données FTP	Le FTP est utilisé pour le transfert des fichiers.
21	Port de contrôle FTP	
22	SSH remote login protocole	utilisé dans certaines applications de connexion à distance
23	Telnet	
25	SMTP	Courrier sortant vers un serveur SMTP .
53	Domain Name Server (DNS)	Permet de détecter si l'adresse IP correspond à une adresse valide. Ce port est utilisé identiquement en UDP et IP.
68	DHCP	Utilisé pour une configuration automatique des adresses IP
80	World Wide Web , http	navigation sur Internet en HTTP
110	POP3 (Post Office Protocol)	Courier entrant
119		utilisé par les news
137	Netbios Name Service	
138	NetBios	Permet le partage de fichiers et d'imprimantes dans un réseau local , éventuellement d'utiliser ce partage via INTERNET
139	NetBios	
143	protocole de courrier sécurisé IMAP 3	
220	protocole de courrier sécurisé IMAP 4	
443		Navigation sur certains sites sécurisés (HTTPS)
445	Netbios	Fonctionnalité supplémentaire implantée à partir de Windows 2000 (pas millenium)
1863	MSN Messenger	Envoyer et recevoir les messages avec le logiciel le messagerie instantanée
7000-7099	logiciel bancaire ISABEL	suivant une adresse TCP/IP locale de départ et une adresse finale (le site).

<http://www.iana.org/assignments/port-numbers>

Multiplexage / Démultiplexage

- Multiplexage = processus qui consiste à pouvoir faire transiter sur une connexion des informations provenant de diverses applications
- Démultiplexage = processus qui consiste à répartir le flux de données sur diverses applications



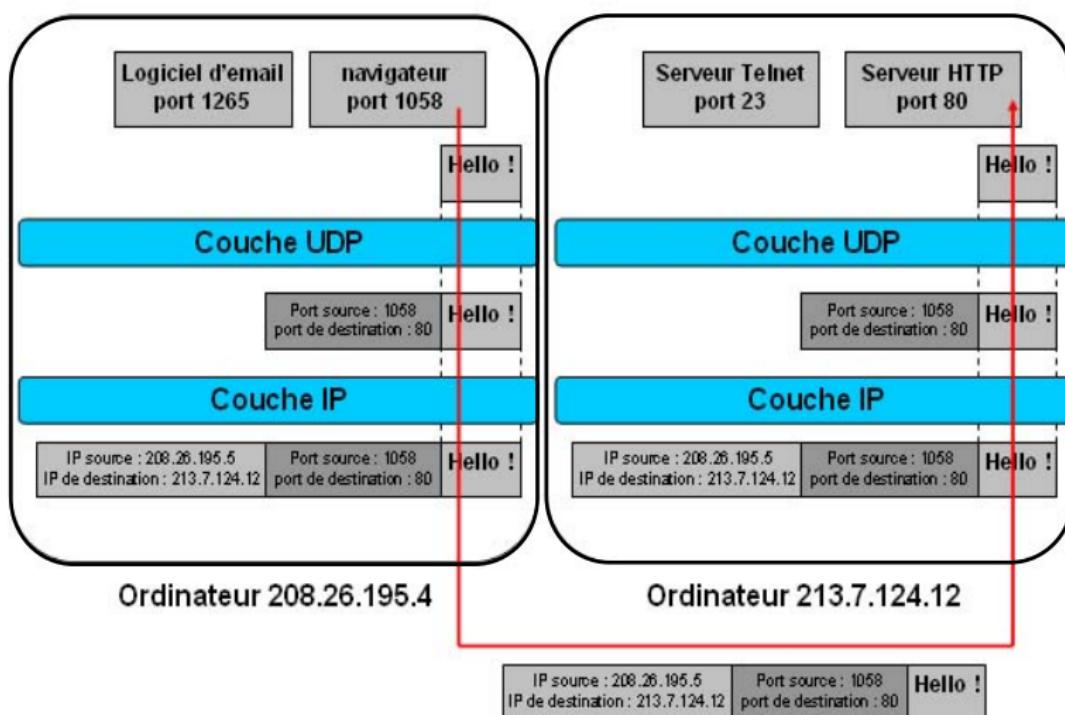
- Ces opérations sont réalisées grâce aux ports qui combinés à une adresse IP permettent d'identifier chaque application sur une machine donnée

<http://www.commentcamarche.net/contents/internet/port.php3>

- UDP permet l'échange entre applications en encapsulant leurs numéros de ports
 - avec le protocole IP, on peut envoyer des données d'un ordinateur A à un ordinateur B
 - avec UDP, on envoie des données d'une application X sur l'ordinateur A vers une application Y sur l'ordinateur B
- UDP est un protocole non fiable et sans connexion (sans état)
- UDP est utilisé quand la rapidité prime sur la fiabilité
 - requêtes d'adressage dynamique (DHCP)
 - requêtes simples DNS
 - applications audio/vidéo, etc

Protocole UDP

- Exemple d'envoi d'un message à un serveur Web :



4

Le Transport des Données

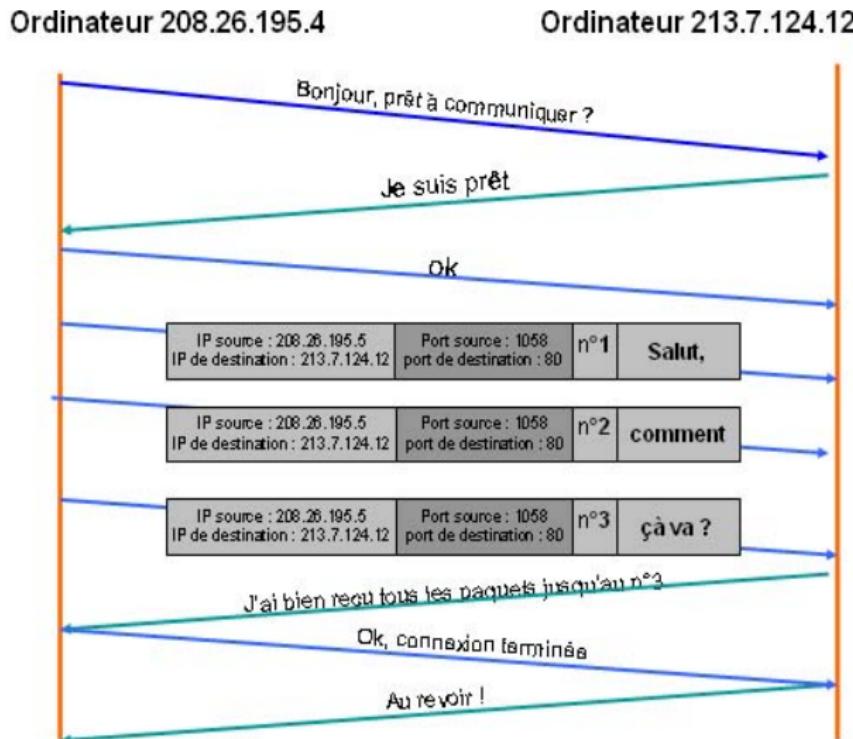
- Introduction
- Le contrôle de flux
- Le protocole UDP
- **Le protocole TCP**

- Le protocole UDP présente néamoins un certain nombre de limites
 - pas de contrôle de la bonne transmission des données
 - taille des paquets IP limitée (environ 1500 octets)
- Le protocole TCP est orienté connexion et permet de
 - faire tout ce que UDP sait faire (gestion des ports)
 - vérifier que le destinataire est prêt à recevoir les données
 - découper les gros paquets de données en paquets plus petits pour que IP les accepte
 - numéroter les paquets et, à la réception, vérifier qu'ils sont tous bien arrivés, redemander les paquets manquants et les rassembler avant de les donner aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées

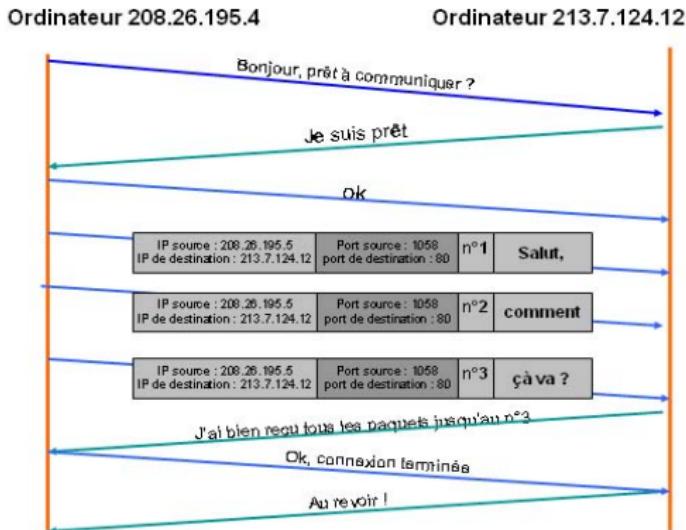
- Trois phases
 - 1 ouverture de la connexion virtuelle
 - 2 transfert des données
 - 3 fermeture de la connexion virtuelle
- Segmentation et réassemblage des données
- Multiplexage des données issus de plusieurs processus hôtes en un seul segment
- Gestion des pertes
 - encapsulation des numéros de séquence et d'acquittement pour savoir combien d'octets ont été transmis et correctement reçus dans les 2 sens
 - utilisation de temporiseurs pour la retransmission
- Contrôle de flux à l'aide de fenêtres gérées localement et dynamiquement
- Gestion des priorités des données et de la sécurité de la communication

Protocole TCP

- Envoi du message "Salut, comment ça va ?" à un serveur Web par TCP



- A l'arrivée sur l'ordinateur 213.7.124.12, la couche TCP
 - reconstitue le message à partir des 3 paquets IP reçus
 - et le donne au logiciel qui est sur le port 80



Format segment TCP

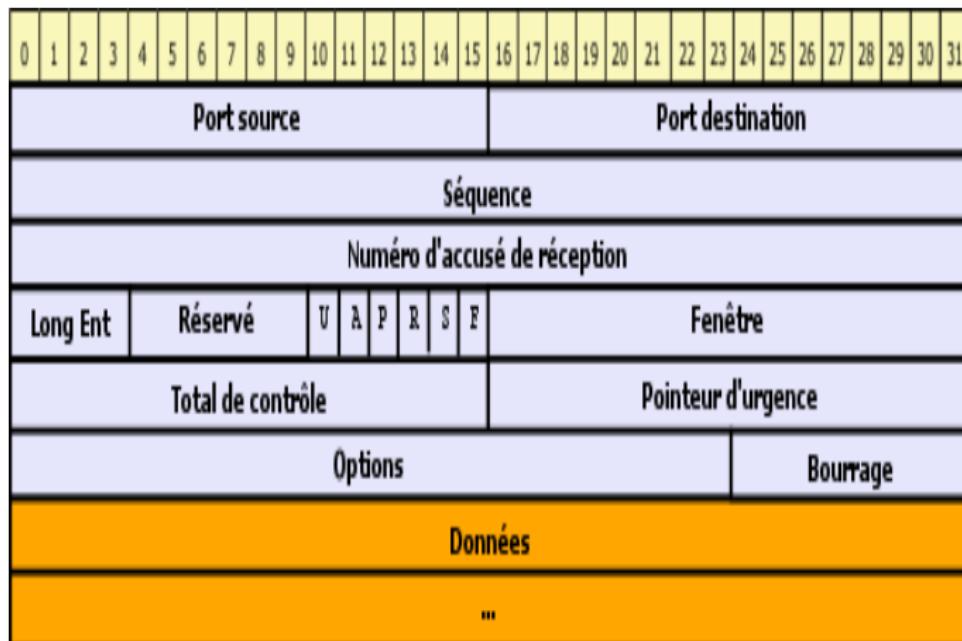
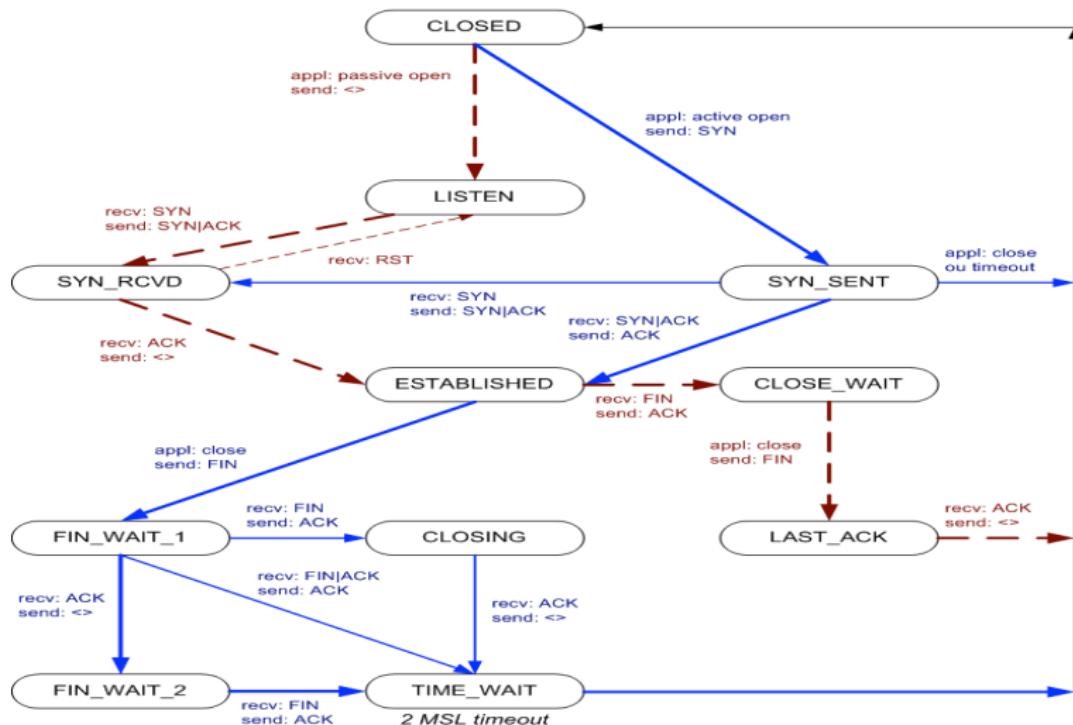


Diagramme d'état TCP

—→ transition client
—→ transition serveur



1 Introduction

2 Les Réseaux et l'Internet

3 Les Services

4 Le Transport des Données

5 L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

6 Sécurité sur Internet

5

L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

Rôle de la couche Internet (couche IP)

- Fournir une méthode d'adressage unique et universelle des machines sur Internet : l'adresse IP
- Assurer une fonction de routage des paquets sur le réseau à partir de l'adresse IP
- Assurer l'interface entre les couches par la fragmentation et le réassemblage des données
- Protocoles disponibles
 - IP = Internet Protocol
 - ICMP = Internet Control Message Protocol
 - IGMP = Internet Group Message Protocol
 - ARP = Address Resolution Protocol
 - protocoles de routage dynamique : RIP, OSPF, BGP, etc
 - protocoles de qualité de service : Diffserv, RSVP, etc

5

L'Adressage et le Routage

- Le rôle de la couche Internet
- **Le protocole IP**
- Le routage
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

- C'est le protocole principal d'Internet
 - initialement décrit dans la RFC 791 en 1981
 - deux versions en 2012 : IPv4 et IPv6
- ⇒ Permet le routage des informations à travers les réseaux pour rallier un destinataire à partir d'un ordinateur expéditeur
- IP est exécuté dans les hôtes et les routeurs
 - gère l'adressage, le routage, la fragmentation et le réassemblage des paquets (datagrammes) IP
 - ne gère pas les erreurs et les pertes, le contrôle de flux ou de congestion

Analogie : envoi d'un courrier par la poste

- Lorsque l'on envoie une lettre par la poste
 - on place la lettre dans une enveloppe
 - sur le recto, on inscrit l'adresse du destinataire
 - sur le verso, on inscrit l'adresse de l'expéditeur



Le message



L'enveloppe



Recto :
Adresse du destinataire



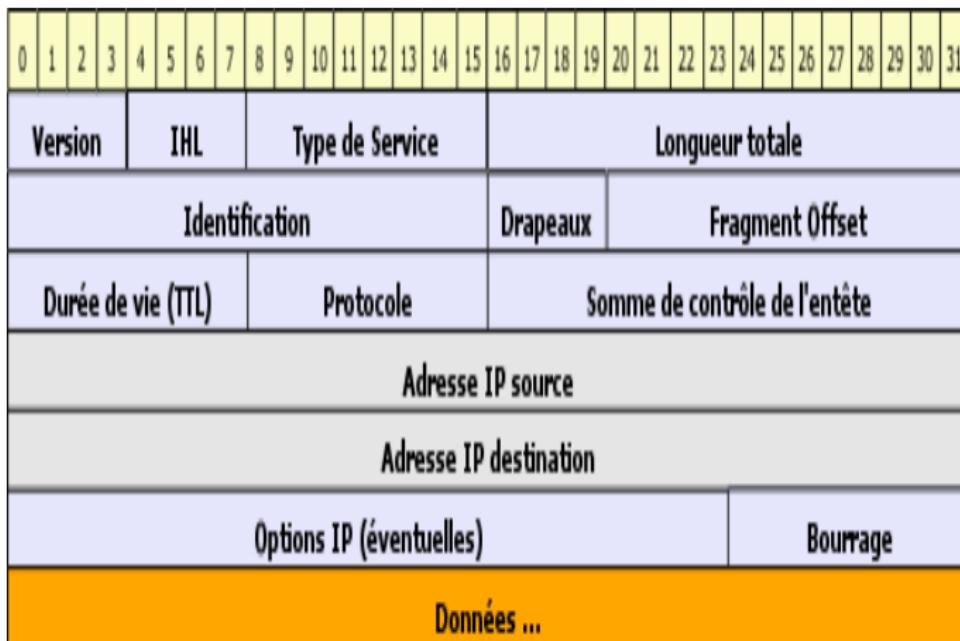
Verso :
Adresse de l'expéditeur

- Ce sont des règles que tout le monde utilise. C'est un protocole

- Sur Internet, chaque message (ou plutôt chaque petit paquet de données) est enveloppé par le protocole IP qui lui ajoute diverses informations :
 - l'adresse de l'expéditeur (son adresse IP)
 - l'adresse IP du destinataire
 - des données supplémentaires qui permettent de bien contrôler l'acheminement du message



Format datagramme IP

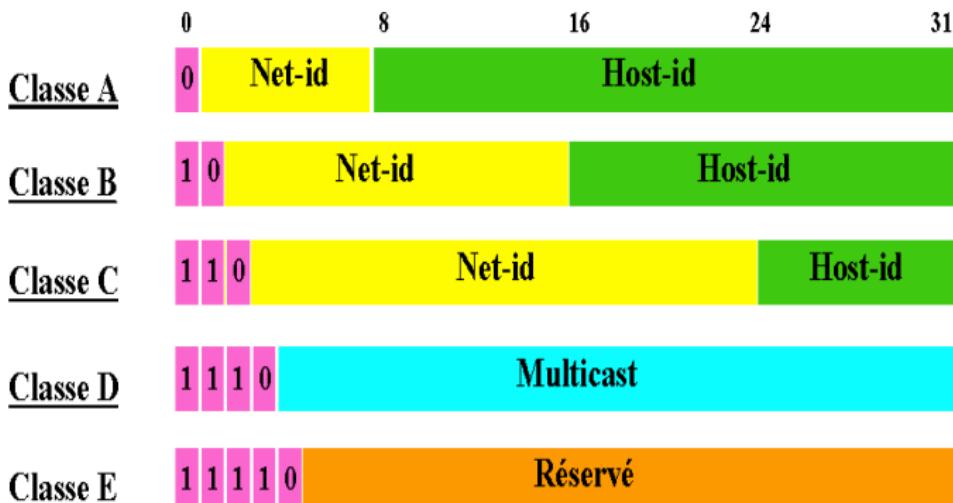


- Le protocole IP utilise des adresses IP pour identifier de manière unique un réseau et une machine sur ce réseau
 - une même machine a autant d'adresses IP que d'interfaces
- Trois types d'adresse
 - unicast : identifie un équipement de manière unique
 - broadcast (de diffusion) : pour transmettre un datagramme à tous les équipements d'un même réseau
 - multicast (de groupe) : pour transmettre un datagramme vers un groupe d'équipements IP
- Deux méthodes d'adressage
 - par classe : méthode initiale
 - sans classe : méthode (CIDR) introduite dans les années 1990 pour faire face à la croissance de l'Internet

- Une adresse IP est codée sur 4 octets et écrite en notation décimale pointée
- Exemples
 - 192.168.0.1
 - 127.0.0.1
 - 172.16.0.1
- Cinq classes d'adresses : A, B, C, D, E
 - E est réservée aux organismes de recherche
 - D est réservée à l'adressage de groupe
 - A, B et C définissent des adresses unicast et sont réservées aux utilisateurs d'Internet (entreprises, administrations, FAI, etc)

Adressage par classes

- Une adresse de classe A, B ou C comprend deux parties
 - une partie identifiant le réseau appelée ID de réseau (Net-id)
 - une partie identifiant l'équipement sur le réseau appelée ID d'hôte (Host-id)



- N et H le nombre de bits alloués au Net-id et Host-id resp.
 - 2^N réseaux différents pouvant être créés sur chaque classe
 - pour la classe A, retirer les adresses réservées comme 0.0.0.0 et 127.0.0.0
 - $2^H - 2$ équipements adressables sur chaque réseau
 - retirer l'adresse du réseau et l'adresse de diffusion

Classe	Valeur de w	Net-id	Host-id	Nombre de réseaux	Nombre d'hôtes réseau
A	1-126	w	x.y.z	$2^7 - 2 / 126$	$2^{24} - 2 / 16777214$
B	128-191	w.x	y.z	$2^{14} / 16384$	$2^{16} - 2 / 65534$
C	192-223	w.x.y	z	$2^{21} / 2097152$	$2^{24} - 2 / 254$
D	224-239	Réservé pour un adressage multi-destinataires			
E	240-254	Réservé pour un adressage multi-destinataires			

- 0.0.0.0
 - utilisée lorsqu'une machine ne connaît pas encore son adresse IP
 - par ex., comme adresse source dans une requête DHCP
- (Net-id, Host-id=0)
 - désigne le réseau dans son ensemble
 - par ex., 193.55.44.0 désigne un réseau de classe C
- 255.255.255.255
 - adresse de diffusion restreinte au réseau local
 - par ex., utilisée comme destination dans une requête DHCP
- (Net-id=127, Host-id !=0)
 - adresse de bouclage (localhost)
 - par ex., utilisée pour les communications inter-processus sur l'ordinateur

- Adresses privées, restreintes au réseau local, non routables sur Internet
 - gratuites
 - on choisit la classe en fonction de la taille de son réseau
 - le plan d'adressage reste inchangé quand on change de FAI
 - la structure interne du réseau est invisible de l'extérieur

Classe	A	B	C
Adresses réseaux	10.0.0.0	De 172.16.0.0 à 172.31.0.0	De 192.168.0.0 à 192.168.255.0

- Il faut toutefois un mécanisme de translation d'adresses (NAT) pour que les datagrammes puissent sortir du réseau privé

- Grandeur associée à un réseau et au format d'adresse IP
 - tous les bits du Net-id à 1
 - tous les bits du Host-id à 0
 - ⇒ un masque contient une suite de 1 de longueur variable de la gauche vers la droite
- Exemple
 - le masque associé au réseau d'adresse 193.55.44.0 est 255.255.255.0
 - car c'est un réseau de classe C dont le Net-id comprend 24 bits

Classe	A	B	C
Masques par défaut	255.0.0.0	255.255.0.0	255.255.255.0

- Utilisé par les routeurs pour identifier le réseau de destination d'un paquet
 - un ET-logique entre l'adresse IP d'une machine et le masque fournit l'adresse du réseau auquel appartient la machine
- Exemple pour l'adresse 193.55.44.12 et le masque 255.255.255.0

Adresse machine	1100 0001 . 0011 0111 . 0010 1100 . 0000 1100
Masque	1111 1111 . 1111 1111 . 1111 1111 . 0000 0000
ET-logique	1100 0001 . 0011 0111 . 0010 1100 . 0000 0000
Ecriture décimale	193 . 55 . 44 . 0

- <http://jodies.de/ipcalc>

- Les trames sont transmises en mode diffusion sur les réseaux locaux
 - cas des réseaux Ethernet et WiFi par exemple
 - inconvenients
 - encombrement du support de transmission
 - gaspillage de ressources (bande passante, temps CPU)
 - pas de confidentialité des données
- L'interconnexion de réseaux hétérogènes (Ethernet, Wifi, TokenRing, etc) exige autant d'adresses IP publiques
- Intéressant de segmenter selon la structure de l'entreprise
 - par ex., un réseau par département

Segmentation en sous-réseaux

- On partage les bits du Host-id en deux parties
 - les bits de segmentation sont contigus au bit le plus significatif du Host-id et situés "à gauche"
 - N bits de segmentation permettent de créer 2^N sous-réseaux
- Segmentation du réseau de classe C d'adresse 193.55.44.0 en trois sous-réseaux :
 - réservier 2 bits du 4ème octet au minimum
 - 4 adresses de sous-réseaux possibles
 - 1 **0000 0000** (0) \Rightarrow 193.55.44.0
 - 2 **0100 0000** (64) \Rightarrow 193.55.44.64
 - 3 **1000 0000** (128) \Rightarrow 193.55.44.128
 - 4 **1100 0000** (192) \Rightarrow 193.55.44.192
 - le masque de segmentation a tous les bits du Net-id et de segmentation à 1, les autres à 0
 \Rightarrow 255.255.255.192

Segmentation en sous-réseaux

- On choisit les trois premières adresses de sous-réseau

	4ème octet : bits identifiant			
	Le sous-réseau	La machine	Valeur décimale du 4ème octet	Adresse de diffusion
Sous-réseau 1 : 193.55.44.0	00	11 1111	63	193.55.44.63
Sous-réseau 2 : 193.55.44.64	01	11 1111	127	193.55.44.127
Sous-réseau 3 : 193.55.44.128	10	11 1111	191	193.55.44.191

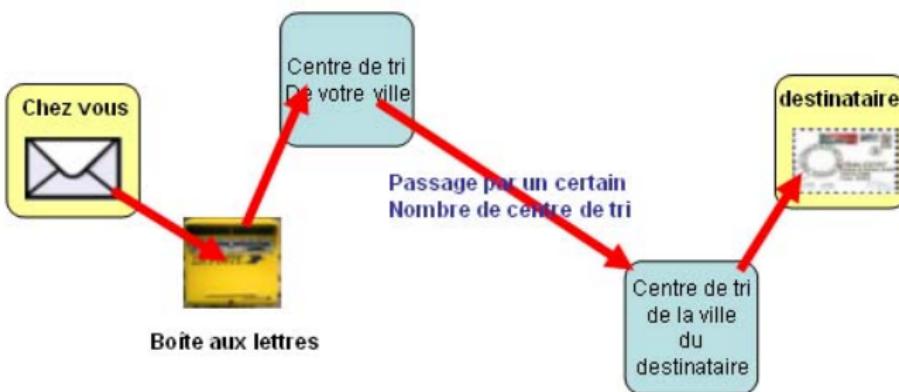
5

L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- **Le routage**
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

Acheminement d'une lettre par la poste

- Pour envoyer une lettre par la poste
 - vous la postez dans la boîte-aux-lettre la plus proche
 - ce courrier est relevé et envoyé au centre de tri de votre ville
 - il est alors transmis à d'autres centres de tri jusqu'à atteindre le destinataire



Acheminement d'un message sur Internet

- Avec Internet c'est à peu près la même chose
 - vous déposez le paquet IP sur l'ordinateur le plus proche (celui de votre FAI)
 - le paquet IP va transiter d'ordinateur en ordinateur jusqu'à atteindre le bon destinataire



- ⇒ Le routage est le mécanisme par lequel des chemins sont sélectionnés dans le réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires

- Les routeurs sont des dispositifs permettant de “choisir” le chemin que les datagrammes vont emprunter à travers le réseau pour arriver à destination
 - routeurs = machines possèdant plusieurs cartes réseau dont chacune est reliée à un réseau différent
- Dans la configuration la plus simple, le routeur n'a qu'à “regarder” sur quel réseau se trouve un ordinateur pour lui faire parvenir les datagrammes en provenance de l'expéditeur
- Toutefois, sur Internet le schéma est beaucoup plus compliqué
 - le nombre de réseaux auxquels un routeur est connecté est généralement important
 - les réseaux auxquels le routeur est relié peuvent être reliés à d'autres réseaux que le routeur ne connaît pas directement

- Les routeurs fonctionnent grâce à des tables de routage et des protocoles de routage selon le modèle suivant
 - ➊ le routeur reçoit une trame provenant d'une machine connectée à un des réseaux auquel il est rattaché
 - ➋ les datagrammes sont transmis à la couche IP
 - ➌ le routeur regarde l'en-tête du datagramme
 - ➍ si l'adresse IP de destination appartient à l'un des réseaux auxquels une des interfaces du routeur est rattaché, l'information doit être envoyée vers ce réseau
 - ➎ si l'adresse IP de destination fait partie d'un réseau différent, le routeur consulte sa table de routage, une table qui définit le chemin à emprunter pour une adresse donnée
 - ➏ le routeur envoie le datagramme grâce à la carte réseau reliée au réseau sur lequel le routeur décide d'envoyer le paquet

- Deux scénarios sont donc envisageables
 - soit l'émetteur et le destinataire appartiennent au même réseau auquel cas on parle de remise directe
 - soit il y a au moins un routeur entre l'expéditeur et le destinataire, auquel cas on parle de remise indirecte
 - Dans le cas de la remise indirecte, le rôle du routeur, notamment celui de la table de routage, est très important
- ⇒ Le fonctionnement d'un routeur est déterminé par la façon selon laquelle cette table de routage est créée
- si la table routage est entrée manuellement par l'administrateur, on parle de routage statique (viable pour de petits réseaux)
 - si le routeur construit lui-même la table de routage en fonctions des informations qu'il reçoit (par l'intermédiaire de protocoles de routage), on parle de routage dynamique

- La table de routage est une table de correspondance entre l'adresse du réseau de la machine visée et le noeud suivant auquel le routeur doit délivrer le message
 - la table de routage est donc un tableau contenant des paires d'adresses
- Grâce à cette table, le routeur va être capable de savoir sur quelle interface envoyer le message
 - ce mécanisme consistant à ne connaître que l'adresse du prochain maillon menant à la destination est appelé routage par sauts successifs (next-hop routing)
- Il se peut que le destinataire appartienne à un réseau non référencé dans la table de routage
 - dans ce cas, le routeur utilise un routeur par défaut (appelé aussi passerelle par défaut)

La table de routage

- Le routeur reçoit sur son interface d'adresse 192.168.3.1 (eth1) un datagramme provenant d'une machine d'adresse 192.168.3.10 et à destination de l'adresse 172.16.0.10
 - la 5ème ligne de la table de routage fournit la destination 172.16.0.0 qui est accessible par le routeur 192.168.4.2 via l'interface eth2
 - le datagramme est alors transmis au protocole de niveau liaison en fournissant l'adresse MAC de 192.168.4.2 (obtenue possiblement avec ARP)

Destination	Masque	Prochain routeur	Interface	Métrique
192.168.1.0	255.255.255.0	192.168.4.2	eth2	2
192.168.2.0	255.255.255.0	192.168.4.2	eth2	2
192.168.3.0	255.255.255.0	192.168.3.1	eth1	1
192.168.4.0	255.255.255.0	192.168.4.1	eth2	1
172.16.0.0	255.255.0.0	192.168.4.2	eth2	3
10.0.0.0	255.0.0.0	192.168.4.2	eth2	3
0.0.0.0	0.0.0.0	192.168.4.2	eth2	

La table de routage

- Le routeur reçoit sur son interface d'adresse 192.168.3.1 (eth1) un datagramme provenant d'une machine d'adresse 192.168.3.10 et à destination de l'adresse 195.1.0.10
 - la dernière ligne de la table de routage fournit la destination 0.0.0.0 qui est accessible par la passerelle par défaut 192.168.4.2 via l'interface eth2
 - le datagramme est alors transmis au protocole de niveau liaison en fournissant l'adresse MAC de 192.168.4.2 (obtenue possiblement avec ARP)

Destination	Masque	Prochain routeur	Interface	Métrique
192.168.1.0	255.255.255.0	192.168.4.2	eth2	2
192.168.2.0	255.255.255.0	192.168.4.2	eth2	2
192.168.3.0	255.255.255.0	192.168.3.1	eth1	1
192.168.4.0	255.255.255.0	192.168.4.1	eth2	1
172.16.0.0	255.255.0.0	192.168.4.2	eth2	3
10.0.0.0	255.0.0.0	192.168.4.2	eth2	3
0.0.0.0	0.0.0.0	192.168.4.2	eth2	

5

L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- **Le CIDR**
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

- Remarques

- la classe A ne contient que 126 réseaux de taille disproportionnée
- la classe C offre des réseaux de trop petites tailles
- seule la classe B offre un meilleur compromis

- Problèmes

- épuisement des adresses de la classe B (64K), la plus propice à la segmentation
- tables de routage de complexité croissante
- possible saturation de l'espace IPv4 tout entier

⇒ L'IETF a proposé au début des années 90 la méthode d'adressage et de routage CIDR (Classless Inter-Domain Routing) pour répondre aux 2 premiers problèmes

- Abandon de la notion figée de classe et Net-id au profit du "préfixe"
- Chaque adresse réseau est représentée par
 - une suite de 4 octets comme les adresses IPv4 classiques
 - puis le caractère /
 - et un nombre décimal indiquant le nombre de bits valant 1 dans le masque associé
- Exemples
 - 192.168.1.0/24 correspond au réseau de classe C
192.168.1.0 associé au masque 255.255.255.0
 - 172.16.0.0/16 correspond au réseau de classe B
172.16.0.0 associé au masque 255.255.0.0

- Aggrégation de routes
 - un FAI peut aggréger 2 adresses réseaux (clients) 200.100.32.0/24 et 200.100.33.0/24 en une seule 200.100.32.0/23 dans ses tables de routage
- Adaptation aux besoins des utilisateurs
 - si un client a besoin de 800 adresses et que le FAI dispose du bloc 200.100.64.0/18
 - soit il opte pour une adresse réseau de classe B qui lui fait perdre environ 64700 adresses
 - soit il opte pour 4 adresses de classe C à répercuter dans ses tables de routage (4 routes)
 - ⇒ CIDR lui permet d'opter pour le bloc 200.100.68.0/22 induisant une perte de 222 ($=2^{10}-2-800$) adresses

5

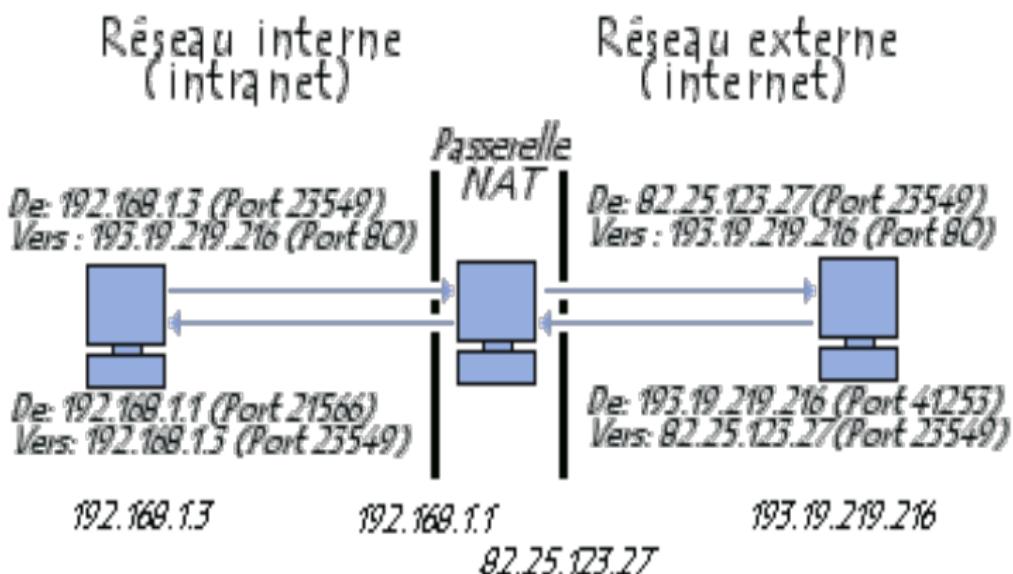
L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- Le CIDR
- La translation d'adresses**
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement

- NAT = Network Address Translation
 - NAT est une réponse à la pénurie d'adresses IP avec le protocole IPv4
 - IPv6 résoudra ce problème à terme
- NAT consiste à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines d'un réseau
 - une unique machine (ordinateur ou routeur), appelée passerelle NAT, est directement connectée à Internet avec une adresse qui lui est propre
 - les autres machines du réseau sont raccordées à cette machine pour accéder à Internet
 - ⇒ translation entre l'adresse privée de ces machines et l'adresse IP de la passerelle
- ⇒ Outre l'économie d'adresses publiques, ce mécanisme sécurise le réseau interne étant donné qu'il camoufle l'adressage interne

- Statique : associer une adresse IP publique à une adresse IP privée interne au réseau
 - ⇒ le routeur (ou passerelle) associe à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique et réalise la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP
 - ⇒ sécurise le réseau mais ne permet pas d'économiser des adresses IP !
- Dynamique : partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé
 - ⇒ toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP (*Mascarade IP*)
 - ⇒ afin de partager une même adresse publique, le NAT dynamique réalise une translation de port : affectation d'un port source différent à chaque requête pour différencier les machines

NAT - Translation d'adresses



<http://www.commentcamarche.net/contents/protect/nat.php3>

5

L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage**
- Exemple de fonctionnement

Protocole ARP (Address Resolution Protocol)

- Fournit l'adresse MAC d'une station dont l'adresse IP est connue
- Détecte les conflits d'adressage sur un réseau local
- Implémenté dans les hôtes et les routeurs
 - la requête ARP est diffusée à tout le réseau local
 - la machine reconnaissant son adresse IP y répond par un paquet ARP unicast
- Les résolutions ARP sont stockées en cache de manière temporaire

- Pour tester la connectivité et aider IP dans la gestion du trafic
- Implémenté dans les hôtes et les routeurs
- Différents types de messages ICMP
 - demande d'écho (echo request)
 - réponse à demande d'écho (echo reply)
 - destination injoignable (destination unreachable)
 - redirection (redirect)
 - durée de vie du datagramme excédée (time exceeded)
unicast

Commandes ping et traceroute

- ping teste la connectivité
 - transporté par ICMP ou UDP
 - informations : délai d'aller-retour (round-trip time), codes d'erreur, taille et TTL des paquets, ...
- traceroute détermine le chemin suivi de la source au destinataire
 - transporté par ICMP ou UDP
 - informations : identité des routeurs traversés, RTTs, ...

Protocole DHCP (Dynamic Host Configuration Protocol)

- Alloue à la demande des adresses IP se connectant au réseau
- Un serveur DHCP est configuré dans le réseau et maintient
 - une table d'adresses IP valides et d'adresses réservées
 - des paramètres de configuration pour les clients : masques, ...
 - durée des baux
- Allocation en 4 étapes
 - 1 découverte : le client envoie une trame de diffusion vers un serveur DHCP
 - 2 offre : tous les serveurs DHCP font une offre
 - 3 demande : le client répond positivement à l'un des serveurs
 - 4 accusé de réception : le serveur choisi confirme le bail avec sa durée et options associées

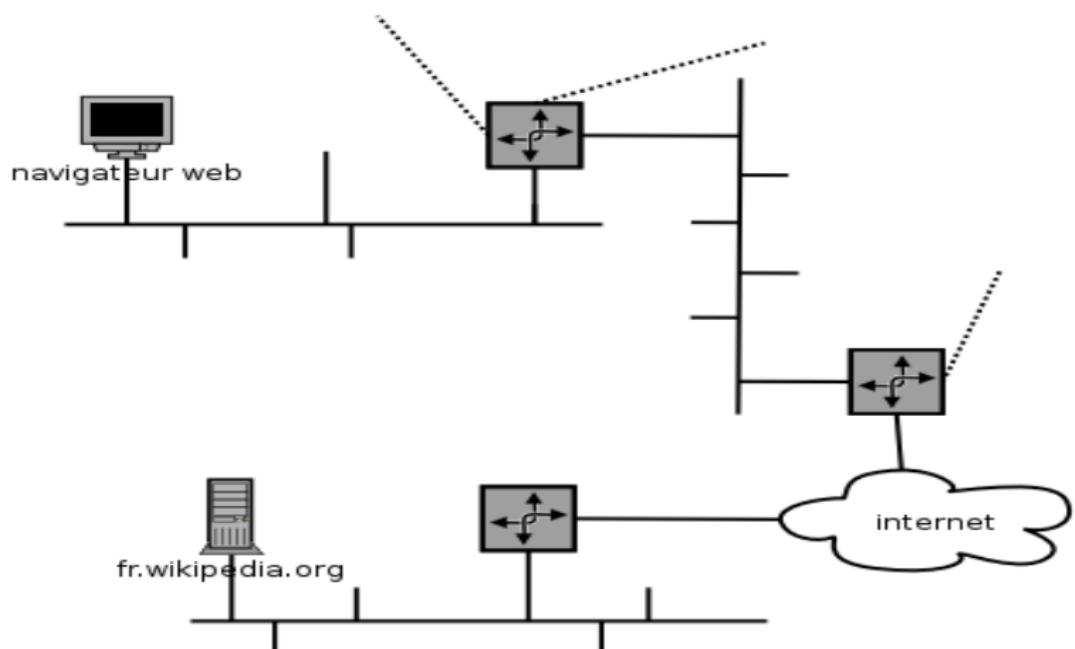
5

L'Adressage et le Routage

- Le rôle de la couche Internet
- Le protocole IP
- Le routage
- Le CIDR
- La translation d'adresses
- Les protocoles et commandes liés à l'adressage
- Exemple de fonctionnement**

Exemple : télécharger la page

<http://fr.wikipedia.org/wiki/Accueil>



- ➊ Le navigateur demande au DNS quelle est l'adresse IP du serveur `fr.wikipedia.org`.
- ➋ Le DNS retourne `207.142.131.203` par exemple
- ➌ Le navigateur envoie la requête HTTP suivante :

GET /wiki/Accueil HTTP/1.1

Host : fr.wikipedia.org

User-Agent :

...

- ➍ Le serveur web répond :

HTTP/1.0 200 OK

Date : Wed, 16 Nov 2005 15:40:41 GMT

Server : Apache

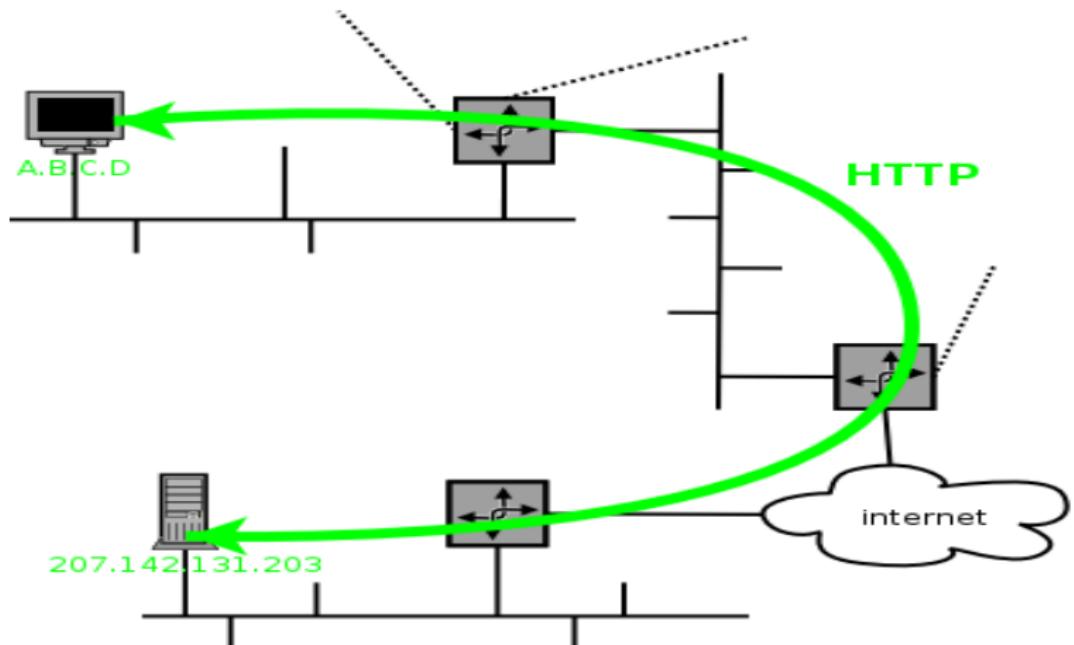
...

<HTML>

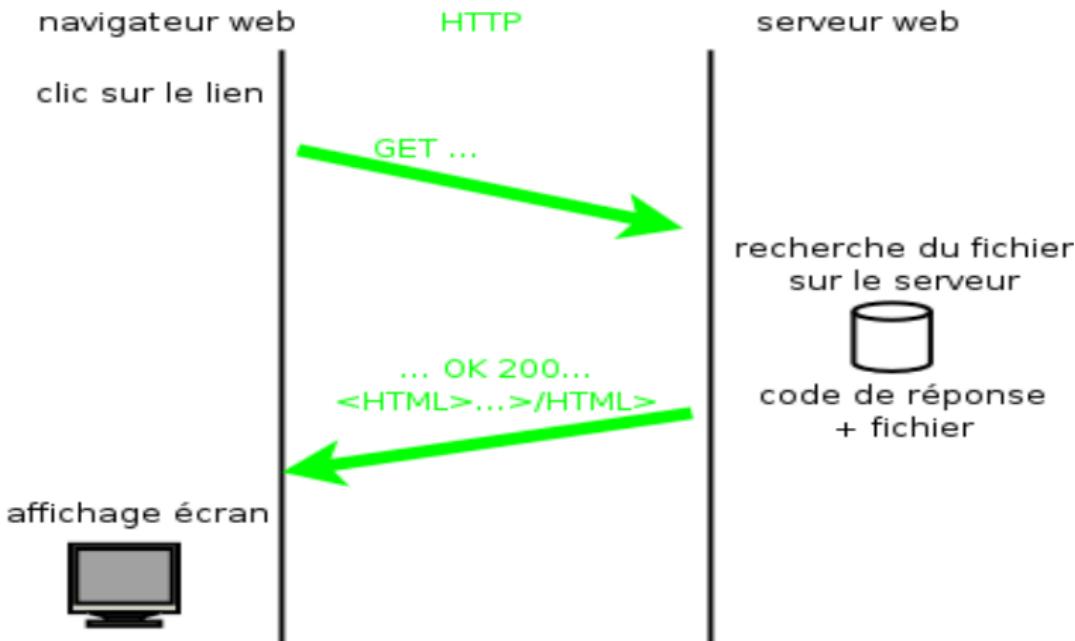
...

</HTML>

Niveau applicatif



Niveau applicatif

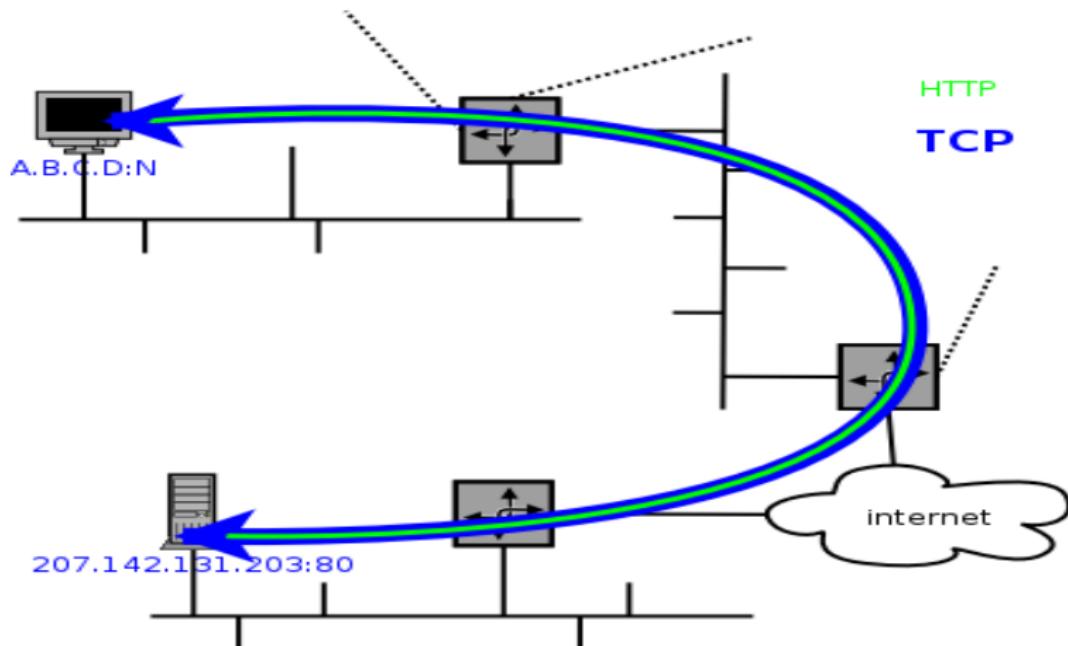


- Le dialogue HTTP s'appuie sur une connexion TCP qui permet de préciser notamment les ports (80 pour le serveur web et un port libre N quelconque pour le client) sur lesquels se fait le dialogue
 - ① établissement de la connexion TCP
 - ② envoi de la requête HTTP du navigateur au serveur : 1 seul segment TCP suffit
 - ③ envoi de la réponse HTTP du serveur au navigateur : plusieurs segments TCP sont nécessaires
 - ④ fermeture de la connexion TCP

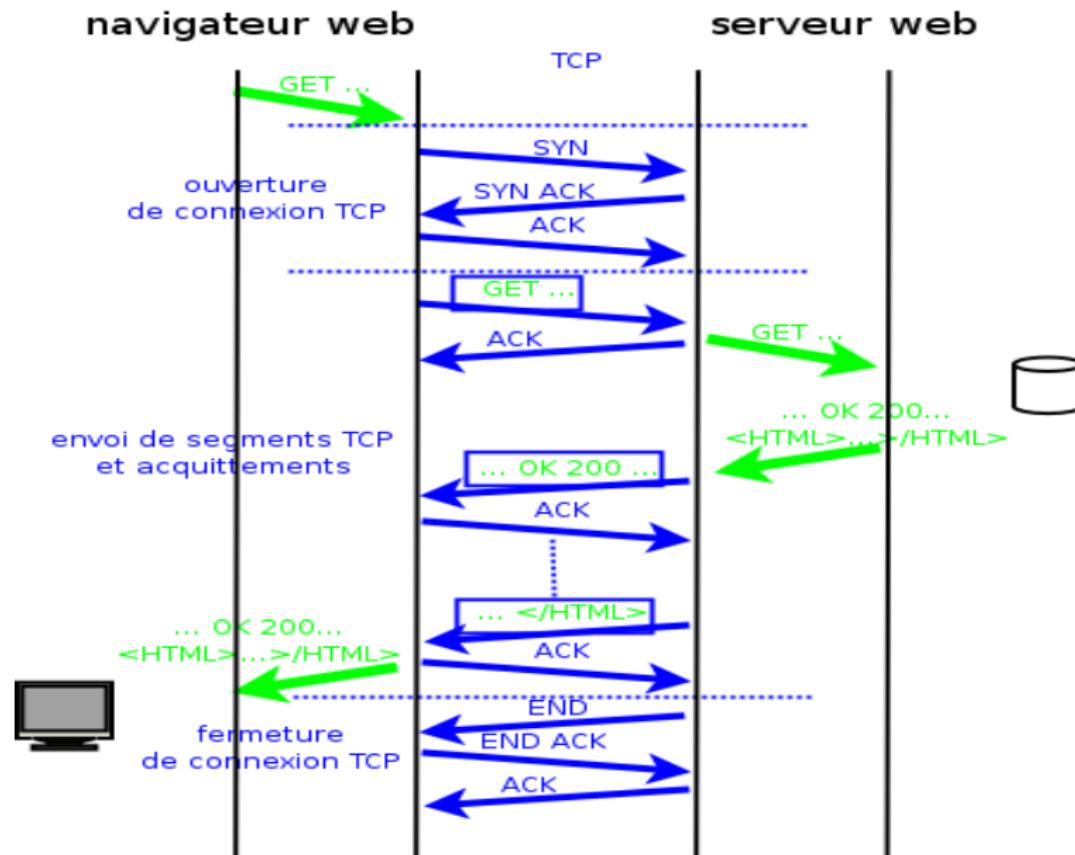
Ce canal de communication est un socket

(A.B.C.D :N, 207.142.131.203 :80)

Niveau TCP

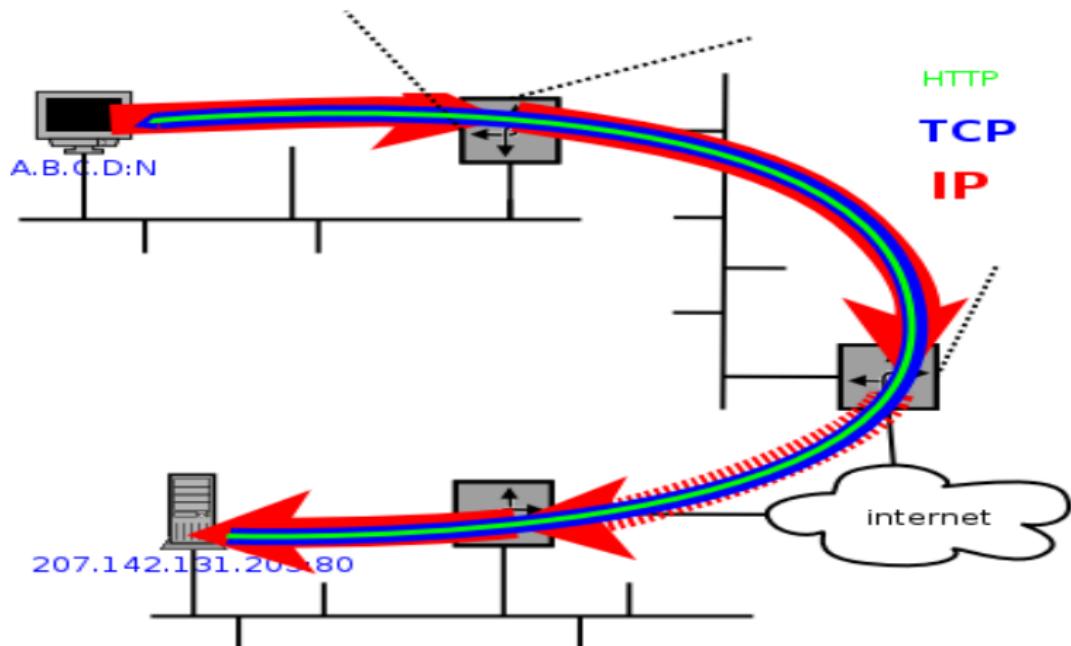


Niveau applications et TCP



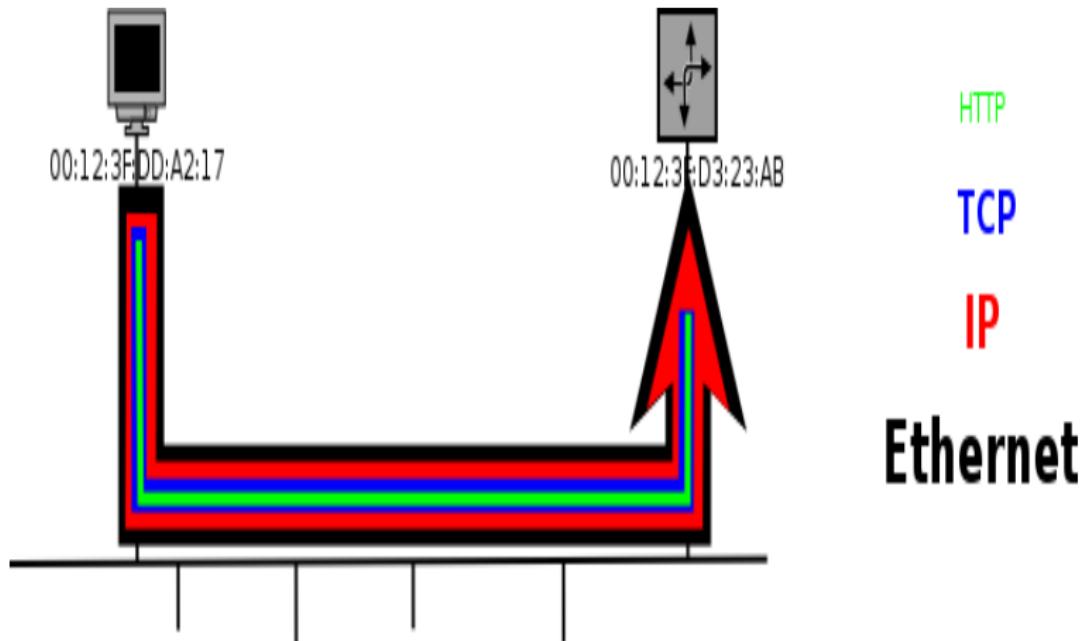
- ➊ Chaque segment TCP est placé dans un paquet IP
- ➋ Chaque paquet IP contient, entre autres informations, l'adresse IP de l'émetteur et l'adresse IP du destinataire final du paquet
- ➌ Chaque paquet va de routeur en routeur jusqu'à sa destination finale
- ➍ A chaque routeur, la table de routage indique l'adresse IP du prochain routeur et l'interface de sortie à emprunter pour atteindre la destination finale

Niveau IP



- ➊ Chaque paquet IP est placé dans une trame Ethernet ou fragmenté entre plusieurs trames Ethernet si nécessaire
- ➋ Chaque trame Ethernet contient, entre autres informations, l'adresse matérielle de l'émetteur dite adresse MAC (Medium Access Control). C'est l'adresse de la carte réseau. Pour Ethernet un nombre de 6 octets représentés en hexadécimal comme 00:12:3F:DD:A2:17
- ➌ Afin de pouvoir envoyer la trame Ethernet à la bonne destination, le protocole ARP sert à trouver l'adresse matérielle correspondant à l'adresse IP de l'interface de l'équipement qu'il faut atteindre

Niveau matériel, ex : Ethernet



1 Introduction

2 Les Réseaux et l'Internet

3 Les Services

4 Le Transport des Données

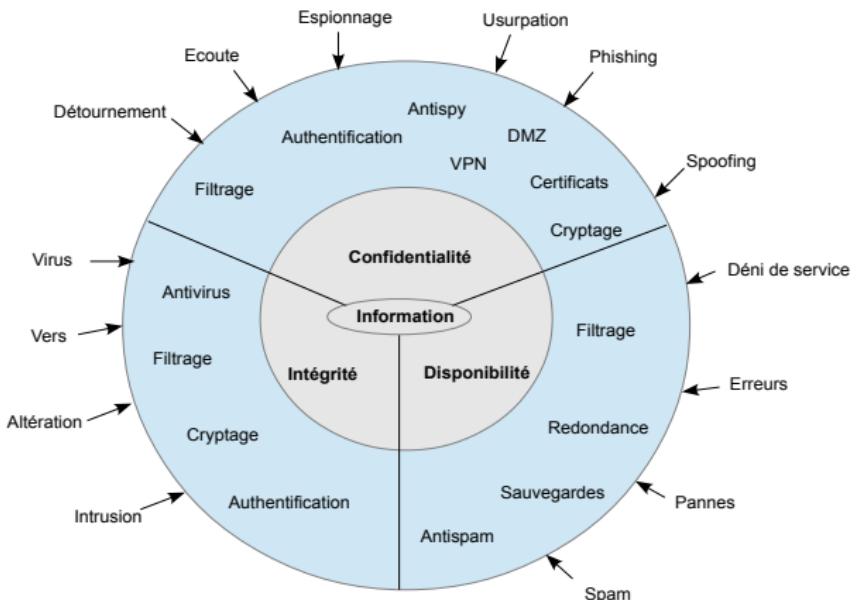
5 L'Adressage et le Routage

6 Sécurité sur Internet

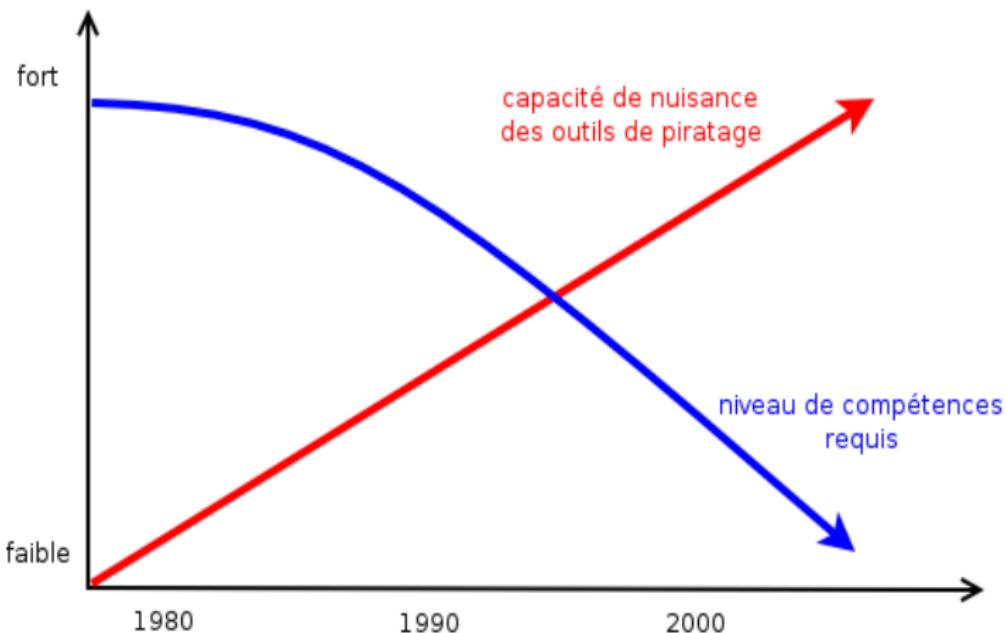
Objectifs de la sécurité informatique

- L'intégrité : garantir que les données échangées sont bien celles que l'on croit avoir échangées. 4 propriétés doivent être vérifiées : non-modification, non-suppression, non-rajout, non-création
- La confidentialité : assurer que seules les personnes en communication ont accès aux données échangées, les autres personnes ne doivent pas pouvoir "comprendre" les informations transmises
- La disponibilité : maintenir le bon fonctionnement du système d'information, l'accès au service ne doit pas être interrompu
- La non-répudiation : garantir qu'une transaction ne peut être niée, pouvoir montrer une "trace" de l'action effectuée
- L'authentification : assurer que seules les personnes autorisées ont accès aux ressources et que chaque personne est certaine de l'identité des autres partenaires de l'échange d'information

Objectifs, moyens et attaques



Importance de la sécurité



- Un virus est un programme informatique qui se loge à l'intérieur d'un autre logiciel. Chaque utilisation du logiciel porteur déclenche l'action du virus qui est généralement néfaste et qui va essayer de se répliquer pour infecter d'autres logiciels.

http://fr.wikipedia.org/wiki/Virus_informatique

- Un ver (worm) est un programme malveillant (script ou macro) qui se propage via le courrier électronique, fameux exemple : http://fr.wikipedia.org/wiki/I_love_you
- Un cheval de Troie (trojan) est un logiciel malveillant que l'utilisateur installe sciemment car il propose des fonctionnalités utiles qui masquent les autres effets.
- Une bombe logique est l'action néfaste provoquée par un virus, un ver, un cheval de Troie, ... à une date particulière ou après une action particulière.

- L'hameçonnage (phishing = phone fishing) consiste à présenter à l'utilisateur une page web ou un courriel identique à celui d'un organisme en lequel il a confiance (sa banque, ...) et à lui demander des informations personnelles (identifiant, mot de passe, ...)
- Un espion logiciel (spyware) collecte des informations sur l'activité d'un utilisateur pour les transmettre à un tiers. Les buts peuvent être publicitaires, délictueux (usurpation de mot de passe, ...), mais également d'administration de systèmes et réseaux
- Une porte dérobée (backdoor) est une option non documentée d'un logiciel qui permet aux utilisateurs informés de réaliser des actions à l'insu de l'utilisateur non informé
- Un enregistreur de touches (keylogger) enregistre tout ce qu'un utilisateur saisit sur son clavier (au moyen d'un logiciel ou d'un équipement branché entre le clavier et l'unité centrale)

- Le SPAM et mailbombing : envoi en grand nombre de courriels non souhaités.
- Se servir de paramètres mémorisés par un utilisateur précédent dans un navigateur web
- Ecouter les échanges réseaux grâce à un analyseur de trames pour récupérer des informations confidentielles
- Se connecter à un ordinateur distant en contournant le contrôle par identifiant+mot de passe
- L'attaque par déni de service (DOS : denial of service) consiste soit à inonder le serveur de requêtes de manière à le rendre inutilisable ou à trouver une faille permettant de rendre l'application inutilisable. (Exemple historique le “ping de la mort”)

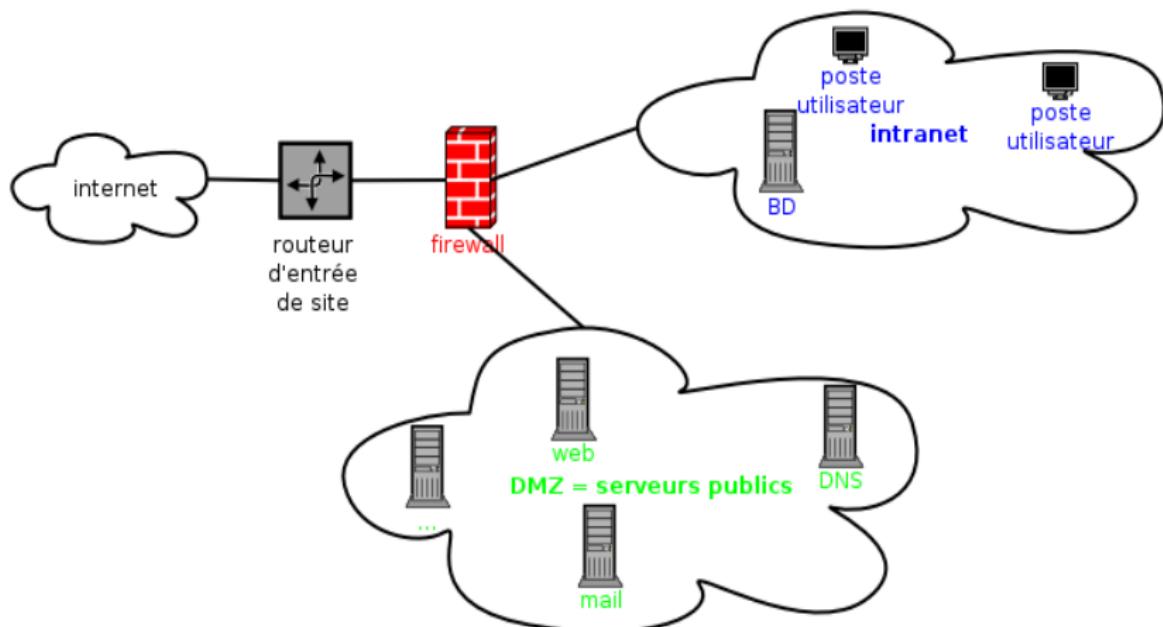
Une politique de sécurité repose sur plusieurs maillons :

- La sensibilisation des utilisateurs aux problèmes de sécurité et établissement de règles de bon usage des logiciels (courrier électronique surtout), de chartes, ...
- La sécurité logique : données, logiciels, systèmes d'exploitation, ...
- La sécurité des télécommunications : services et serveurs, technologies réseau, réseau interne, accès (entrée/sortie) à l'Internet, ...
- La sécurité physique : infrastructures matérielles, salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail, ...

- Tout le monde est concerné, car une machine “sans importance” peut servir de relais à une attaque vers un système important
- Comportement humain : choix des mots de passe (multiples, complexe, cachés, . . .), ne pas être naïf, vérifier ses sources
- Utiliser un antivirus, un antispam, un antispyware et les mettre à jour très régulièrement (automatiquement)
- Se méfier des canulars (hoax) www.hoaxbuster.com pour ne pas propager de fausses nouvelles
- Privilégier la diversité logicielle car les attaques auront un impact moindre
- Utiliser des logiciels libres : le code source étant disponible, les portes cachées et les bugs sont découverts et corrigés plus rapidement

Exemples de mesures de sécurité

- Architecturer le réseau de manière à contrôler les accès avec des systèmes de parefeux (firewall), de réseaux privés virtuels (VPN), ...



- Filtre les accès entre l'Internet et le réseau local ou entre deux réseaux locaux
- Possède autant d'interfaces que de réseaux connectés
 - filtrage spécifique à chaque interface
 - ex. blocage des adresses privées entrantes, autorisation accès entrant vers serveur d'identification
- Filtre par analyse des en-têtes de trames/paquets entrant/sortant
 - adresse MAC
 - adresse IP source ou destination
 - flags de l'en-tête : SYN, ACK, ...
 - type de message ICMP
 - type et contenu de messages applicatifs : HTTP, SMTP, POP, ...

Configuration de pare-feux

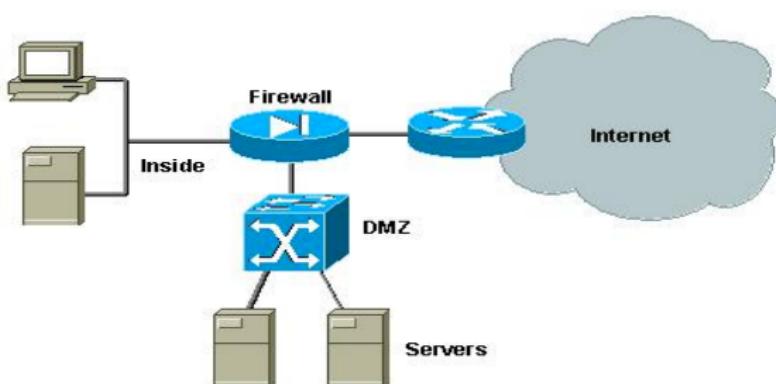
- Ecriture d'une suite de règles qui décrivent les actions à effectuer suivant les informations contenues dans le paquet/trame

Règle	Direct.	@source	@dest.	Prot.	Port src.	Port dest.	ACK =1	Action
A	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	80		Autorisé
B	Entrant	0.0.0.0	192.168.0.0	TCP	80	>1023		Autorisé
C	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	25		Autorisé
D	Entrant	0.0.0.0	192.168.0.0	TCP	25	>1023	Oui	Autorisé
E	Tous	Tous	Tous	Tous	Tous	Tous		Refusé

- Positionnement général : LAN < Pare-feu < Routeur < NAT < Internet
 - le filtrage des trames/paquets sortant s'effectue avant le routage qui s'effectue avant la translation d'adresse
 - le NAT s'applique aux trames/paquets entrant avant le routage qui s'effectue avant le filtrage

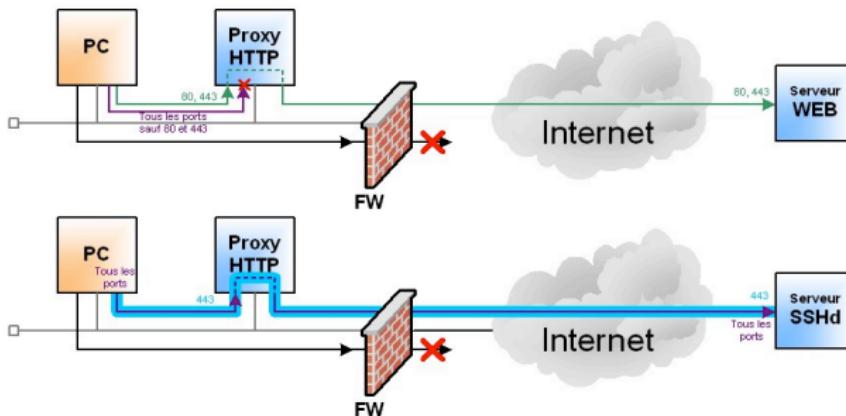
DMZ (DeMilitarized Zone)

- Zone de réseau privée ne faisant partie ni du réseau local privé ni de l'Internet ("zone franche")
- Permet de regrouper des ressources nécessitant un niveau de protection intermédiaire



Serveurs mandataires (Proxy)

- Joue le rôle de mandataire pour les machines locales en exécutant leurs requêtes
- Configuré pour certains protocoles (ex. HTTP, SMTP)
- Permet de centraliser et sécuriser les accès extérieurs : filtrage applicatif, enregistrement des connexions, masquage des adresses clients, ...



- Installer des serveurs web sécurisés pour l'échange des données sensibles (HTTPS)
- Préférer les protocoles sécurisés :
 - ssh plutôt que rlogin, telnet et rsh pour la connexion à une machine distante
 - sftp plutôt que ftp pour le transfert de fichiers
- Développer une infrastructure à clé publique (PKI)

http://fr.wikipedia.org/wiki/Cryptographie_asymétrique

- Mettre en place une surveillance réseau matérielle, logicielle et consacrer des moyens humains à cette tâche