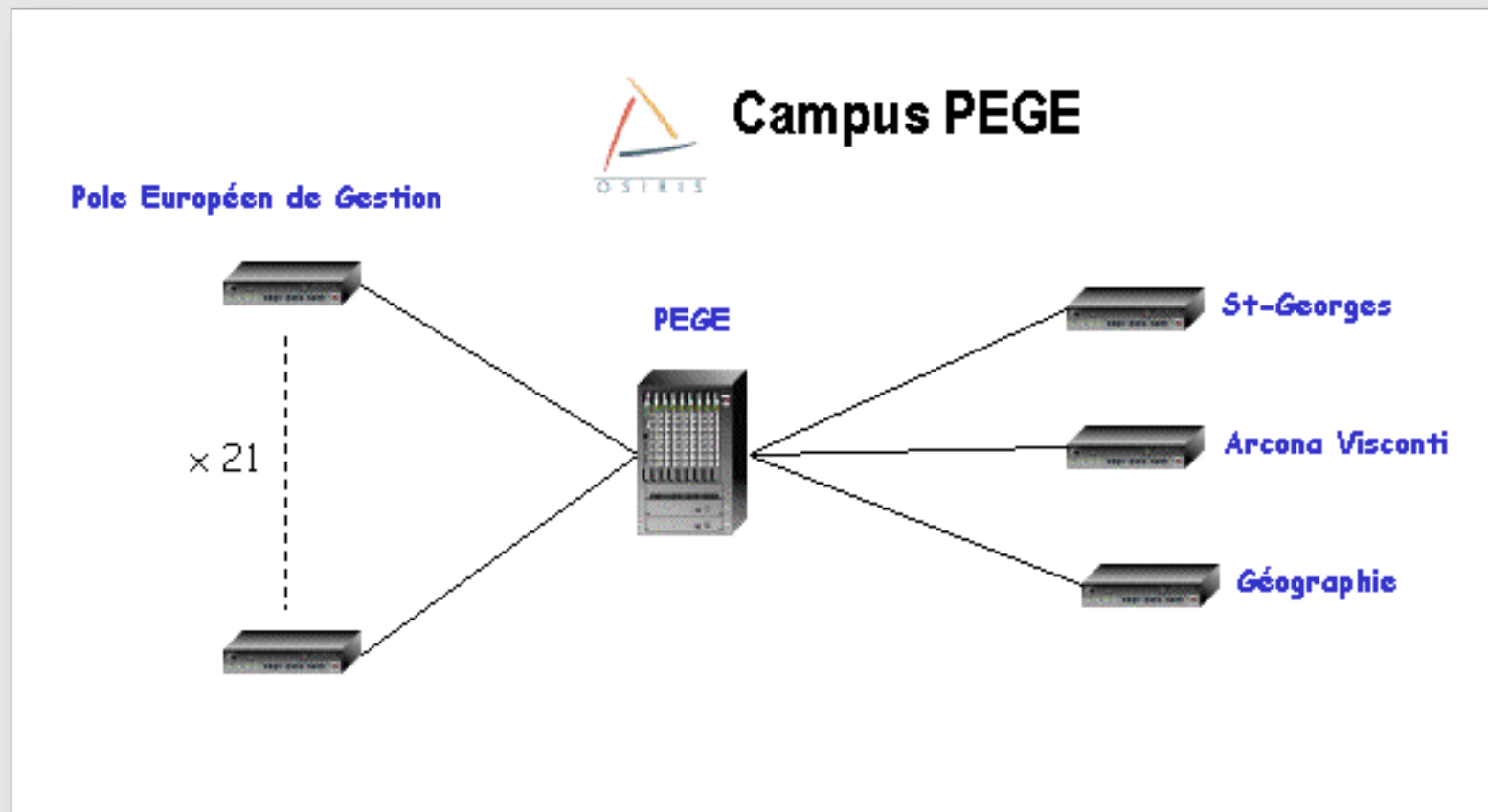


Pratique des réseaux

Stéphane Genaud
<stephane.genaud@iecs.edu>

Exemple de réseau

Un des sites du réseau : l'IECS



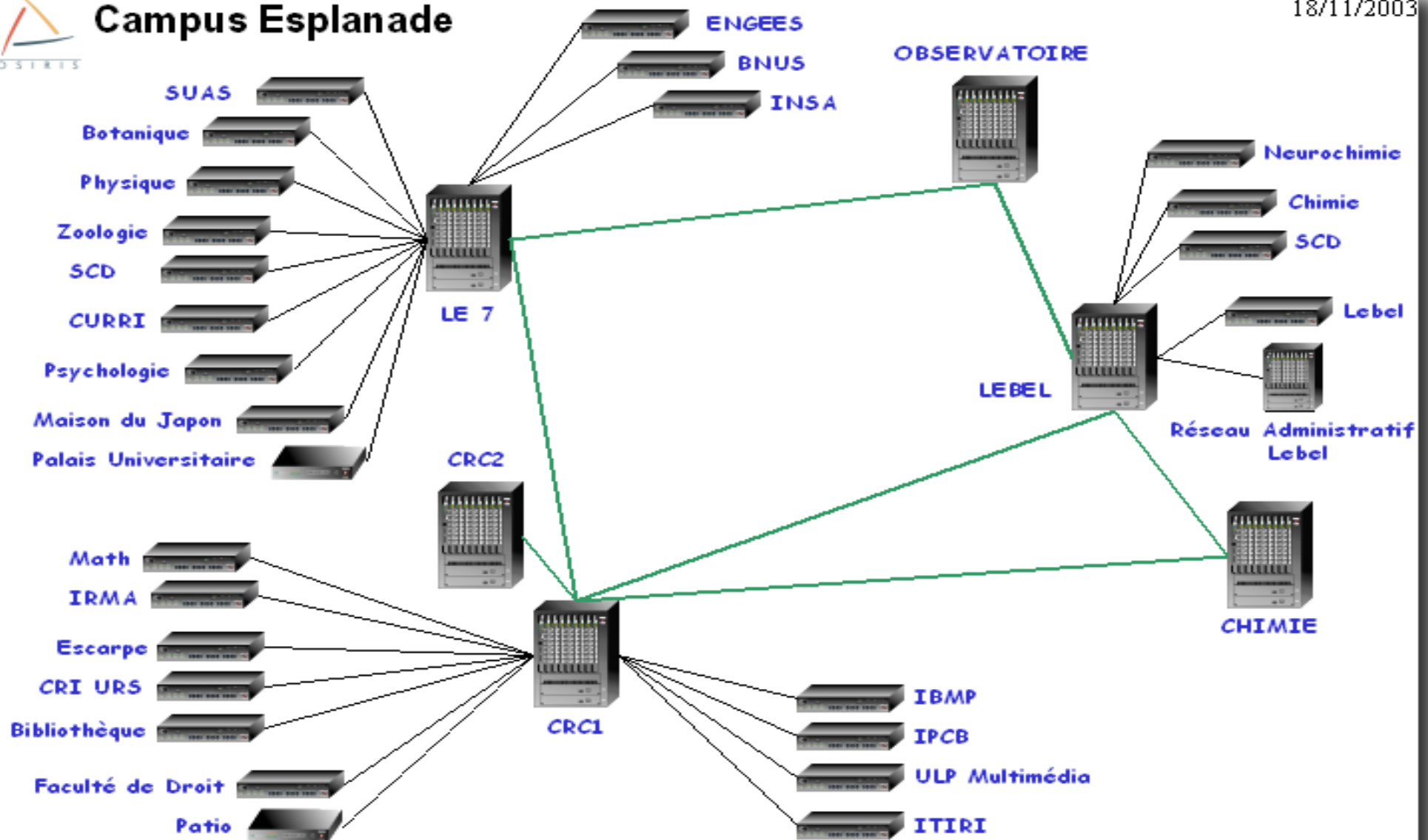
Parmi d'autres ...

Exemple de réseau

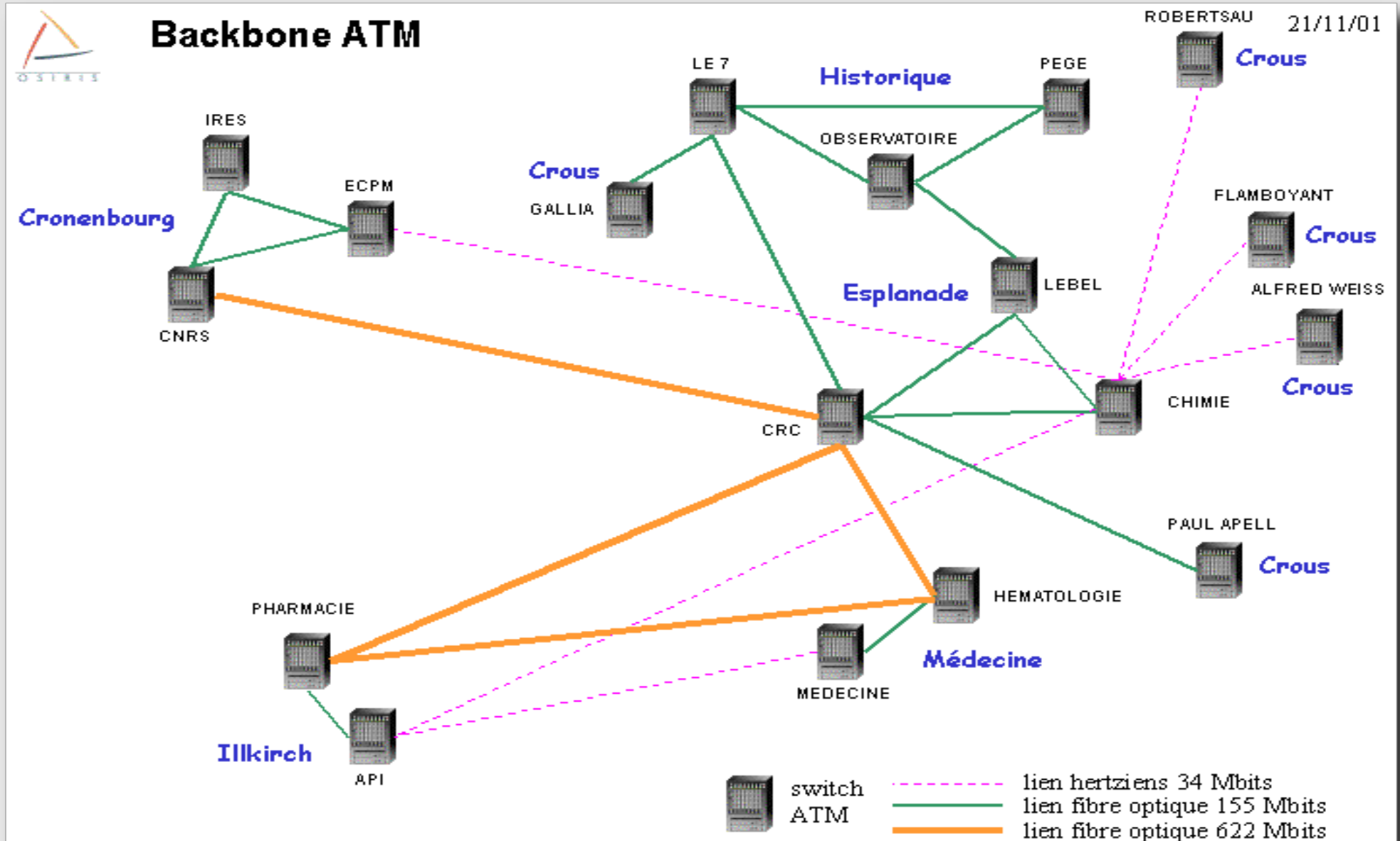


Campus Esplanade

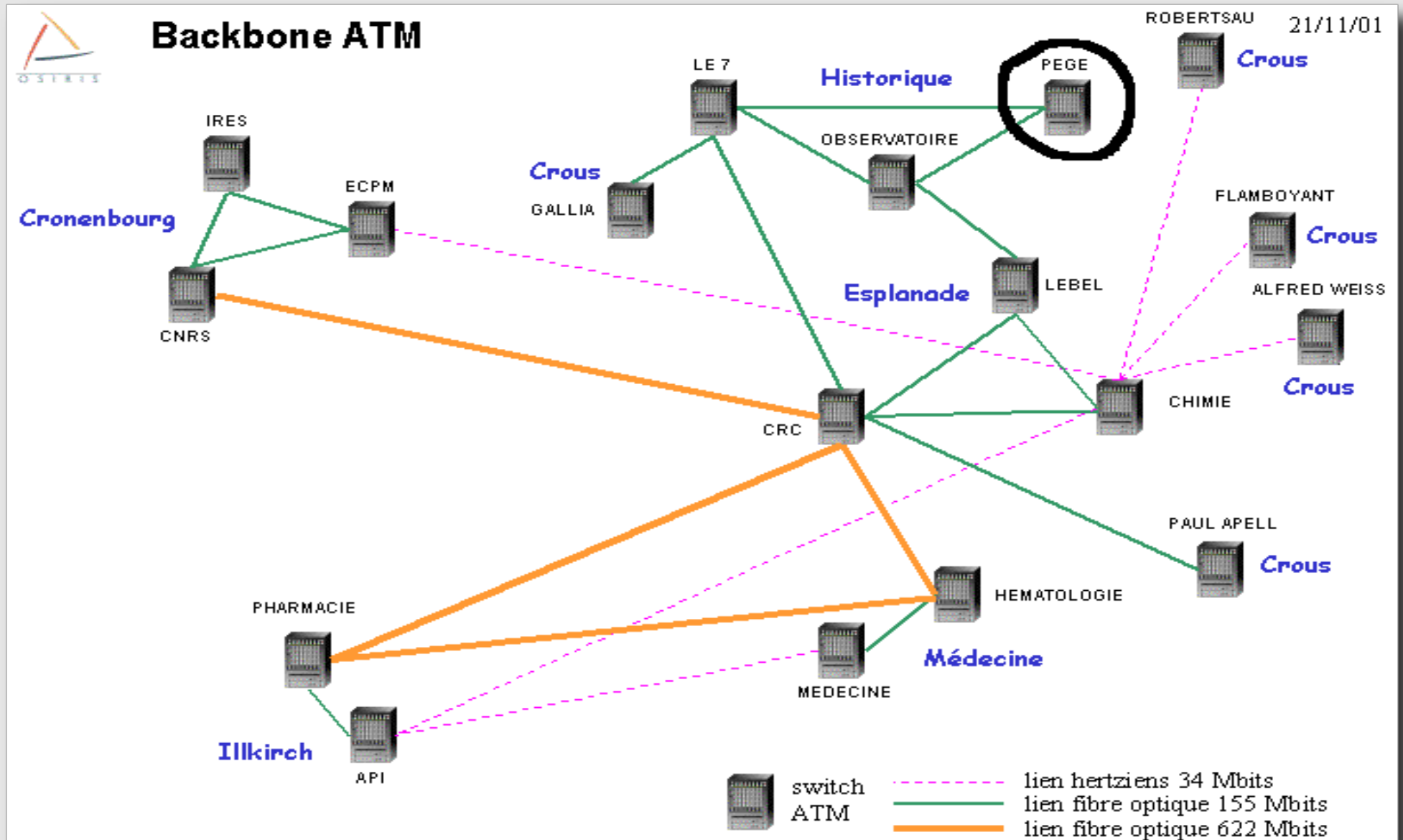
18/11/2003



Exemple de réseau



Exemple de réseau



Un réseau : du matériel et du logiciel

➔ Matériel

- Connectique
- Hubs, Routeurs, Switchs, ...

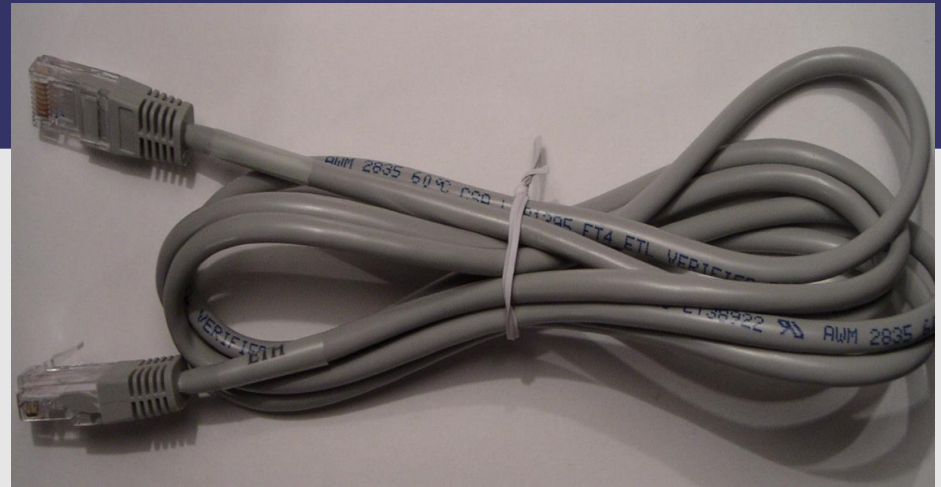
➔ Logiciel

- Logiciel inclus dans le système d'exploitation
- Applications exploitant le réseau

Connectique (1)

➔ Câble pour Ethernet

- connecteur RJ45
- paire torsadée
 - Catégorie 1 : Câble téléphonique traditionnel (transfert de voix mais pas de données)
 - Catégorie 2,3,4 : Transmission des données à 4, 10, et 16 Mbit/s maximum resp. Désuet.
 - Catégorie 5 : 100 Mbit/s maximum. Le minimum aujourd'hui.
 - Catégorie 5e : 1000 Mbit/s maximum.
 - Catégorie 6: 2.5 Gbit/s maximum.

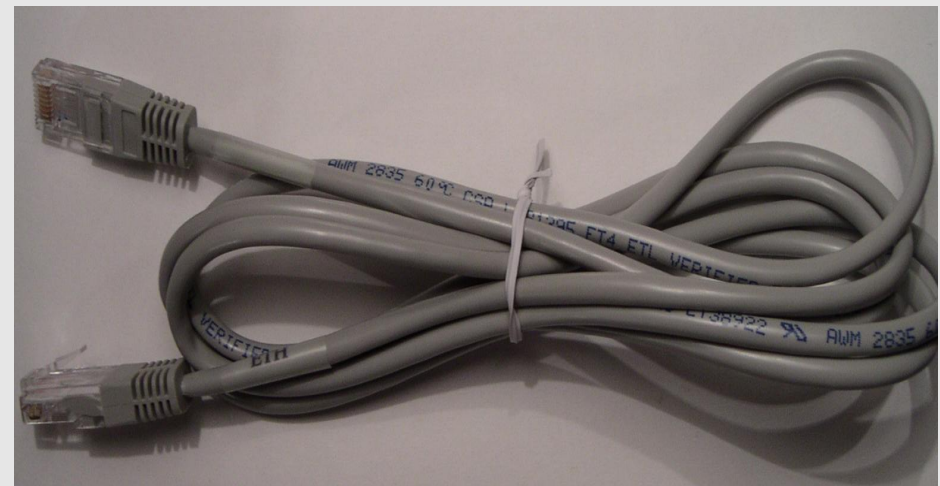


Connectique (2)

- ➔ capacité : capacité théorique et pratique
 - 10baseT => 10 Mb/s , et ~ 1Mo/s
 - 100baseT (fast ethernet) => 100 Mb/s et ~7-8 Mo/s
 - 1000baseT (gigabit ethernet) => 1000 Mb/s et ~70 Mo/s

➔ Remarques :

- ➔ Le câble coaxial est tombé en désuétude pour ethernet
- ➔ Les autres types de réseaux (Token Ring, AppleTalk) deviennent marginaux



Connectique (3)

➔ Carte Ethernet

- Avec fil, norme IEEE 802.3 10/100/1000baseT
- Sans fil, norme IEEE 802.11b et 802.11g
 - Capacité : débits de 11 Mb/s et 54Mb/s resp.



Connectique (3)

- ➔ Bâtiments pré-câblés : possèdent prises murales et/ou point d'accès sans fil.
 - Réseau destiné au grand public (ex: Noos) (RJ45)
 - Réseau d'entreprise (RJ45)
- ➔ Bâtiments munis de prise téléphoniques (RTC).
 - Utilisation d'un modem ADSL (USB/Ethernet + RTC)
 - Utilisation d'un modem analogique (RTC)



Connectique (4)

- ➔ Modem analogique
 - Plafond atteint à 56 Kb/s
- ➔ Modem ADSL
 - Offres actuelles (bande passante dédiée) :
 - Min: 128/64 Kb/s (16/8 Ko/s)
 - Moyen non-dégroupé: 512/128 Kb/s (64/16 Ko/s)
 - 1024/512 Kb/s (128/64 Ko/s)
 - ADSL2+ : jusqu'à ~20 Mb/s



Hubs et routeurs

➞ Hubs (ou concentrateurs)

- Ce sont des répéteurs de signaux (niveau 1-2 du modèle OSI)

➞ Switch (ou commutateurs)

- Décode l'entête pour connaître le destinataire et n'envoie que vers le port Ethernet associé. (niveau 1-2-3 du modèle OSI)

➞ Routeurs

- Route les messages en utilisant l'adresse IP.



Adressage des matériels

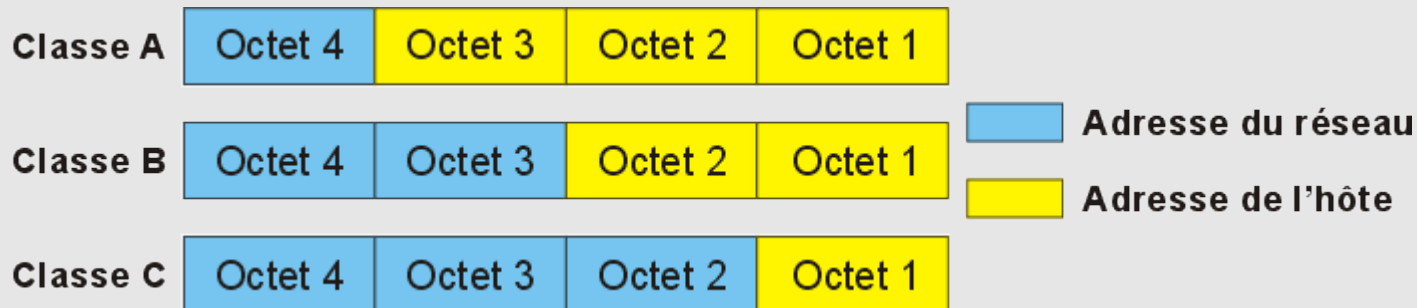
- ➔ Comment arrive t-on à localiser un ordinateur distant ?
 - Chaque matériel réseau possède un identifiant unique sur internet : son **numéro IP** ou **adresse IP** (Internet Protocol).
 - Le numéro IP reflète la localisation du matériel.
 - Sa forme : 4 octets, notée habituellement en décimal.
 - Exemple 192.132.12.165
 - Attribué par l'administrateur réseau dont le matériel dépend.
 - Un particulier l'obtient de son FAI
 - Mode d'attribution :
 - Fixe ou dynamique (donné par DHCP, valable pendant la connexion)

Adressage des matériels (2)

- ➔ Attribution d'une IP: gestion hiérarchique
 - Instance internationale ICANN chargée de la gestion
 - Délègue auprès d'instances régionales (Internet Registries)
 - APNIC (Asie-Pacifique)
 - ARIN (Amérique du Nord)
 - RIPE NCC (Europe)
 - Les instances régionales accordent une plage à des instances locales (FAI, grandes entreprises,...)
 - Environ 200 en France
 - Les administrateurs réseaux de ces LIR distribuent des numéros aux utilisateurs

Adressage des matériels (3)

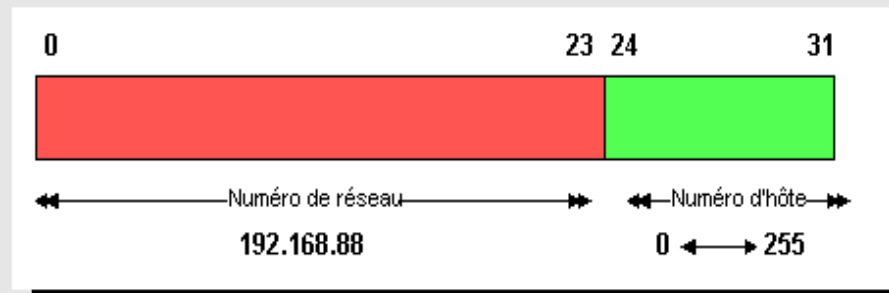
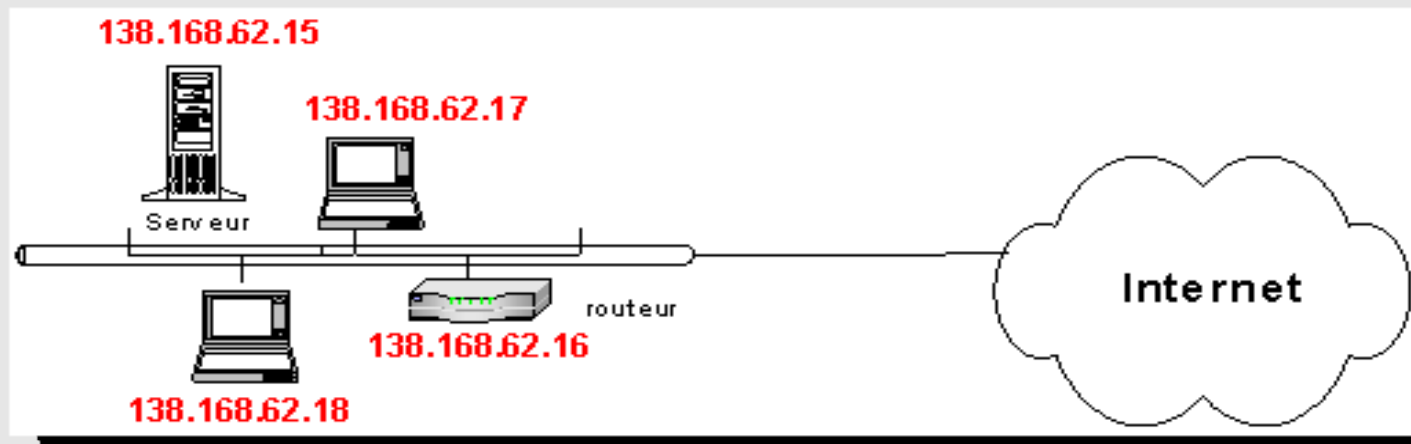
- ➔ L'adresse IP à une signification « variable »
 - Chaque administrateur réseau doit choisir la part du numéro IP qui désignera
 - Le réseau
 - La machine (l'hôte)
 - Les répartitions types sont appelées **classes** de réseau



La classe peut être déterminée à partir des 3 premiers bits
Ex : classe C : 192.0.0.1 à 223.255.255.254), classe B : 128.0.0.1 à 191.255.255.254)

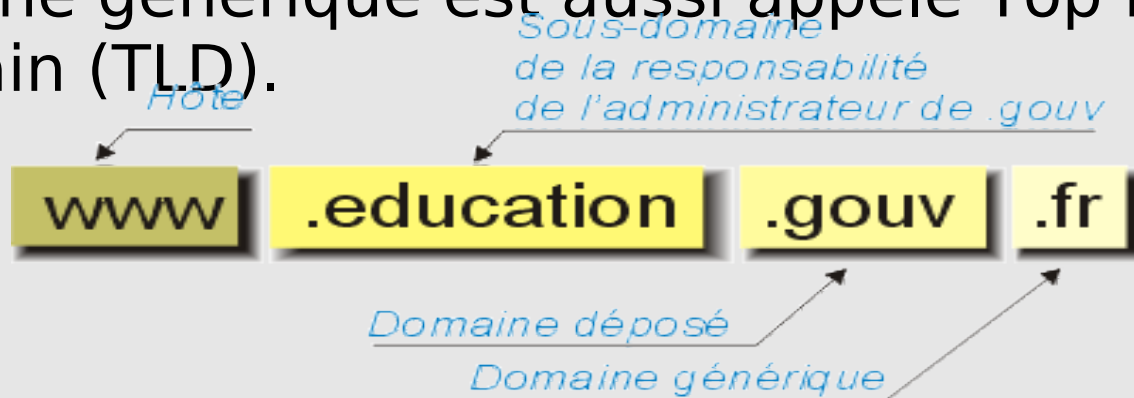
Adressage des matériels (4)

- ➔ L'adresse IP permet de faire du routage
- Connaissant la classe, le système détermine rapidement où envoyer le paquet.



Le DNS - principe

- ➔ Les humains préfèrent les noms aux numéros
 - Nous utilisons avantageusement www.free.fr au lieu de 212.27.32.5
 - Le système DNS (Domain Name Server) assure la correspondance : service de **résolution de noms**.
 - `[genaud@iso]$ nslookup www.free.fr`
 - Address: 212.27.32.5
 - Le nom d'une machine suit des règles (FQDN). Le domaine générique est aussi appelé Top Level Domain (TLD).



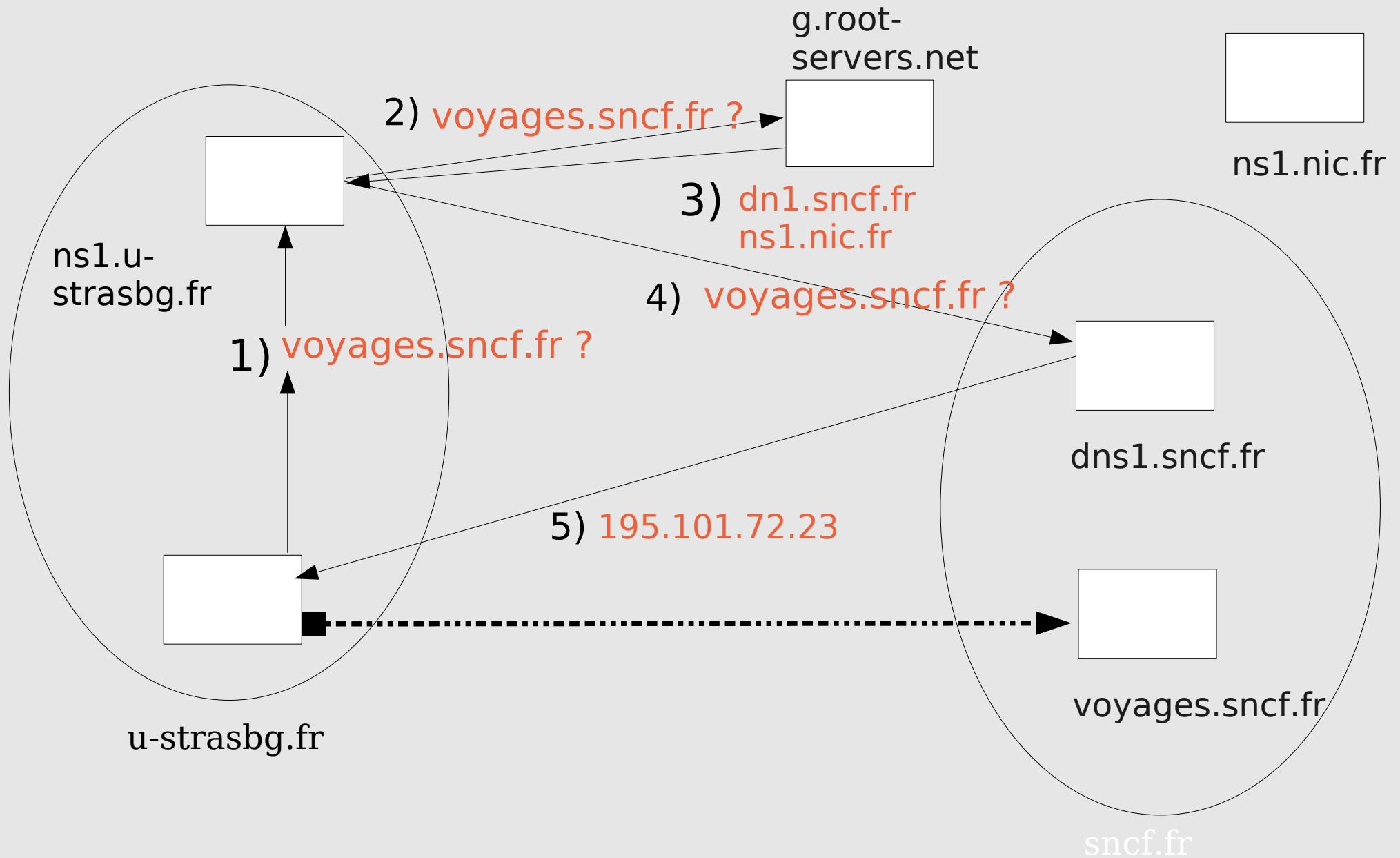
Le DNS - configuration client

- ➔ Pour accéder au service du DNS, il faut que le système connaisse au moins une machine qui héberge ce service (son adresse IP bien sûr).
 - Pour une IP fixe, la demander à l'administrateur réseau.
 - Pour les IP dynamique, le bail DHCP contient généralement l'adresse du DNS (transparent).
- ➔ C'est ce DNS qui prendra en charge toutes vos requêtes.
- ➔ On peut spécifier plusieurs DNS : serviront en cas de défaillance du premier.

Le DNS - mécanisme

- ➔ Le DNS auquel vous vous adressez ne connaît pas toutes les machines d'internet. Imaginez un système de millions de machines en perpétuel changement, et obtenir une réponse en quelques millisecondes.
- ➔ Il existe une « colonne vertébrale » de l'internet : 13 serveurs : A.root-servers.net, ... , M.root-servers.net identiques. (
`ftp://ftp.rs.internic.net/domain/named.root`)
- ➔ Ces serveurs connaissent les serveurs DNS capables de donner des adresses pour un TLD donné .

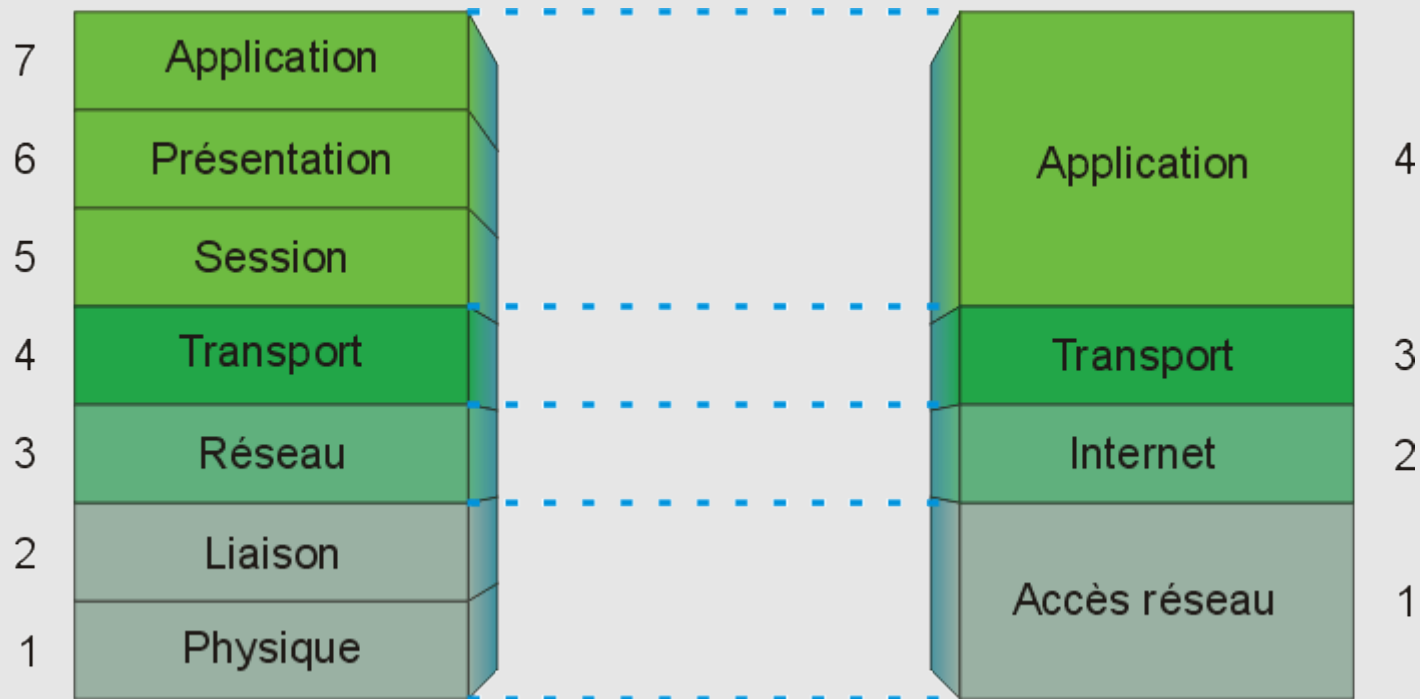
Le DNS - mécanisme



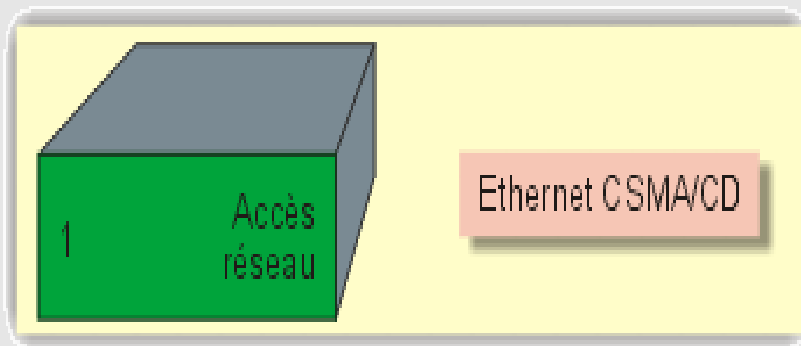
Modèles Réseau

Modèle OSI

Modèle DOD (TCP/IP)

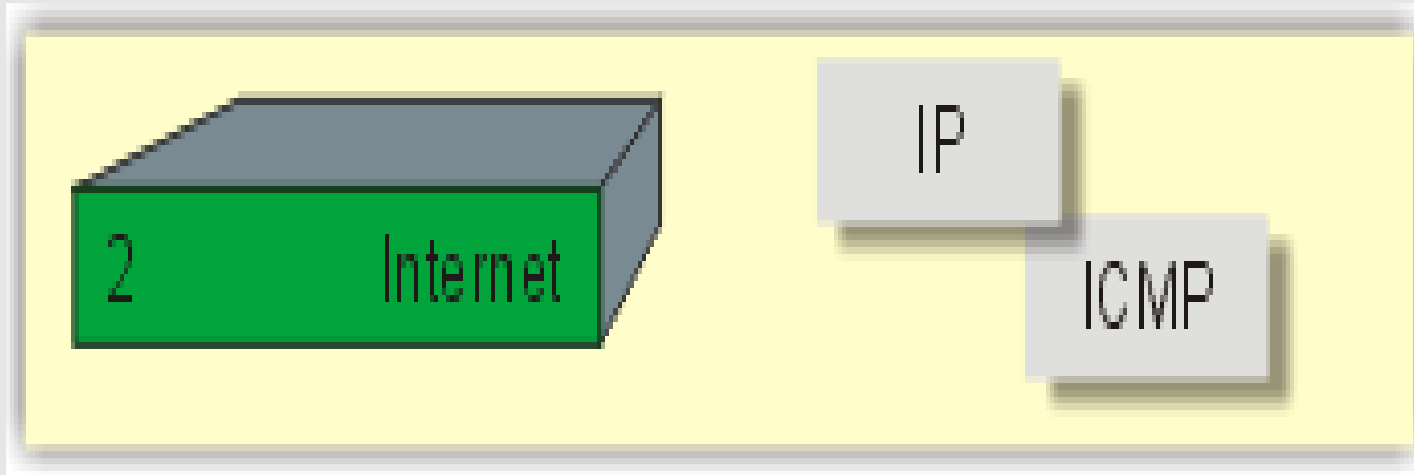


Réseau (*bas niveau*)



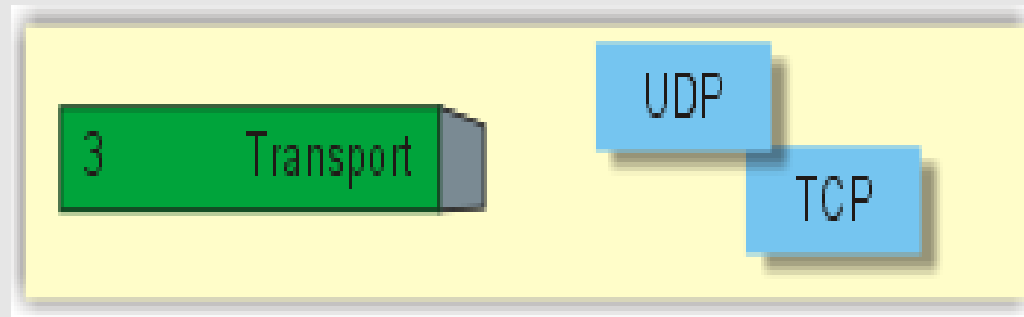
- Protocole bas niveau
- Gère accès au médium
- Détecte collisions
- Achemine messages en utilisant des adresses MAC

Réseau (haut niveau)



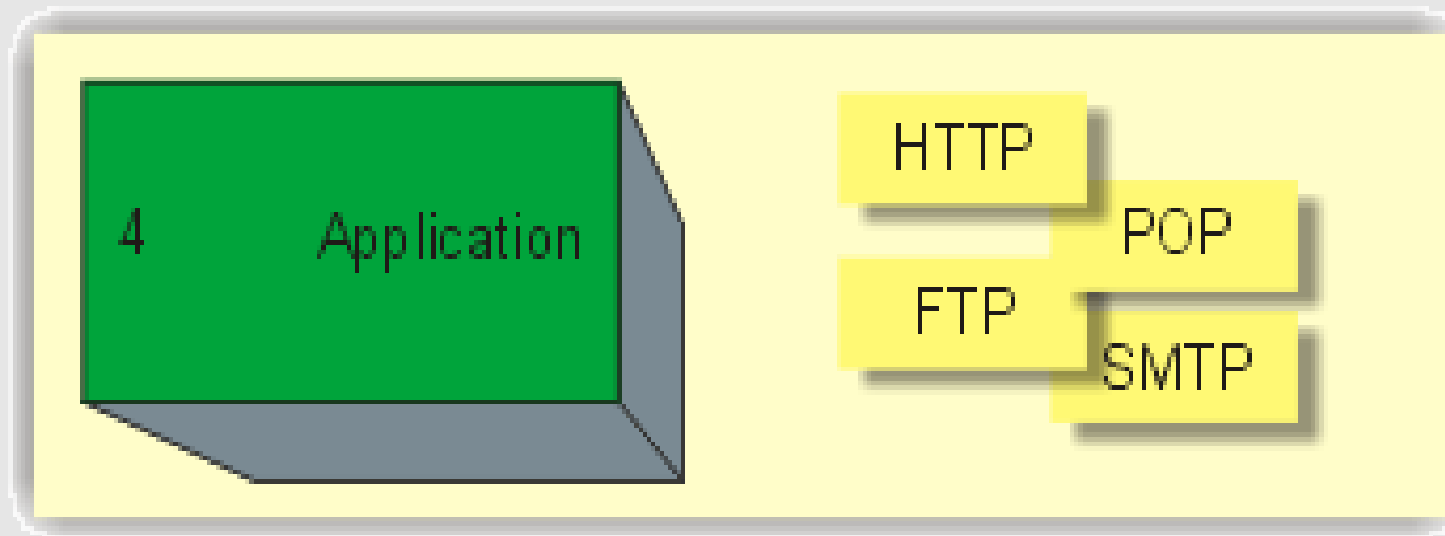
- Protocole haut niveau du réseau
- Permet routage entre réseaux
- Utilisation de l'adressage IP
- ICMP : gestion des erreurs
(signalisation, trace)

Transport données



- Protocoles orientés transport de données
- Synonyme de fiabilité des données
- TCP : mode connecté (ACK/trame)
- UDP : mode non connecté

Niveau application



- Protocoles variés et de haut niveau
- Modélise dialogue client/serveur
- HTTP, FTP, SMTP, POP sont quelques uns des innombrables protocoles définis

Protocole HTTP (Web)

```
GET http://www.free.fr HTTP/1.0
Accept: text/html
UserAgent : Netscape/7.0 (MacOS/X)
```

```
HTTP/1.1 200 OK
Date: Wed, 05 Feb 2003 10:41:17 GMT
Server: Apache/1.3.20 (Unix) Debian/GNU
Last-Modified: Wed, 05 Feb 2003 10:40:01 GMT
Accept-Ranges: bytes
Content-Length: 35637
Connection: close
Content-Type: text/html
```

```
<html>
<head><title>FREE - ACCUEIL</title>
```

Protocole SMTP (Mail)

```
Mail from:<genaud@nerim.net>
```

```
250 OK
```

```
rcpt to:<tom@free.fr>
```

```
250 OK
```

```
DATA
```

```
354 End data with
```

```
<CR><LF>
```

```
Ceci est un essai.
```

```
.
```

```
250 OK
```

```
QUIT
```

```
221 Bye
```

Protocole FTP (Transfert fichiers)

```
login : genaud
```

```
331 Password required for genaud
```

```
password : sandy
```

```
230 User genaud logged in.
```

```
ftp>dir
```

```
drwx-----  9231   4096 Apr 15  2002 archive.zip
```

```
ftp>get archive.zip
```

```
226 Transfer complete.
```

```
ftp>quit
```

```
221 Goodbye.
```

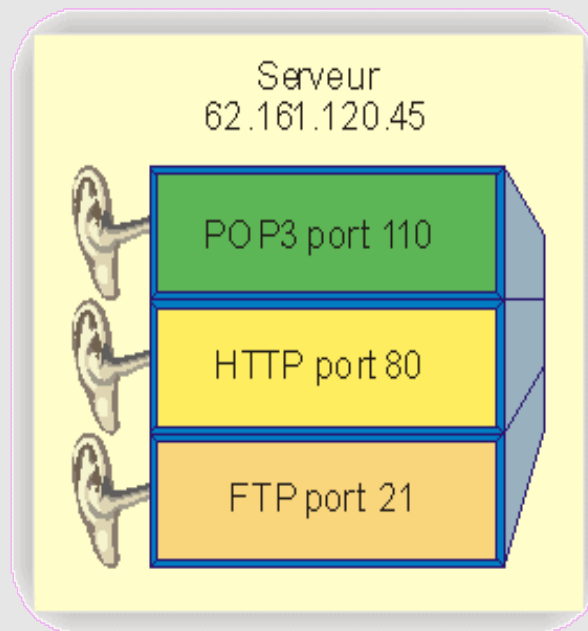
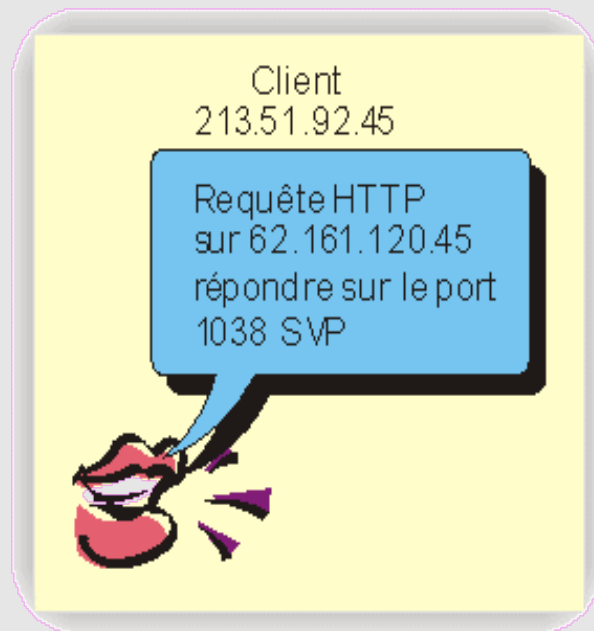
Serveurs, services

- ➔ Ambiguïté du mot serveur. Désigne:
 - Un matériel
 - Une fonctionnalité (service)
- ➔ Un serveur peut abriter plusieurs services
 - Un service de mail (SMTP)
 - Un service de transfert de mail (POP3)
 - Un service web (http)

Ports et sockets

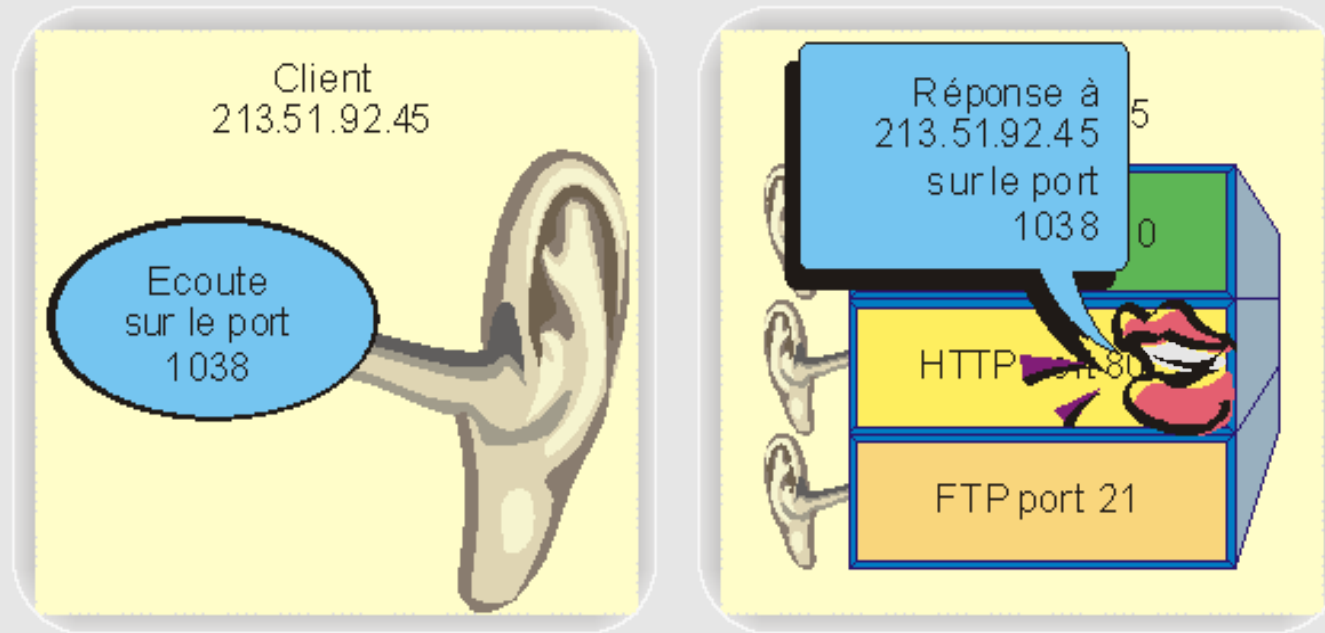
Comment s'adresser à un service particulier sur une même machine ?

Le système d'exploitation d'une machine gère des *ports*



Port + IP = socket

Ports et sockets



Remarques

- Un client peut dialoguer avec plusieurs services en même temps
- Les services doivent utiliser des ports conventionnels (IANA)

Protocole HTTP

Requête :

```
<Commande> <URL> <version><crLf>
<entete><crLf>
....
<entete><crLf><crLf>
```

```
<Commande> =
GET,
POST,
PUT,
DELETE
```

Réponse :

```
<version><code><explication>
<entete>
....
<entete>
```

```
<entete> =
Accept, Accept_Charset,
Content-Language,
Content-Length,
Referer, User-Agent, ...
```

POP (Gestion mail)

Session POP 3

```
USER genaud
PASS sandy
LIST
TOP 1 0
RETR 1
DELE 1
RSET
QUIT
```

Utilisateur et mot de passe (en clair !)*

- Liste des messages reçus
- Entête du premier message
- Retirer tout le premier message
- Supprimer ce message
- Oops ! Je change d'avis (restaure)
- Quitte. Les opérations ne sont enregistrées qu'à ce moment.

* sauf si APOP supporté par serveur

Numéros de ports : conventions

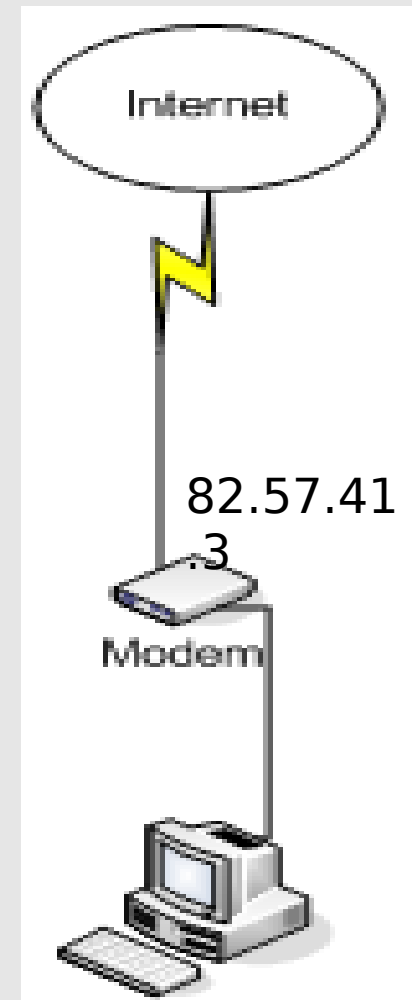
<http://www.iana.org/assignments/port-numbers>

Service	port
---------	------

ftp	21
ssh	22
telnet	23
smtp	25
http	80
pop3	110
imap	143

Configuration typique modem

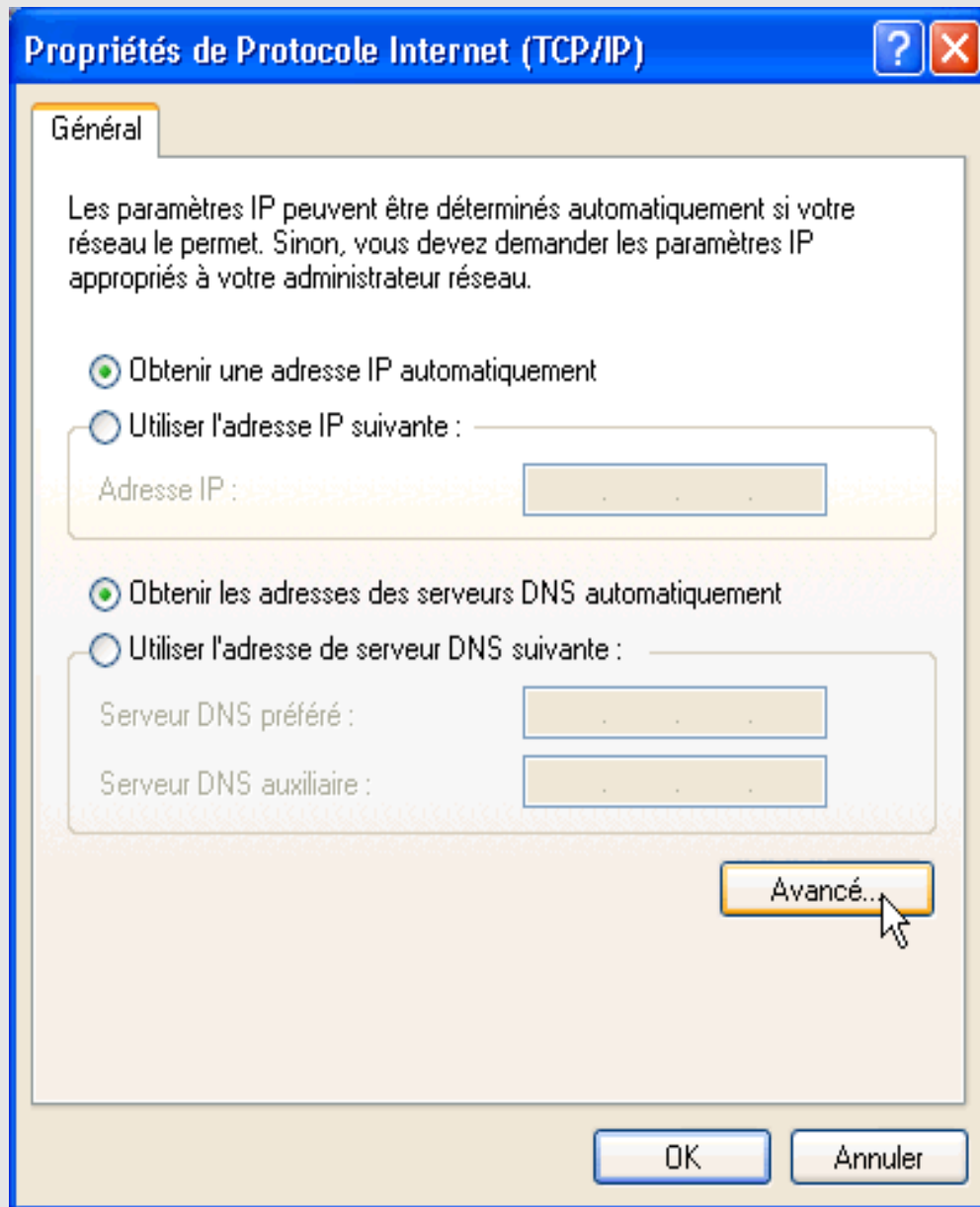
- ➔ Modem ADSL ou câble
- ➔ Le modem a une IP publique (dynamique ou fixe)
- ➔ 1 (seul) ordinateur est connecté au modem par câble ...
 - USB
 - Ethernet (pppoe)



Protocole DHCP

- ➔ Utilisé pour l'attribution d'adresses IP (IP dynamiques)
- ➔ Simplifie la gestion des configurations
- ➔ Principe :
 - un client diffuse un paquet DHCPDISCOVER ,
 - Le serveur DHCP diffuse en retour un paquet DHCPOFFER contenant une configuration valable pour une durée limitée (un bail).
 - Un client peut demander le renouvellement de son bail (DHCPREQUEST) ou l'abandonner (DHCPRELEASE).
- ➔ Protocole décrit par RFC 2131.

DHCP - Windows

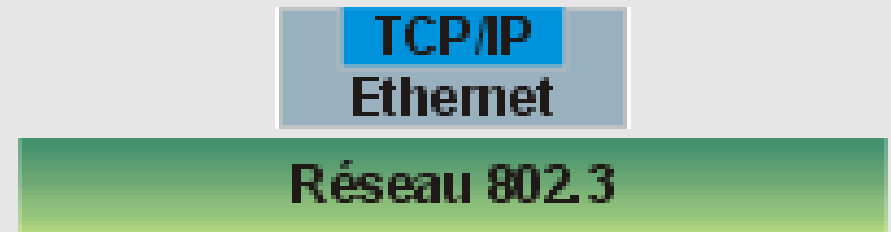


Vocabulaire Windows:

- Obtenir IP automatiquement = IP dynamique (DHCP)
- Configuration manuelle : IP statique

Protocole PPP

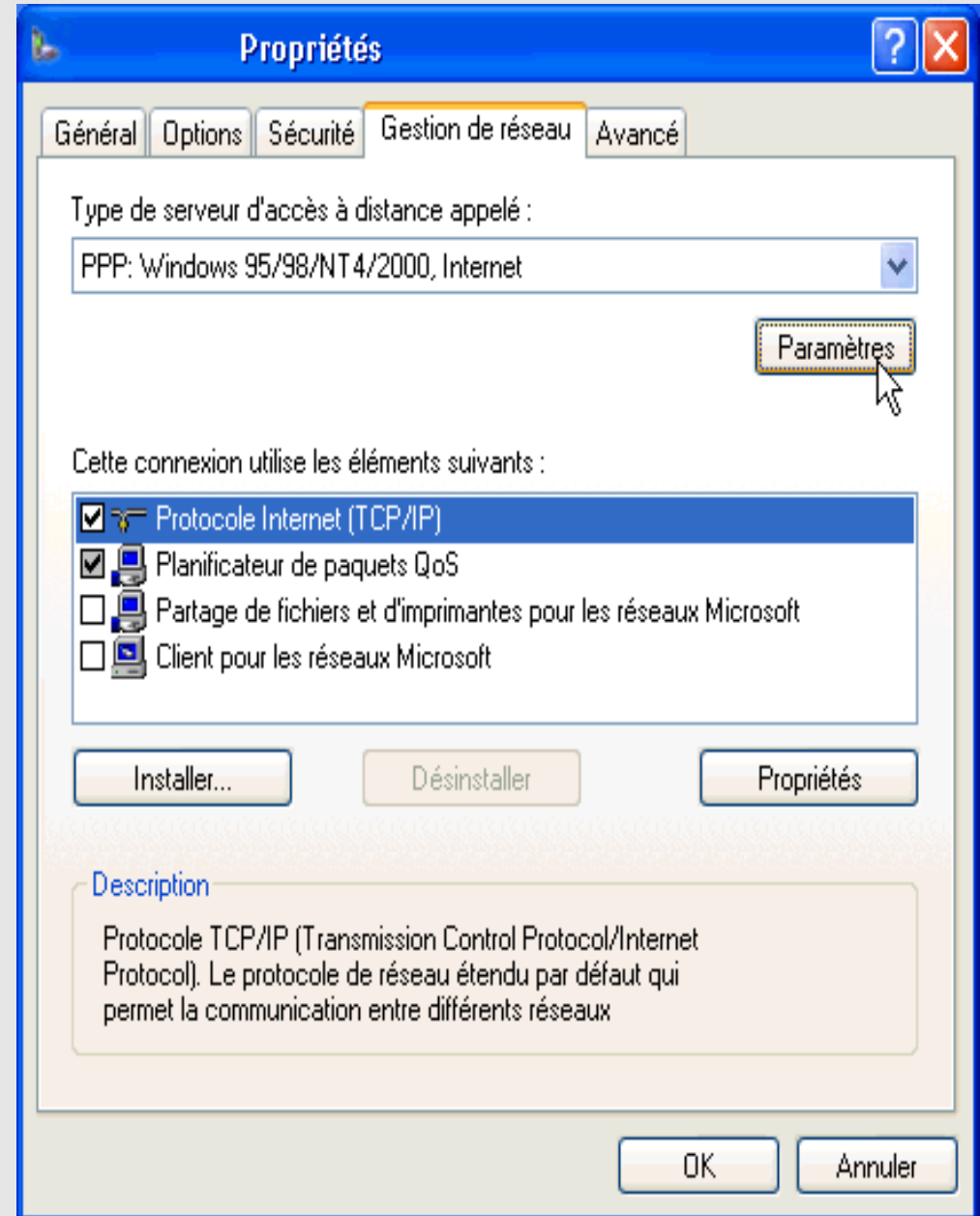
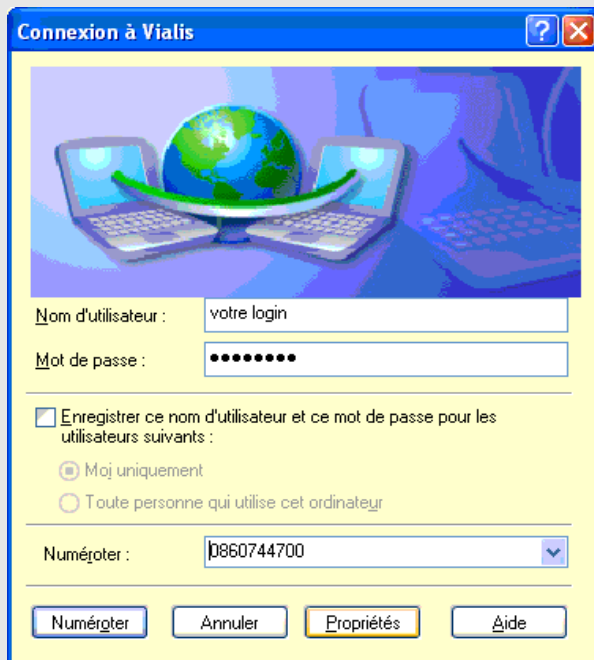
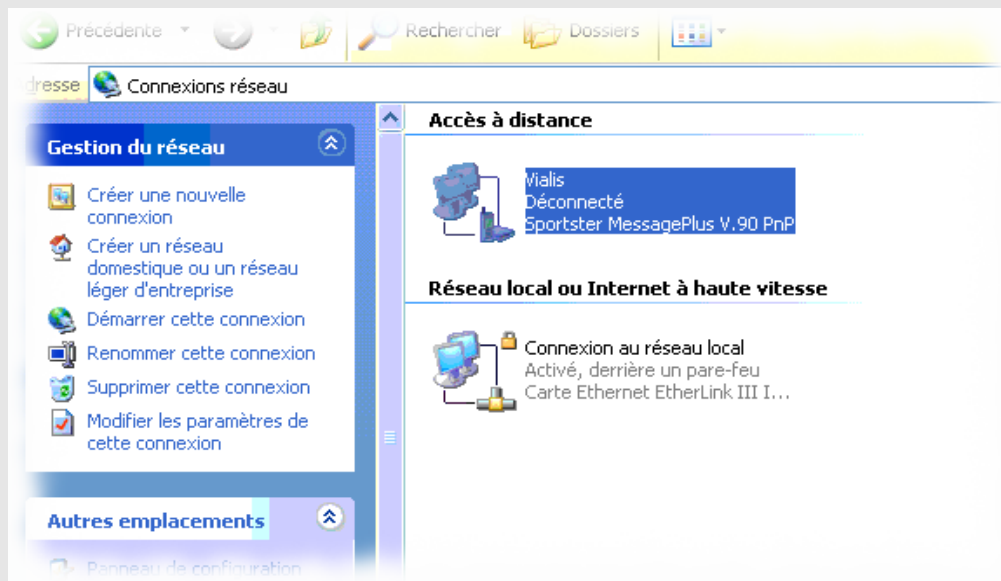
- ➔ PPP a pour objectif d'établir et connexion point à point.
- ➔ Ensemble de 3 protocoles:
 - Protocole d'encapsulation de datagrammes
 - Protocole de contrôle de liaison
 - Protocole de contrôle de réseau
- ➔ Utilisation typique: liaison modem <-> carte réseau PC



Relations entre un réseau ethernet (en haut) et un réseau sur liaison série (bas).

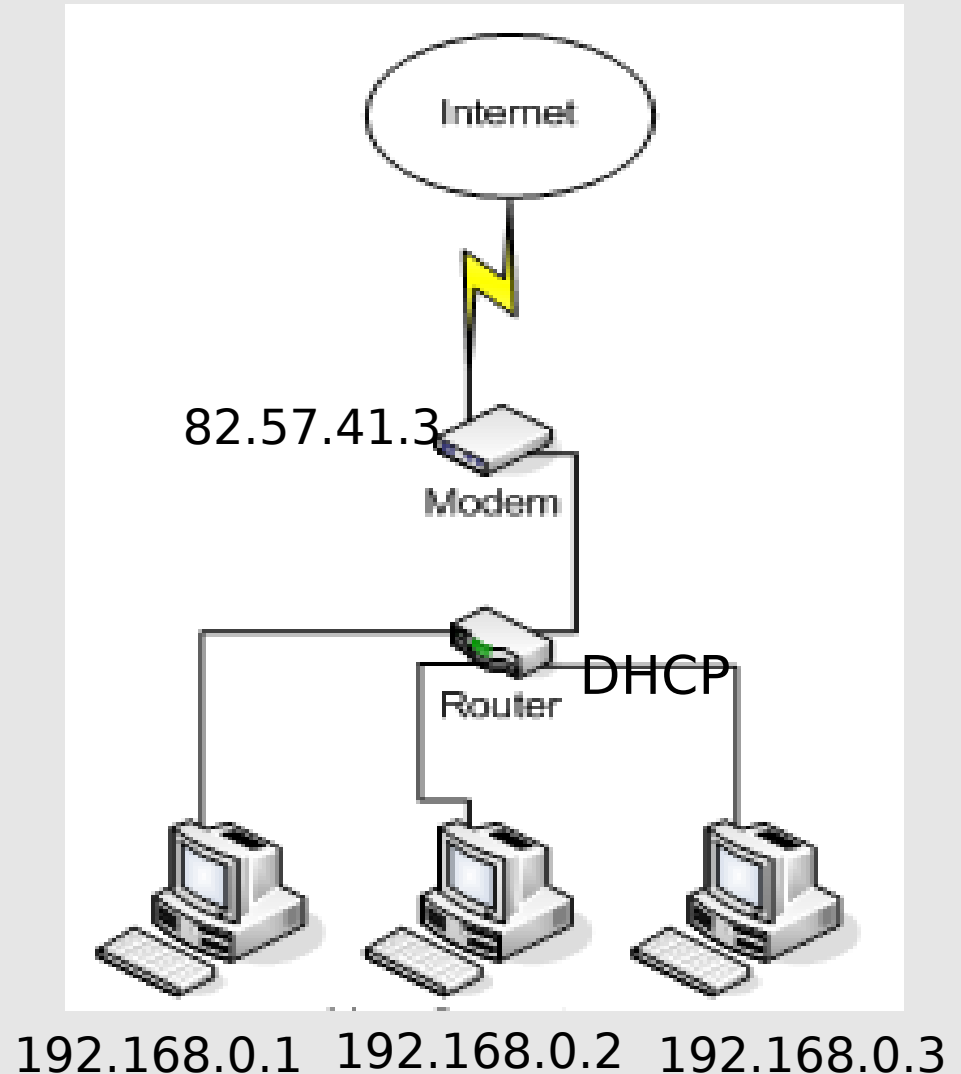


PPP avec Windows



Configuration typique modem+routeur

- ➔ Modem + routeur (e.g. Routeur WIFI)
- ➔ Le modem a une IP publique (dynamique ou fixe)
- ➔ Plusieurs ordinateurs ont des adresses **privées** (dynamiques ou fixes).
- ➔ Le routeur doit faire la traduction d'adresses (NAT).



Routeur

- ➔ Un modem-routeur peut être paramétré pour router les paquets arrivant sur l'IP publique vers une des adresses privées.

Exemple de paramétrage d'une freebox en mode routeur.

Routeur - Mozilla Firefox

Fichier Edition Affichage Aller à Marque-pages Outils Aide

Précédente Suivante Actualiser Arrêter Accueil OK connexion a distan

P3: Documents Routeur

Freebox Interface de gestion

MODE ROUTEUR

S'abonner

- Freebox
- Free 50 heures
- Accès gratuit

Freebox

- WiFi - Routeur
- Téléphonie
- Télévision
- Plateforme multimédia

Espace Abonnés

- Identifiez-vous

Plus d'infos

- Nos offres
- Le dégroupage

Assistance

- Documentations
- Faq

Vous souhaitez activer ce service: Activation ☒ Désactivation ☐

IP freebox 192.168.

DHCP activé Oui ☒ Non ☐

Debut DHCP 192.168.

Fin DHCP 192.168.

Ip DMZ 192.168.

Ip du Freeplayer 192.168.

Réponse au ping ☒

Proxy WOL (Wake On Lan) activé ☐

Redirections de ports:

Port	Protocole	Destination	Port
6013	tcp	192.168. 0 1	6013
9701	tcp	192.168. 0 1	9701
9701	udp	192.168. 0 1	9701
9700	tcp	192.168. 0 1	9700
9700	udp	192.168. 0 1	9700

Sécurité : sources d'attaques

- ➔ Fichiers nocifs transmis par mail (binaire, scripts, macros, ...) adoptant souvent un comportement de virus.
- ➔ Attaque de type *déni de service* (DoS).
- ➔ Attaque contre des vulnérabilités de services (services web, ftp, ... ou tout logiciel serveur).

Sécurité : virus

➔ Comment cela arrive :

- Profite de l'étourderie ou ignorance de l'utilisateur
- Profite des systèmes faibles : ceux où l'utilisateur peut modifier les fichiers systèmes

➔ Objectifs :

- Provoquer des dysfonctionnements ou perte de temps
- Survivre en se propageant (virus)

Sécurité : virus

➞ Effets possibles :

- S' « installe » dans les zones systèmes et peut ouvrir des « portes dérobées »
- Peut provoquer des dégâts dans les fichiers locaux
- Peut rendre la machine agressive

➞ Comment se protéger :

- Faire les mises-à-jour de sécurité
- Mettre à jour les anti-virus
- Avoir une politique d'administration

Sécurité : vulnérabilité

➔ Comment cela arrive :

- Un service logiciel ou le S.E. présente une faille (bug).
- Des programmes d'attaques interrogent systématiquement les ordinateurs connectés à la recherche de cette faille.

➔ Objectifs :

- Prendre le contrôle de la machine.
- Disposer d'un espace disque et d'une nouvelle « tête de pont ».

➔ Effets possibles :

- Trafic réseau démesuré, espace disque confisqué.
- Complicité involontaire dans de nouvelles attaques.

Sécurité : vulnérabilité

➔ Comment se protéger :

- Procéder aux mises-à-jour de sécurité.
- Installer logiciel un pare-feu (firewall) individuel.
- Utiliser un système de surveillance des modifications.
- Installer une machine pare-feu sur le réseau.