02 - Principes généraux (suite)

Gaétan Richard
gaetan.richard@info.unicaen.fr

DNR2I - M1

1. TCP/UDP

Au service de tous

Présentation :

- Assure le transfert d'information ;
- pour de nombreux protocoles.

Problème : On ne peut pas avoir une donnée *type* exhaustive.

Solution : On utilise la notion de port.

Port

Le port est un entier sur 16bits correspondant à un accès (virtuel) séparé sur une machine.

- Un programme peut choisir d'écouter sur un port donné d'une machine et recevra alors le trafic à destination de ce port.
- Un seul programme peut écouter par port

Zoologie des ports

- Il y a $65\,536$ ports ;
- les 1024 premiers sont réservés au super utilisateur (*root*) ;
- De nombreux ports sont associés avec des protocoles / programmes (voir la standardisation de l'*IANA*).

Le ports peuvent être :

- ouvert (une application écoute) ;
- fermé (personne n'écoute) ;
- filtré (quelqu'un bloque la communication).

nmap

Le logiciel **nmap** permet de faire une analyse des états des ports sur une machine distante. Il permet également de reconnaître un certain nombre de protocoles utilisés dans la couche application.

Attention : **nmap** est un logiciel intrusif et peut être considéré comme une tentative d'attaque. Cet outils sert principalement à vérifier les ports ouverts sur une de vos machine.

Quelques ports courants

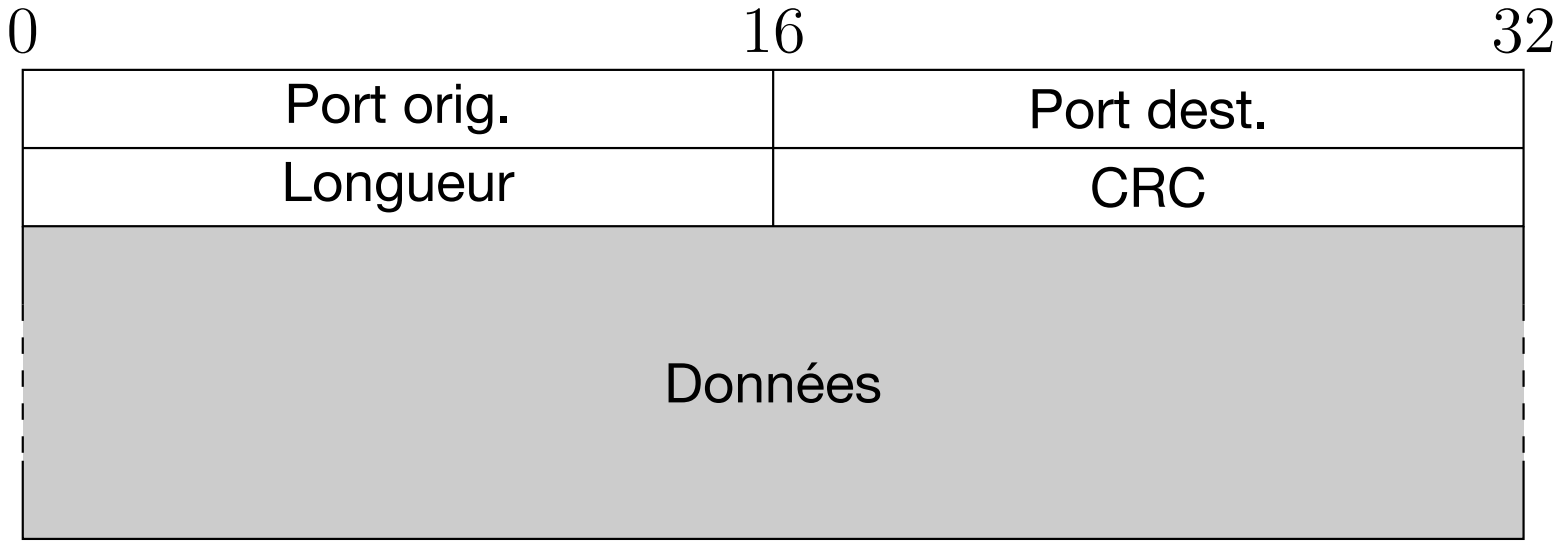
21	ftp
22	ssh
25	SMTP
53	DNS
80	http
110	POP3
143	IMAP
443	https
465	SMTPS
993	IMAPS
995	POPS

UDP : Présentation

UDP : (User Datagram Protocol)

- Assure l'intégrité des données reçues ;
- Assure la connexion avec la couche application (port).

Datagramme



TCP : Présentation

TCP : (Transmission Control Protocol)

- Assure l'intégrité des données reçues ;
- assure la connexion avec la couche application (port) ;
- assure la transfert (réception) des données ;
- assure l'ordre des données ;
- permet l'établissement (et la fermeture) d'une connexion.

Principe de l'acquittement

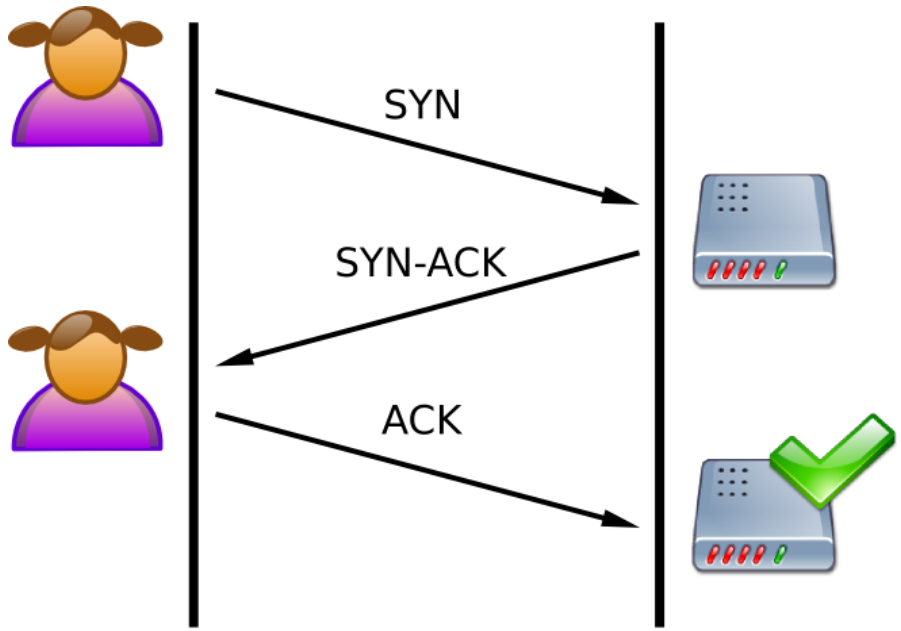
- L'émetteur envoie un paquet avec un identifiant ;
- le récepteur envoie un accusé de réception ACK pour ce message.

Cas de TCP :

- Les messages sont numérotés de façon consécutive ;
- Si l'accusé de réception n'est pas reçu après un temps t, essayer automatiquement à nouveau d'envoyer le message ;
- Après un certain nombre de tentatives infructueuses, considérer que la transmission est un échec.

Établissement de la connexion

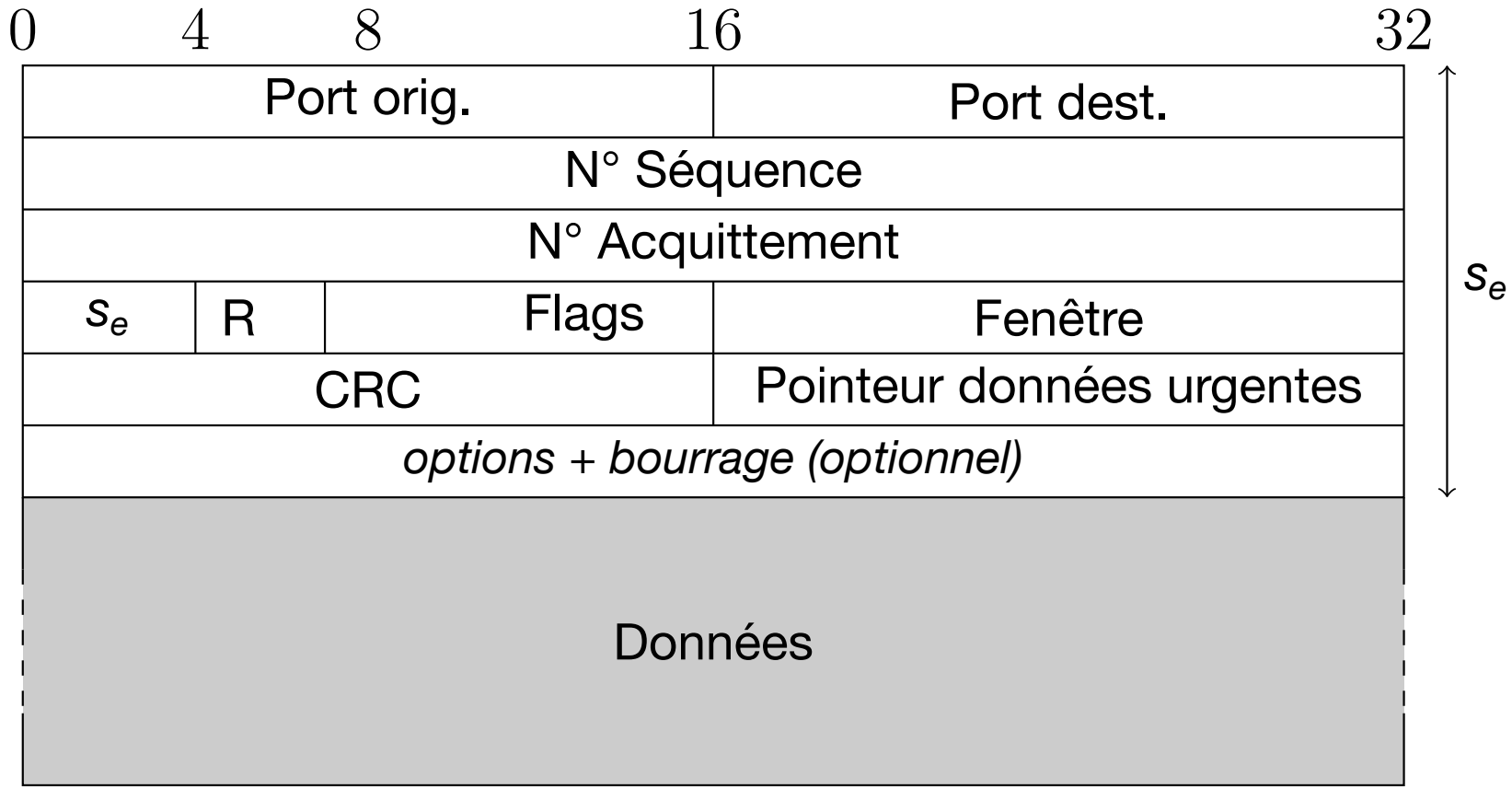
Pour établir, on envoie un signal SYN. Le récepteur envoie également un signal SYN avec un ACK de notre signal. Pour finir, on émet un ACK du signal SYN reçu.



Clôture de la connexion

La clôture de la connexion se passe de la même façon que l'ouverture, on utilise juste le flag `FIN`.

Datagramme


0
4
8
16
32
Port orig.
Port dest.
N° Séquence
N° Acquittement
s_e
R
Flags
Fenêtre
CRC
Pointeur données urgentes
options + bourrage (optionnel)
Données
s_e

Fenêtre glissante

Principe : Pour accélérer le transfert, l'émetteur n'attend pas la réception de l'acquittement du paquet précédent pour transmettre le suivant. Il en transmet un certain nombre (*fenêtre*).
La taille de cette fenêtre est évolutive : elle augmente si le transfert se passe bien et diminue s'il y a des erreurs de transmissions.

2. Protocoles applicatifs

La couche application

- Couche la plus haute ;
- Grande variété d'applications ;
- Spécifique à chaque application.

DNS : Présentation

Objectif :

- Associe une adresse IP à un nom de machine ;
- Et réciproquement.

Fonctionnement :

Système de questions / réponses.

Une adresse

Exemple :

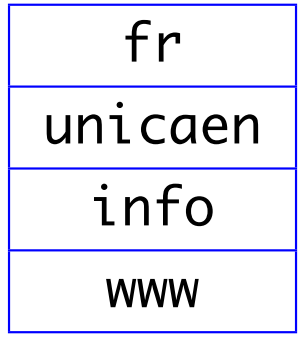
`www.info.unicaen.fr`

Une adresse

Exemple :

`www.info.unicaen.fr`

Hiérarchie :



Serveur DNS

Les serveurs DNS :

- Responsable d'une zone ;
- Travaille en collaboration avec les autres serveurs DNS (délégation) ;
- Quasi toujours dupliqué (serveur secondaire, …)
- Utilise le cache.

Fonctionnement

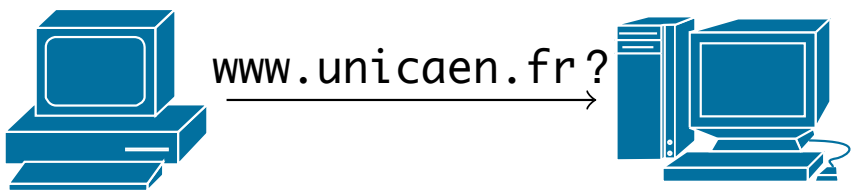
dns

dns racine

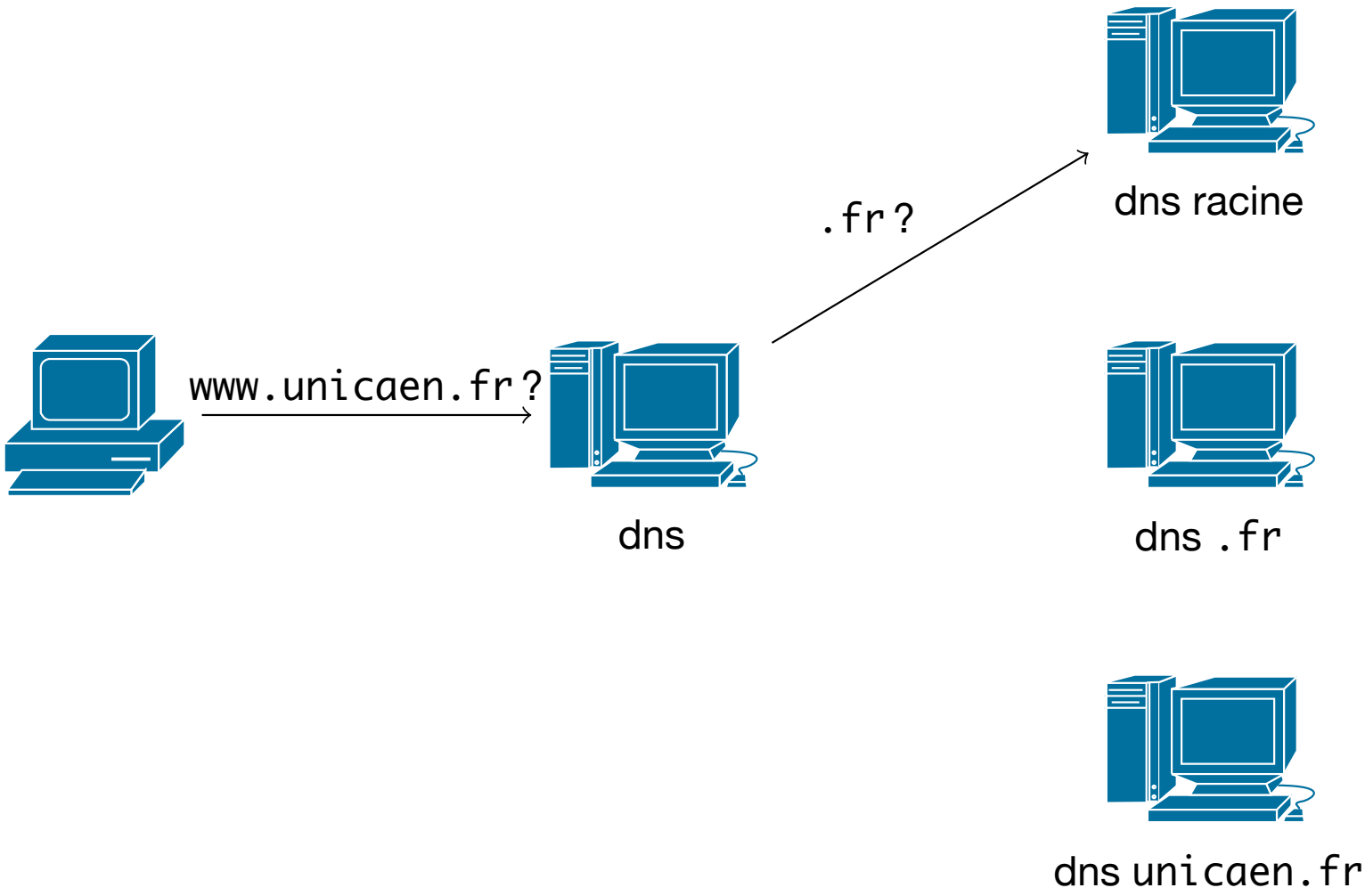
dns `.fr`

dns `unicaen.fr`

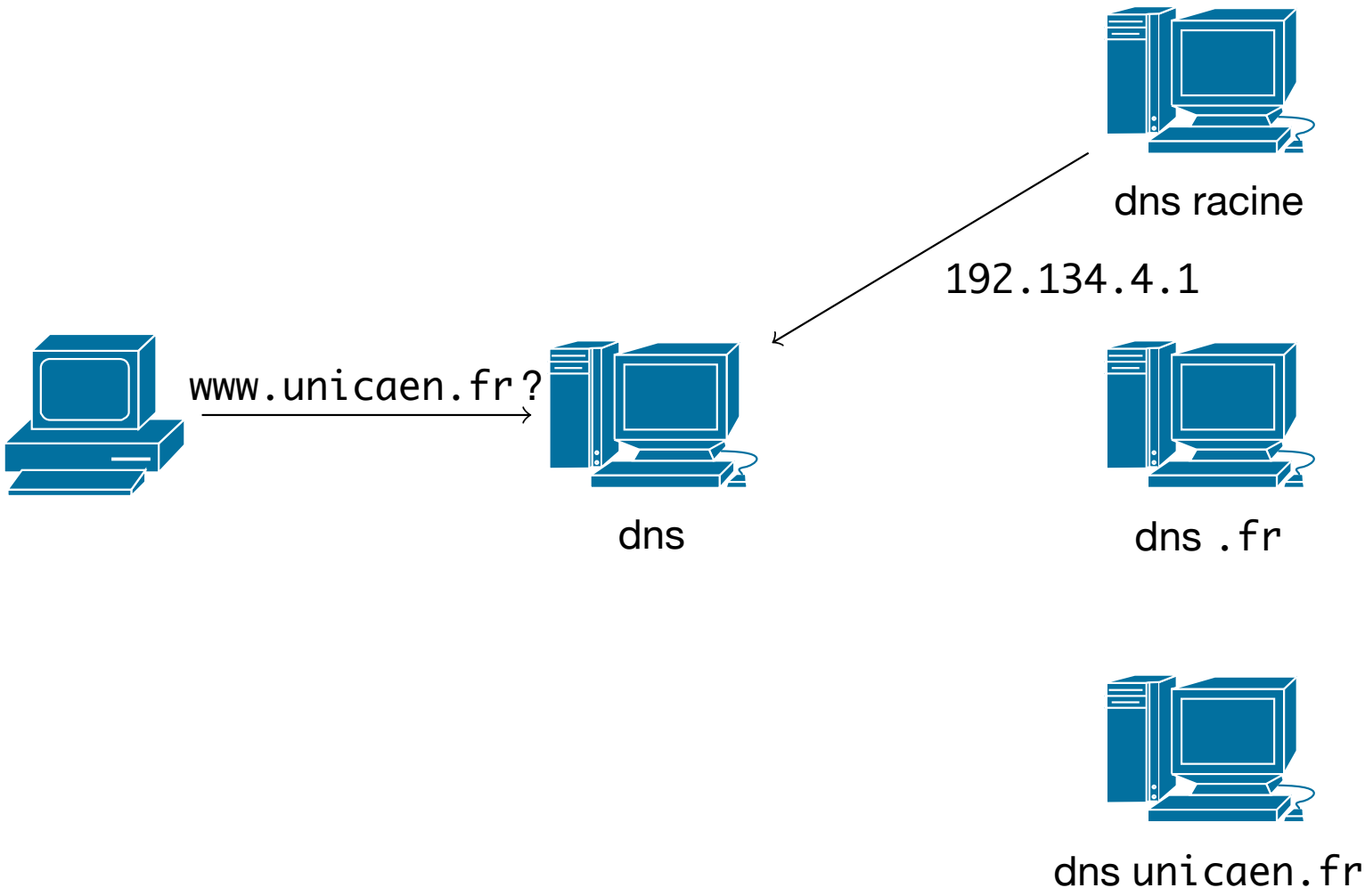
Fonctionnement



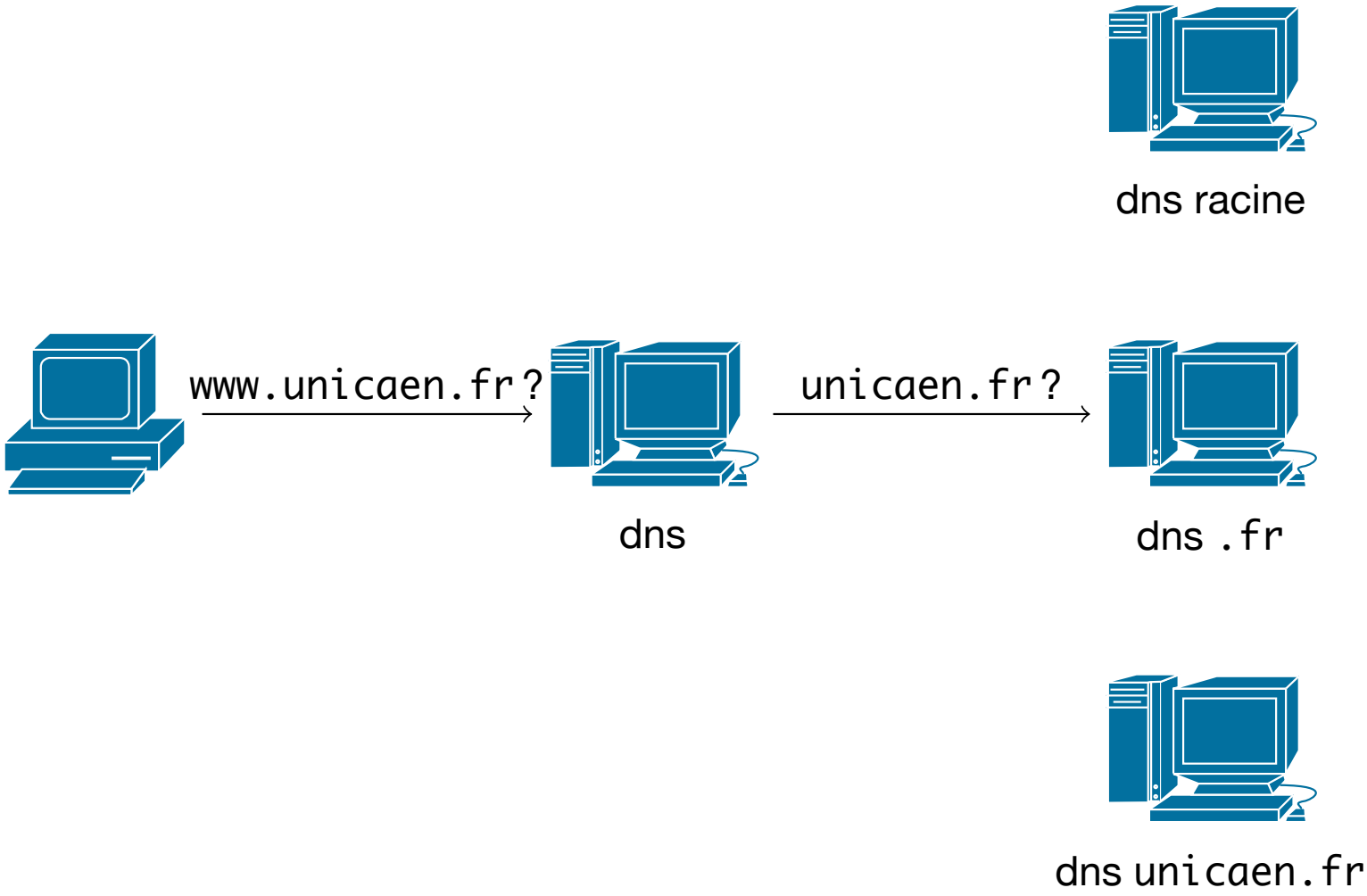
Fonctionnement



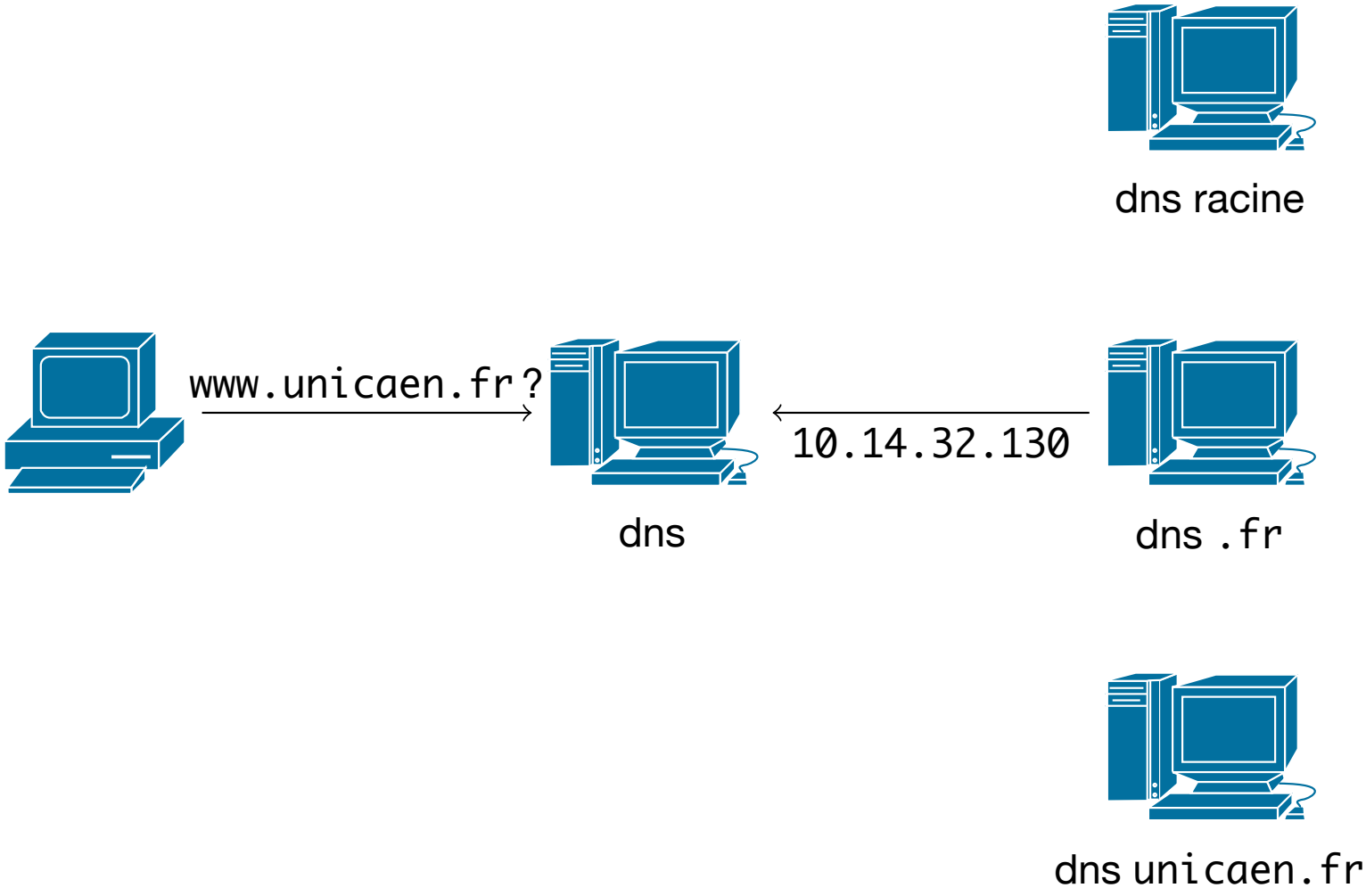
Fonctionnement



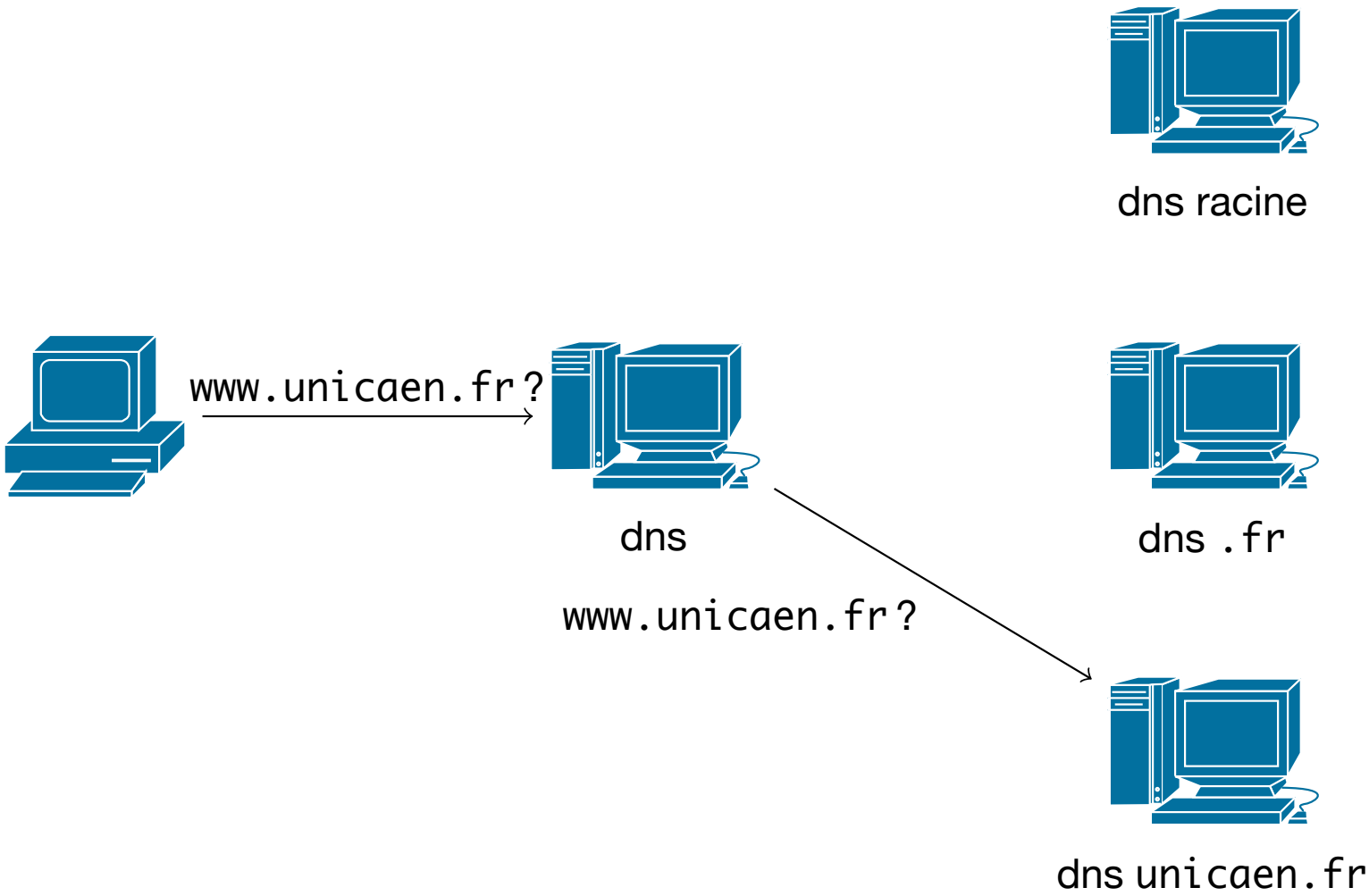
Fonctionnement



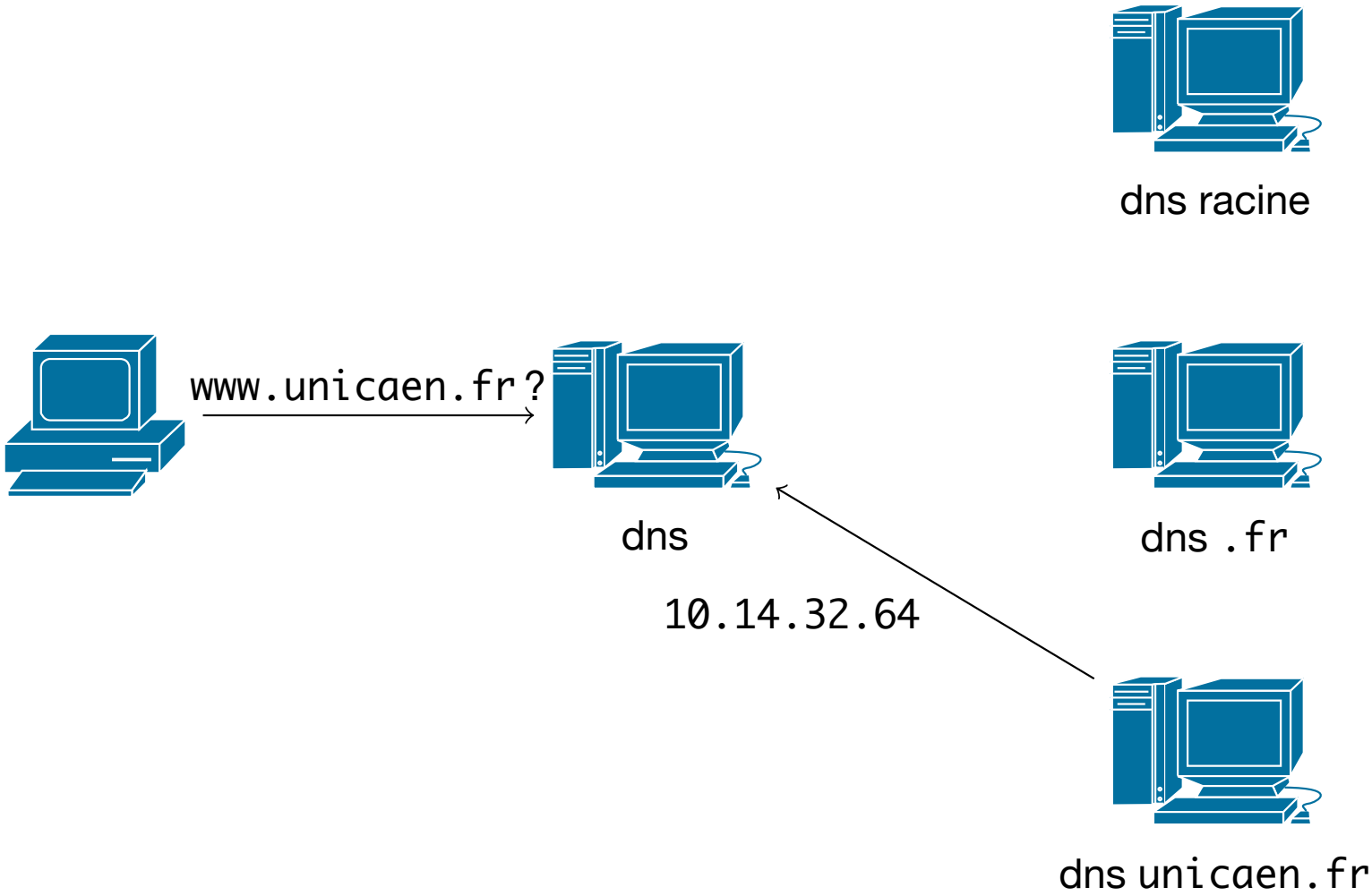
Fonctionnement



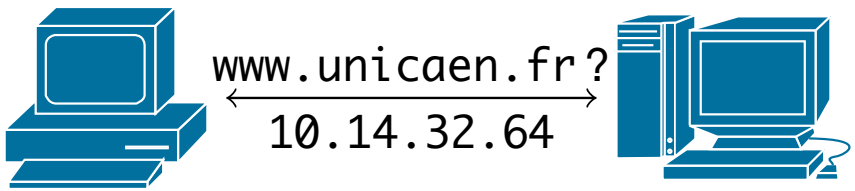
Fonctionnement



Fonctionnement



Fonctionnement

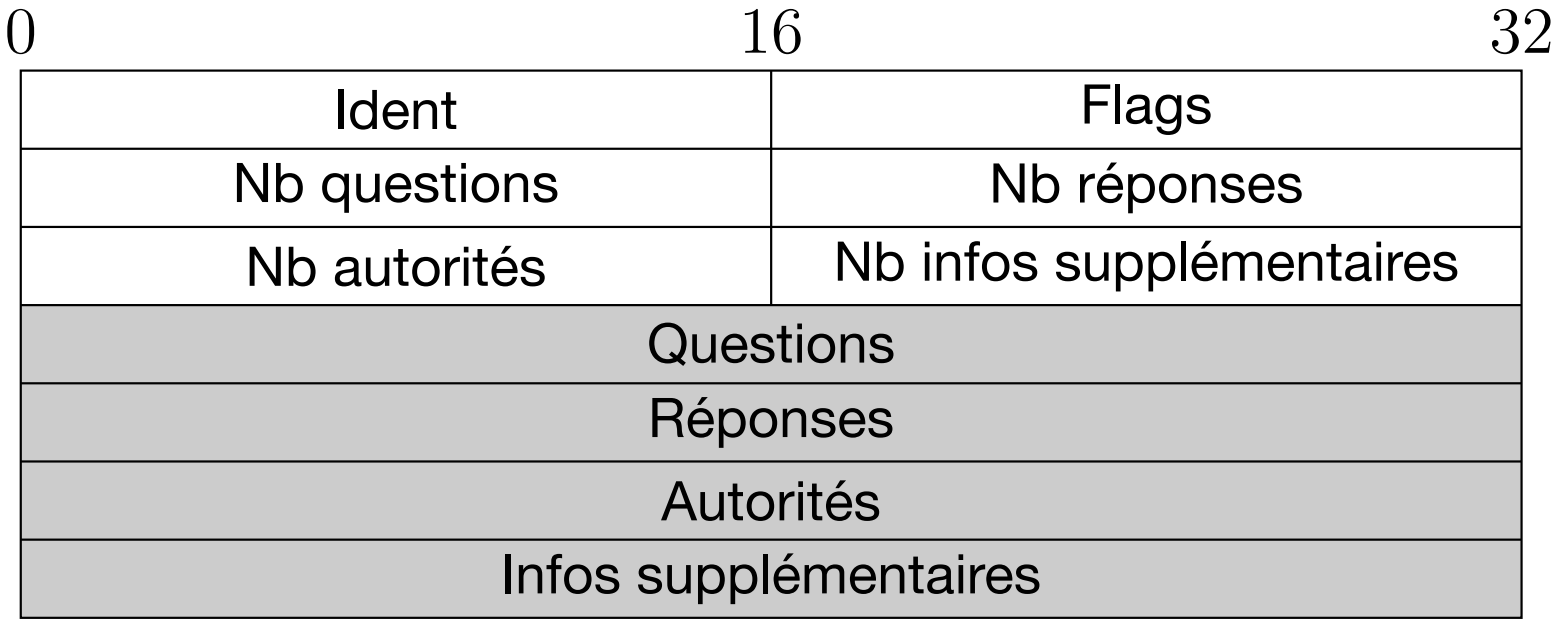


Mise en place

Utilisation :

- Utilise le port 53 ;
- Encapsulé dans de l'UDP.

Datagramme :



La résolution inverse

Objectif :

Adresse IP $\rightarrow$ nom.

Principe :

On demande l'adresse IP en renversant les champs et en ajoutant le bon suffixe.

Exemple :

- `216.239.59.104` $\rightarrow$ `104.59.239.216.in-addr.arpa`
- `2001 :4860 :a005 ::68` $\rightarrow$ `8.6.0.<...>.0.0.5.0.0.a.0.6.8.4.1.0.0.2.ip6.arpa`

Les différents champs possibles

- `SOA` : Infos sur la zone
- `A` : adresse ipv4
- `AAAA` : adresse ipv6
- `CNAME` : alias
- `PTR` : pointer (résolution inverse)
- `MX` : mailer.

Utilisation

Programme :

la commande **host** permet d'effectuer une requête DNS.

Exemple :

```
$ host www.info.unicaen.Fr
www.info.unicaen.Fr is an alias for panoramix.info.unicaen.Fr.
panoramix.info.unicaen.Fr has address 193.55.128.20
panoramix.info.unicaen.Fr has IPv6 address 2001 :660 :7101 ::7
```

Mail

Le mail

- Élément devenu critique et indispensable ;
- Stocké sur un serveur ;
- Envoi et réception ;
- Ports 25, 465 (envoi) ;
- Ports 110, 995, 143, 993 (lecture) ;
- Version sécurisé ou en clair.

Fonctionnement :

- Envoi : serveurs SMTP ;
- Récupération par POP / IMAP.

Suivre un mel

```
Return-Path : <wlaplace@users.sourceforge.net>
Delivered-To : Gaetan.Richard@lif.univ-mrs.fr
Received : from localhost (localhost.localdomain [127.0.0.1])
by platine.lidil.univ-mrs.fr (Postfix) with ESMTP id 06E582BC0068
for <Gaetan.Richard@lif.univ-mrs.fr>; Tue, 10 Nov 2009 22 :47 :49 +0100 (CET)
X-Virus-Scanned : amavisd-new at lidil.univ-mrs.fr
Received : from platine.lidil.univ-mrs.fr ([127.0.0.1])
by localhost (platine.lidil.univ-mrs.fr [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id vmp45fV7zN5c for <Gaetan.Richard@lif.univ-mrs.fr>;
Tue, 10 Nov 2009 22 :47 :48 +0100 (CET)
Received : from mso1k193.u-3mrs.fr (mso1k193.u-3mrs.fr [195.221.207.193])
by platine.lidil.univ-mrs.fr (Postfix) with ESMTP id C18C72BC0063
for <Gaetan.Richard@lif.univ-mrs.fr>; Tue, 10 Nov 2009 22 :47 :48 +0100 (CET)
X-IronPort-Anti-Spam-Filtered : true
X-IronPort-Anti-Spam-Result : Apg1ACJu+UqTXkAC/2dsb2JhbAAMgUKKNIRCAYoXDJRtpjCJAIEIgzYE
X-IronPort-AV : E=Sophos;i="4.44,718,1249250400";
   d="scan'208";a="21980327"
Received : from gyptis.univ-provence.fr (HELO gyptis.cmi.univ-mrs.fr) ([147.94.64.2])
  by mso1k206.u-3mrs.fr with ESMTP; 10 Nov 2009 22 :47 :48 +0100
Received : from mso1k193.u-3mrs.fr (mso1k193.u-3mrs.fr [195.221.207.193])
          by gyptis.cmi.univ-mrs.fr (8.13.8+Sun/jtpda-5.4) with ESMTP id nAALlmZl013898
          for <gaetan.richard@cmi.univ-mrs.fr>; Tue, 10 Nov 2009 22 :47 :48 +0100 (MET)
Date : Tue, 10 Nov 2009 22 :47 :48 +0100 (MET)
Message-Id : <200911102147.nAALlmZl013898@gyptis.cmi.univ-mrs.fr>
Received : from mx.sourceforge.net ([216.34.181.68])
  by mso1k206.u-3mrs.fr with ESMTP; 10 Nov 2009 22 :47 :48 +0100
```

Le web

Principe (simplifié) : Un serveur web affiche la page demandée.

Exemple :

```
$ nc www.info.unicaen.fr 80
GET / HTTP/1.1
Host : www.info.unicaen.fr

HTTP/1.1 200 OK
Date : Thu, 25 Nov 2010 05 :54 :36 GMT
Server : Apache/2.2.9 (Debian) DAV/2 SVN/1.5.1 PHP/5.2.6-1+lenny9 with Suhosin-Patch proxy_html/3.0.0 mod_ssl/2.2.9 OpenSS
X-Powered-By : PHP/5.2.6-1+lenny9
Transfer-Encoding : chunked
Content-Type : text/html

1f49
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "DTD/xhtml1-strict.dtd">
<html xmlns="http ://www.w3.org/1999/xhtml" xml :lang="fr" lang="fr">
<head>
...
```

Transfert de fichiers :

- **FTP** ;
- **HTTP** ;
- **SMB** ;
- **SFTP** ;
- …

Autres services :

- **LDAP** (Lightweight Directory Access Protocol) ;
- **NFS** (Network file system) ;
- **RAID** (Redundant array of independant/inexpensive disks)
- **NTP** (Network Time Protocol) ;
- **Kerberos** ;
- …

3. Un exemple complet

Lire un site web