Principes généraux

Gaétan Richard
gaetan.richard@unicaen.fr

M2 E-Secure

1. Introduction

Qu'est ce qu'un réseau ?

Définition :

...

d) INFORMAT. *Réseau informatique*. Interconnexion de un ou plusieurs ordinateurs avec plusieurs terminaux distants par l'intermédiaire des voies de transmission (Mess. Télém. 1979).

...

CNRTL - TLFI

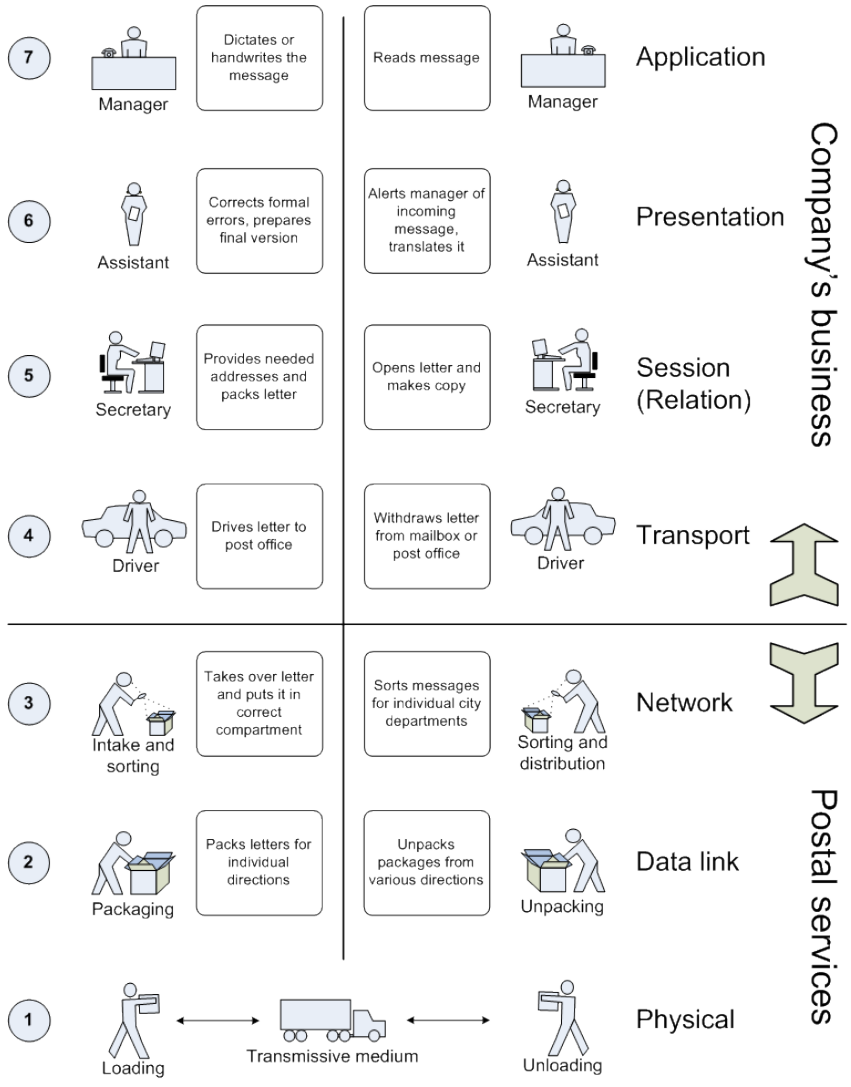
Objectif : Échanger des informations.

Décomposition en couches

Principe :

- On décompose les tâches à effectuer en couches ;
- Chaque couche ne peut parler qu'avec le couche immédiatement inférieure ;
- Les couches de niveau *n* communiquent à l'aide d'un protocole
- On a donc une pile d'encaspulation des protocoles.

Le modèle OSI par l'exemple



RM – OSI and letter communication parallel

`http://commons.wikimedia.org/wiki/File:Rm-osi_parallel.png`

2. Les données

Codage

Méthodes :

- Analogique : avec des grandeurs proportionnelles à la valeur encodée ;
- Numérique : sous forme d'entiers, le plus souvent écrit en binaire.

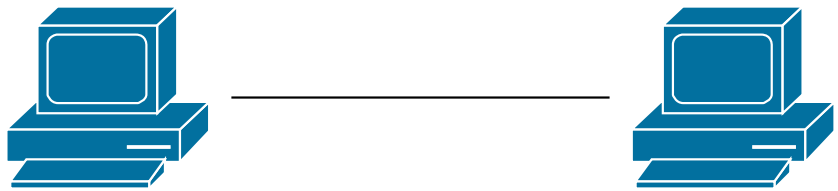
Binaire : écriture en base 2 à l'aide des chiffres 0 et 1.
Exemples : 00101010110, 10111110101, ...

3. Interface réseau

Couche physique

Principe : Envoi et réception de bits entre deux machines directement reliées par l'intermédiaire d'un médium.

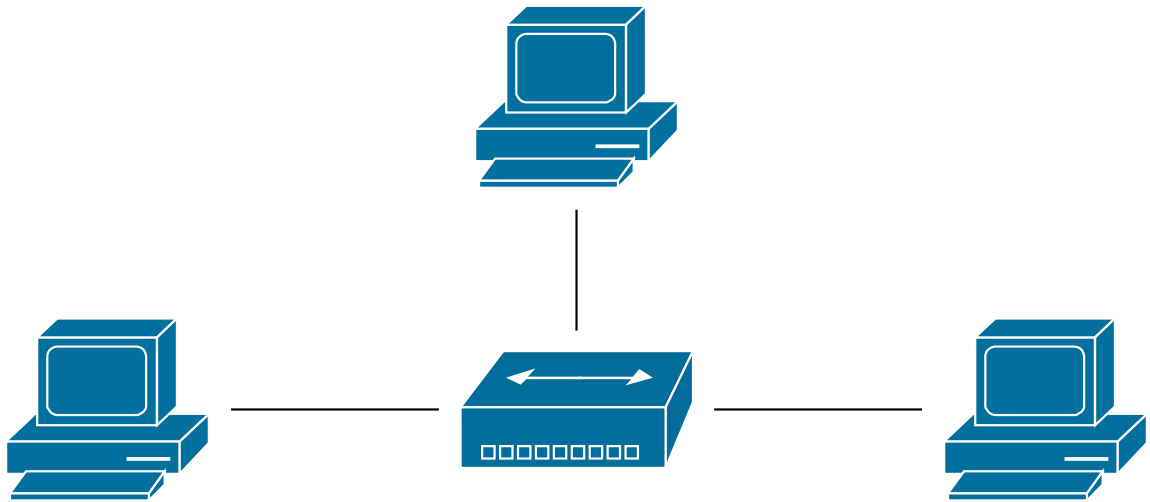
Couche physique



Principe : Transmission d'une suite de bits entre deux machines directement reliées par l'intermédiaire d'un médium en assurant :

- l'absence de perte ;
- l'absence d'erreur ;
- l'absence de duplication.

Connections multiples



- Plusieurs machines sont connectées à un même médium ;
- Toutes les machines reçoivent toutes les communications ;
- Il peut y avoir des problèmes de collisions.

Un peu de technique

Implémentation :

- Utilisation de trames auto-délimité ;
- Écoute quasi-simultanée avec l'écriture afin de detecter les collisions ;
- Utilisation de modulation de fréquance ou d'amplitude pour les signaux analogiques.

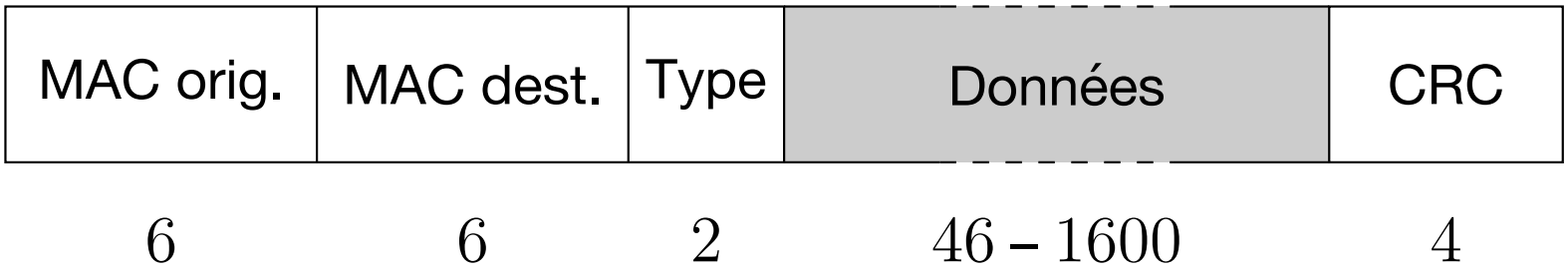
Adresse MAC

Identifiant : Chaque interface d'un machine possède un identifiant *unique* : l'adresse MAC. Cette adresse se compose de 5 blocs de 8 bits (octets) que l'on écrit usuellement en hexadécimal séparé par des `:`.

Ex : `00:26:4a:19:a1:70`

Décomposition : cette adresse se décompose en une portion constructeur et un compteur.

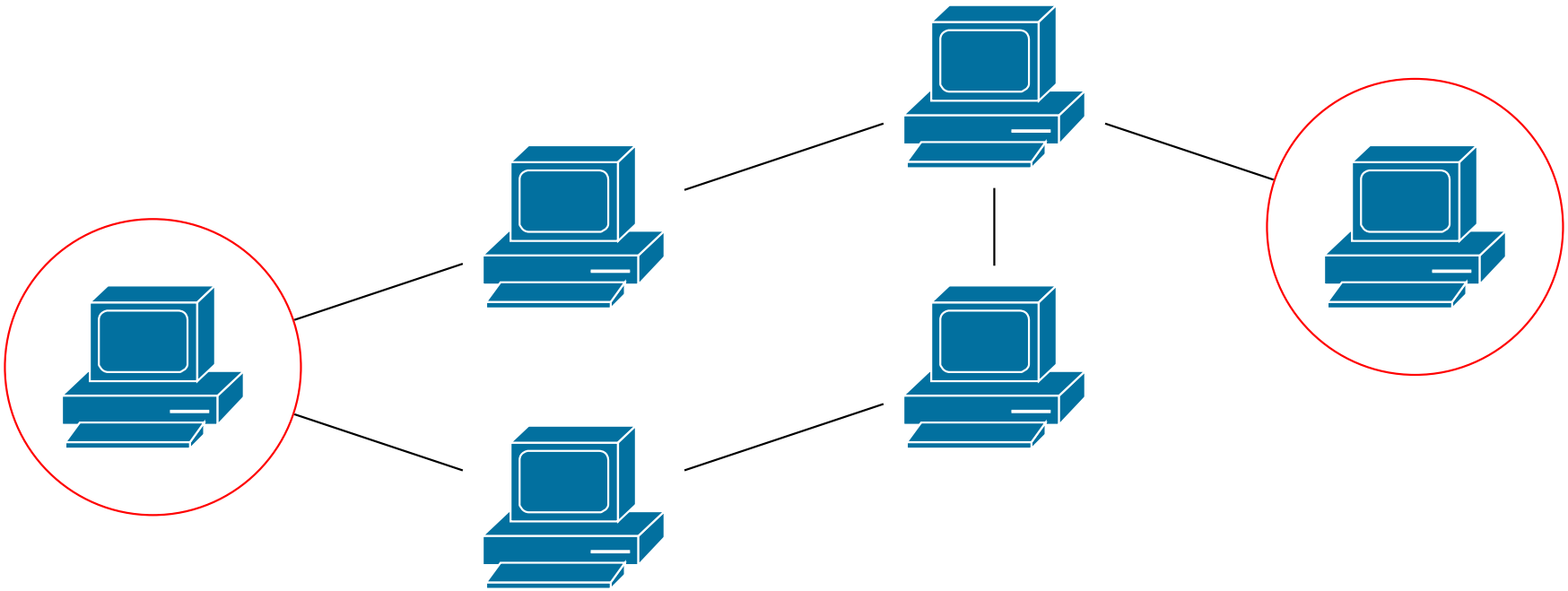
Trame Ethernet



- Les adresses MAC sont uniques ;
- Chaque ordinateur émet quand il a besoin ;
- Il écoute pour savoir s'il y a eu collision ;
- En cas de collision, l'ordinateur attend un temps aléatoire avant de réémettre.

4. Internet

Couche réseau



Principe : Assure l'acheminement des données entre deux machines du réseau à l'aide de relais intermédiaires (les messages peuvent être perdus / dupliqués / changer d'ordre).

Adresse

- Constituée de 4 octets (32 bits) ;
- Représentée sous la forme d'une suite de 4 nombres entre 0 et 255.
- $4\,294\,967\,296$ adresses possibles

Exemples :

- `127.0.0.1`
- `193.55.128.20`
- ...

Sous-réseaux

Pour grouper les adresses ensembles, on utilise la notion de sous-réseau (*netmask*).

10	74	254	1
00001010	01001010	11111110	00000001

Sous-réseaux

Pour grouper les adresses ensembles, on utilise la notion de sous-réseau (*netmask*).

10	74	254	1
00001010	01001010	11111110	00000001

- On sépare une partie identifiant réseau de la partie identifiant machine ;

Sous-réseaux

Pour grouper les adresses ensembles, on utilise la notion de sous-réseau (*netmask*).

10	74	254	1
00001010	01001010	11111110	00000001
11111111	11111111	11100000	00000000
255	255	224	0

- On sépare une partie identifiant réseau de la partie identifiant machine ;
- On obtient alors un masque réseau ;

Sous-réseaux

Pour grouper les adresses ensembles, on utilise la notion de sous-réseau (*netmask*).

10	74	254	1
00001010	01001010	11111110	00000001
11111111	11111111	11100000	00000000
255	255	224	0

- On sépare une partie identifiant réseau de la partie identifiant machine ;
- On obtient alors un masque réseau ;
- On peut également noter ce réseaux `10.74.254/19`

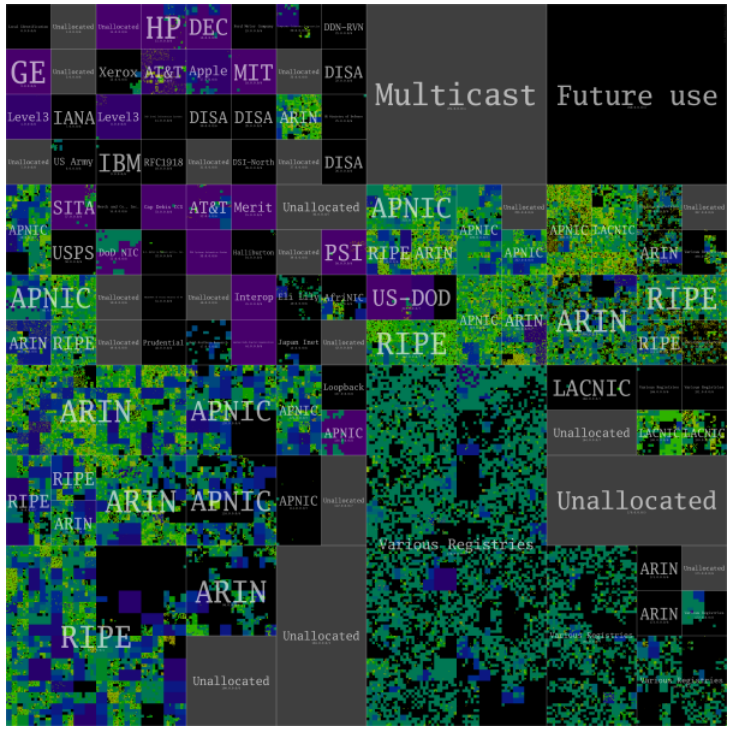
Classe d'adressage

Les adresses IPv4 sont attribuées par l'*IANA* (Internet Assigned Numbers Authority) par blocs.

Classes :

Type :	Début :	Fin :	Masque :
Classe A	0.0.0.0	127.255.255.255	255.0.0.0 (/8)
Classe B	128.0.0.0	191.255.255.255	255.255.0.0 (/16)
Classe C	192.0.0.0	223.255.255.255	255.255.255.0 (/24)
Multicast	224.0.0.0	239.255.255.255	
Réservé	240.0.0.0	255.255.255.255	

Attribution des adresses IPv4



Fin de l'IPv4 : l'IANA ne dispose plus de bloc IPv4 libre à distribuer depuis le 31 janvier 2011. Les RIR : APNIC (asie) , RIPE NCC (europe), LACNIC et l'ARIN (amériques) sont dans le même cas.

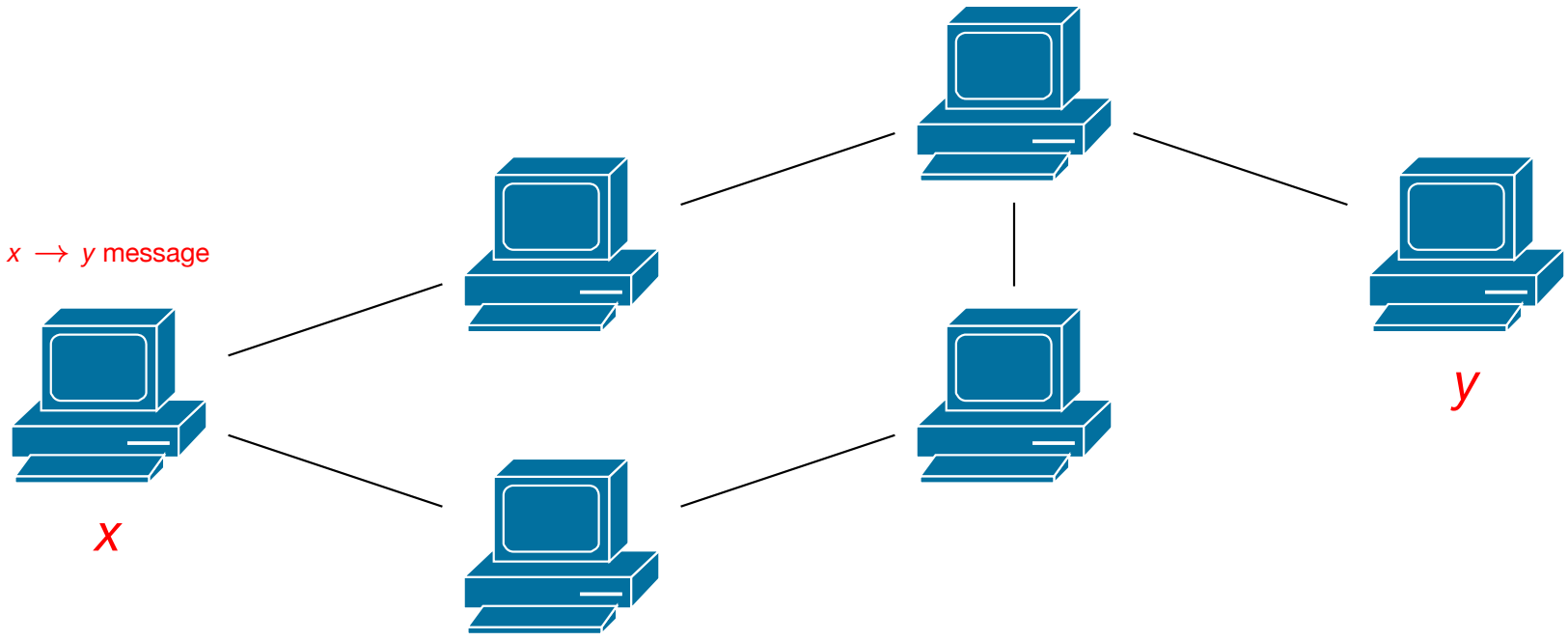
Adressage privé

Certaines adresses sont réservées pour un usage privé (*c-à-d* local) et peuvent être utilisé librement.

Les classes privées :

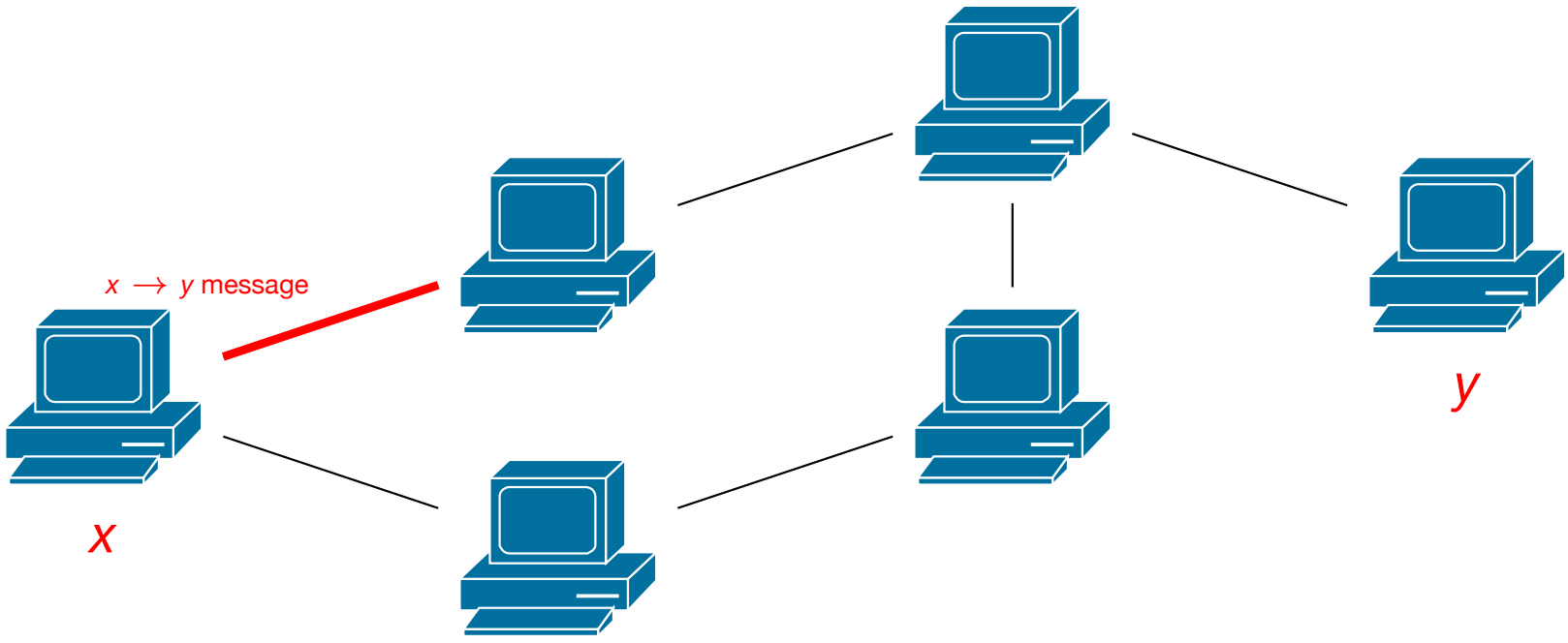
- `127.0.0.1` (*localhost*)
- `10.0.0.0` — `10.255.255.255`
- `172.16.0.0` — `172.31.255.255`
- `192.168.0.0` — `192.168.255.255`

Routage



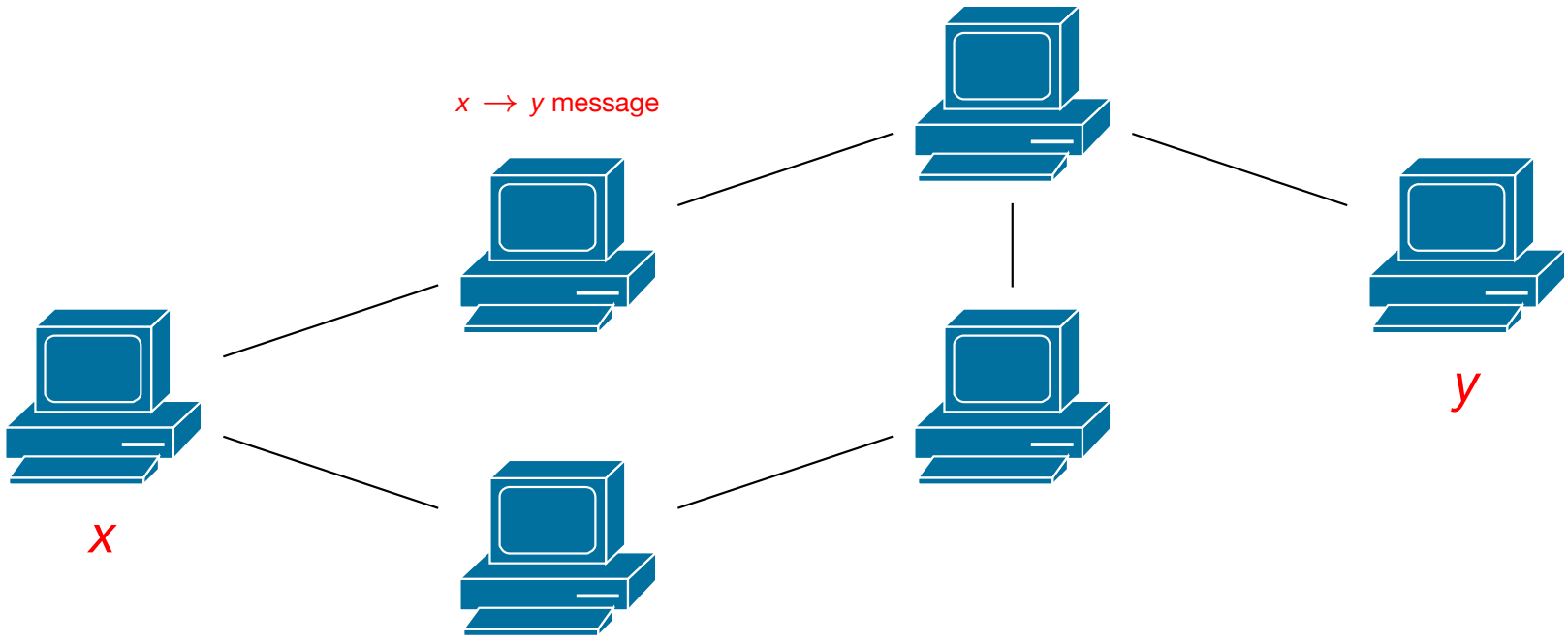
- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



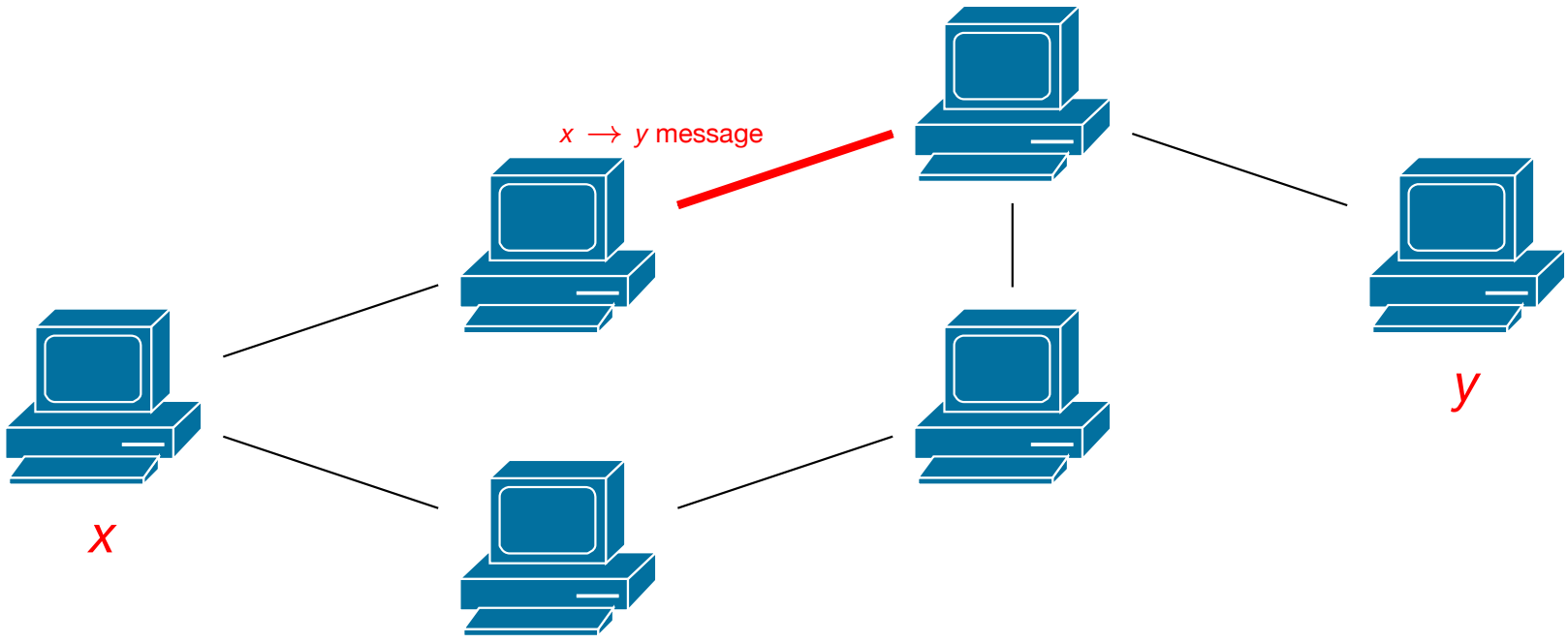
- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



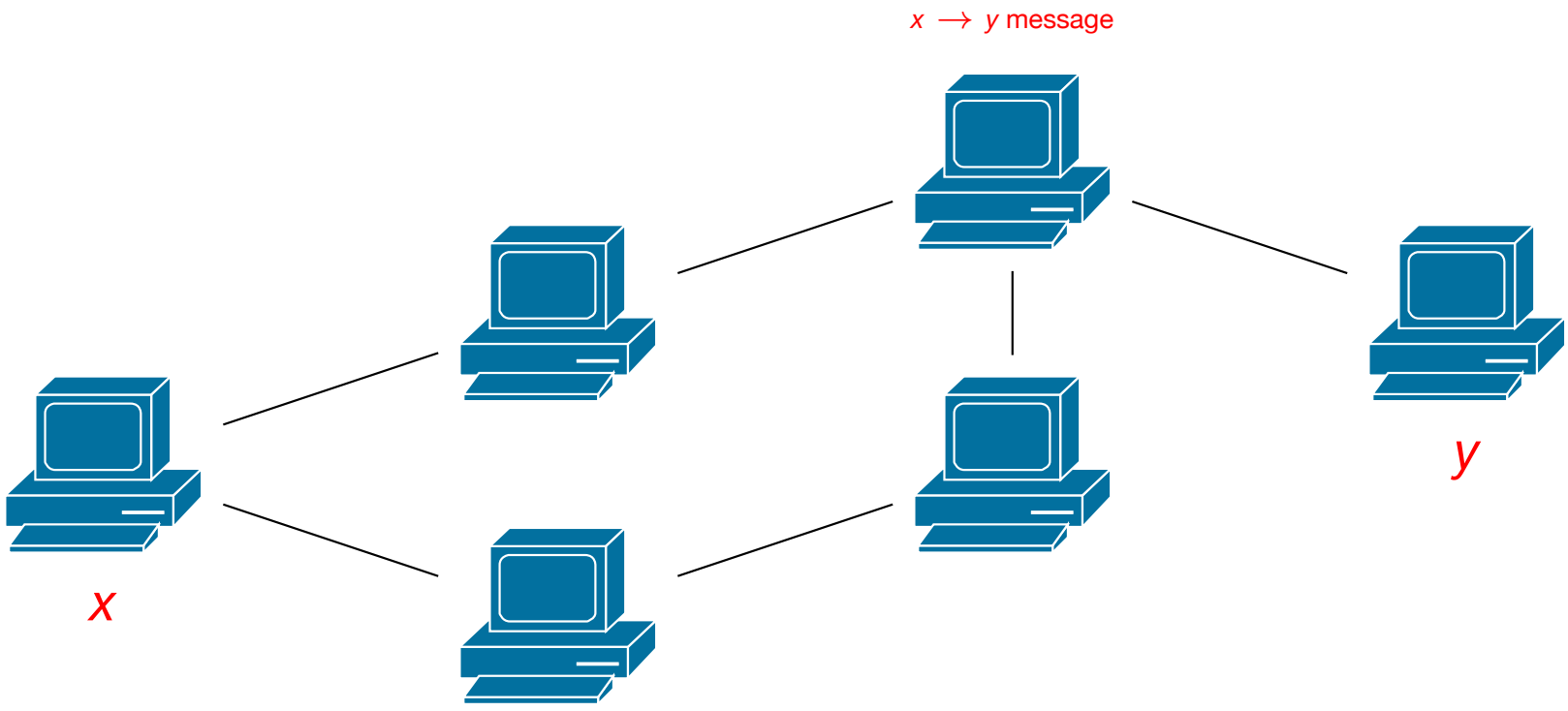
- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



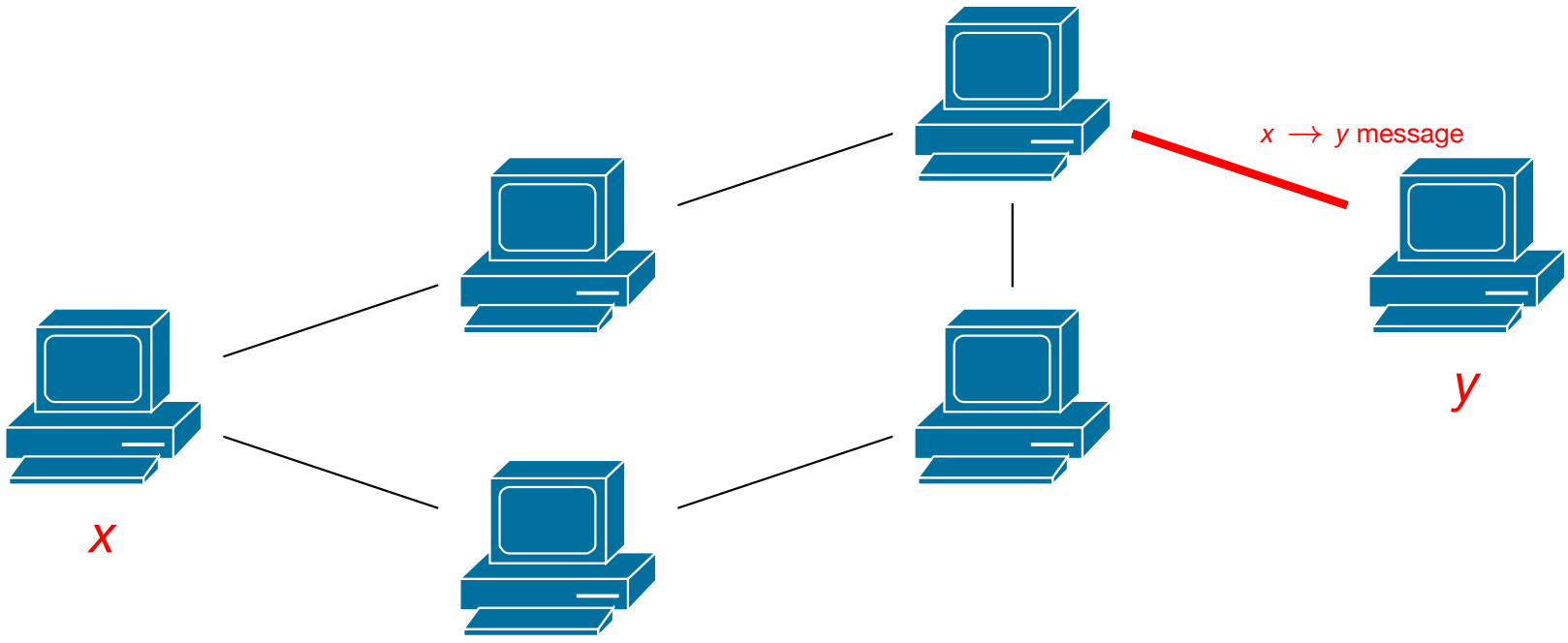
- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



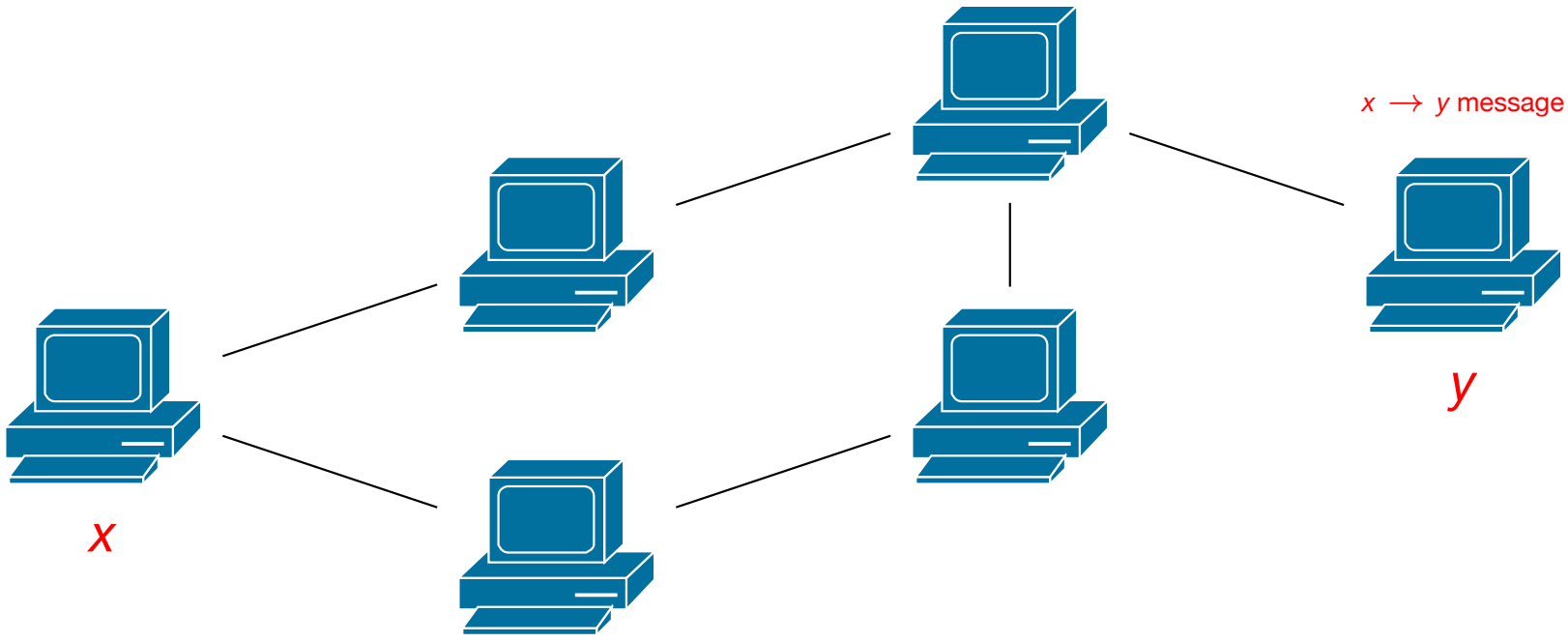
- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



- Donner un identifiant à chaque machine ;
- Relayer les messages.

Routage



- Donner un identifiant à chaque machine ;
- Relayer les messages.

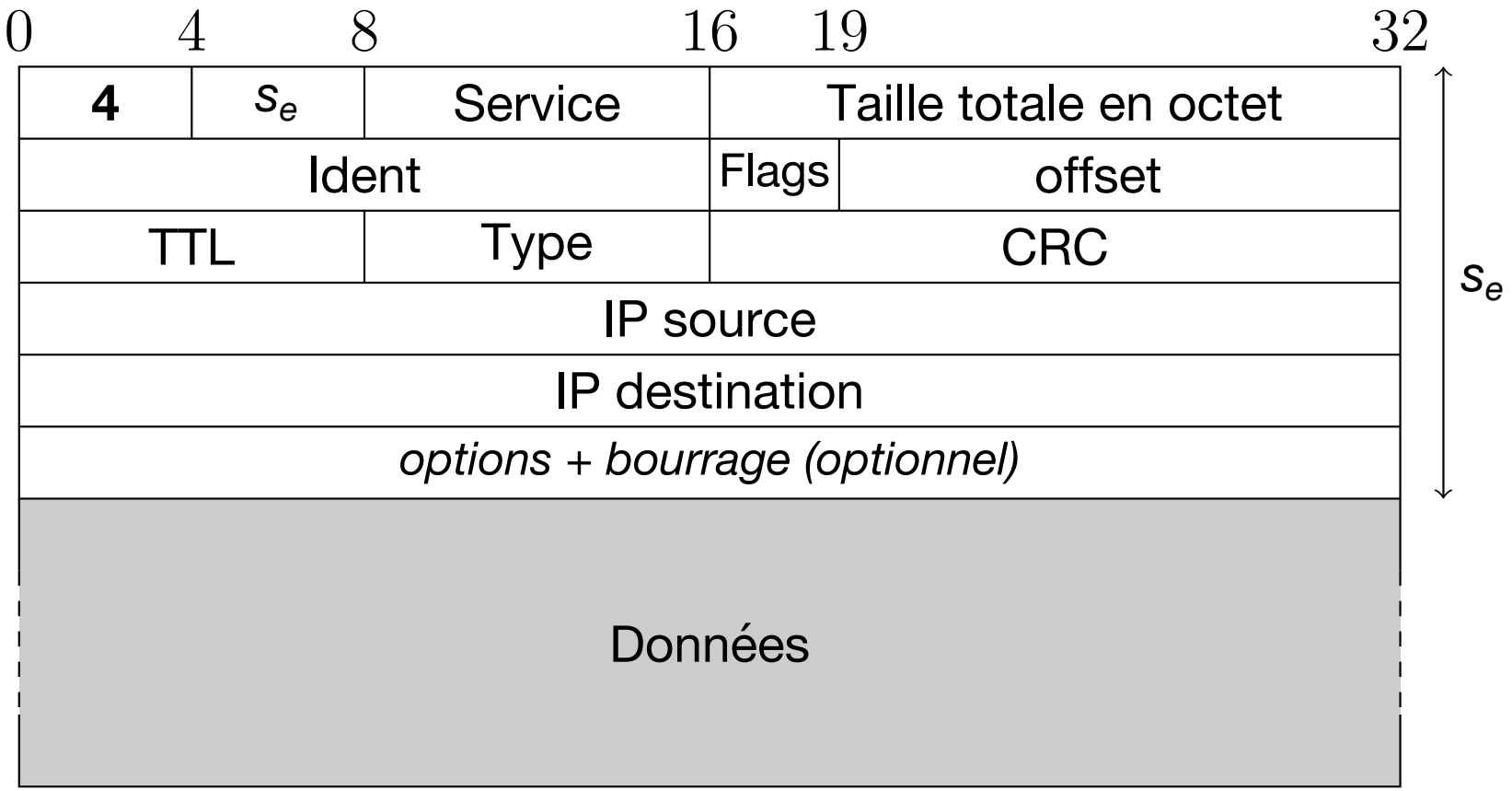
Table de routage

Principe : Chaque machine possède une table de routage qui lui indique quoi faire des paquets.

```
$ /sbin/route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
10.130.4.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.129.0   10.130.4.254    255.255.255.0   UG    0      0        0 eth0
192.168.128.0   10.130.4.254    255.255.255.0   UG    0      0        0 eth0
192.168.0.0     10.130.4.254    255.255.128.0   UG    0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
0.0.0.0         10.130.4.1      0.0.0.0         UG    100    0        0 eth0
```

Trame IPv4

Structure :

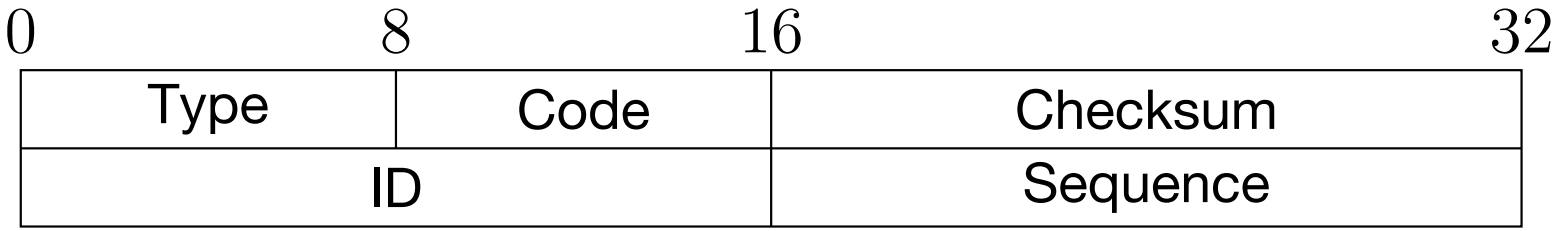


ICMP Présentation

Internet Control Message Protocol :

- Sert à la gestion des erreurs dans le transfert de paquets IP ;
- Encapsulé dans un paquet IP ;
- Existe en v4 et en v6 (*ICMPv6*) ;
- Sert également au contrôle du réseau.

Datagramme v4



Exemples :

- Type 0 : “Echo Reply”
- Type 3 : “Destination Unreachable”
  - Code 0 : “Destination network unreachable”
  - Code 1 : “Destination host unreachable”
  - …
- Type 8 : “Echo Request”
- Type 12 : “Parameter Problem : Bad IP header”
- …

5. 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

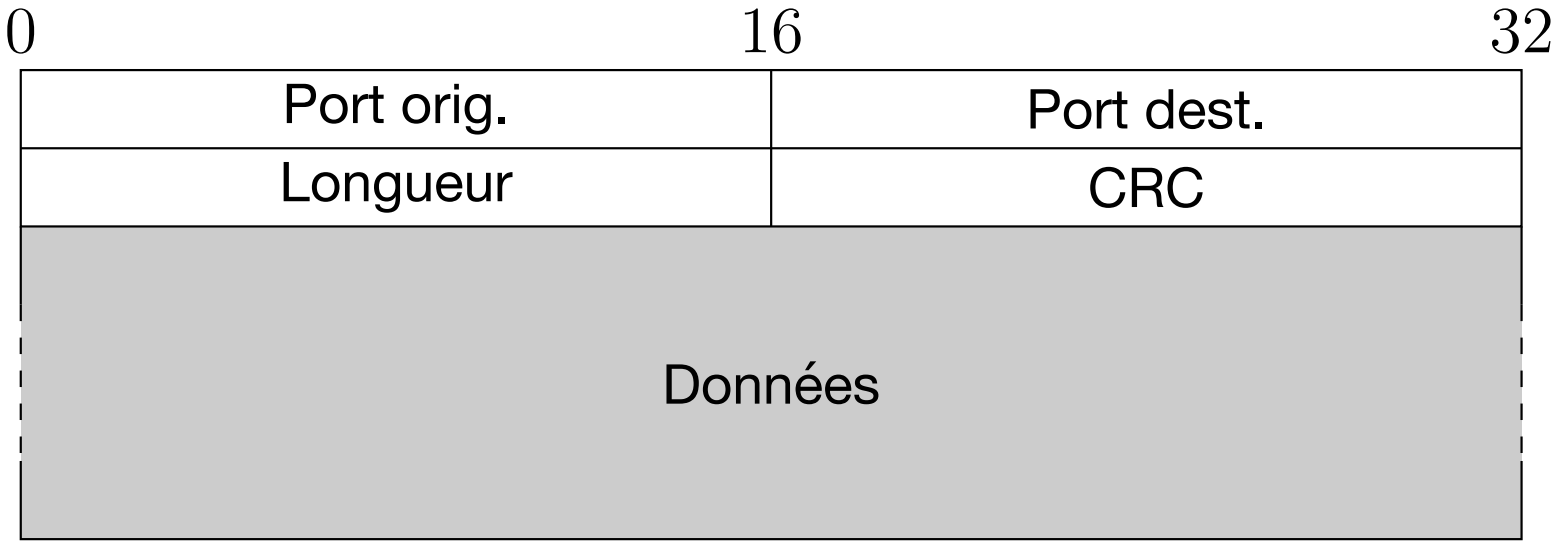
21	ftp
22	ssh
25	SMTP
53	DNS
80	http
110	POP3
143	IMAP
443	https
465	SMTPS
993	IMAPS
995	POPS

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

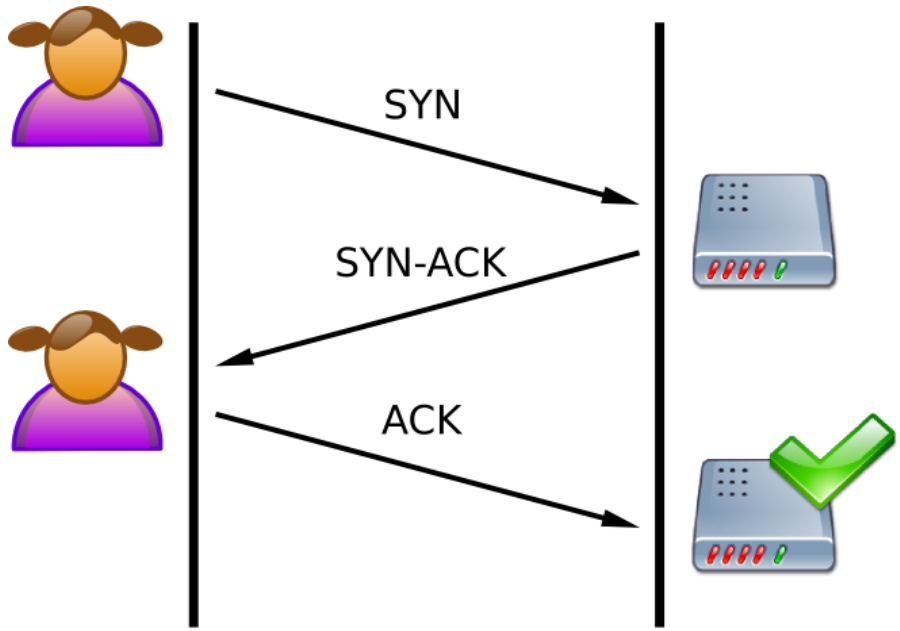
- L'émetteur envoie un paquet avec un identifiant ;
- le récepteur envoie un accusé de réception ACK pour ce message.

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

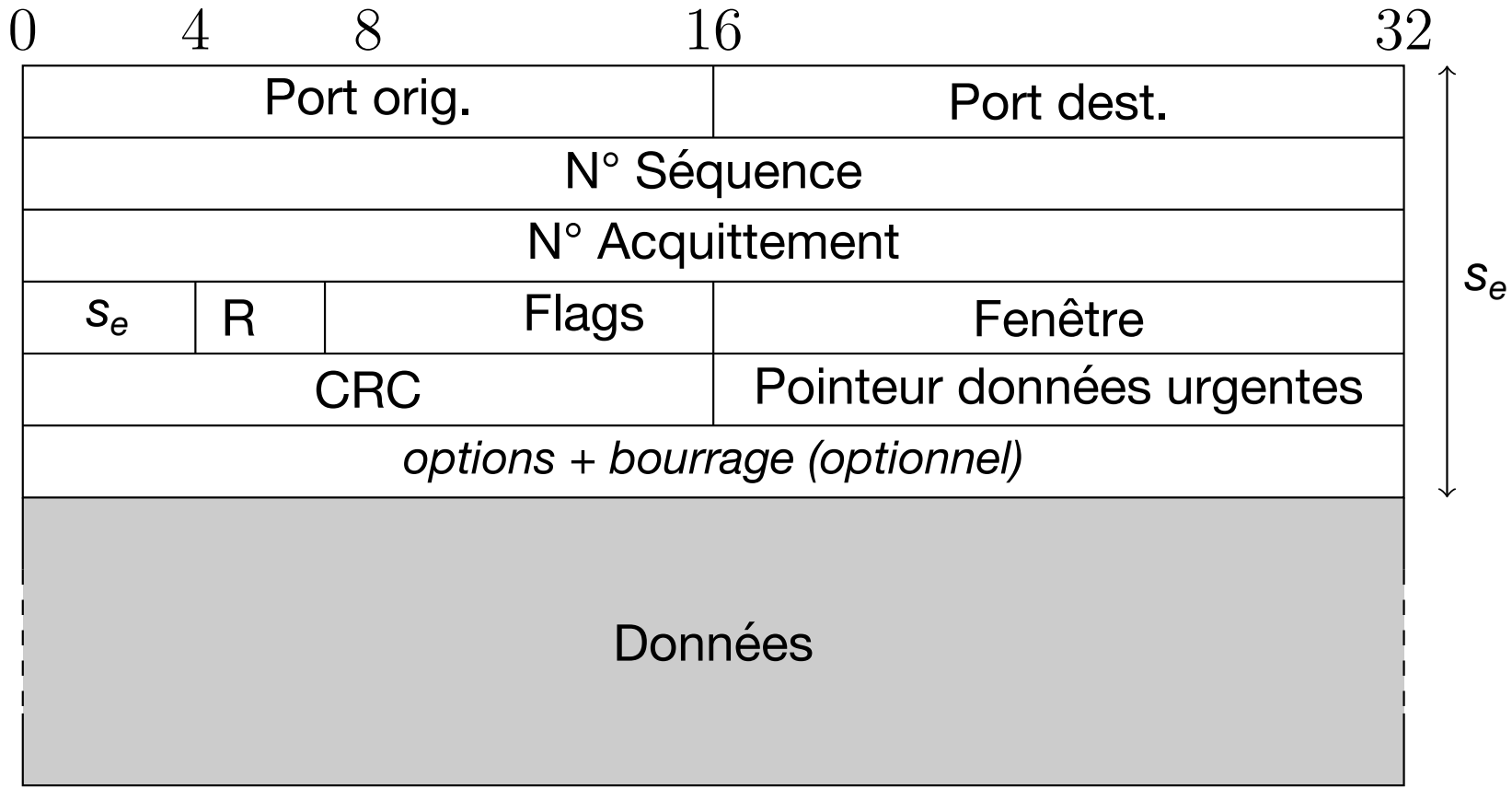
Pour établir, on envoie un signal SYN. Le récepteur envoie également un signal SYN avec un ACK de notre signal. Pour finir, on émet un ACK du signal SYN reçu.



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.

6. 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 :

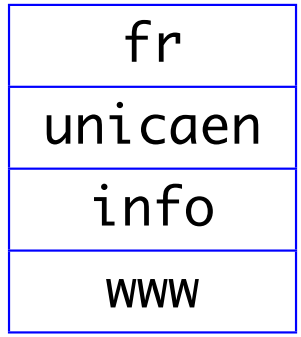
`www.info.unicaen.fr`

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

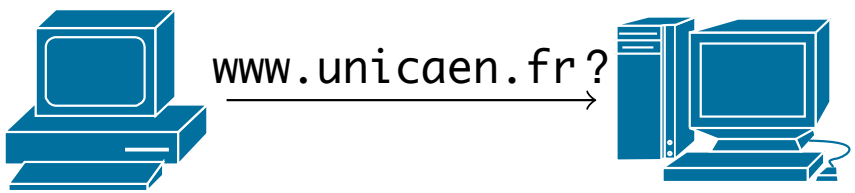
dns racine

dns

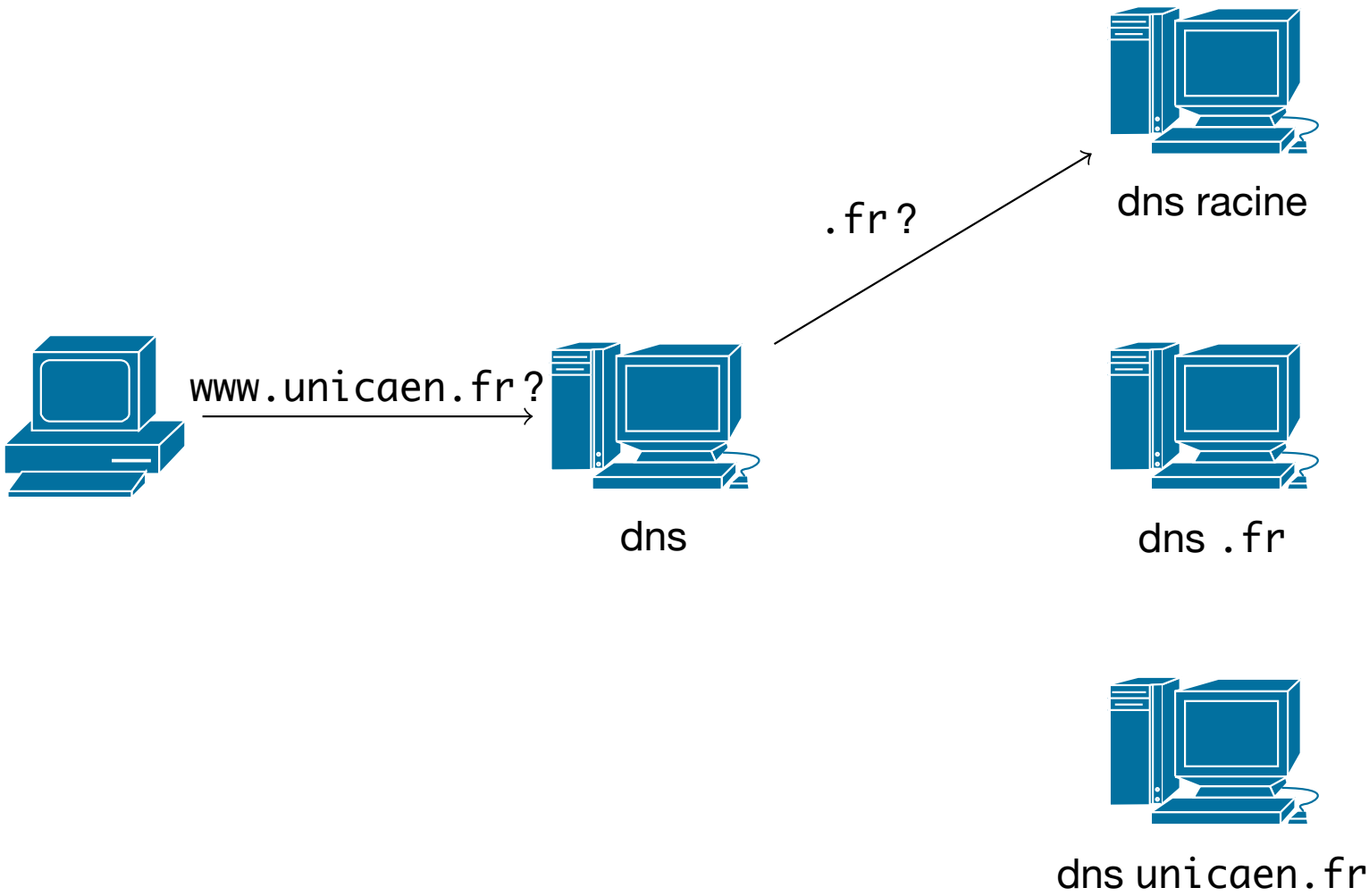
dns `.fr`

dns `unicaen.fr`

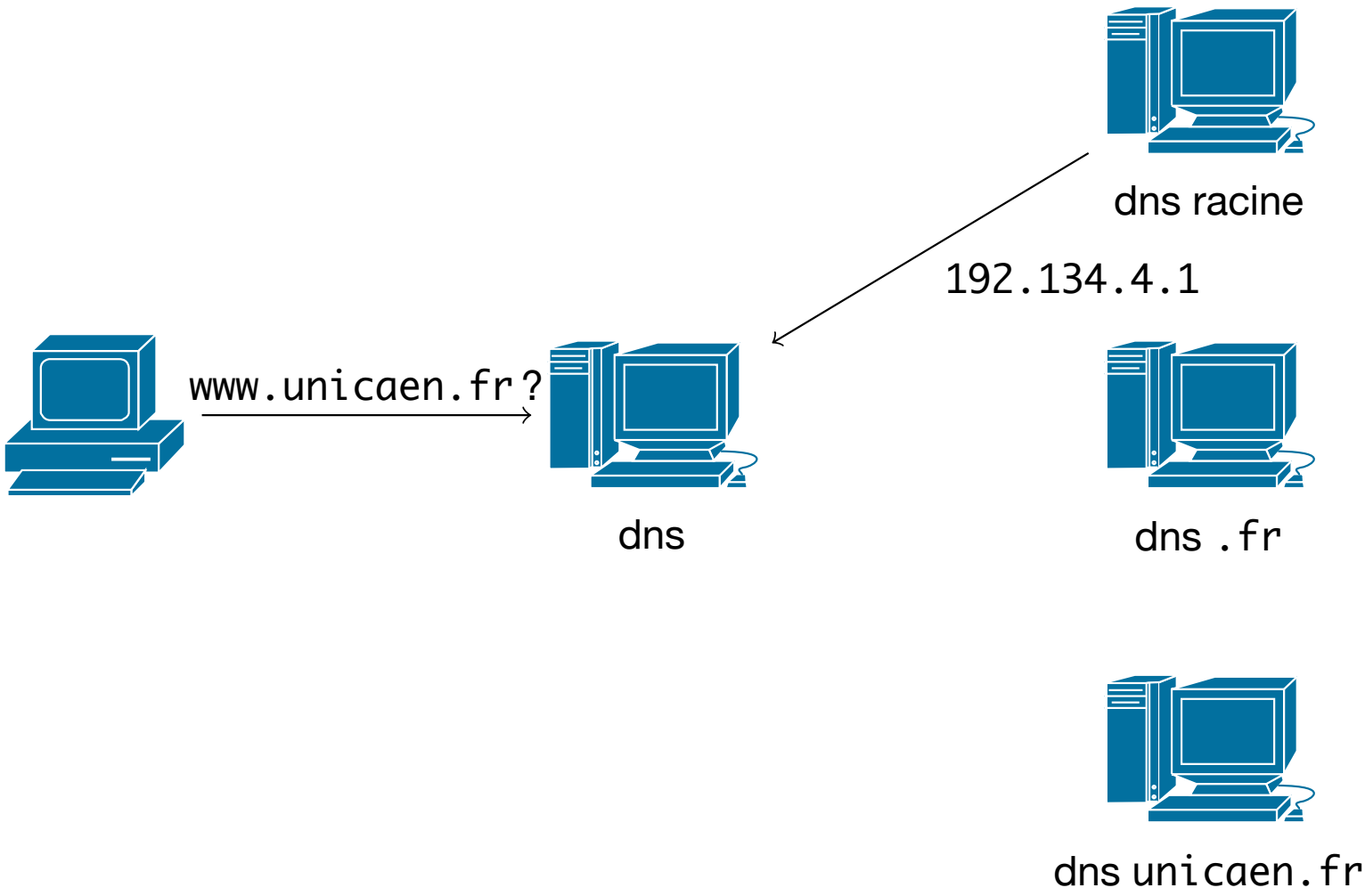
Fonctionnement



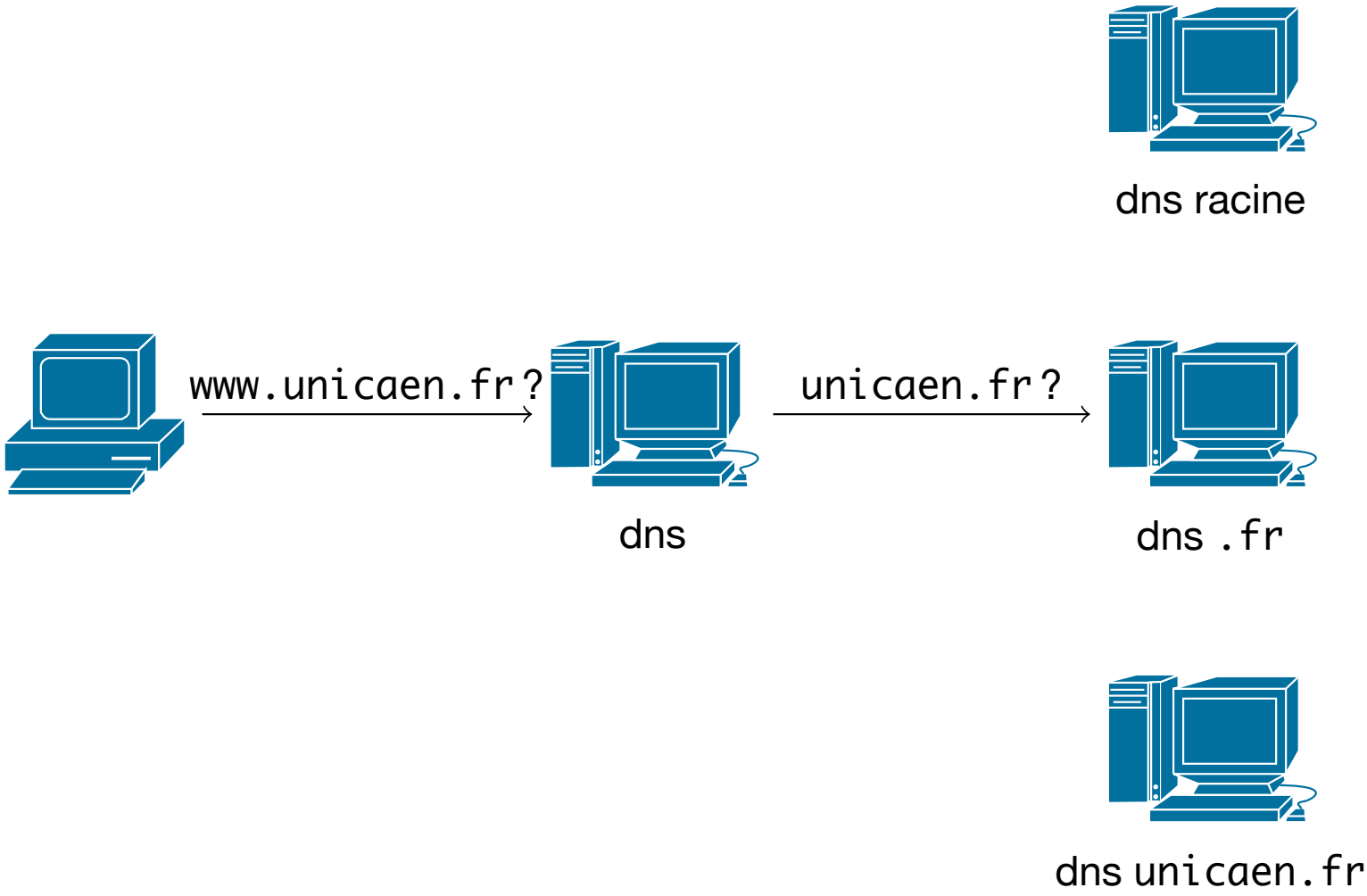
Fonctionnement



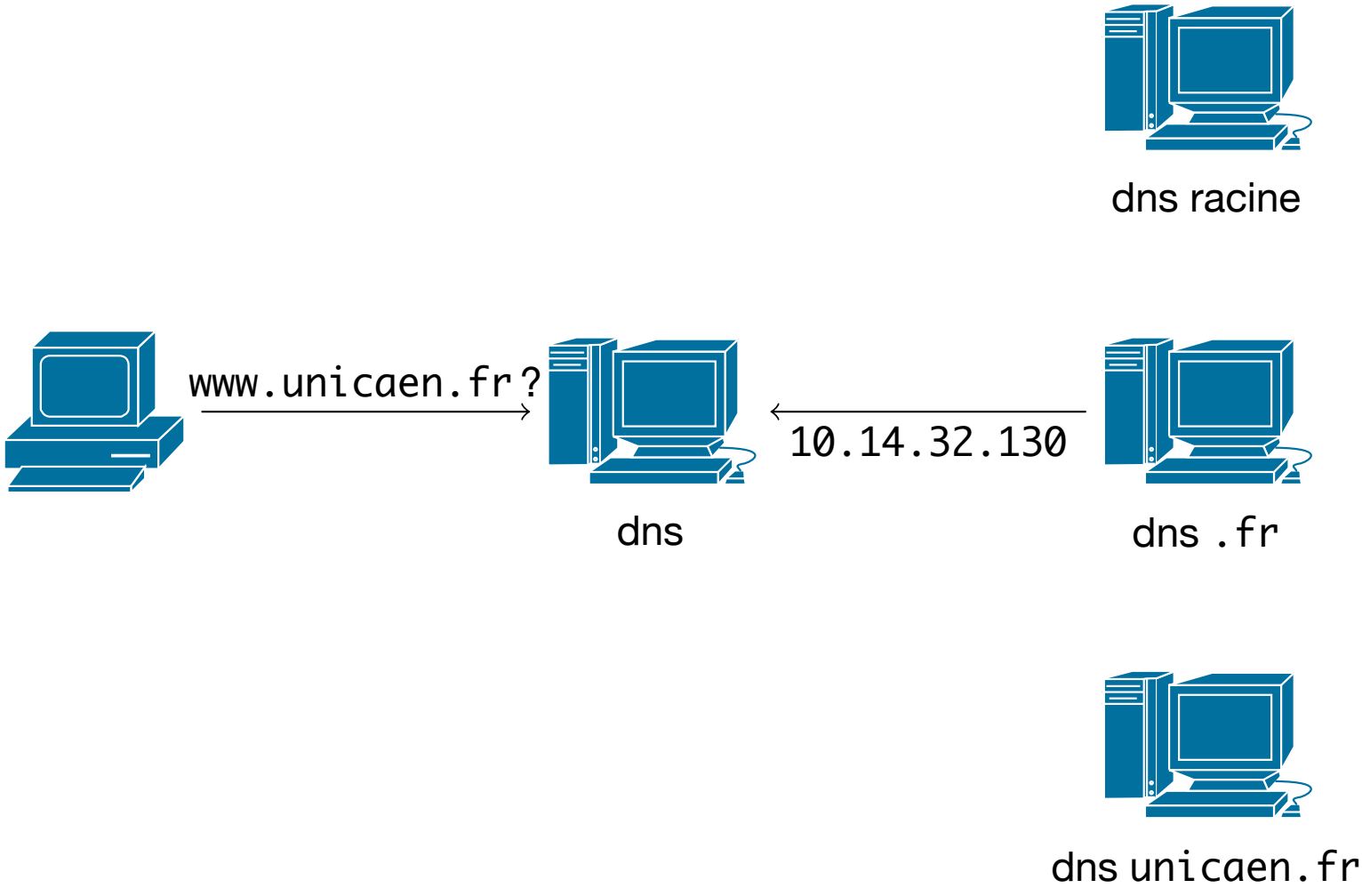
Fonctionnement



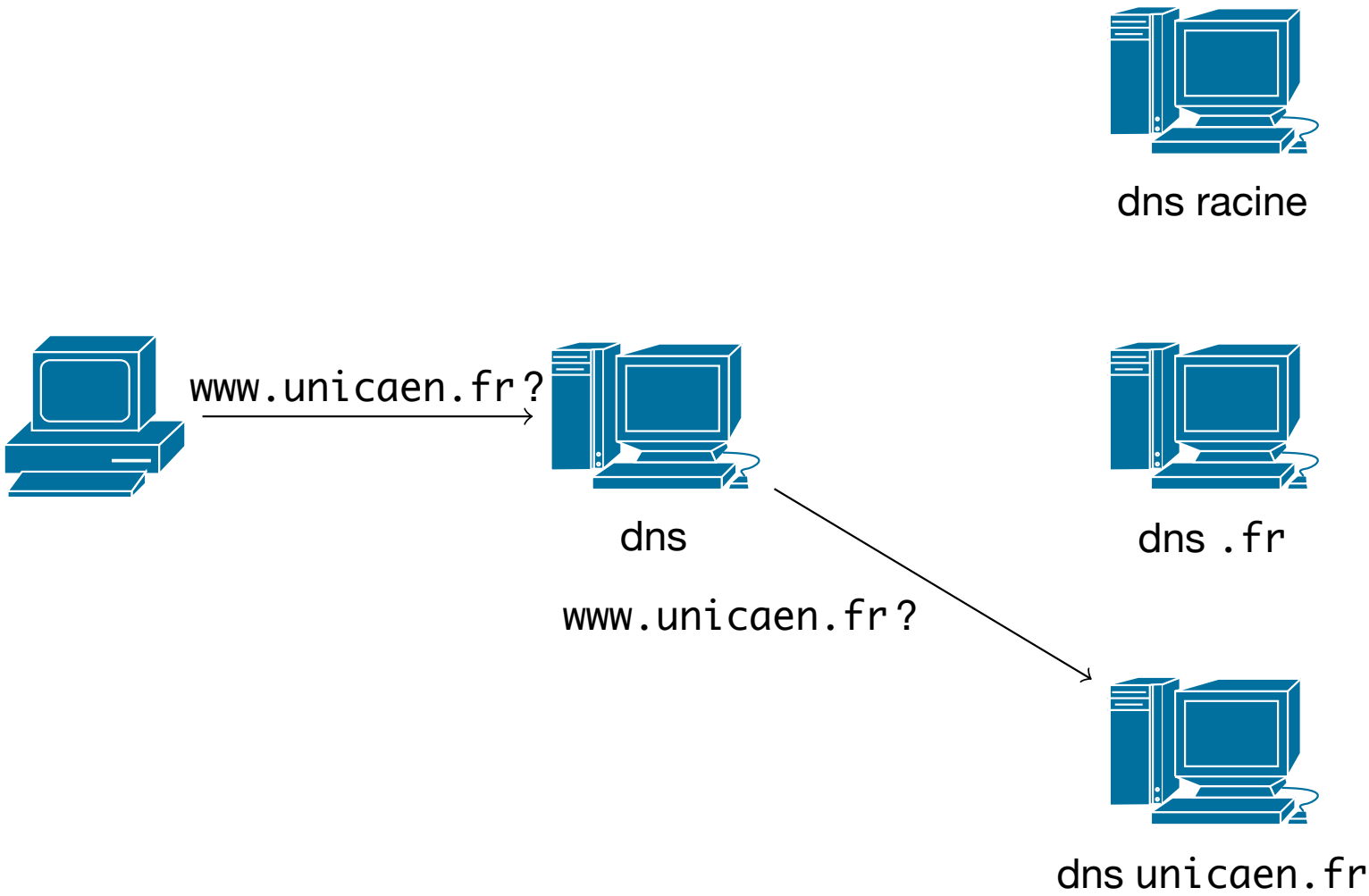
Fonctionnement



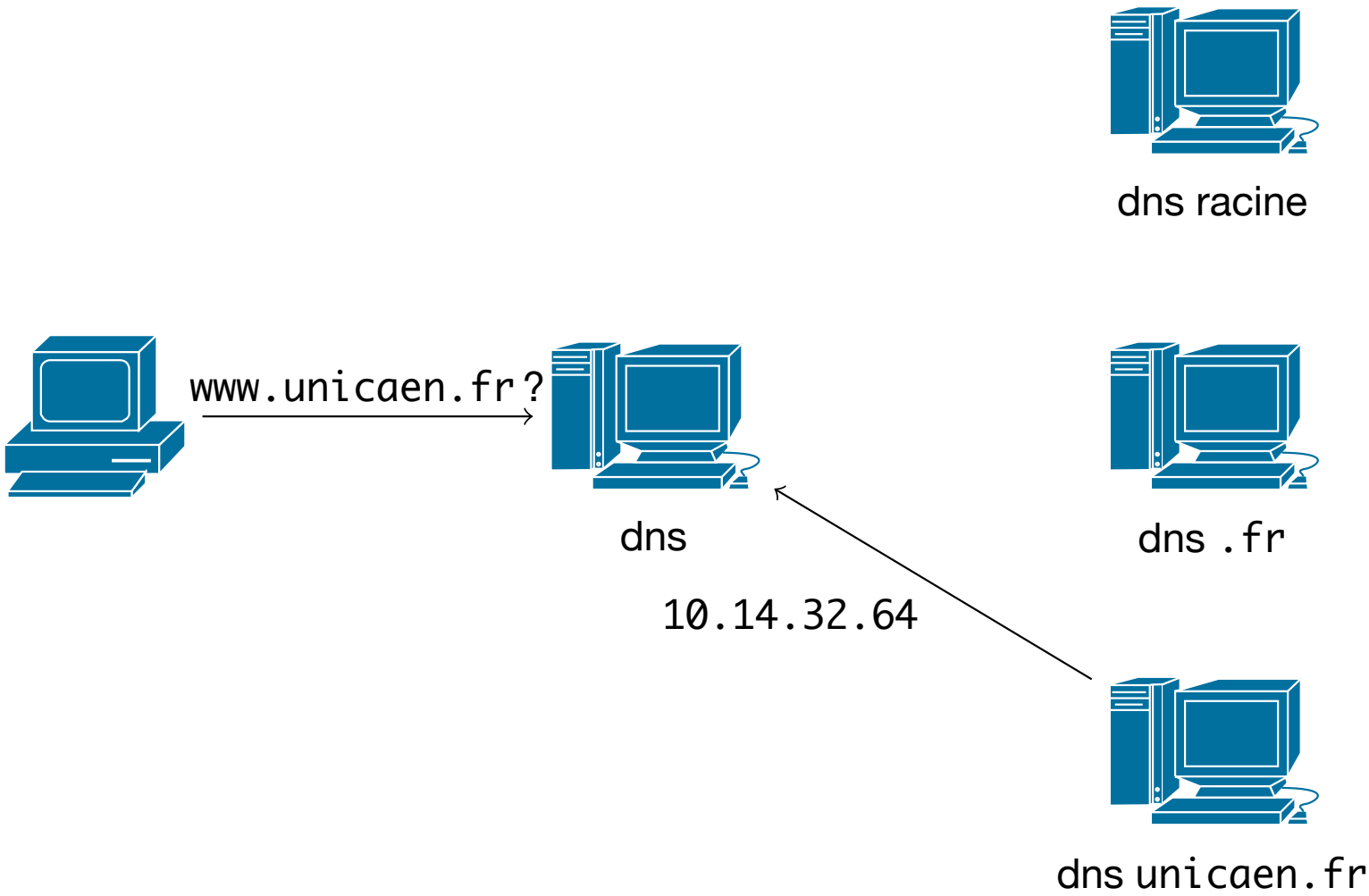
Fonctionnement



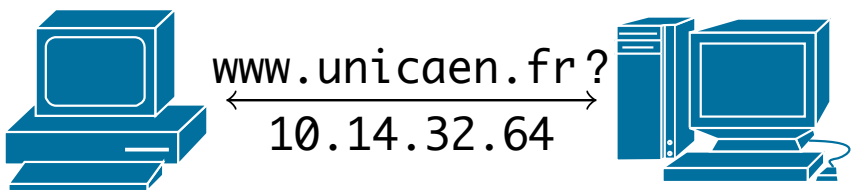
Fonctionnement



Fonctionnement



Fonctionnement

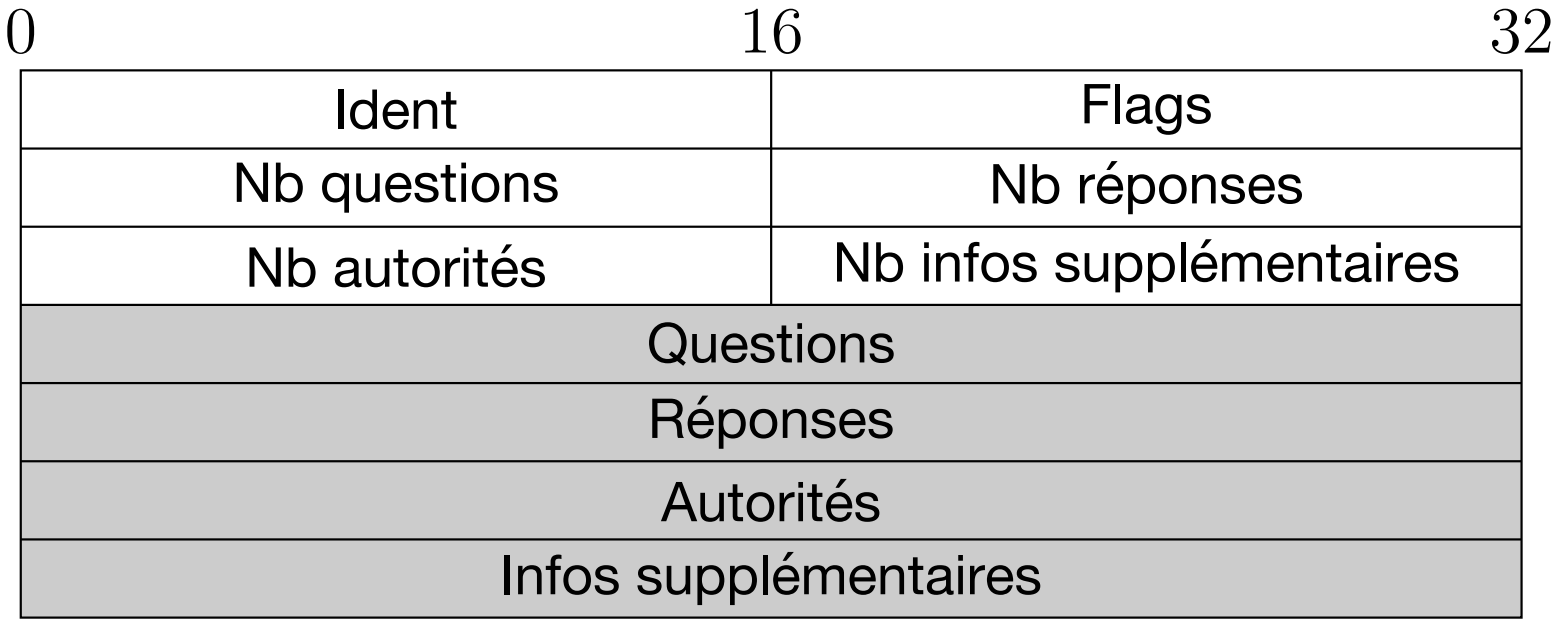


Mise en place

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 : univ.communaute-owner@liste.unicaen.fr
Received : from wzproxy02.unicaen.fr (LHLO zmtp.unicaen.fr) (10.14.1.187) by
 wzstore08.unicaen.fr with LMTP; Thu, 3 Sep 2015 10 :34 :44 +0200 (CEST)
Received : from localhost (localhost [127.0.0.1])
    by zmtp.unicaen.fr (Postfix) with ESMTP id B2F331813BC;
    Thu,  3 Sep 2015 10 :34 :44 +0200 (CEST)
X-Virus-Scanned : amavisd-new at unicaen.fr
Received : from zmtp.unicaen.fr ([127.0.0.1])
    by localhost (wzproxy02.unicaen.fr [127.0.0.1]) (amavisd-new, port 10026)
    with ESMTP id m21lGkSbxvwN; Thu,  3 Sep 2015 10 :34 :44 +0200 (CEST)
Received : from lsmtp1.unicaen.fr (lsmtp1.unicaen.fr [10.14.1.21])
    by zmtp.unicaen.fr (Postfix) with ESMTP id 58F34180815;
    Thu,  3 Sep 2015 10 :34 :44 +0200 (CEST)
Received : from smtpcc.unicaen.fr (lsmtpcc1.unicaen.fr [10.14.1.16])
    by lsmtp1.unicaen.fr (Postfix) with ESMTP id 2EA1641C9409;
    Thu,  3 Sep 2015 10 :34 :44 +0200 (CEST)
Received : from lsympa1.unicaen.fr (unknown [10.14.128.132])
    by smtpcc.unicaen.fr (Postfix) with ESMTP id 373034F6A0E7;
    Thu,  3 Sep 2015 10 :18 :15 +0200 (CEST)
<...>
Received : from wzstore05.unicaen.fr (unknown [10.14.32.200])
    by lsmtp2.unicaen.fr (Postfix) with ESMTP id 61E124E9C433;
    Thu,  3 Sep 2015 10 :17 :49 +0200 (CEST)
Date : Thu, 3 Sep 2015 10 :17 :49 +0200 (CEST)
From : ”communication.listes@unicaen.fr” <communication.listes@unicaen.fr>
Reply-To : logistique.direction@unicaen.fr
To : univ.communaute@liste.unicaen.fr, univ.etu@liste.unicaen.fr
Message-ID : <1914055538.2459715.1441268269276.JavaMail.zimbra@unicaen.fr>
In-Reply-To : <1770058945.2435315.1441260750569.JavaMail.zimbra@unicaen.fr>
MIME-Version : 1.0
X-Originating-IP : [10.14.1.187]
X-Mailer : Zimbra 8.0.9_GA_6191 (ZimbraWebClient - GC44 (Win)/8.0.9_GA_6191)
Thread-Topic : Stationnement =?utf-8?Q?g=C3=AAnant?=
```

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 Op
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** ;
- …

7. Un exemple complet

Lire un site web