Architecture des réseaux - R3.06
Rappels & DHCP & DNS

IUT-2
Département Informatique

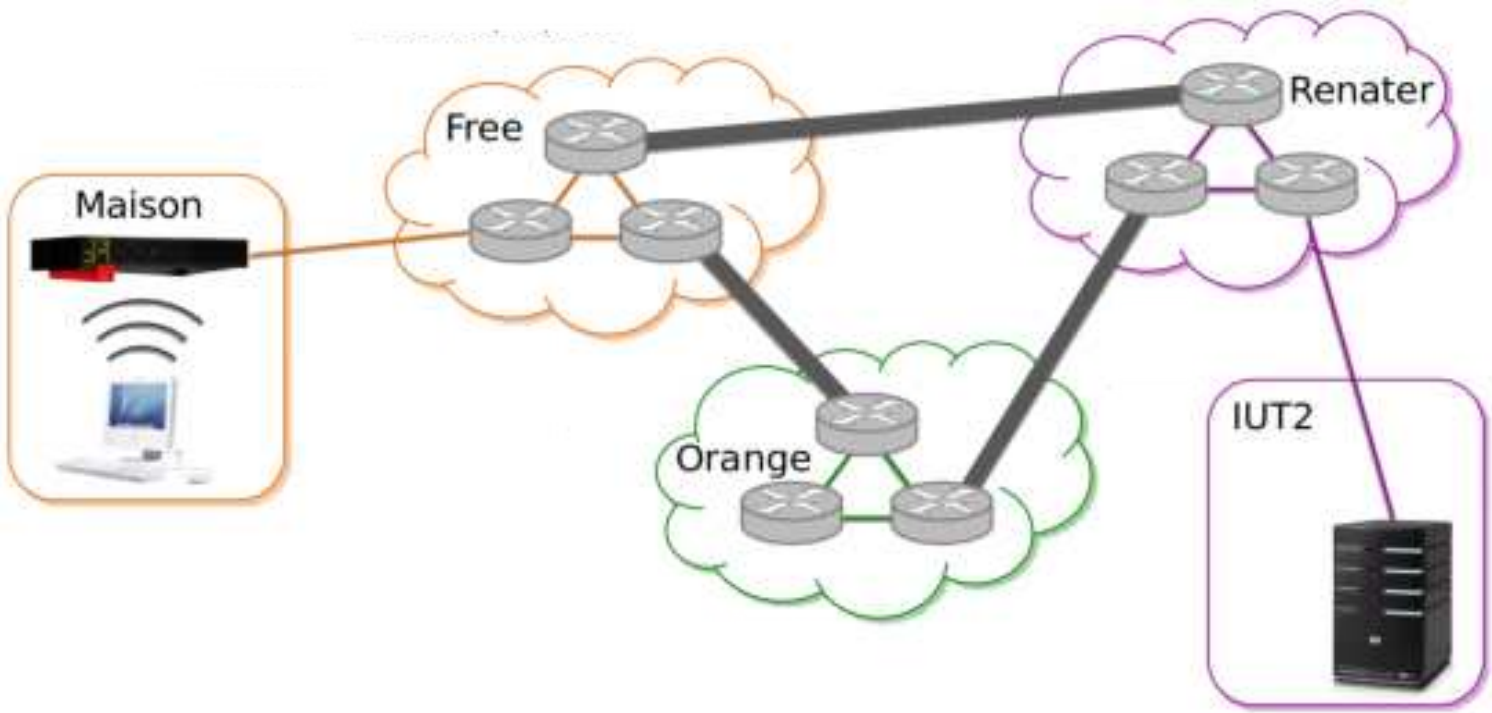
10 septembre 2024

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

Internet et Routage

Internet (INTERconnected NETworks) :
Choix d'un chemin en fonction de l'IP destination
Tables de routage mise à jour
Différents protocoles, algorithmes
Communication de proche en proche par commutation de paquets



IUT2 A
Université Grenoble Alpes
Département INFO

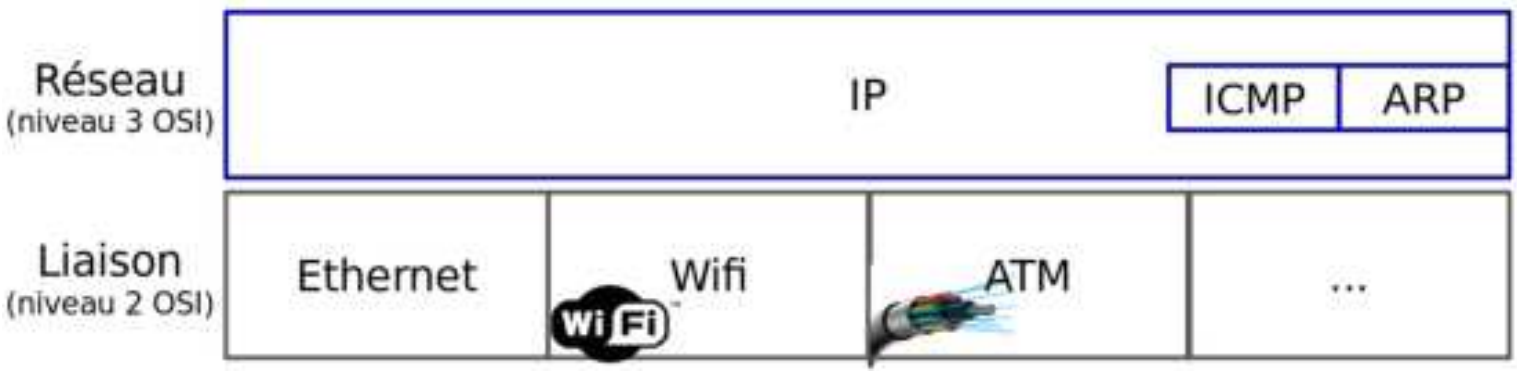
Les couches du modèle TCP/IP

Couche	Sous-problème	Implanté dans	Protocole(s)
7 : Application	Communication utilisateur/application	Logiciel	http, ftp, ssh...
4 : Transport	Assurer la communication entre deux processus	Système d'exploitation	TCP, UDP
3 : Réseau	Trouver le chemin pour chaque paquet de données à envoyer entre deux machines de réseaux locaux différents	Système d'exploitation	IP
2 : Liaison de données	Gérer l'accès au médium (câble, ondes...)	Carte réseau	Ethernet, WiFi...
1 : Physique	Traduire l'information binaire en ondes électromagnétiques sur le lien physique	Carte réseau	Ethernet, WiFi...

IUT2 Université Grenoble Alpes
Département INFO

Les couches du modèle TCP/IP

Couche 2 : Interface d'accès aux différents LANs



IUT2 Université Grenoble Alpes
Département INFO

Couche 3 : IP

Services offerts
Couche commune à tous réseaux
Ethernet, Wifi, ATM, ADSL, etc.
Interconnexion

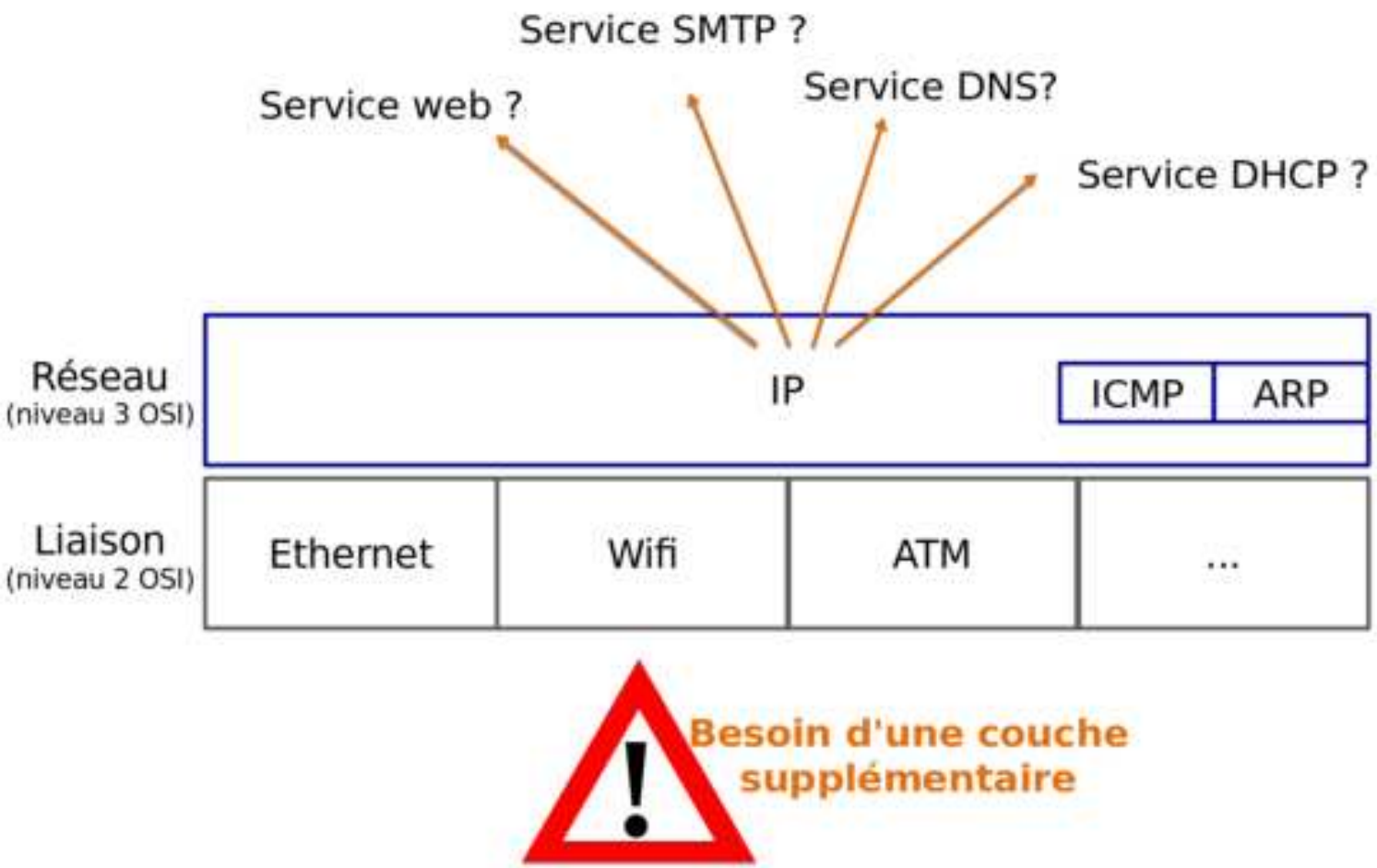
Protocole uniforme
Identification des machines : adresse IP
Format de données : datagramme IP

Envois fragmentés

Gestion d'erreurs (ICMP)

IUT2 A
Université Grenoble Alpes
Département INFO

Les couches du modèle TCP/IP



Couche 3 : IP

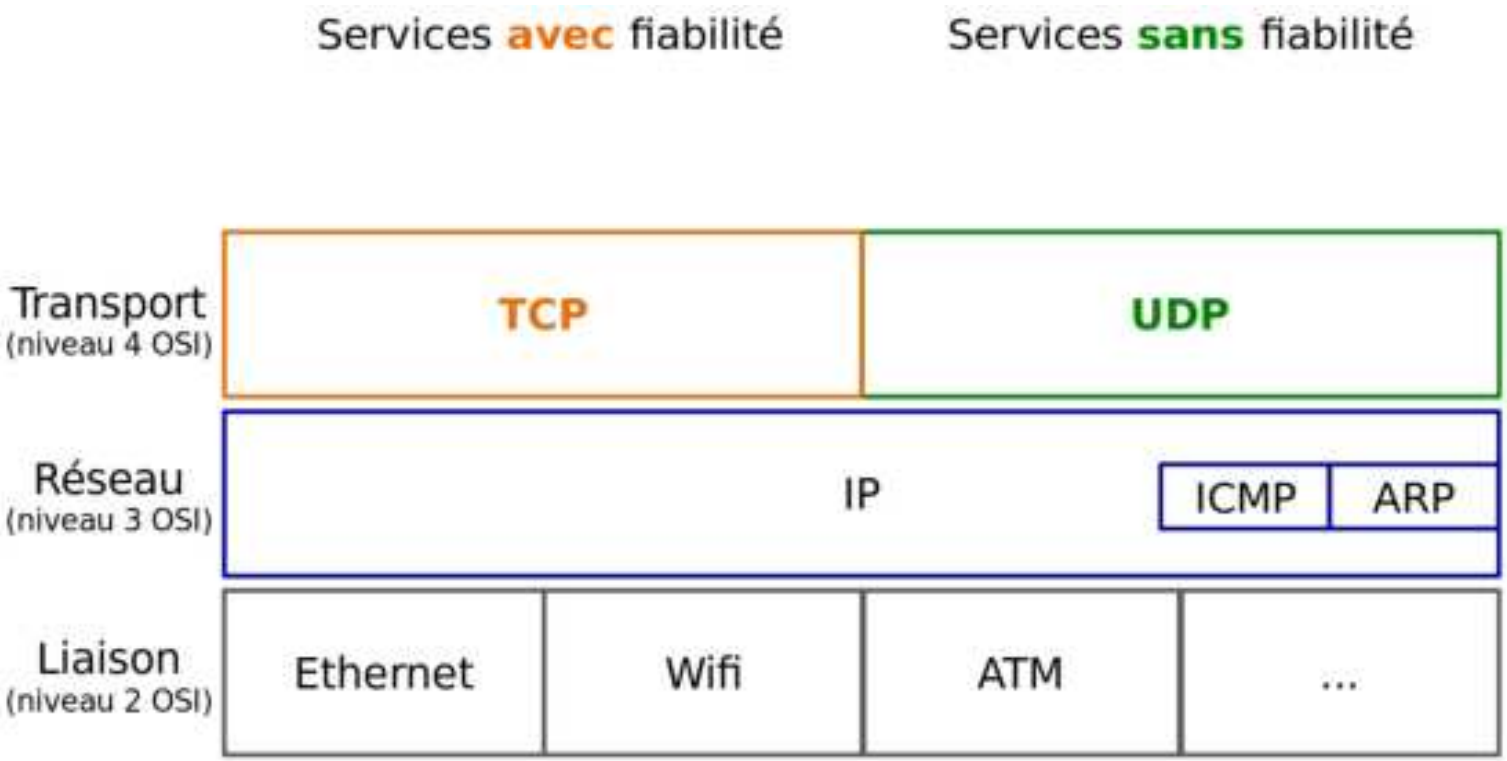
Limites

- Pas d'identification de services : web ? e-mail ?
- Pas de garantie de livraison (perte, doublons, ordre)
- Pas de gestion des flux

IUT2 Université Grenoble Alpes
Département INFO

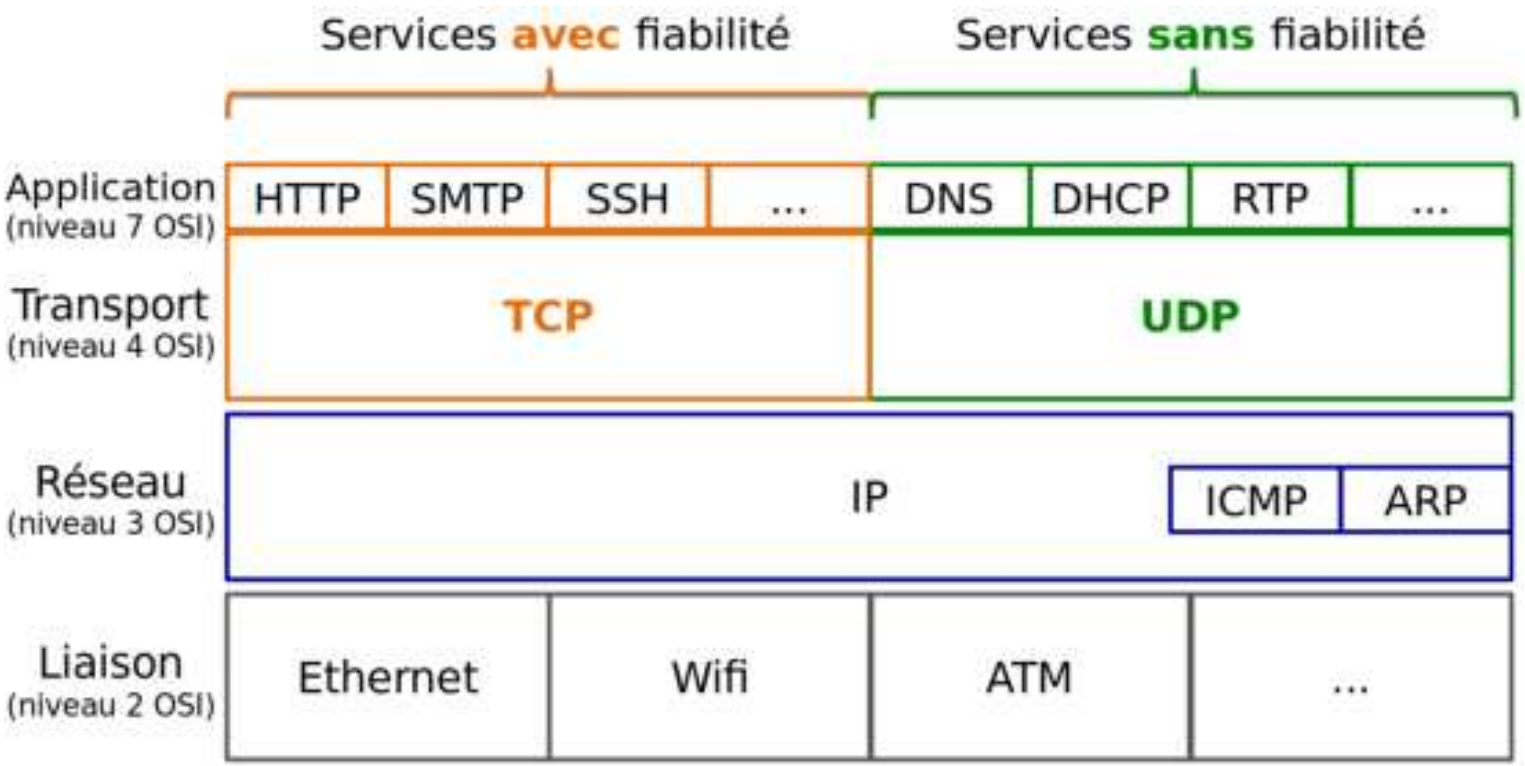
Les couches du modèle TCP/IP

Services à l'utilisateur : web, email Services de gestion : DNS, DHCP, LDAP



IUT2 Université Grenoble Alpes
Département INFO

Les couches du modèle TCP/IP



IUT2 Université Grenoble Alpes
Département INFO

Identifiants dans l'architecture TCP/IP

Adresse physique du niveau interface (accès réseau) :

- dépend du réseau physique (ex. adresses **Media Access Control (MAC)**)

Adresse du niveau réseau :

- **Adresse IP** : adresse « logique », comprenant une partie identifiant le réseau et une partie identifiant la machine dans le réseau.
- Par exemple : `192.131.15.17`
- Une (parfois plusieurs) adresse IP par interface

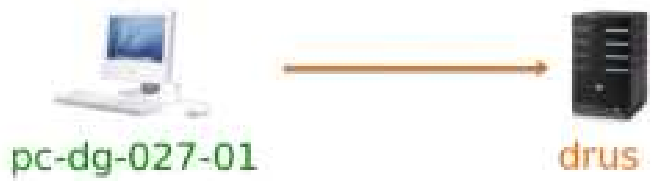
Identification des processus au niveau transport :

- adresse IP + **numéro de port**

Identification des utilisateurs/ressources dans les applications : **adresse mail**, **URL** ...

IUT2 Université Grenoble Alpes
Département INFO

Exemple : courrier électronique



Numéro de port destination => identifie le service

25 => envoi de mail

Application	titi.toto@iut2. . .	etu-info-s3@iut2. . .
TCP/UDP	32550	25
IP	192.168.141.121	193.55.51.242
Liaison	C8 :2A :14 :28 :4F :99	00 :23 :ae :8b :63 :3b

IUT2 Université Grenoble Alpes
Département INFO

Le protocole Ethernet

Fonction

Transmettre des unités de données « trames » entre deux machines directement connectées (ou via un commutateur).

- Service avec retransmission en cas de collision.
- Pas de correction si le Frame Check Sequence (FCS) est erroné.
- Longueur max des données 1500 octets par trame.
- Couvre les couches 1 et 2 du modèle Open Systems Interconnection (OSI).

Adresse MAC : Identité d'une machine 6 octets = constructeur (3 octets) + numéro (3 octets) Ex. C8 :2A :14 :28 :4F :40

IUT2 A
Université Grenoble Alpes
Département INFO

Le protocole IP

Fonction

Assurer l'acheminement des unités de données « paquets IP » dans l'inter-réseau

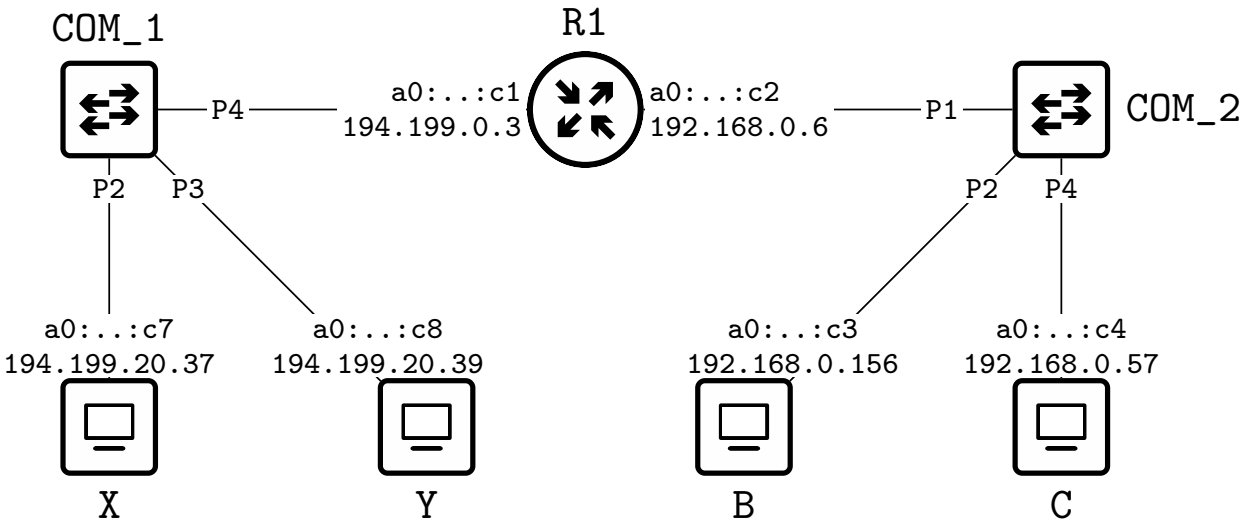
- Service sans contrôle d'erreur ni contrôle de flux de bout en bout.
- Service de base de type Best Effort (BE)
- Service de fragmentation de données si les réseaux traversés ont des Maximum Transfer Unit (MTU) de valeurs différentes.

Deux versions du protocole :

- IPV4 : adresse sur 32 bits [rfc, 1981]
- IPV6 : adresse sur 128 bits [Hinden et Deering, 1998]

IUT2 A
Université Grenoble Alpes
Département INFO

Exemple



Combien de trames pour un paquet IP de Y vers X ?
Combien de trames pour un paquet IP de Y vers C ?

trame n°	@MAC source	@MAC destination	@IP source	@IP destination
1 Y → X				
2 Y → C				
...				

Sommaire

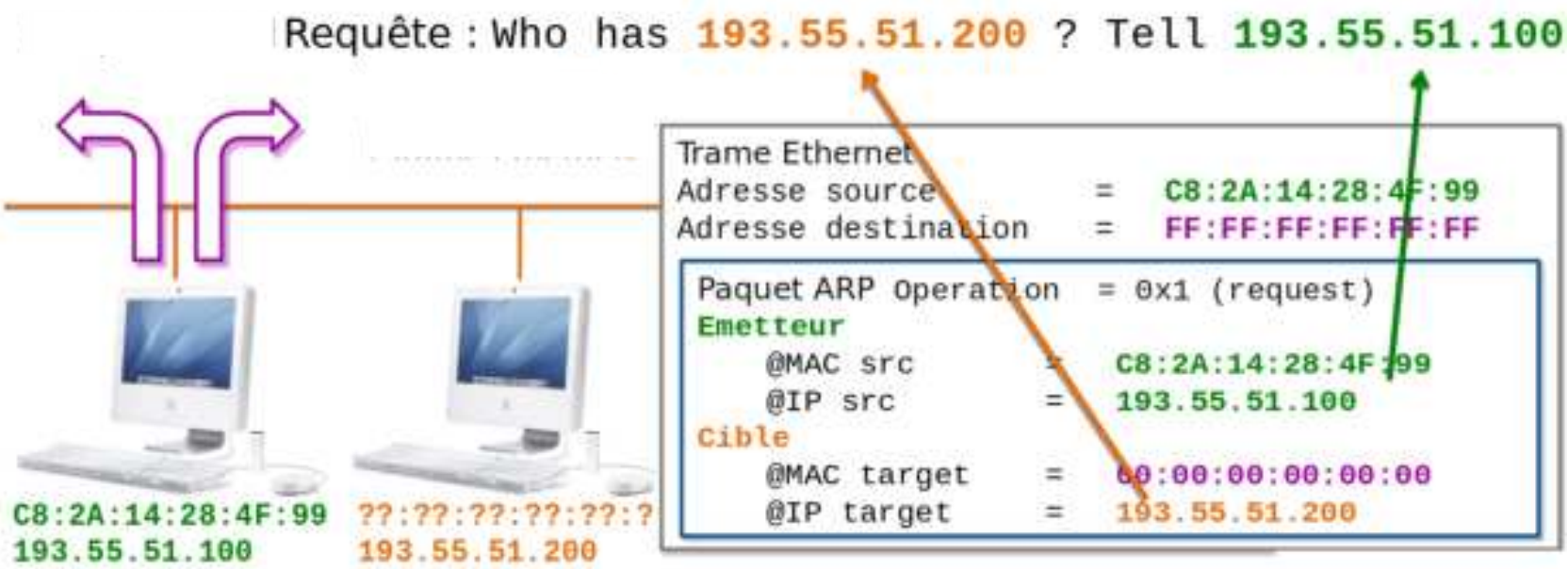
IUT2 Université Grenoble Alpes
Département INFO

Communication sur un réseau local Ethernet

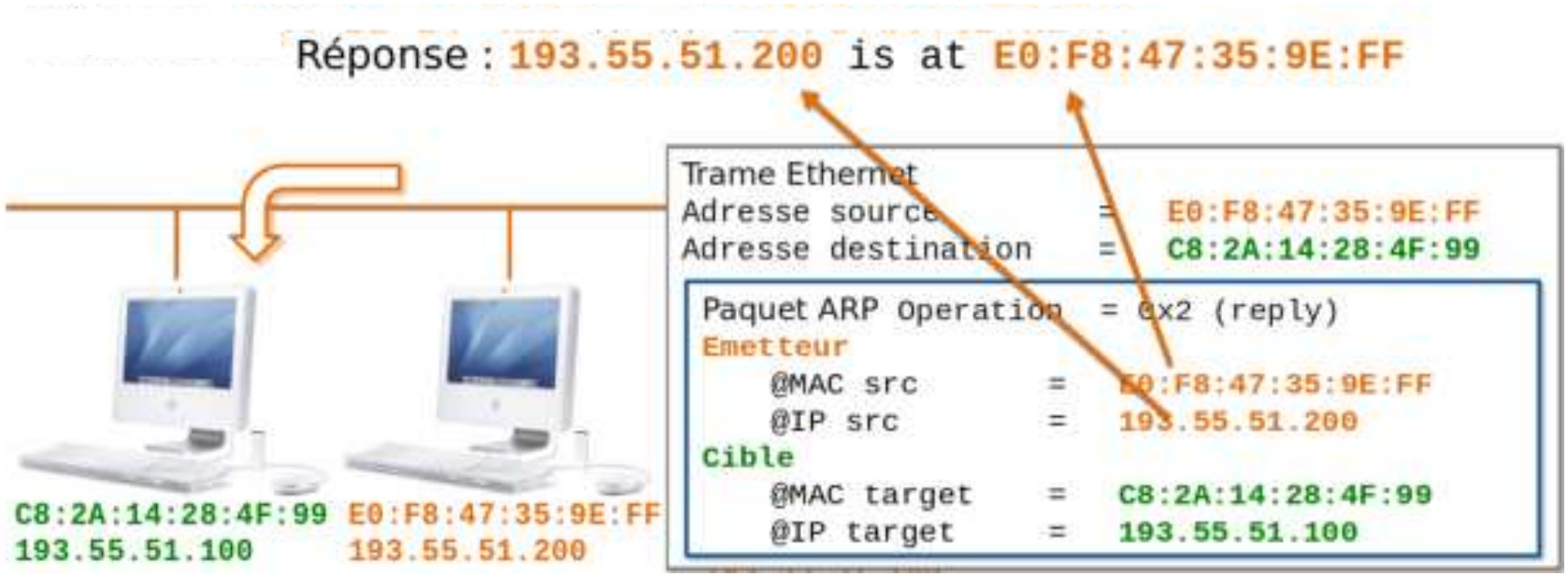
→ **Protocole Address Resolution Protocol (ARP)**

IUT2 Université Grenoble Alpes
Département INFO

Requête ARP


Requête : Who has 193.55.51.200 ? Tell 193.55.51.100
Trame Ethernet
Adresse source = C8:2A:14:28:4F:99
Adresse destination = FF:FF:FF:FF:FF:FF
Paquet ARP Operation = 0x1 (request)
Emetteur
@MAC src = C8:2A:14:28:4F:99
@IP src = 193.55.51.100
Cible
@MAC target = 00:00:00:00:00:00
@IP target = 193.55.51.200
C8:2A:14:28:4F:99
193.55.51.100
??:??:??:??:??:?
193.55.51.200

Réponse ARP


Réponse : 193.55.51.200 is at E0:F8:47:35:9E:FF
Trame Ethernet
Adresse source = E0:F8:47:35:9E:FF
Adresse destination = C8:2A:14:28:4F:99
Paquet ARP Operation = 0x2 (reply)
Emetteur
@MAC src = E0:F8:47:35:9E:FF
@IP src = 193.55.51.200
Cible
@MAC target = C8:2A:14:28:4F:99
@IP target = 193.55.51.100
C8:2A:14:28:4F:99
193.55.51.100
E0:F8:47:35:9E:FF
193.55.51.200

Nécessité d'une adresse IP

Tous les échanges sur le réseau reposent sur l'adresse IP.
Par exemple : `ping iut2-univ-grenoble-alpes.fr` provoquera une requête DNS qui renverra une adresse IP

Chaque adresse IP doit être liée à une adresse physique

Les adresses physiques sont choisies par le constructeur (adresse MAC)

Comment obtenir une adresse IP ?

1. Manuellement
   - Nécessite d'en obtenir une publique
   - Nécessite d'être administrateur de sa machine
   - Complexe pour le nomadisme
2. Dynamiquement
   - Obtention de la configuration IP par un serveur

   → Dynamic Host Configuration Protocol (DHCP)
   - Pas besoin d'être administrateur de sa machine

IUT2 Université Grenoble Alpes
Département INFO

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

DHCP

DHCP [Droms, 1997] permet de

- configurer *dynamiquement* (les paramètres réseau) d'une station connectée au sein d'un LAN.

DHCP est principalement utilisé pour distribuer des adresses IP sur un réseau

- filaire
- wifi

Conçu comme complément au protocole Bootstrap Protocol (BOOTP) utilisé pour installer des machines à travers un réseau [rfc, 1985].
BOOTP fonctionne en deux phases :

1. *address determination and bootfile selection*
2. *file transfer*

IUT2 Université Grenoble Alpes
Département INFO

DHCP entités et type d'allocation

DHCP suit un modèle client-serveur : les **serveurs DHCP** allouent des adresses réseau et fournissent des paramètres de configuration aux **clients** configurés dynamiquement.

DHCP se compose de deux éléments :

1. un **protocole applicatif** pour délivrer des paramètres de configuration spécifiques à un hôte
2. un mécanisme d'**allocation d'adresses** réseau aux hôtes.

DHCP prend en charge trois mécanismes d'attribution d'adresses IP

1. "allocation manuelle" (ou statique) $\rightarrow$ attribution d'une adresse IP par l'administrateur réseau (p.ex. en fonction de l'@Mac)
2. "allocation dynamique" $\rightarrow$ attribution d'une adresse IP pour une période limitée (bail)
3. "allocation automatique" $\rightarrow$ attribution dynamique d'une adresse IP permanente

Un réseau particulier utilisera un ou plusieurs de ces mécanismes, en fonction des politiques de l'administrateur réseau.

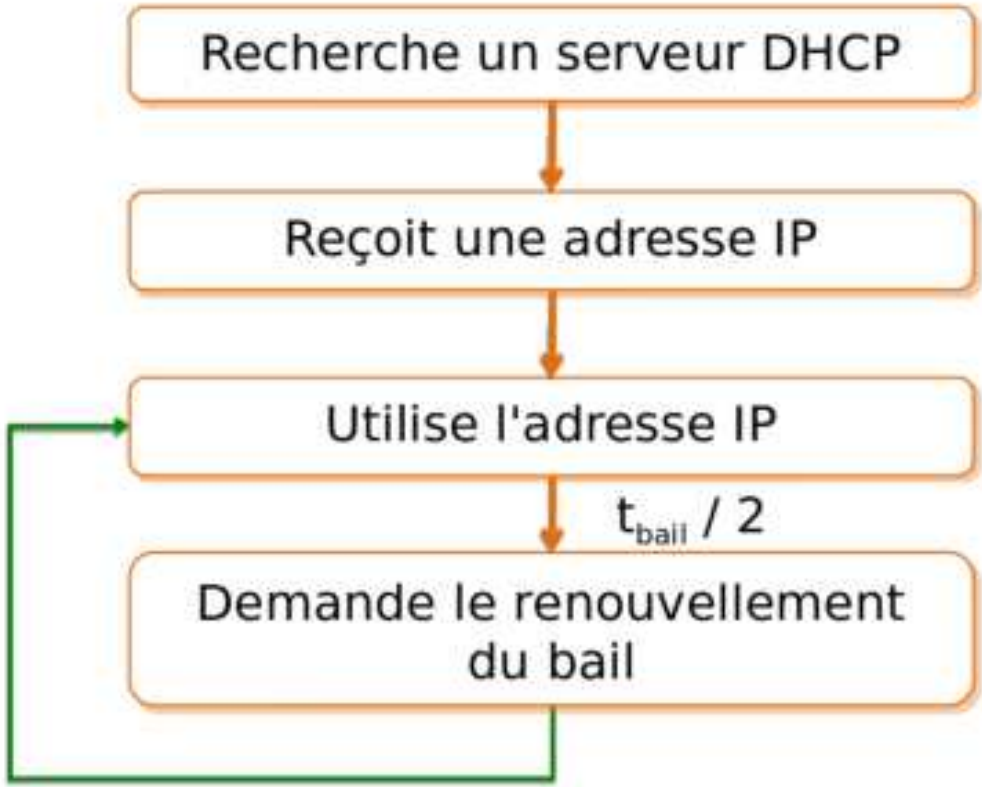
IUT2 Université Grenoble Alpes
Département INFO

Sommaire

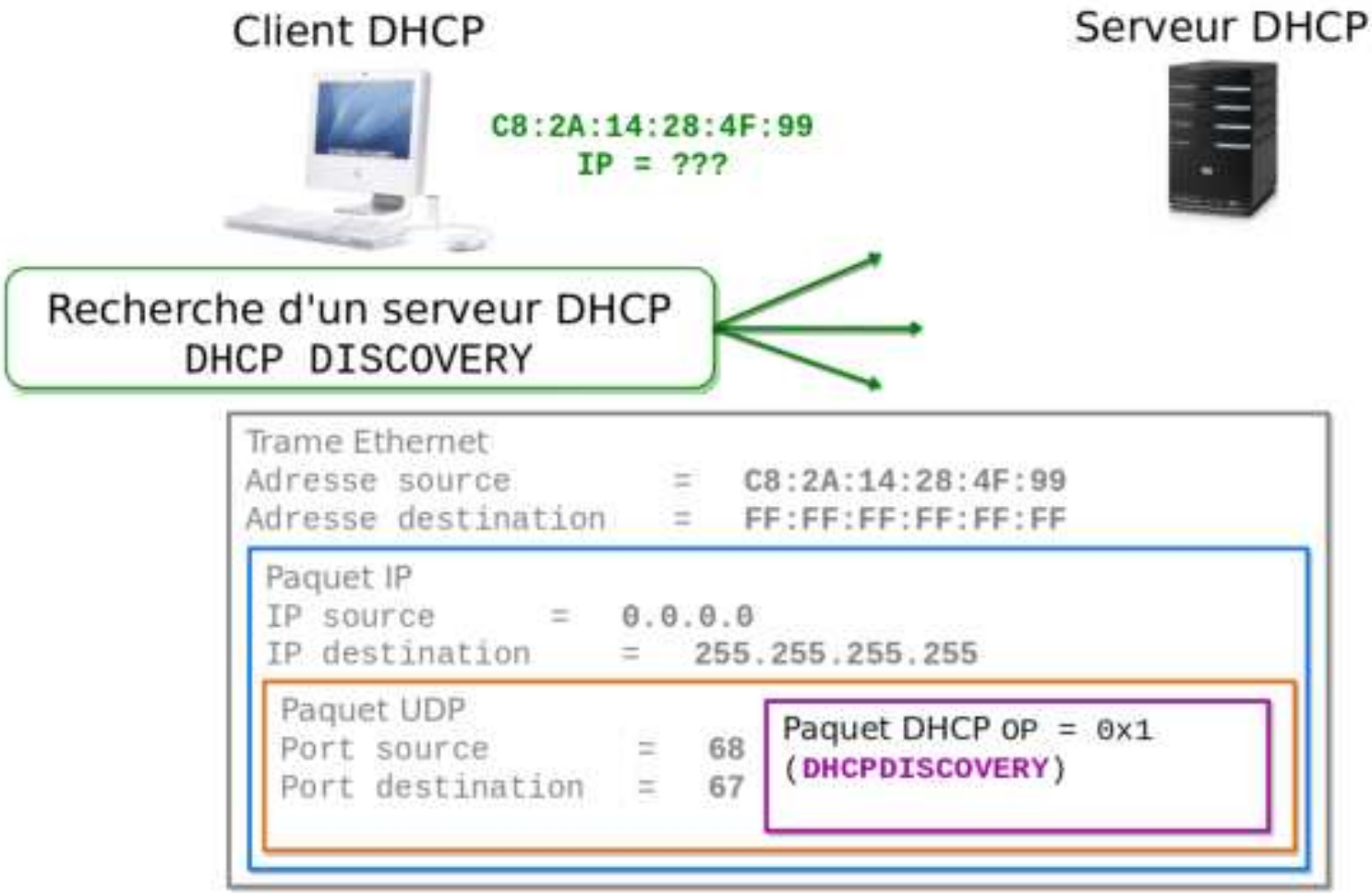
IUT2 Université Grenoble Alpes
Département INFO

DHCP principe

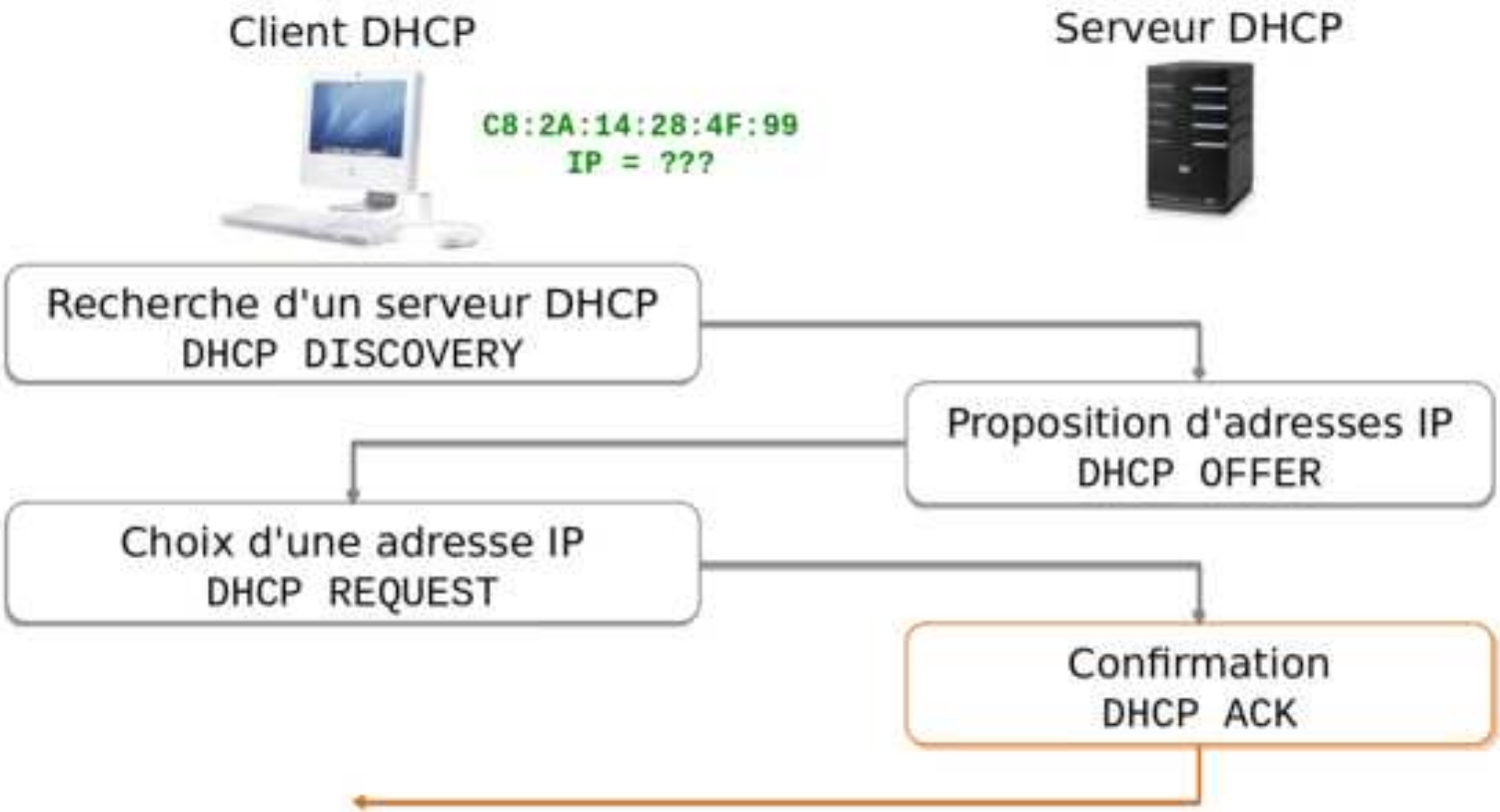
Client DHCP



DHCP échanges



DHCP échanges



Période de bail

En allocation dynamique, les adresses IP ne sont délivrées que sur une période limitée : **un “bail”**.

- Un client qui voit son bail arriver à terme peut demander au serveur une prolongation du bail par un DHCPREQUEST.
- Également le serveur émettra un paquet DHCPNAK pour demander au client s'il veut prolonger son bail. Si le serveur ne reçoit pas de réponse valide, il rend disponible l'adresse IP.

La durée des baux est fonction du nombre de machines connectées de la fréquence d'arrivée et départ des machines.

- Important de limiter le broadcast (DHCP repose principalement par broadcast) dans les réseaux de bande passante limitée.

IUT2 A
Université Grenoble Alpes
Département INFO

Configuration d'un serveur DHCP

- Plage d'adresses
  - IP du début
  - IP de fin
  - Masque
- Passerelle (gateway)
- Serveurs DNS (Adresse, domaine)
- Durée du bail
- Associations <@MAC, @IP>

IUT2 Université Grenoble Alpes
Département INFO

DHCP – Bilan

Dynamic Host Configuration Protocol

Assigne une configuration IP
IP, netmask, passerelle, DNS, etc.
Durée de vie limitée dans le temps (bail)

Couche application

Repose sur IP/UDP

Intérêt ?

Simplifie l'administration
Configuration automatique
Clients nomades
Gestion d'un pool d'adresses : économie
Modification du plan d'adressage

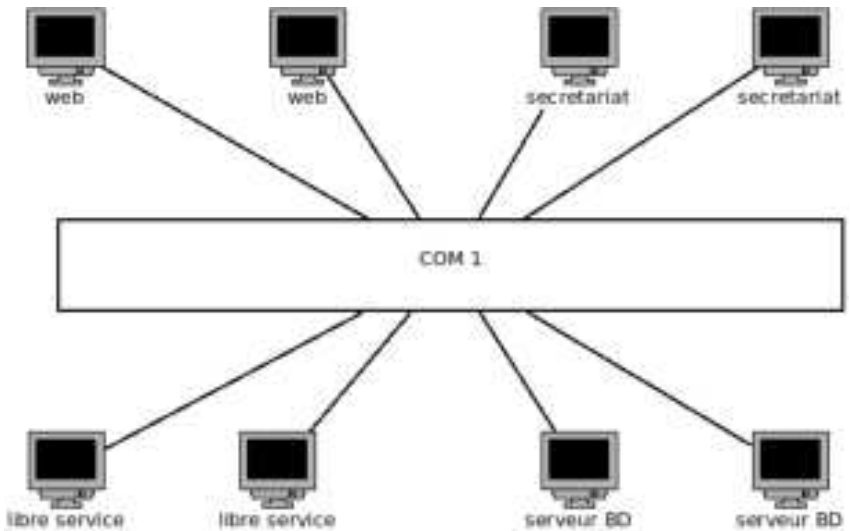
IUT2 A
Université Grenoble Alpes
Département INFO

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

Réseau exemple

Soit le Local Area Network (LAN) ci-dessous qui pourrait être celui d'une bibliothèque



Propriétés d'un tel réseau :

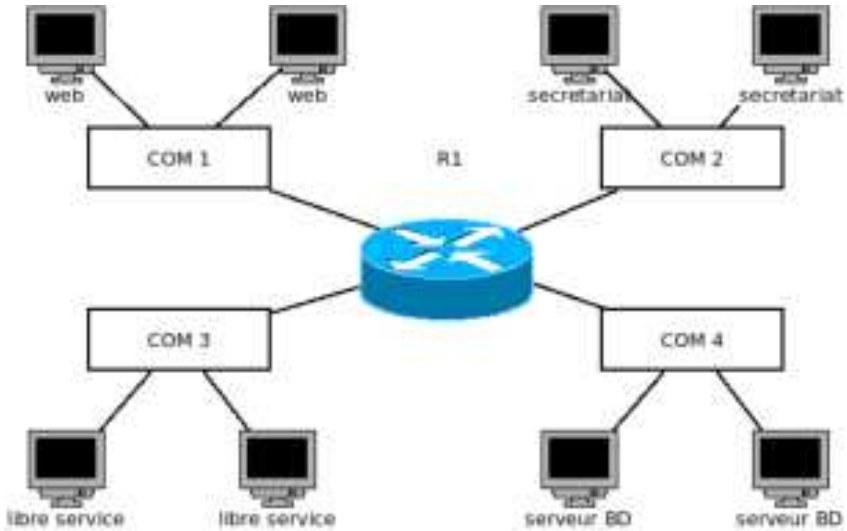
+ simple
- manque de sécurité (accès via web ou libre-service)
- trafic important → *broadcast* arrivant sur toutes les machines

Comment amener une meilleure isolation ?
→ faire des sous-réseaux

IUT2 Université Grenoble Alpes
Département INFO

Exemple avec des sous-réseaux.

Les sous-réseaux pourraient être implantés de la manière ci-dessous.



Propriétés d'un tel réseau :

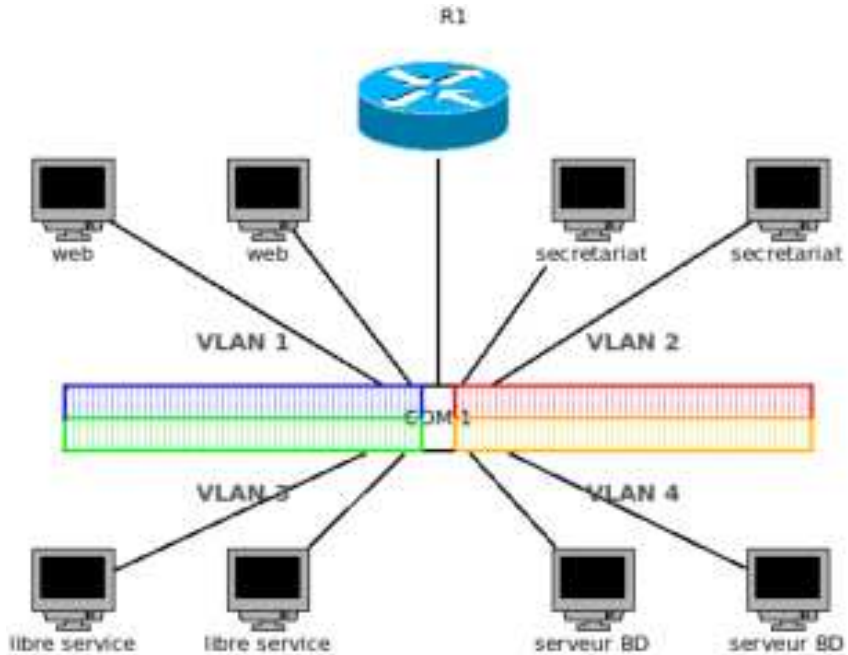
+ isolation des sous-réseaux
  - implique un coût important (achat matériel, maintenance, espace, énergie)
  - difficile à configurer

→ utiliser un seul commutateur avec des réseaux locaux virtuels (VLAN)

IUT2 Université Grenoble Alpes
Département INFO

Exemple avec des VLANs

En isolant les ports à l'"intérieur" du commutateur on peut obtenir :



Propriétés d'un tel réseau :

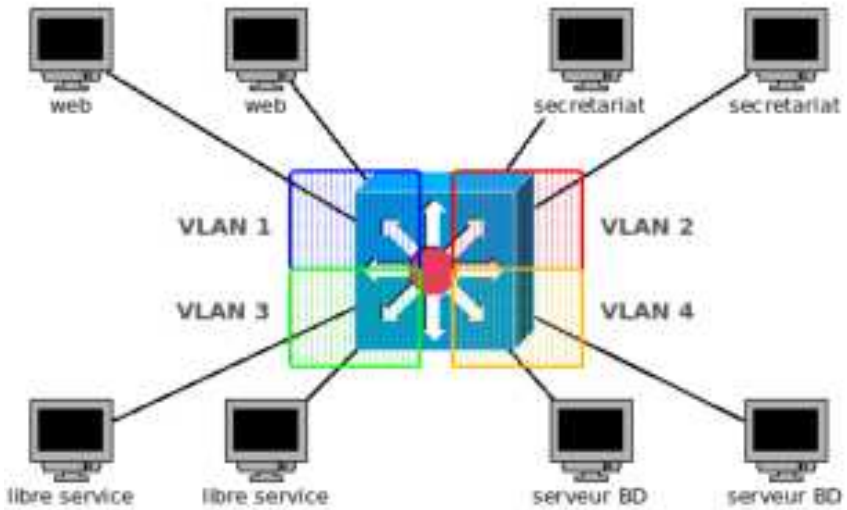
- \+ séparation des sous-réseaux au niveau des ports (*broadcast* et sécurité)
- \+ Un seul commutateur est utilisé
- \+ grande flexibilité (modification des machines), facile à configurer

→ toujours besoin d'un routeur pour gérer la communication entre Virtual Local Area Network (VLAN)s

IUT2 Université Grenoble Alpes
Département INFO

Exemple avec des VLANs et un switch2-3

En utilisant un switch 2-3 :



Propriétés d'un tel réseau :

+ Séparation des sous-réseaux au niveau des ports (*broadcast* et sécurité).
+ Un seul matériel est utilisé qui joue le rôle de commutateur **ET** routeur.
+ Grande flexibilité (modification des machines), facile à configurer.

IUT2 Université Grenoble Alpes
Département INFO

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

Qu'est-ce qu'un VLAN ? Un switch 2-3 ?

- Réseau local virtuel (VLAN : Virtual Local Area Network) :
  - Réseau local : technologie Ethernet (ou Wi-Fi).
  - Virtuel : dissociation entre la structure matérielle du réseau et la définition de réseaux IP.
  - Principe : diviser un réseau local (physique) en plusieurs réseaux logiques (IP) appelés VLAN.
  - Équipements permettant les VLANs : certains commutateurs et le switch2-3.

- Le switch2-3 (ou commutateur-routeur, ou switch multi-niveau). Il assure à la fois :
  - Une fonction de commutation Ethernet (niveau 2 de la couche OSI = niveau liaison).
  - Une fonction de routage IP (niveau 3 de la couche OSI = réseau).

IUT2 A
Université Grenoble Alpes
Département INFO

Pourquoi créer des VLANs ?

Améliorer la bande passante.

- LAN avec beaucoup de stations → un grand domaine de diffusion (*broadcast*).
- Périphériques sont exposés à un grand nombre de messages de broadcast ce qui nécessite un temps de traitement important.
- Un LAN de 500 stations sera plus encombré que 10 VLANs de 50 stations.

Améliorer la sécurité.

- Les attaques utilisant le broadcast sont contenues au sein d'un VLAN (*ARP cache poisoning*, *DHCP spoofing*, attaque *smurf*, *MAC table overflow*).
- Les VLANs peuvent être connectés via des routeurs et des pare-feux.

Faciliter la gestion.

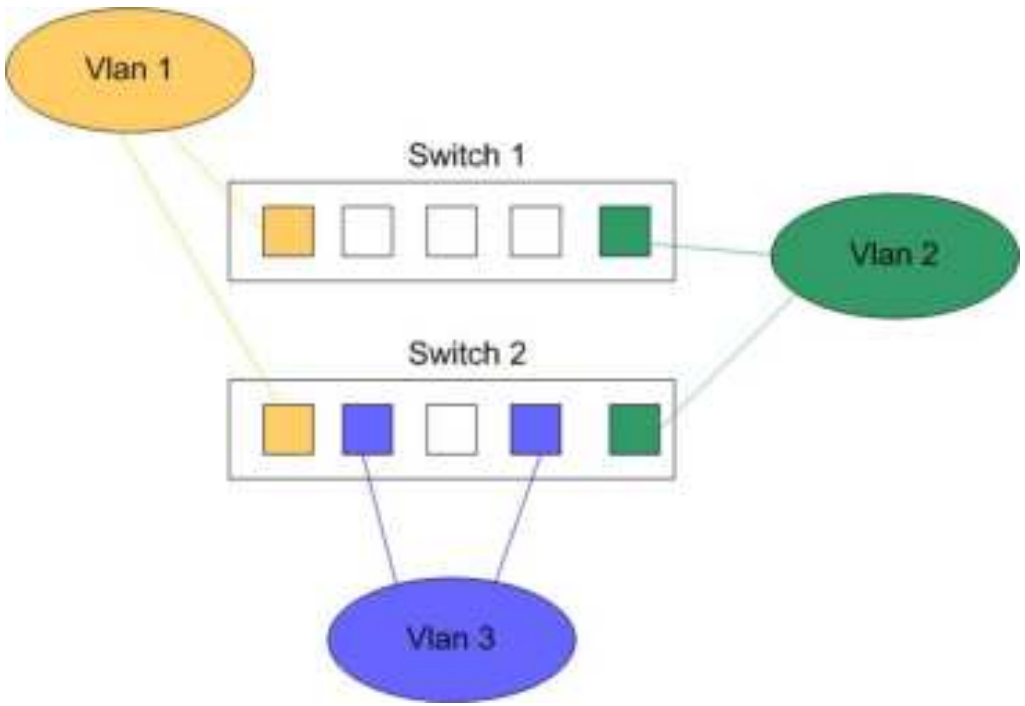
- Flexibilité de définition de VLANs, moins de matériel à maintenir.
- Séparation logique en fonction des départements ou des groupes de travail ou toute autre logique.
- Amélioration de la QoS : On peut favoriser certains VLANs plus que d'autres (priorité)

IUT2 Université Grenoble Alpes
Département INFO

VLAN de niveau 1

Répartition des stations dans les VLANs en fonction des ports des commutateurs :

- Mise en place simple sauf si les VLANs sont sur plusieurs switchs (utiliser 802.1Q).
- Très bonne sécurité.



Source : http ://www-igm.univ-mlv.fr/ dr/XPOSE2006/SURZUR-DEFRANCE/vlan.html

IUT2 Université Grenoble Alpes
Département INFO

VLAN de niveaux 2 et 3

Niveau 2 : chaque VLAN est défini par la liste des **@MAC des stations**.

- Configuration centralisée entre commutateurs.
- Sécurité moyenne (usurpation d'@MAC)

Niveau 3 : chaque VLAN est défini par son **@IP de réseau**.

- Appartenance automatique d'une station par son @IP (mais plus lent, car niveau 3).
- Sécurité faible (usurpation d'@IP).

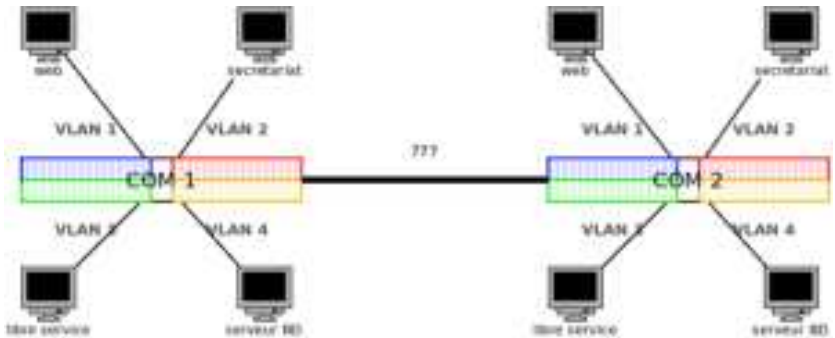
IUT2 Université Grenoble Alpes
Département INFO

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

Exemple avec des VLANS

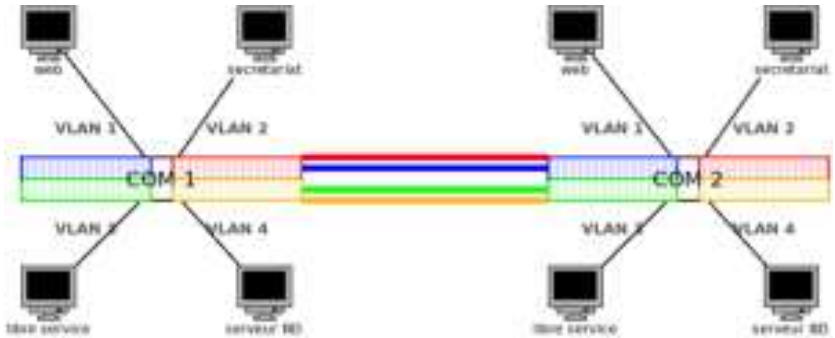
Les VLANs sont souvent repartis sur plusieurs équipements :



Comment faire passer le trafic de plusieurs VLAN entre plusieurs commutateurs

IUT2 A
Université Grenoble Alpes
Département INFO

Vlan sur deux commutateurs : solution inefficace

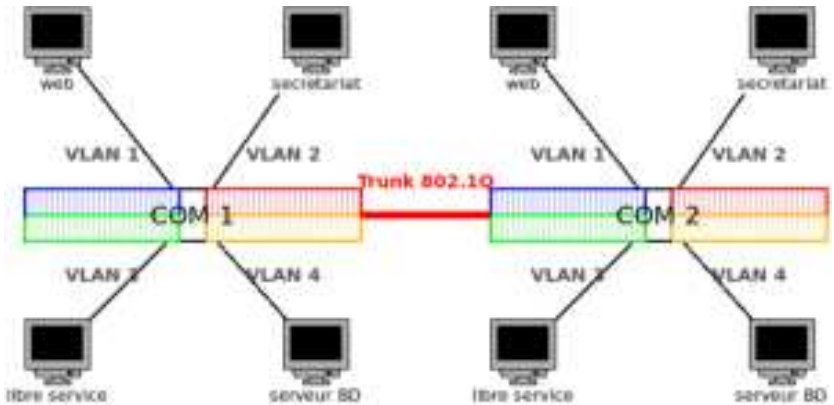


Solution stupide : on sacrifie 4 ports par commutateur pour faire passer le trafic de chaque VLAN.

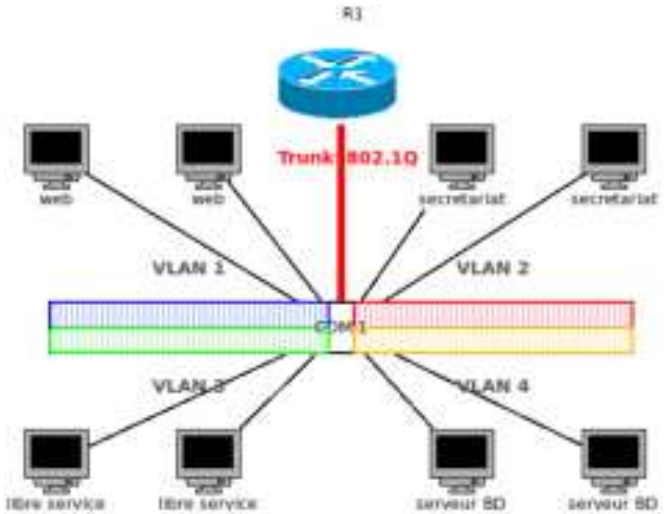
Est-ce que cela passe à l'échelle ?

IUT2 Université Grenoble Alpes
Département INFO

Exemple avec des VLANS



ou

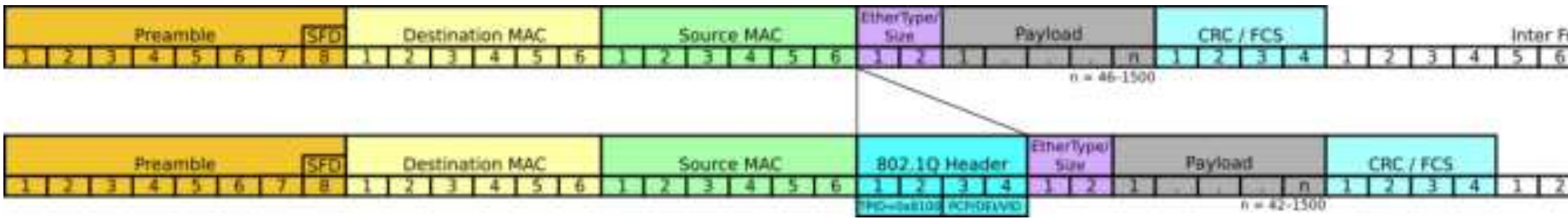


Comment faire passer le trafic de plusieurs VLAN sur **un seul port** ?
→ Utiliser des *balises* dans la trame Ethernet qui vont "marquer" le numéro du VLAN : c'est la **trame 802.1q**

IUT2 Université Grenoble Alpes
Département INFO

Format de trame 802.1q

Le standard IEEE 802.1Q [IEEE, 1999] définit le contenu de la balise de VLAN (VLAN tag) qui complète l'en-tête de trame Ethernet avec 4 octets supplémentaires.

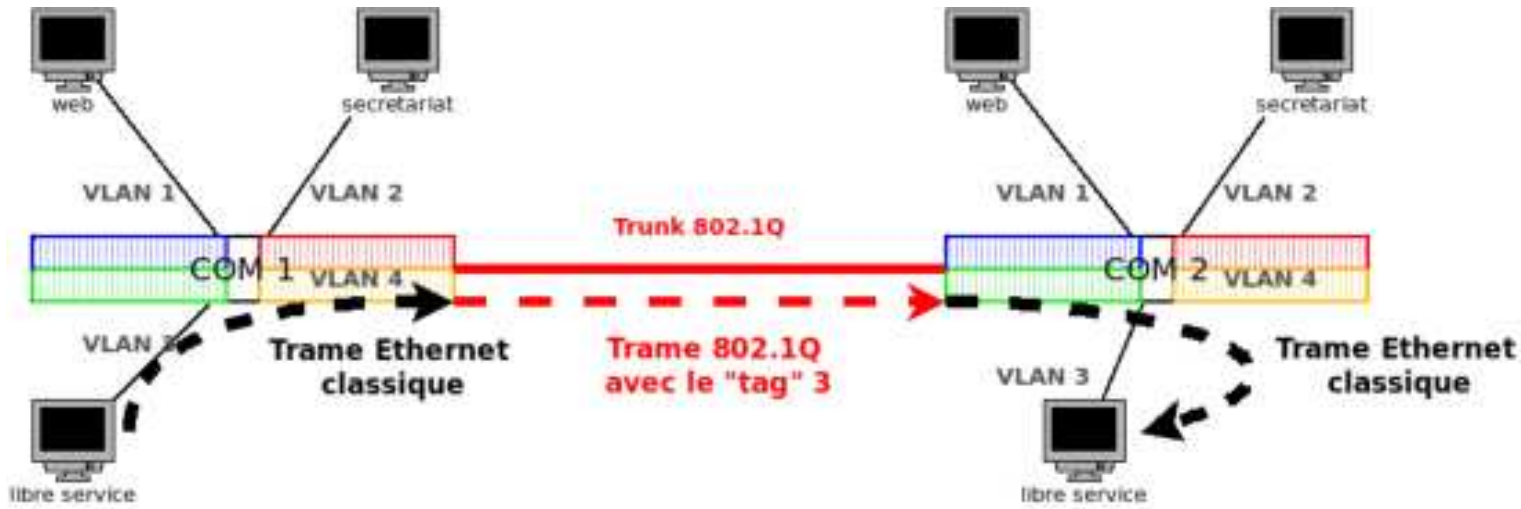


Source : wikipedia

- **Champ TPID = 0x8100** pour identifier le mode « tagged trame » du protocole 802.1Q.
  Il permet aussi de le différencier des trames Ethernet simples qui ont juste le champ Type.
- Une trame 802.1Q a une taille maximale de 1522 octets au lieu de 1518 pour une trame Ethernet classique.
- Le champ FCS est recalculé après l'insertion de la balise de VLAN.

IUT2 Université Grenoble Alpes
Département INFO

Exemple utilisation des balises



1. La station du VLAN3 génère une trame Ethernet classique qui arrive au commutateur COM1
2. le commutateur COM1 devant envoyer la trame à travers un trunk (tronc) 802.1Q, va réécrire la trame Ethernet comme une trame 802.1Q ajoutant l'identifiant du VLAN 3.
3. le commutateur COM2 récupère la trame, analyse à quel VLAN et port elle est destinée et réécrit la trame Ethernet en supprimant la partie 802.1Q.

Toute l'opération est transparente pour les stations

IUT2 Université Grenoble Alpes
Département INFO

Capture trame 802.1q

```
Frame 103 (1518 bytes on wire, 1518 bytes captured)
Ethernet II, Src: 00:14:f2:75:ed:72, Dst: 00:10:5a:de:9d:d7
    Destination: 3com_de:9d:d7 (00:10:5a:de:9d:d7)
    Source: Cisco_75:ed:72 (00:14:f2:75:ed:72)
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0011 = ID: 11
    Type: IP (0x0800)
Internet Protocol, Src: 172.17.0.2 (172.17.0.2), Dst: 172.16.80.19 (172.16.80.19)
Transmission Control Protocol, Src Port: www (80), Dst Port: 1548 (1548)
```

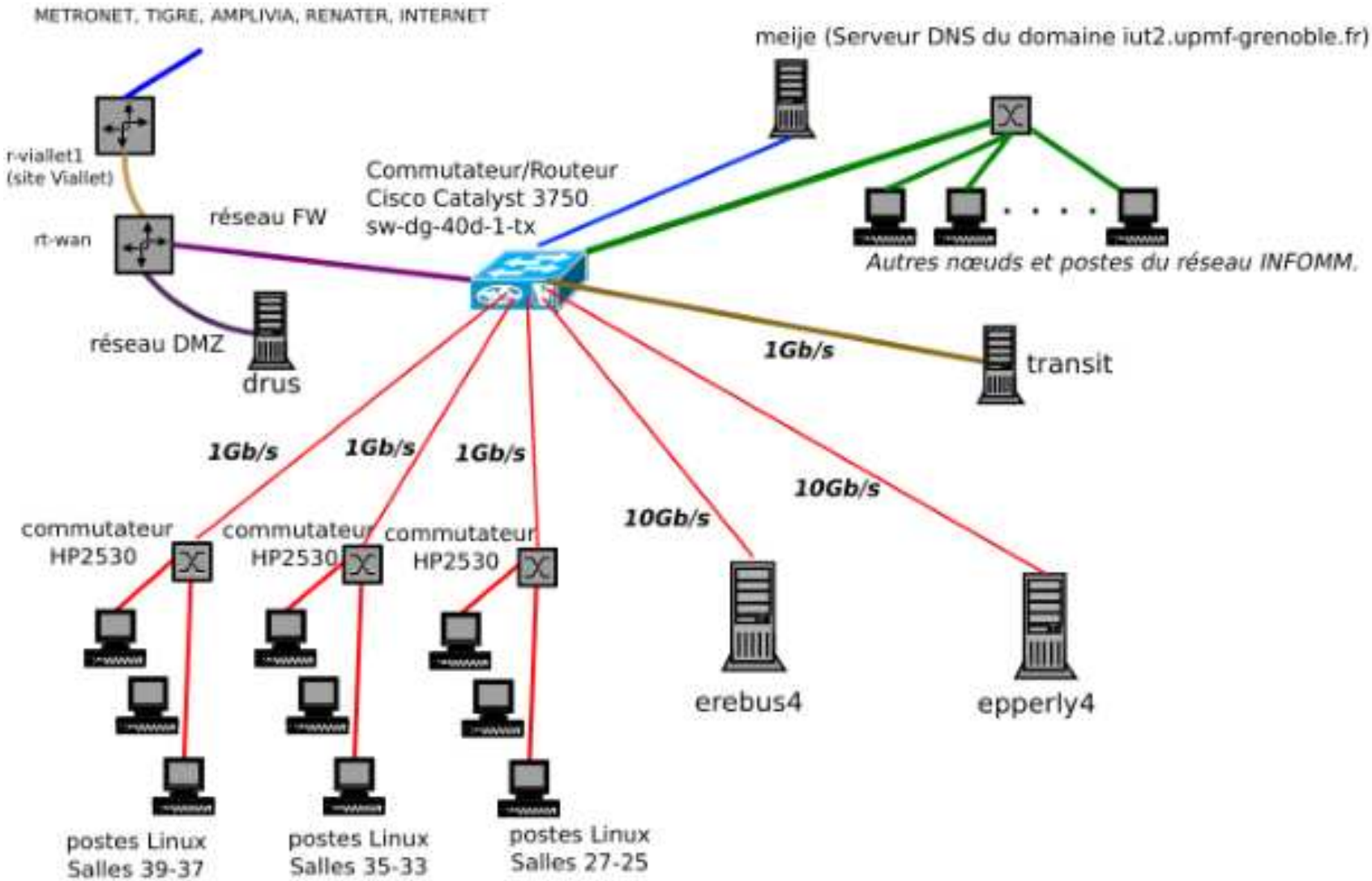
- Type : la valeur 0x8100 désigne une trame "taggée" IEEE 802.1Q.
- Priority : Code sur 3 bits 8 niveaux de priorités entre trames (standard IEEE 802.1P).
- CFI (Canonical Format Identifier) : un seul bit, 0 pour Ethernet standard, 1 pour un autre format.
- ID (VLAN Identifier) : Champ de 12 bits sert à identifier le réseau local virtuel auquel appartient la trame.
  Il est théoriquement possible de coder 4094 ($2^{12} - 2$) identifiants de VLAN.

IUT2 Université Grenoble Alpes
Département INFO

Sommaire

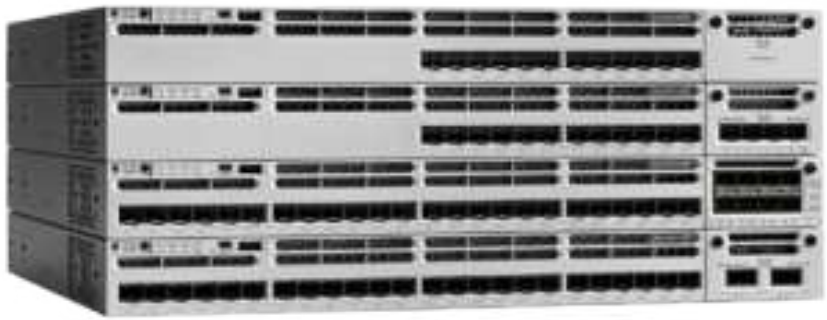
IUT2 Université Grenoble Alpes
Département INFO

Le switch2-3 de l'IUT2



Le switch2-3 de l'IUT2

Cisco Catalyst WS-C3850-24T-L



Quelques propriétés

- Rackable, 1 Rack Unit
- 24 ports Ethernet 10/100/1000
- Deux ports 10 Gigabit Ethernet ou quatre ports 10 Gigabit Ethernet
- Support logiciel pour le routage IPv4 et IPv6, routage multicast, QoS modulaire

IUT2 Université Grenoble Alpes
Département INFO

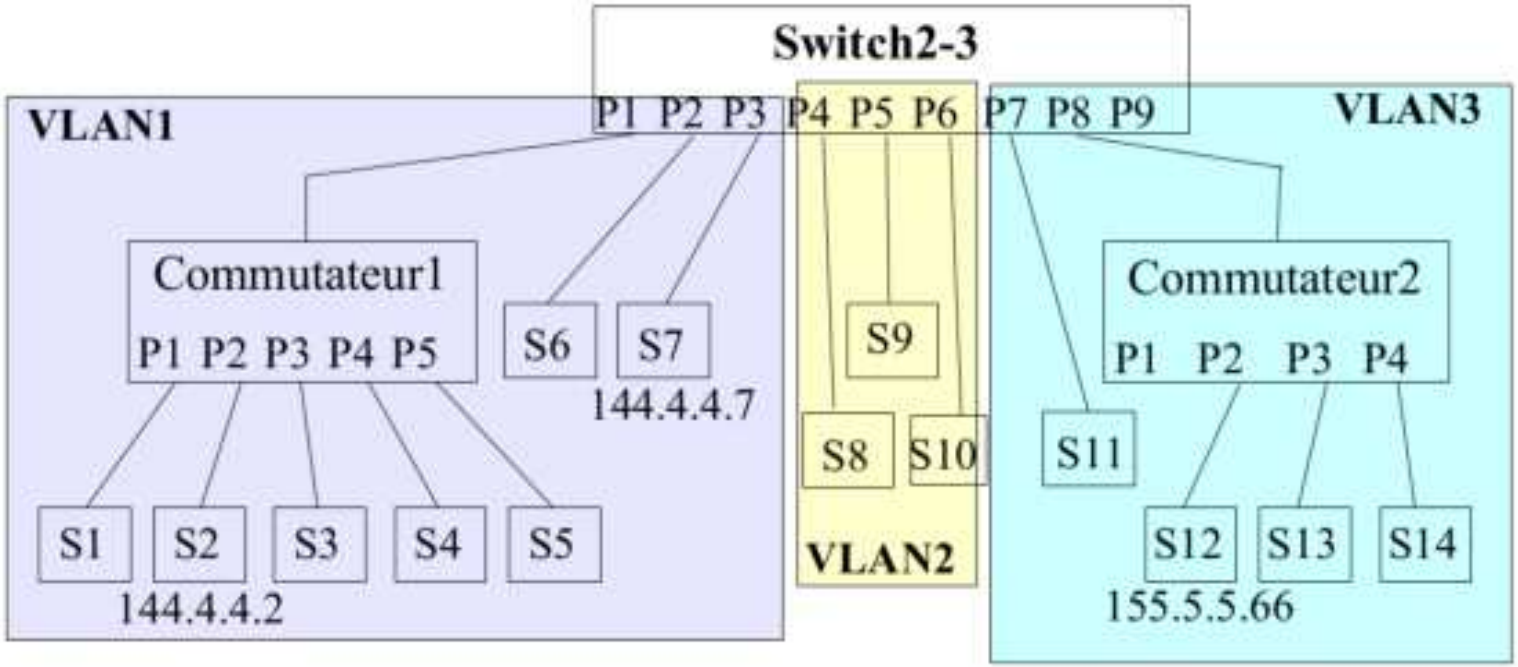
Principe de fonctionnement

Un switch2-3 permet de répartir les stations qui lui sont connectées en plusieurs réseaux IP virtuellement indépendants (VLANs)

- Un VLAN fonctionne comme un réseau local Ethernet : les stations d'un même VLAN font partie du même réseau Ethernet (et donc du même réseau IP).
- Chaque VLAN étant un réseau IP, il a une adresse de réseau IP et un espace d'adresses IP avec une @IP par station qui en fait partie, plus une @IP pour le switch2-3.
- Le switch2-3 utilise la commutation Ethernet pour faire communiquer les stations d'un même VLAN (table de commutation : N° de ports du switch $\leftrightarrow$ adresses MAC).
- Pour les échanges entre stations de VLANs différents, le switch2-3 utilise le routage IP (table de routage, @ IP).

IUT2 Université Grenoble Alpes
Département INFO

Exemple de configuration statique



Trois VLANs :

1. VLAN1 : (P1, P2, P3) @IP :144.4.4.0/24
2. VLAN2 : (P4, P5, P6) @IP :155.5.5.32/27
3. VLAN3 : (P7, P8, P9) @IP : 155.5.5.64/26

IUT2 Université Grenoble Alpes
Département INFO

Adresses du switch2-3

C'est un routeur IP : il a donc autant d'adresses IP que de réseaux VLAN IP qu'il définit :

- @IP dans le VLAN1 : 144.4.4.32
- @IP dans le VLAN2 : 155.5.5.48
- @IP dans le VLAN3 : 155.5.5.65

À ces adresses IP sont associées des adresses MAC :

- @MAC (P1, P2, P3) : `00:0d:29:e3:63:44`
- @MAC (P4, P5, P6) : `00:0d:29:e3:63:45`
- @MAC (P7, P8, P9) : `00:0d:29:e3:63:46`

IUT2 Université Grenoble Alpes
Département INFO

Tables du switch2-3

Table de commutation utilisée pour tous les échanges entre stations d'un même VLAN (équivalente à 3 tables de commutation).

@MAC dest	n° port
@MAC S1 à S5	P1
@MAC S6	P2
@MAC S7	P3
@MAC S8	P4
@MAC S9	P5
@MAC S10	P6
@MAC S11	P7
@MAC S12 à S14	P8

Table de routage pour les autres échanges :

Destination	Gateway	Genmask	Iface
144.4.4.0	0.0.0.0	255.255.255.0	vlan1
155.5.5.32	0.0.0.0	255.255.255.224	vlan2
155.5.5.64	0.0.0.0	255.255.255.192	vlan3

IUT2 Université Grenoble Alpes
Département INFO

Routage depuis une station

Les tables de routage des stations du **VLAN1** sont de la forme :

Destination	Gateway	Genmask	Iface
144.4.4.0	0.0.0.0	255.255.255.0	eth0
0.0.0.0	144.4.4.32	0.0.0.0	eth0

Les tables de routage des stations du **VLAN2** sont de la forme :

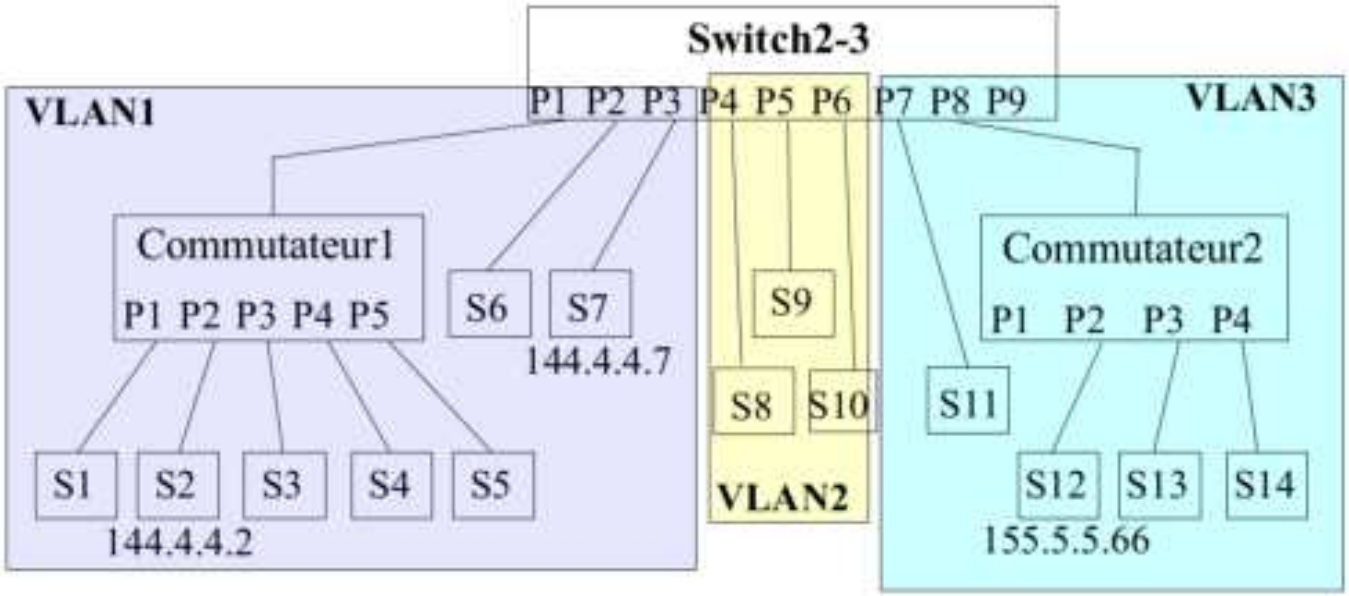
Destination	Gateway	Genmask	Iface
155.5.5.32	0.0.0.0	255.255.255.224	eth0
0.0.0.0	155.5.5.48	0.0.0.0	eth0

Les tables de routage des stations du **VLAN3** sont de la forme :

Destination	Gateway	Genmask	Iface

IUT2 Université Grenoble Alpes
Département INFO

Fonctionnement du switch2-3 : commutation ou routage ?

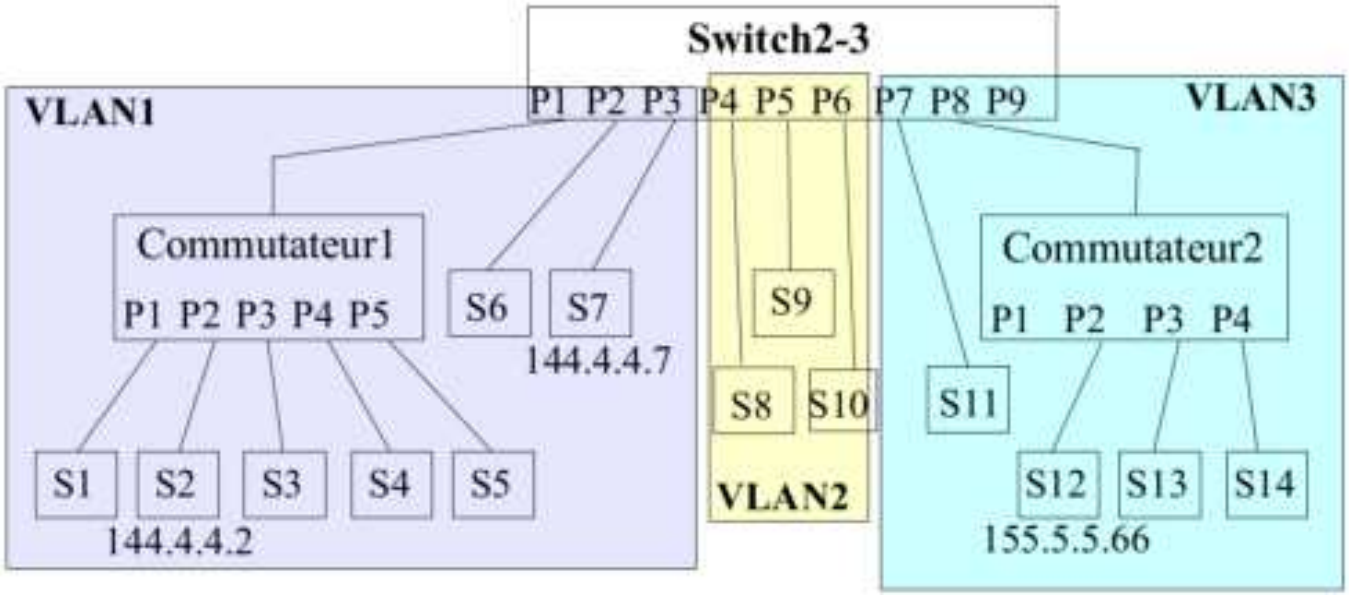


Cas 1 : S2 envoie un paquet à S7 :

- Sa table de routage indique que le « gateway » est elle-même.
- S2 envoie donc directement une trame dont l'adresse destination Ethernet est l'adresse de S7.
- Le switch2-3 reçoit une trame dont il n'est pas le destinataire : il utilise donc sa table de commutation pour envoyer cette trame sur le port 3 où est situé S7.

IUT2 Université Grenoble Alpes Département INFO

Fonctionnement du switch2-3 : commutation ou routage ?



Cas 2 : S2 envoie un paquet à S12 :

- Sa table de routage lui indique que le « gateway » est le switch2-3 d'adresse IP 144.4.4.32.
- S2 envoie donc une trame Ethernet dont l'adresse destination est l'adresse MAC du switch2-3 (`00:0d:29:e3:63:46`) sur le réseau 144.4.4.0.
- Le switch2-3 va faire appel à sa table de routage IP pour pouvoir acheminer ce paquet vers S12.

IUT2 Université Grenoble Alpes
Département INFO

Sommaire

IUT2 Université Grenoble Alpes
Département INFO

Résolution de Nom, pourquoi est-ce nécessaire ?

Pour transporter du flux HTTP, IP doit obtenir une adresse IP source et destination.

Il faudrait donc connaître l'ensemble des adresses IP des serveurs auxquels on souhaite accéder.

Cependant, une adresse IP est difficile à retenir. Par exemple, à quoi correspond ?

151.101.130.132	Debian debian.org
195.83.24.194	IUT 2 iut2.univ-grenoble-alpes.fr
213.36.253.103	linuxfr linuxfr.org

...Plus facile de mémoriser un nom qu'un numéro !

IUT2 Université Grenoble Alpes
Département INFO

Principe élémentaire du service de résolution de nom

Associe un nom à une machine
Retrouve l'adresse IP à partir du nom
Résolution de nom
Repose sur une table de correspondance <**Nom, adresse IP**>
Exemple : `ping epperly2`

IUT2 Université Grenoble Alpes
Département INFO

fichier *hosts*

Création d'alias sur une adresse IP (p.ex. fichier `/etc/hosts`) :

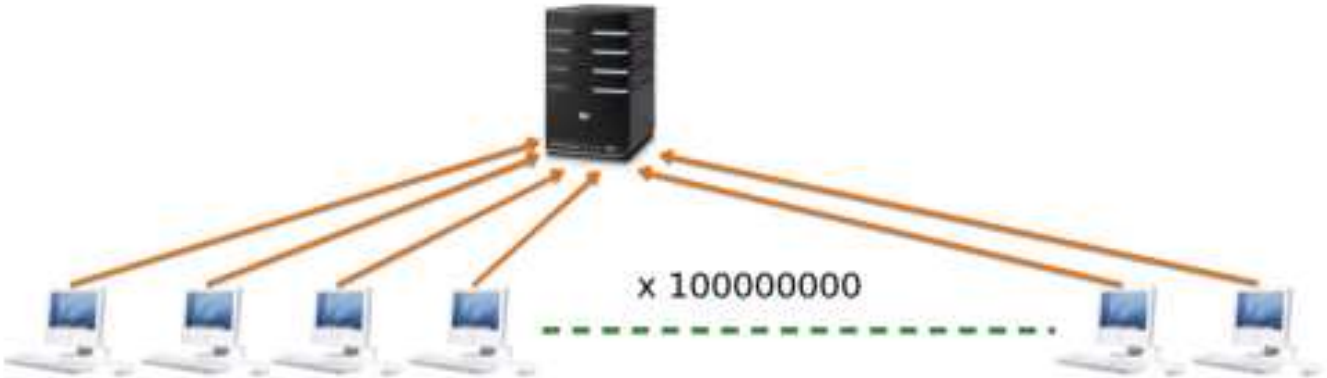
```
127.0.0.1         localhost
151.101.130.132   debian
213.36.253.103    linuxfr
```

Cependant, le fichier hosts est limité, car

- Maintenance du fichier :
  $\rightarrow$ taille du fichier 2^{32} adresses IPv4 + 2^{128} adresses IPv6
  $\rightarrow$ service fermé, transféré ou nouveau : fichier hosts trop difficile à maintenir manuellement
- la machine idéale n'est pas toujours la même (mobilité)

IUT2 A
Université Grenoble Alpes
Département INFO

serveur centralisé



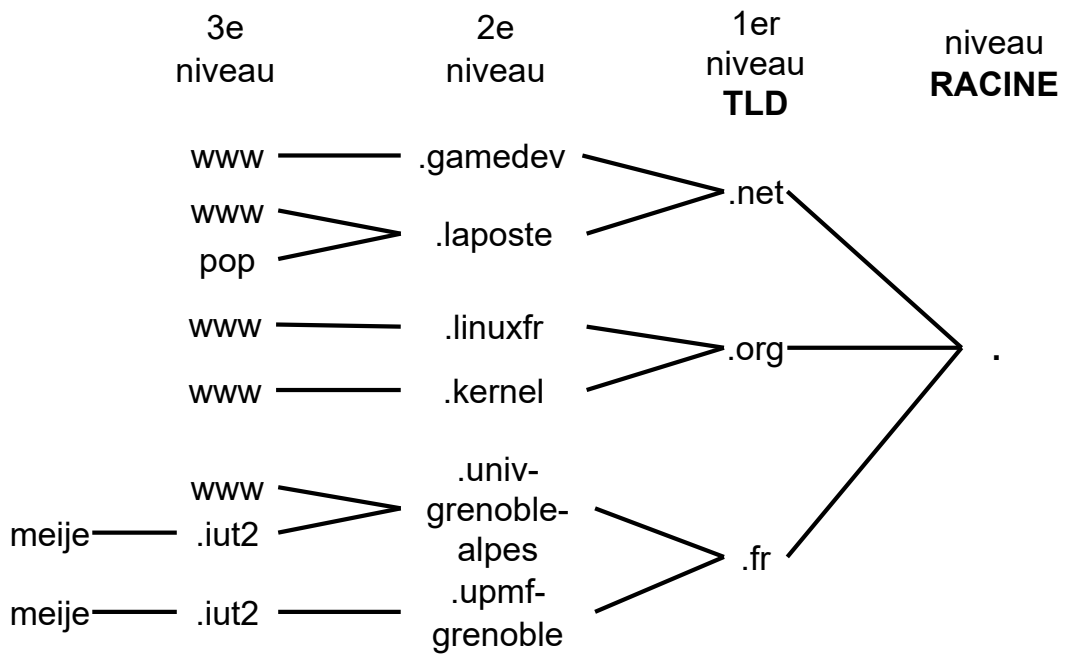
+ Facilite la maintenance
- Ne passe pas à l'échelle
  - Taille de la table
  - Charge et temps de réponse
  - Panne

Création d'un système unifié de nommage hiérarchique et d'association de nom → IP : le Domain Name System (DNS) [rfc, 1983a, rfc, 1983b]

IUT2 Université Grenoble Alpes
Département INFO

DNS un système hiérarchique et distribué

Caractéristiques : Structure arborescente de l'espace de nom
Organisation en domaines et sous-domaines
Base distribuée



Nom = position dans l'arbre
Nœud ≈ Serveur DNS
Feuille = Machine(s)

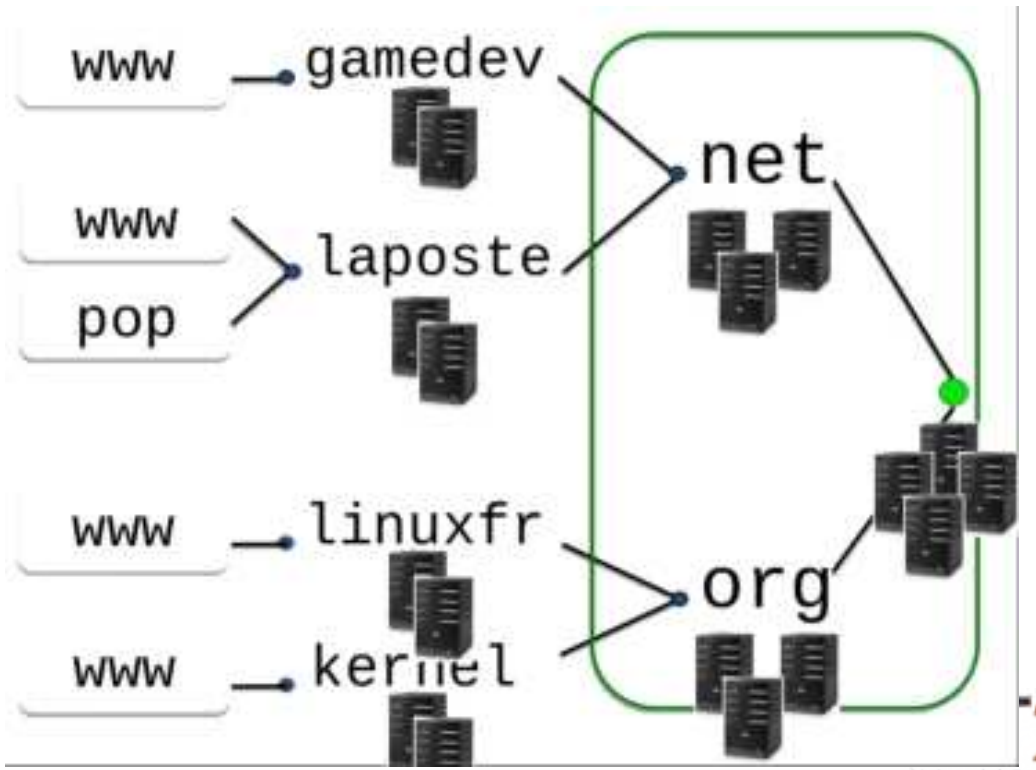
Exemple :
www.gamedev.net
www.laposte.net
pop.laposte.net

IUT2 Université Grenoble Alpes
Département INFO

DNS : Top-Level Domain (TLD)

Racine : liaison entre domaines de premier niveau
Par exemple :
.net et **.org** $\Rightarrow$ sont des **Top-Level Domain (TLD)**

Le domaine racine est noté **"."**



Université Grenoble Alpes
Département INFO

Nom de Domaine

Un nom de domaine (ou Domain Name (DN)) est un alias sur une (ou plusieurs) adresse(s) IP.

```
linuxfr.org -> 213.36.253.103
debian.org -> 151.101.130.132, 151.101.66.132, 151.101.2.132, 15
```

Un DN est plus simple à retenir et référencer qu'une adresse IP.

par exemple `www.univ-grenoble-alpes.fr`
LOGIN@univ-grenoble-alpes.fr
réfèrent tous les deux au nom de domaine `univ-grenoble-alpes.fr`

Un domaine peut créer des sous-domaines :
`iut2.univ-grenoble-alpes.fr`
→ `iut2` est un sous-domaine qui dépend entièrement du domaine principal

Pour consulter des noms de domaine → `whois`

IUT2 Université Grenoble Alpes
Département INFO

Nom de domaine pleinement qualifié

Le nom doit être un Fully Qualified Domain Name (FQDN) qui doit contenir l'ensemble des domaines supérieurs.

- `www.laposte.net.` est un FQDN
- `www.laposte` n'est pas un FQDN
- `www.net` n'est pas un FQDN

Dans le DNS, le FQDN est ponctué par un point final `.`, qui représente le domaine racine

IUT2 A
Université Grenoble Alpes
Département INFO

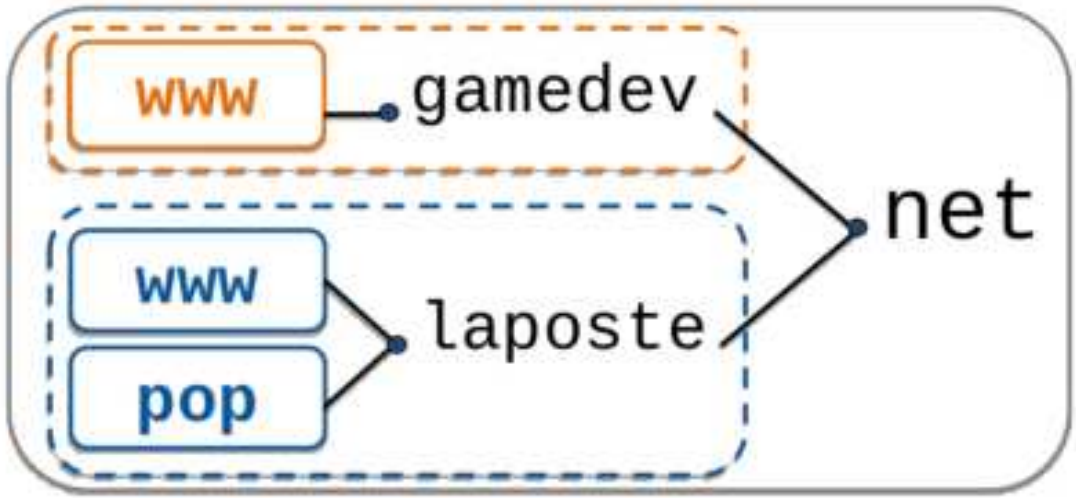
Sommaire

IUT2 A
Université Grenoble Alpes
Département INFO

DNS organisation hiérarchique : feuilles

=> nom de machine associée à un sous-domaine

ex. `www.gamedev.net = 64.91.255.13`



Exemple

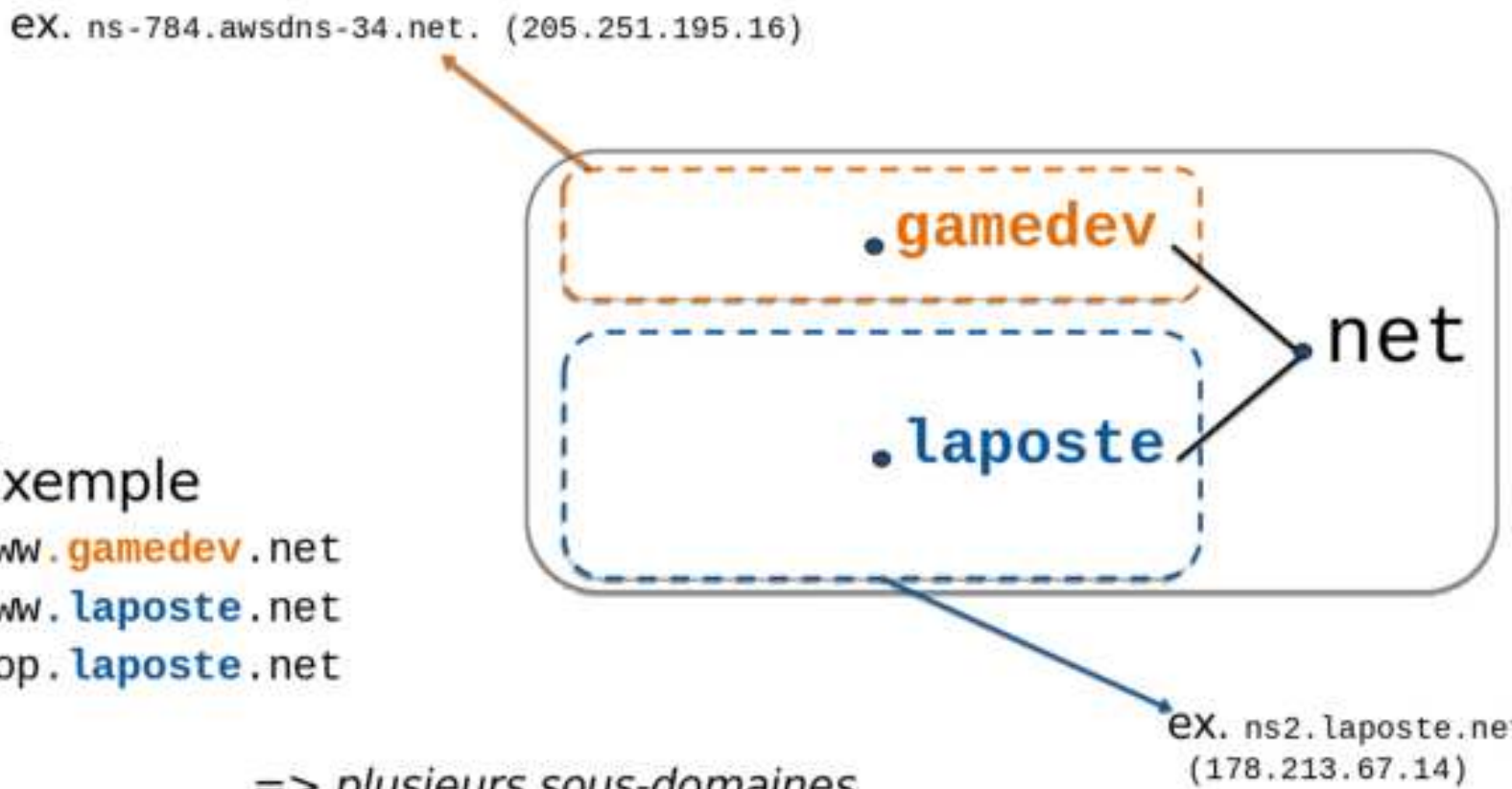
`www.gamedev.net`
`www.laposte.net`
`pop.laposte.net`

ex.
```
www.laposte.net = 130.193.27.21
pop.laposte.net = 194.117.213.10
```

Quelle(s) machine(s) gère l'association entre les noms et les adresses IP ?

IUT2 Université Grenoble Alpes
Département INFO

DNS organisation hiérarchique : serveurs DNS



Exemple

www.gamedev.net
www.laposte.net
pop.laposte.net

=> *plusieurs sous-domaines*

=> *différents serveurs DNS par sous-domaine*

IUT2 Université Grenoble Alpes
Département INFO

DNS : notion de zoning

Comment administrer les DN ?

→ Quand on cherche une IP, on interroge un serveur DNS.

→ Les serveurs DNS contiennent les informations (associations nom ↔ IP) de leur **zone**

→ Ces informations sont stockées dans un fichier.

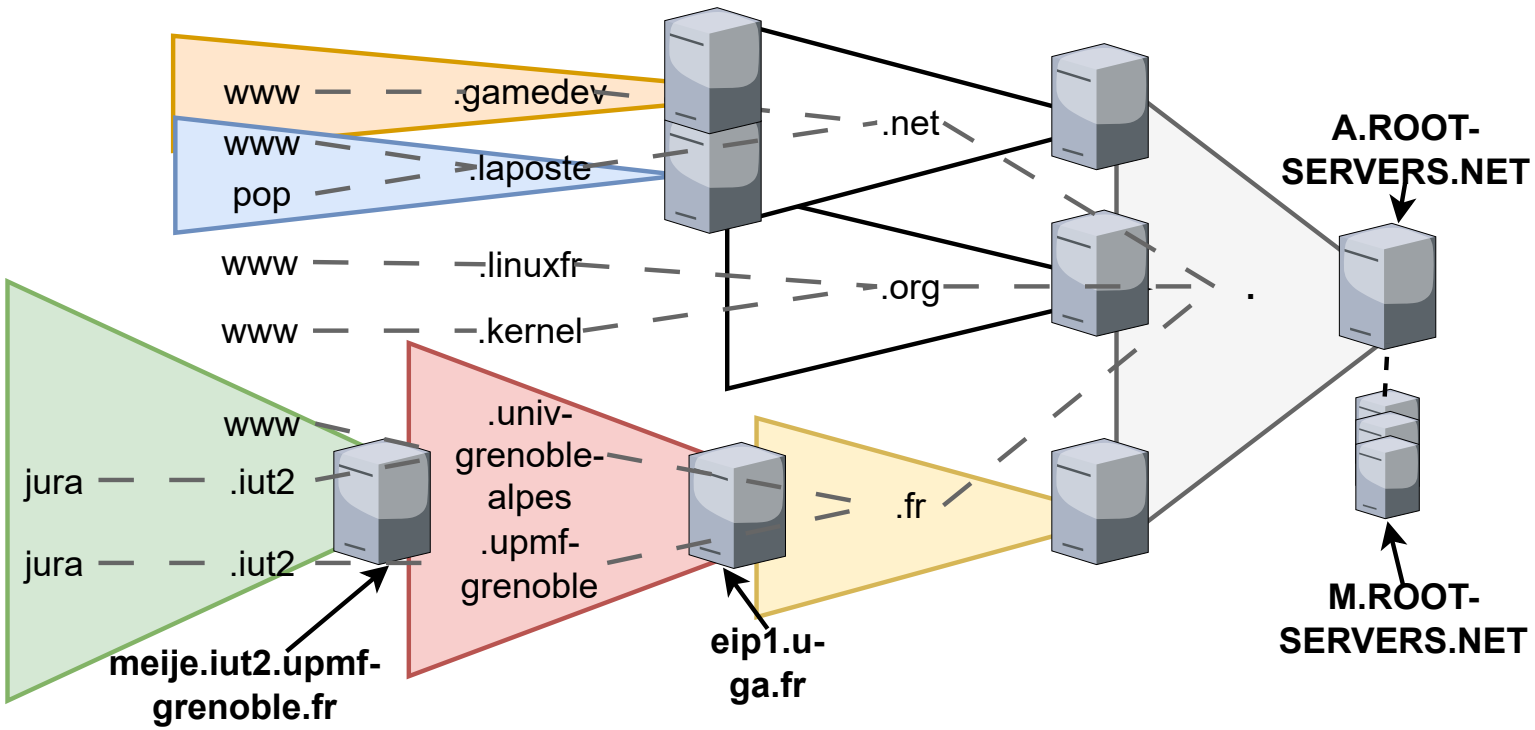
→ Chaque zone est gérée par au moins un serveur DNS **primaire** et plusieurs serveurs DNS **secondaires**

Qu'est-ce qu'une **zone** ?

- Une zone couvre un ou plusieurs domaines ou sous-domaines
- Le *zoning*, c'est le partitionnement administratif de la hiérarchie DNS
- Par exemple, les serveurs de Cloudfare (cloudfare.com) gèrent plusieurs domaines (p. ex. www.carrefour.fr)

IUT2 Université Grenoble Alpes
Département INFO

DNS et zones


www
.gamedev
www
pop
.laposte
www
.linuxfr
www
.kernel
.net
.org
.
A.ROOT-
SERVERS.NET
www
jura
.iut2
jura
.iut2
.univ-
grenoble-
alpes
.upmf-
grenoble
.fr
M.ROOT-
SERVERS.NET
meije.iut2.upmf-
grenoble.fr
eip1.u-
ga.fr

Serveurs du domaine racine

13 serveurs : de A à M
Ex : G.ROOT-SERVERS.NET (192.112.36.4)

DNS local (ex. meije.iut2.upmf-grenoble.fr)
Connaît les serveurs du domaine racine

```
.                       3600000   IN   NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000        A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000        AAAA  2001:503:BA3E::2:30

.                       3600000        NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000        A     192.228.79.201
B.ROOT-SERVERS.NET.     3600000        AAAA  2001:500:84::B

.                       3600000        NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000        A     192.33.4.12
C.ROOT-SERVERS.NET.     3600000        AAAA  2001:500:2::C
```

(Extrait du fichier named.cache)

IUT2 Université Grenoble Alpes
Département INFO

DNS : type d'entrée

```
A       : association <nom, @IPv4>

AAAA    : association <nom, @IPv6>

PTR     : association <@IP, nom>

CNAME   : association <alias, nom>

MX      : serveur SMTP du domaine

NS      : serveur DNS du domaine

SOA     : serveur DNS principal du domaine
```

SOA = *Start Of Authority*

IUT2 Université Grenoble Alpes
Département INFO

SOA : *Start Of Authority*

Section DNS contenant des informations sur le serveur primaire de la zone

Résultat d'une requête

```
nslookup -query=soa iut2.univ-grenoble-alpes.fr
```

```
NOM       : iut2.univ-grenoble-alpes.fr
PRIMAIRE  : meije.iut2.upmf-grenoble.fr
MAIL      : hostmaster.iut2.upmf-grenoble.fr
SERIAL    : 2023101101
REFRESH   : 21600
RETRY     : 7200
EXPIRE    : 1209600
TTL       : 18000
```

IUT2 Université Grenoble Alpes
Département INFO

Sommaire

IUT2 A
Université Grenoble Alpes
Département INFO

Comment traduire un nom de domaine en adresse IP ?

La résolution est généralement faite par un serveur DNS local au domaine de la machine hôte qui fait l'interrogation. Ce serveur travaille de manière *récursive*.

Deux cas de figure se présentent :

1. Le DNS local fait partie du domaine (ou la réponse est dans son cache)
   $\rightarrow$ retourne l'adresse IP correspondant à la requête
2. Le DNS local ne fait **pas** partie du domaine
   $\rightarrow$ demande aux serveurs racines puis successivement aux serveurs de chaque zone intermédiaire.

IUT2 A
Université Grenoble Alpes
Département INFO

Résolution de requête DNS

Fonctionnement du DNS
Envoi d'une requête au serveur DNS local
UDP ou TCP, port 53
Relayée au serveur DNS de la zone cible

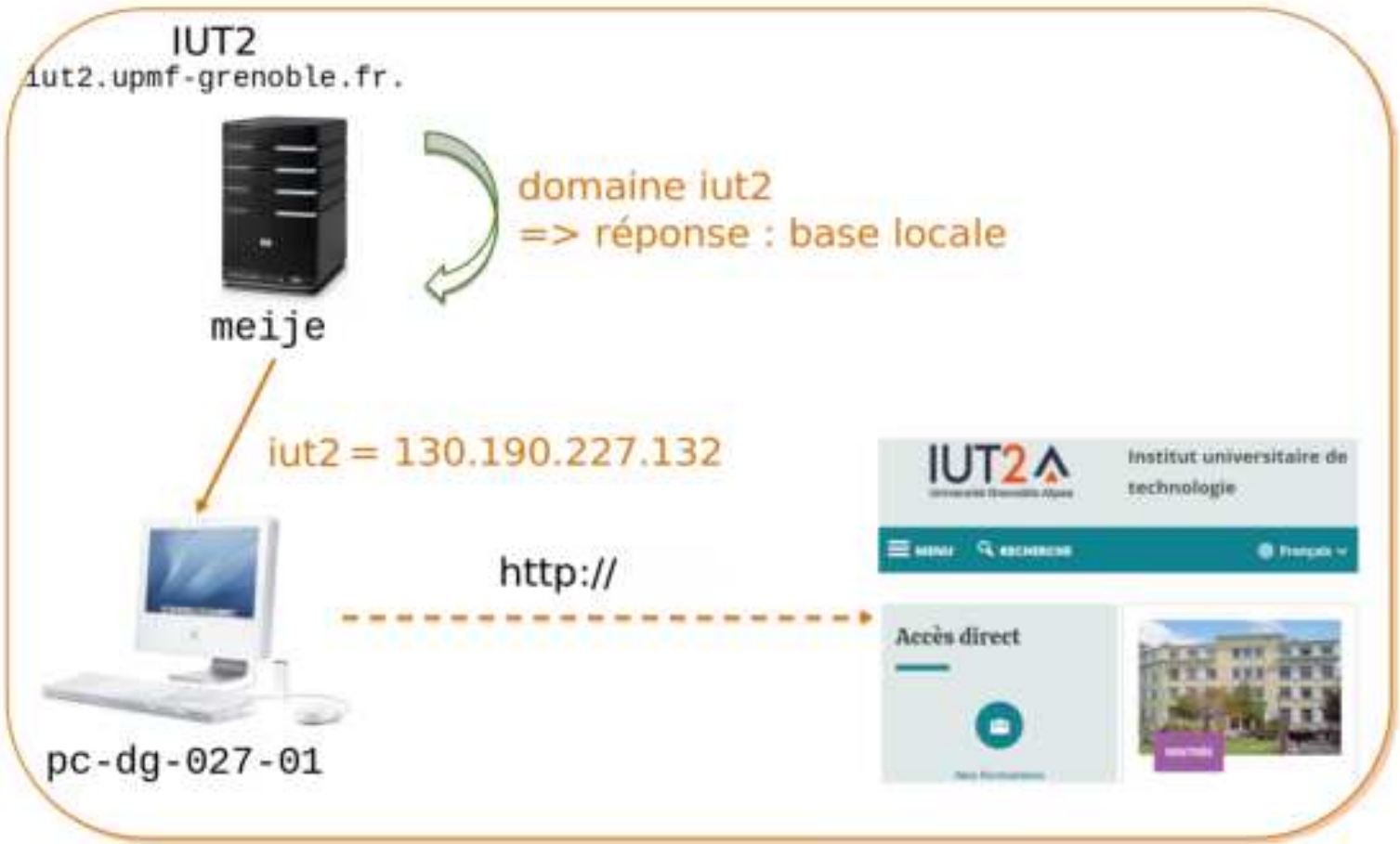
IUT2 Université Grenoble Alpes
Département INFO

Résolution de requête DNS

Exemple : consultation du site `iut2.upmf-grenoble.fr`

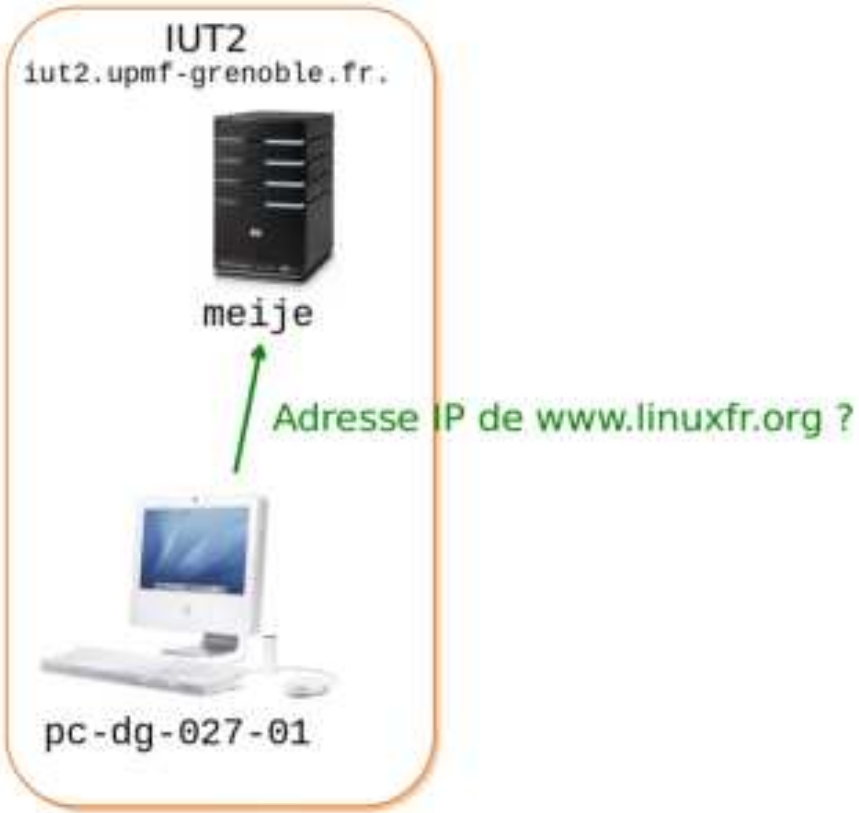
Résolution de requête DNS

Exemple : consultation du site `iut2.univ-grenoble-alpes.fr`



Résolution de requête DNS

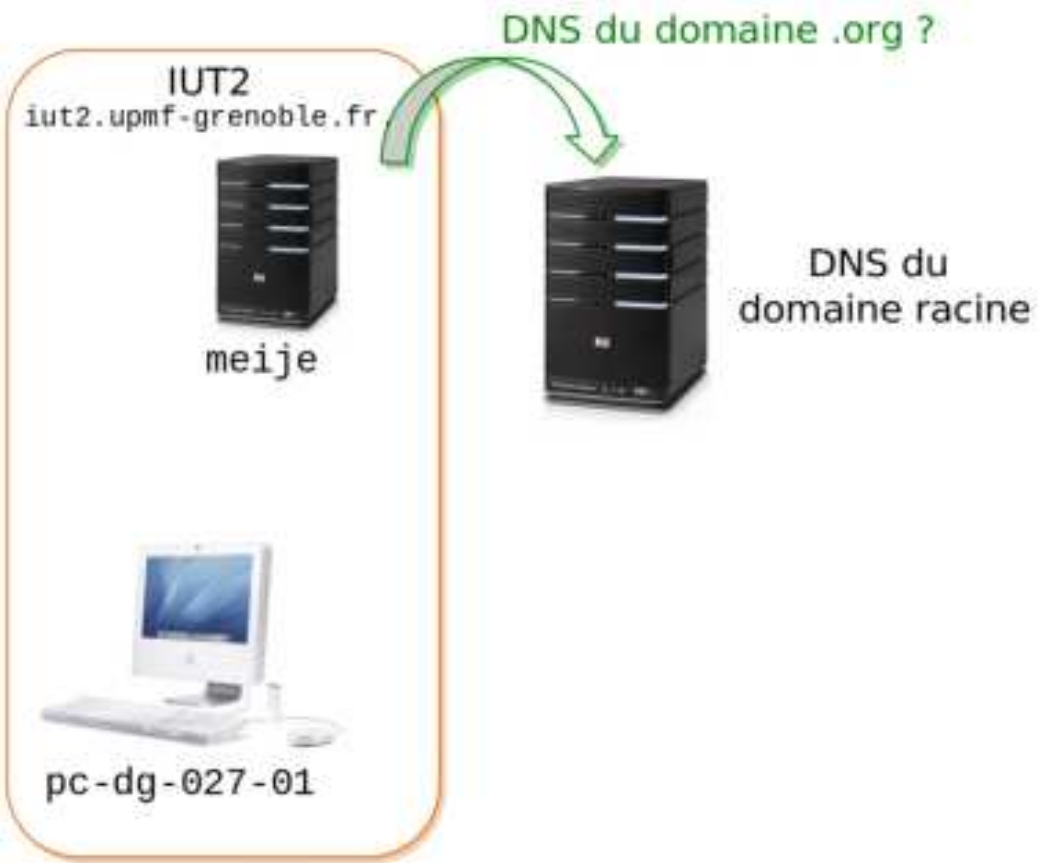
Exemple : consultation du site `www.linuxfr.org`



IUT2 Université Grenoble Alpes
Département INFO

Résolution de requête DNS

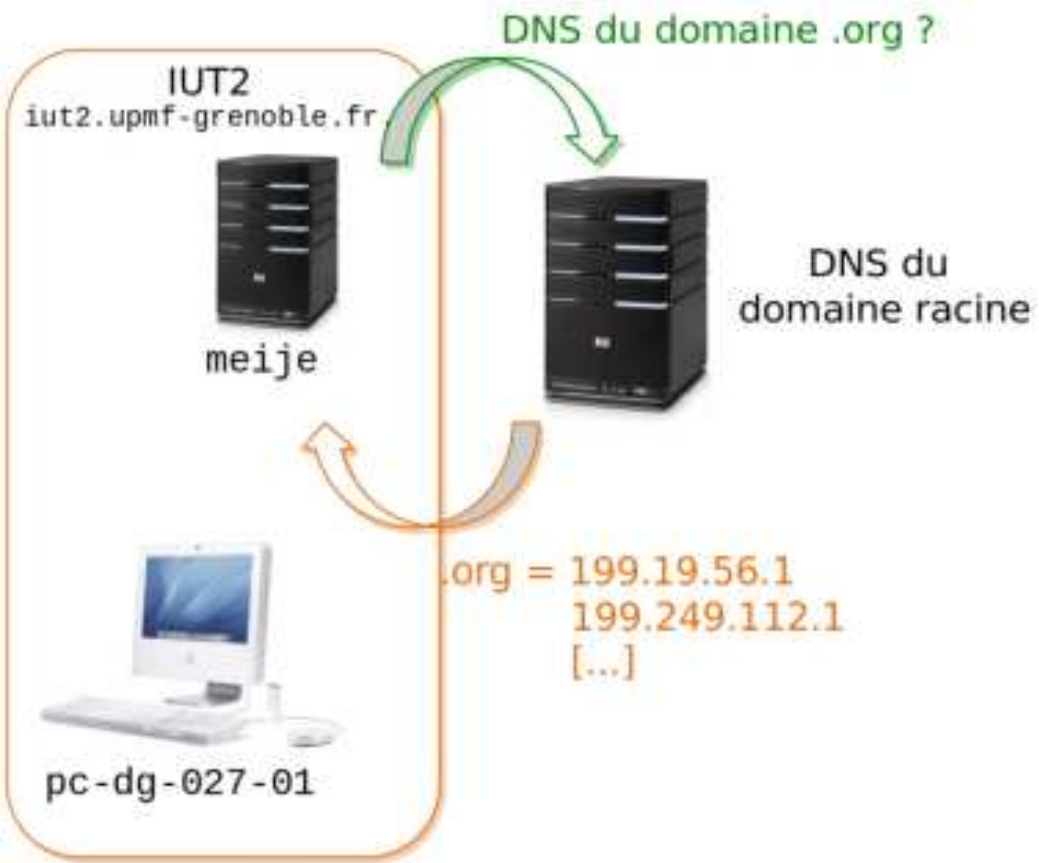
Exemple : consultation du site `www.linuxfr.org`



IUT2 Université Grenoble Alpes
Département INFO

Résolution de requête DNS

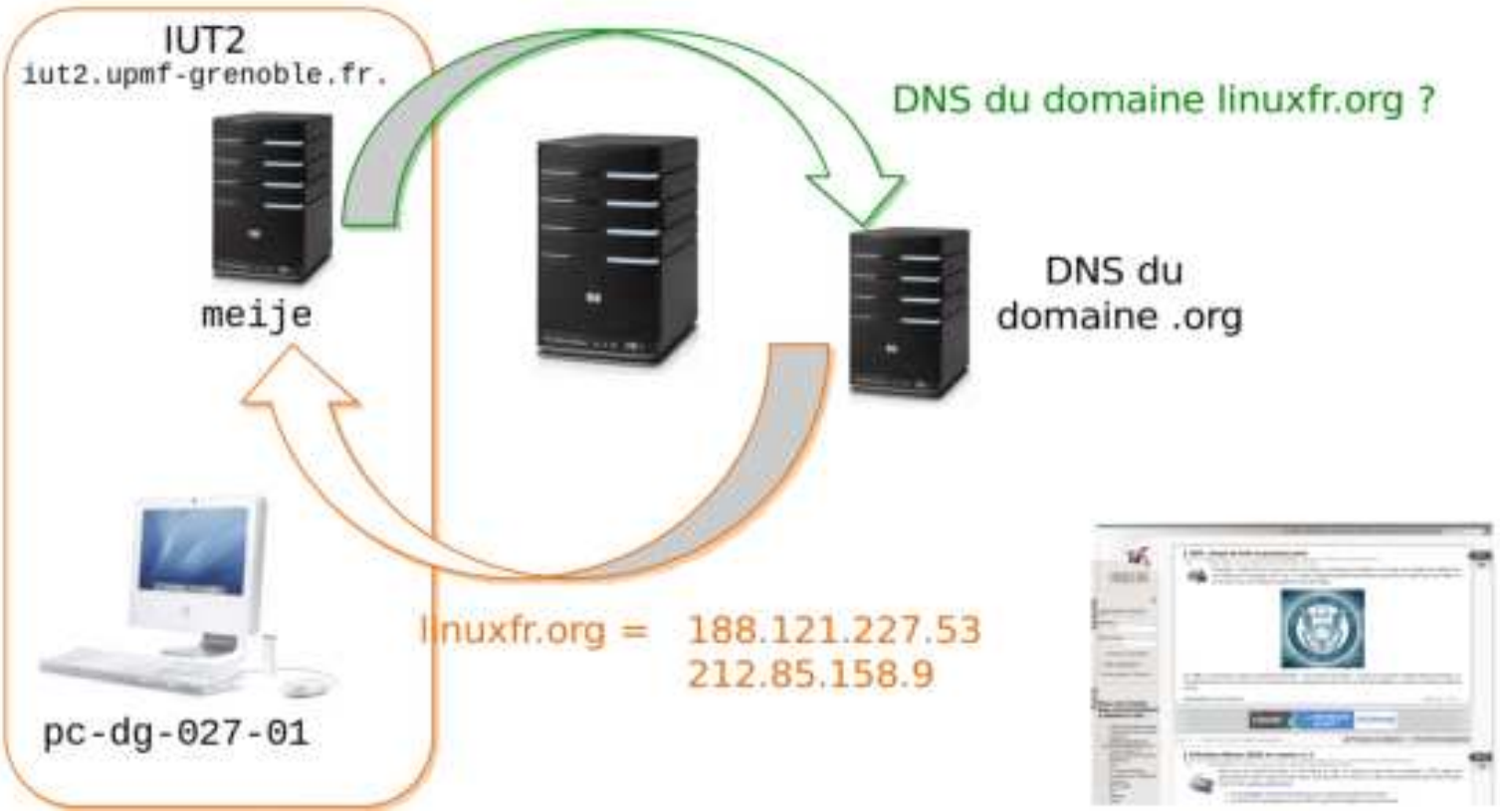
Exemple : consultation du site `www.linuxfr.org`



IUT2 Université Grenoble Alpes
Département INFO

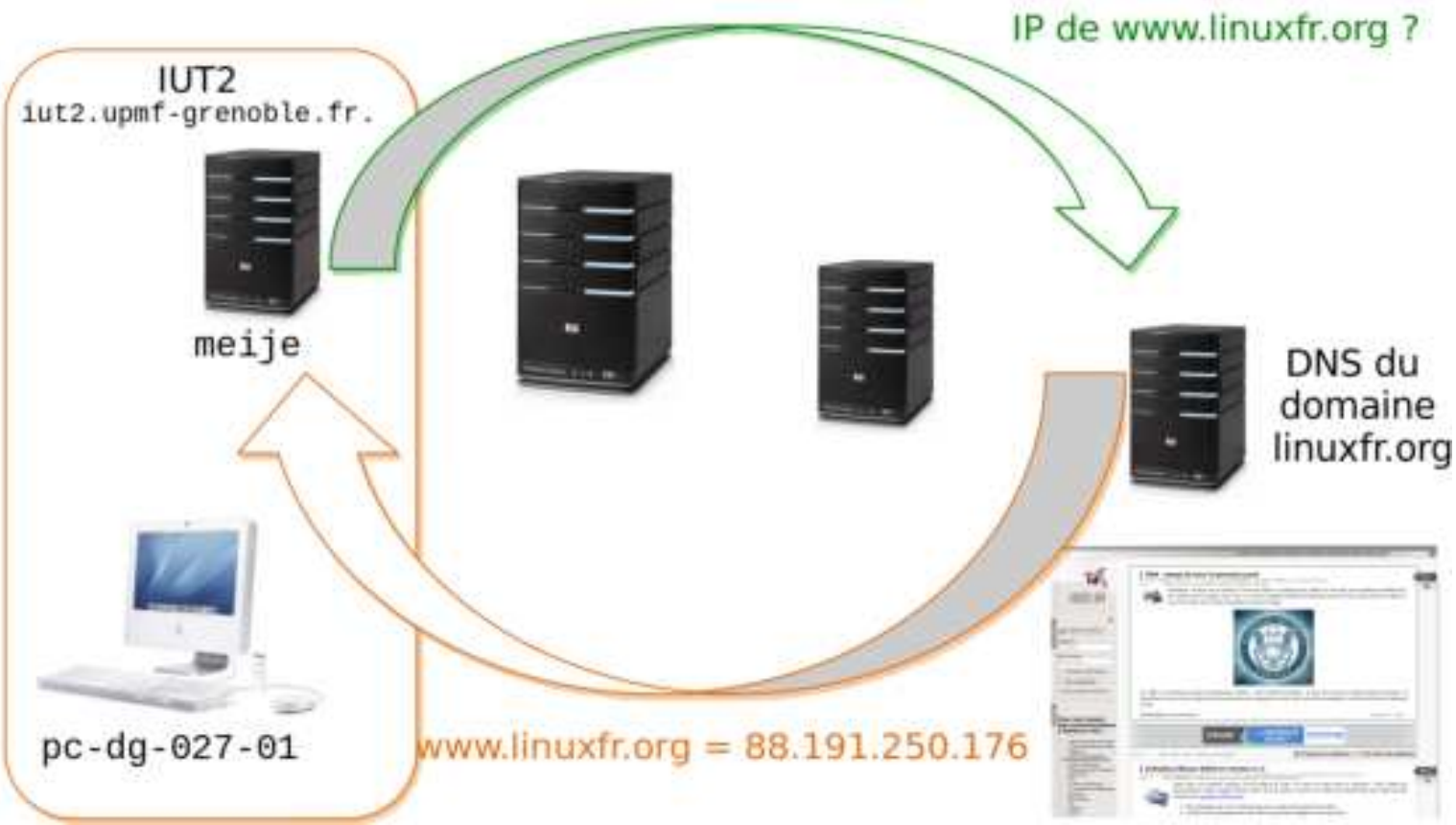
Résolution de requête DNS

Exemple : consultation du site `www.linuxfr.org`



Résolution de requête DNS

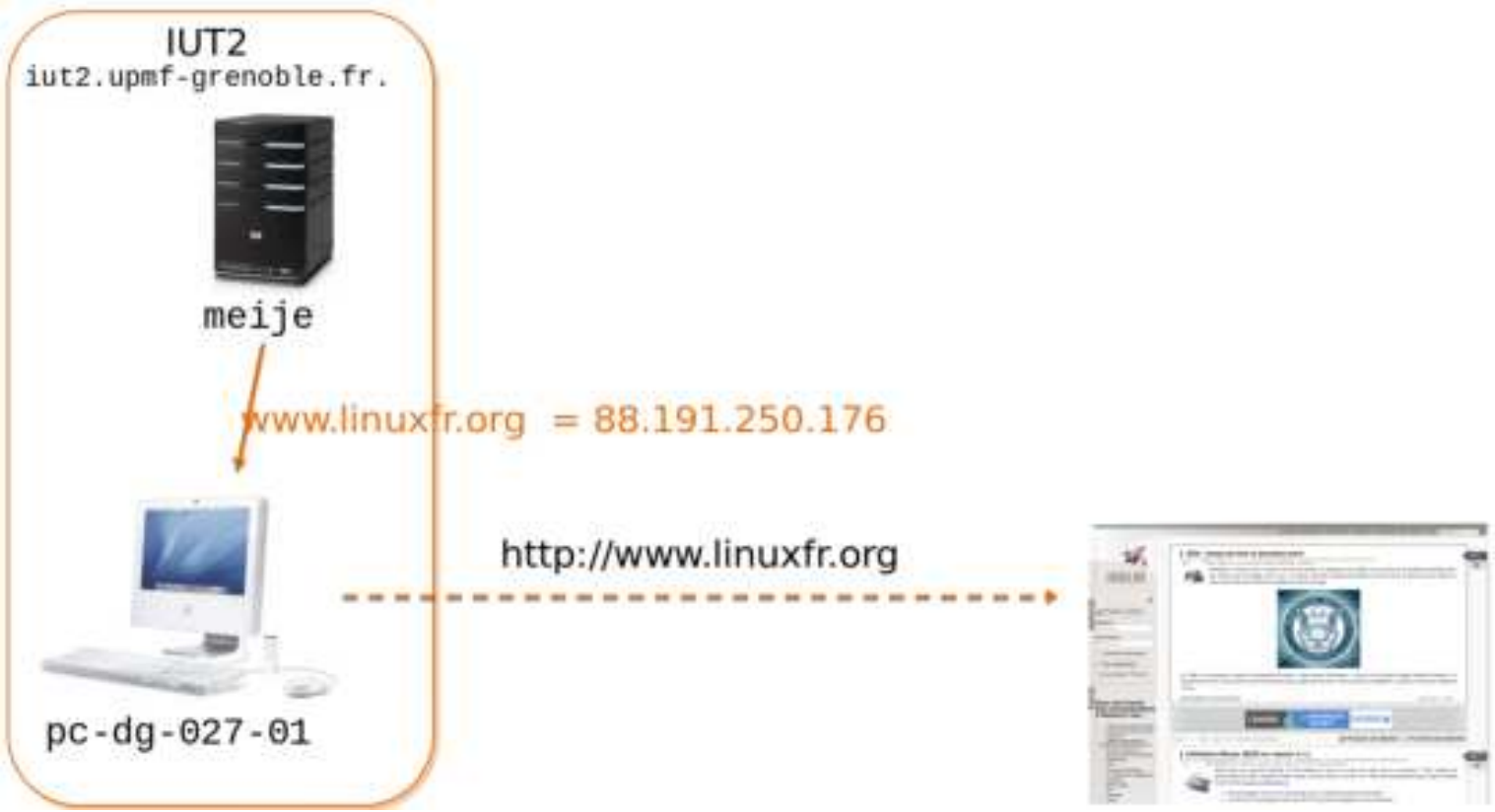
Exemple : consultation du site `www.linuxfr.org`



IUT2
Université Grenoble Alpes
Département
INFO

Résolution de requête DNS

Exemple : consultation du site `www.linuxfr.org`



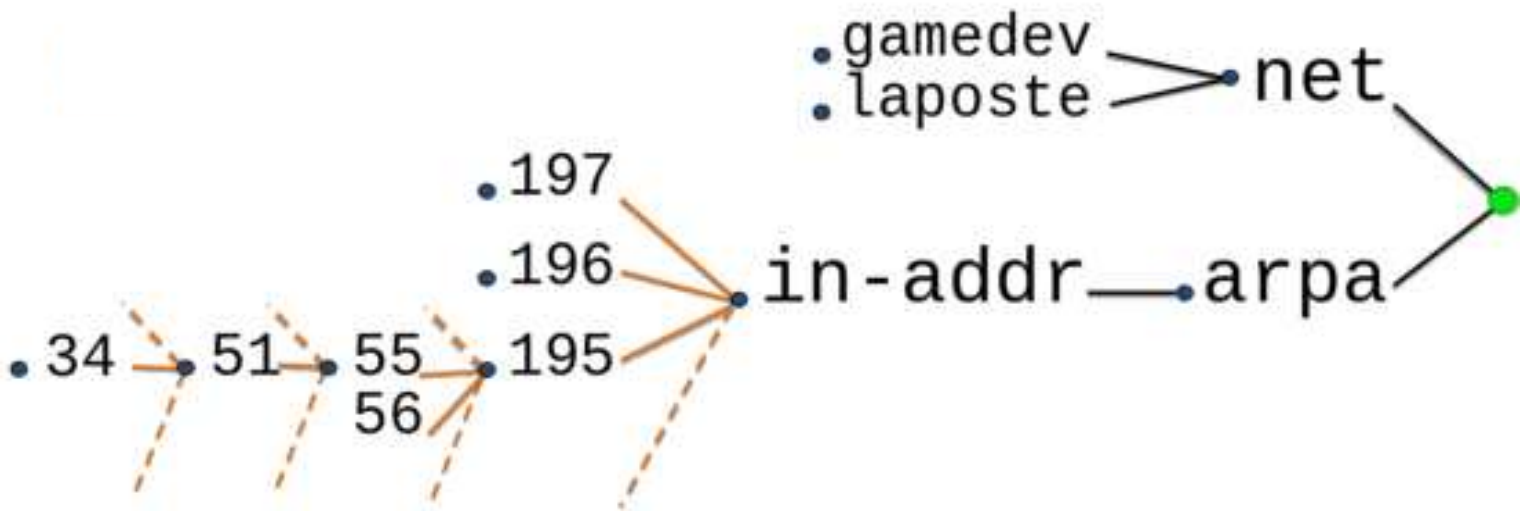
IUT2 Université Grenoble Alpes
Département INFO

Résolution inverse

Retrouver un nom à partir d'une adresse IPv4
Entrée de type `PTR <@IPv4, nom>`
Une base DNS contient deux entrées

1. Résolution de nom : `<nom, @IPv4>` de type `A`
2. Résolution d'IP : `<@IPv4, nom>` de type `PTR`

Arbre de résolution inverse



34.51.55.195.in-addr.arpa. => meije.iut2.upmf-grenoble.fr

IUT2 Université Grenoble Alpes
Département INFO

Sous-domaines du domaine .arpa

```
.in-addr.arpa.   : adresses IPv4
.ip6.arpa.       : adresses IPv6
.uri.arpa.       : ressources (ex. http:// ftp://)
.e164.arpa.      : numéro de téléphone (SIP, VoIP)
```

IUT2 Université Grenoble Alpes
Département INFO

DNS, HTTP et TCP/IP

La grande majorité des requêtes sur le web font appel au DNS.

Une requête : http://de.wikipedia.org
sera interprétée grâce au DNS en : http://185.15.58.224:80/
Pour former les paquets IP (@IP destination v4 ou v6) et les messages TCP.

La structure DNS hiérarchique a pour conséquences :

- Les attaques sur les serveurs DNS peuvent perturber le trafic sur Internet. La duplication de serveurs racines a toujours évité un fort impact de ces attaques (serveurs racines)
- Les noms de domaines sont gérés de manière centralisée.
- Les autorités peuvent bloquer la résolution DNS de certains sites.

IUT2 Université Grenoble Alpes
Département INFO

Glossaire I

ARP Address Resolution Protocol. 17

BE Best Effort. 14
BOOTP Bootstrap Protocol. 22

DHCP Dynamic Host Configuration Protocol. 20, 22
DN Domain Name. 65
DNS Domain Name System. 62

FCS Frame Check Sequence. 13
FQDN Fully Qualified Domain Name. 66

LAN Local Area Network. 32

MAC Media Access Control. 11
MTU Maximum Transfer Unit. 14

OSI Open Systems Interconnection. 13

TLD Top-Level Domain. 64

VLAN Virtual Local Area Network. 34, 38, 45

IUT2 Université Grenoble Alpes
Département INFO

Références I


(1981).
Internet Protocol.
RFC 791.


(1983a).
Domain names : Concepts and facilities.
RFC 882.


(1983b).
Domain names : Implementation specification.
RFC 883.


(1985).
Bootstrap Protocol.
RFC 951.


Droms, R. (1997).
Dynamic Host Configuration Protocol.
RFC 2131.


Hinden, B. et Deering, D. S. E. (1998).
Internet Protocol, Version 6 (IPv6) Specification.
RFC 2460.


IEEE (1999).
IEEE standards for local and metropolitan area networks : Virtual bridged local area networks.
IEEE Std 802.1Q-1998, pages 1–214.

IUT2 Université Grenoble Alpes
Département INFO