Réseaux IP sans configuration

« Bonjour »
Avancée réelle ou illusion ?

JRES 2005 - Marseille

Laurent.Ghys@ircam.fr

Plan

- Motivations pour cette présentation
- Les réseaux IP sans configuration
- Les adresses IPv4 de lien local
- Le DNS multicast sur le lien local
- La découverte des services
- Implémentations
- Perspectives

Un utilisateur …

Un iUtilisateur …

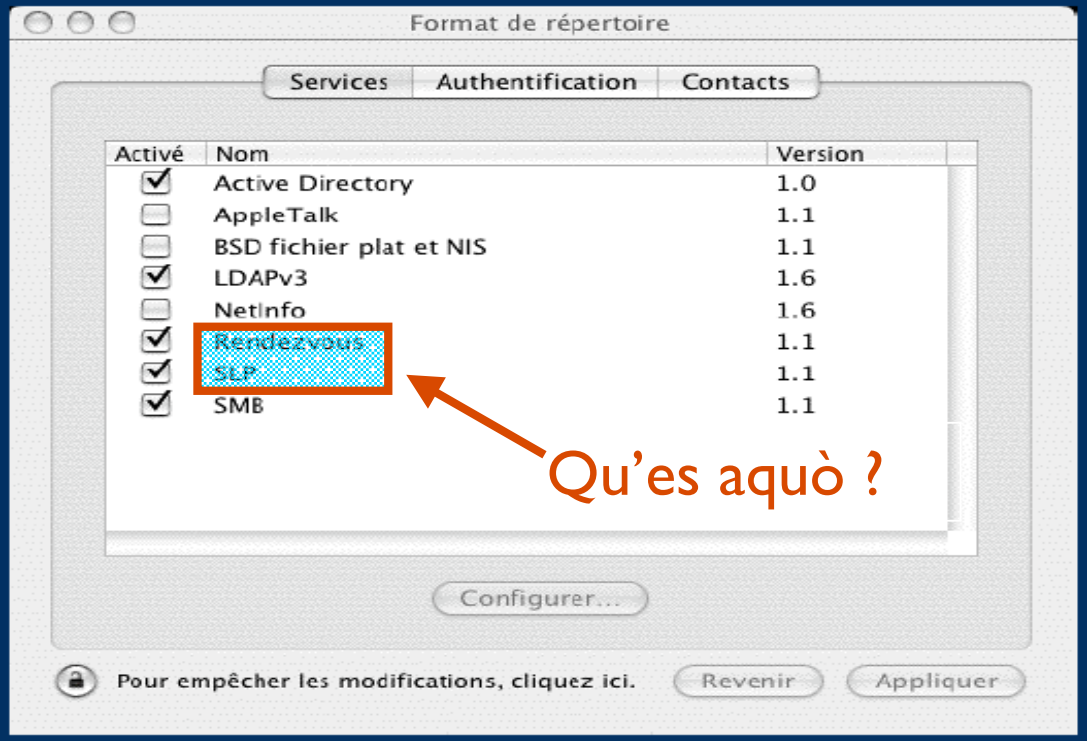
À la maison, j'ai quelques Macs,
des caméras IP, une imprimante couleur
et une borne Airport connectée à Internet.
Je ne comprends pas …
Je n'ai rien configuré, même pas une seule adresse IP,
et pourtant tout a fonctionné du premier coup !
iTunes, iPhoto, iChat, iAdb, iDVD, iCal, iMovie, …
*C'est avec **RendezVous** que ça marche,*
c'est bien ça ?

Un iUtilisateur …

JRES 2003 dans une présentation …

Annuaire

- NetInfo
- NIS
- Active Directory
- LDAP



09/12/2003 LAAS 20

Des paquets bizarres sur *mon* réseau !!!

Dépannage réseau avec tcpdump, vu au milieu du trafic :

```
IP 169.254.162.171.mdns          > 224.0.0.251.mdns
fe80::203:93ff:fe4f:6fe4.mdns > ff02::fb.mdns
```

- Qu'est-ce donc que ce protocole **mdns** (port 5353) ?
- Et ces adresses **`169.254/16`** (! = RFC 1918) ?
- Et cette adresse multicast v4 **`224.0.0.251`** ?
- Et cette adresse multicast v6 **`ff02::fb`** ?

Recherche rapide sur Internet : la réponse tombe …

Zeroconf

Les réseaux IP sans configuration

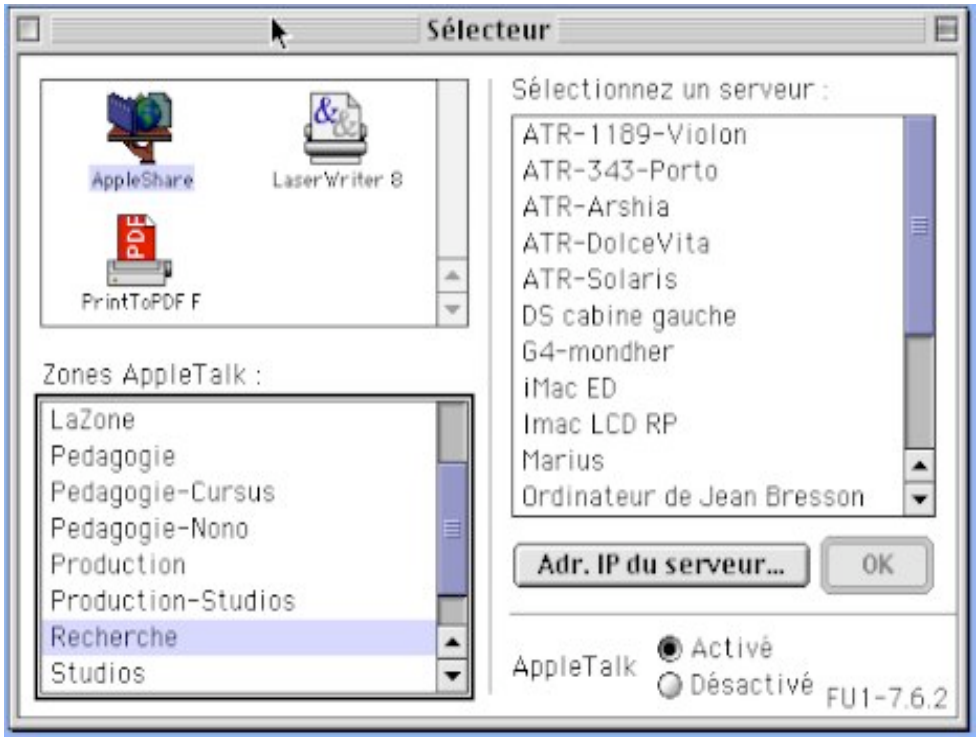
Groupe de travail IETF Zeroconf

- Créé en septembre 1999
- À l'initiative de Stuart Cheshire
- Dirigé par Erik Guttman
- Clôturé en août 2004
- En relation proche avec le groupe DNSEXT
- A laissé des sites web, plusieurs Dratfs et un RFC.

Les réseaux sans configuration

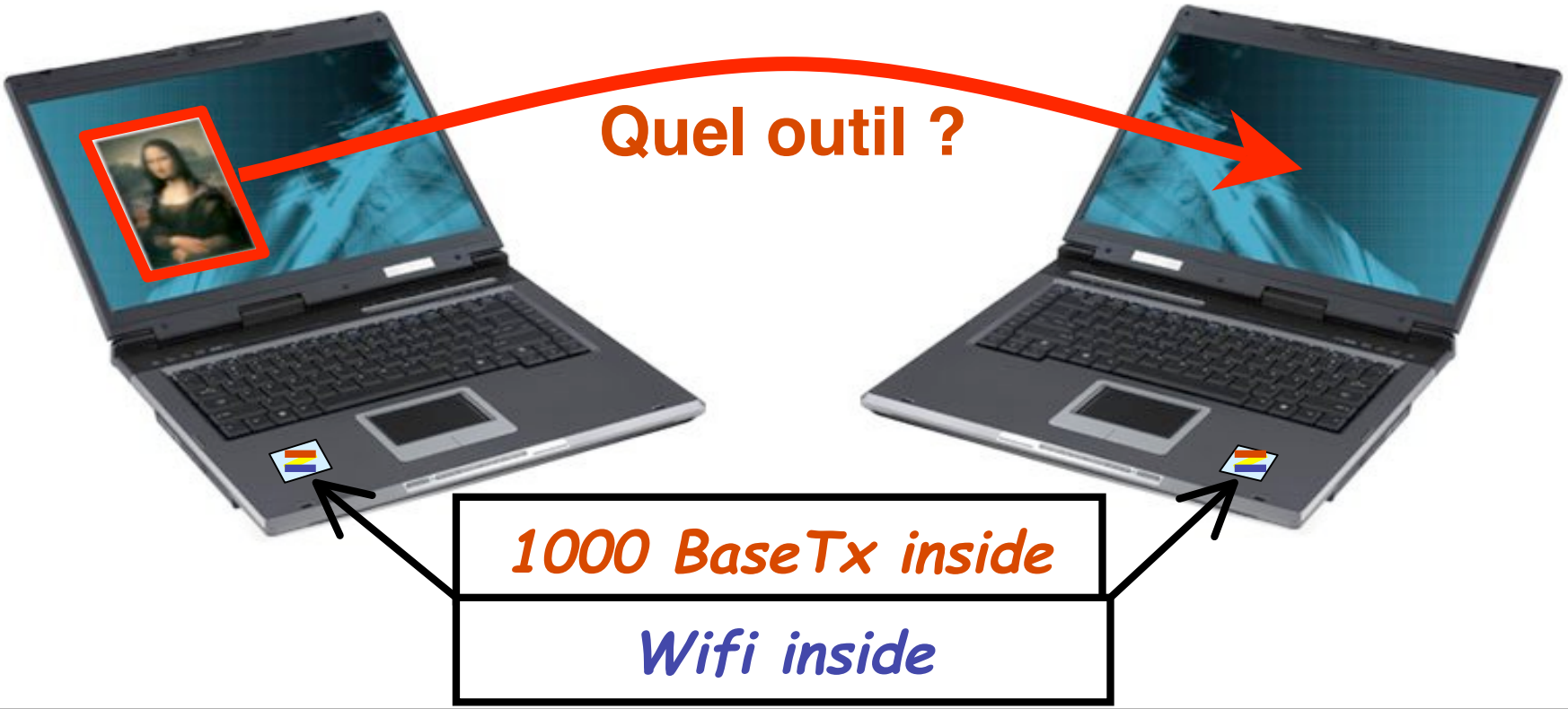
Les ancêtres :

- AppleTalk (Apple)
- NetBios/SMB (Microsoft)
- IPX (Novell)



Un problème simple

Comment copier un fichier ?



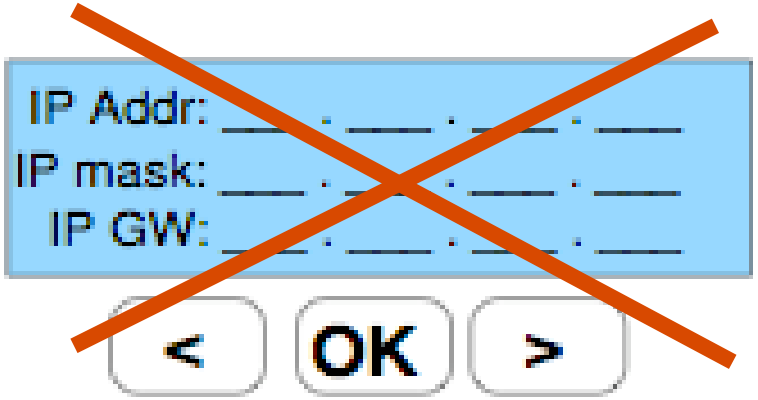
Solution dans X % des cas : la clé USB !!!

Réseaux IP sans configuration

Ce problème est appelé au sein de l'IETF :

« Le bureau du dentiste »

- Principe n°1 : **pas de serveur DHCP ni DNS**
- Principe n°2 : **pas de configuration manuelle**
- Principe n°3 : **pas d'intervention humaine.**



Les équipements IPv6, dans leur immense majorité, ne seront pas configurables manuellement.

Réseaux IP sans configuration

Objectifs du groupe Zeroconf :

- Autoconfiguration des adresses,
- Résolution des adresses <--> noms,
- Découverte des services,
- Allocation d'adresses multicast.

Configuration automatique des adresses IPv4 sur le lien local

Adresses IPv4 lien-local

1) Ce n'est pas une nouveauté :
   - Existent depuis MacOS 8.5 et Windows 98
   - Réservées dans le RFC 3330 (sept 2002)
2) RFC 3927 paru fin mai 2005
   - *Merci à l'IETF du cadeau spécial JRES !*
3) Disponibles sur tous les bons systèmes
   - Zcip, autoip, etc.

Différences IPv4 - IPv6

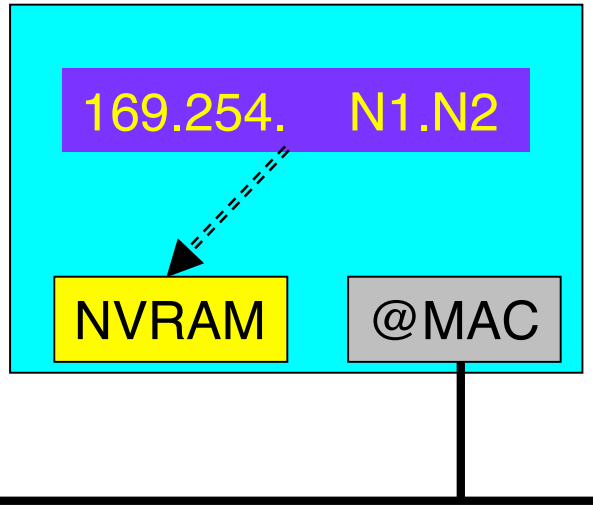
@ lien-local IPv6	@ lien-local IPv4
`FE80::EUI-64`	`169.254.m1.m2`
Prévues dès la conception du protocole IPv6	Officialisées en 2005
Permanentes Cohabitation avec les autres @	Provisoires Ne cohabitent pas avec les autres @
Étape dans l'autoconfiguration générale (c.f. découverte de voisins)	Utilisées uniquement si pas d'autres @ opérationelles.
Uniques pour une interface (cf. EUI-64)	Plusieurs valeurs possibles pour une interface mais *f*(@MAC) si possible.

Précautions à respecter

Les adresses lien-local IPv4 « RFC 3927 » :

- Ne sont **pas routables :**
  - Elles ne doivent **jamais** être envoyées à un **routeur** pour y être **relayées**.
- Sont **réservées pour l'autoconfiguration** :
  - Elles ne doivent **pas** être **configurées à la main,**
  - Elles ne doivent **pas** être **enregistrées** dans **DHCP,**
  - Elles ne doivent **pas** être **résolues** par le **DNS,**
  - Les clients ne doivent **pas** faire de **requêtes DNS** classique pour des noms appartenant au domaine **`254.169.in-addr.arpa.`**

Configuration automatique



1) @IP[17…32] = ***f*** (@MAC)

2) Test si @IP libre : ARP probes

3) - Si @IP libre : annonces ARP

   - Si @IP en conflit : aller à 1)

4) Si possible sauve. @IP NVRAM

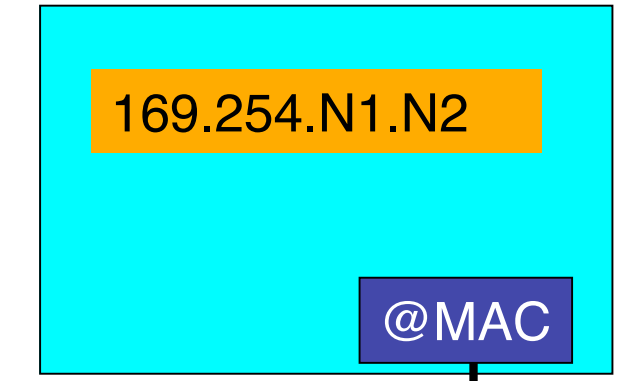
@MAC > ff:ff:ff:ff:ff:ff ARP who-has 169.254.N1.N2 tell 0.0.0.0
…
@MAC > ff:ff:ff:ff:ff:ff ARP who-has 169.254.N1.N2 tell 0.0.0.0

@MAC > ff:ff:ff:ff:ff:ff ARP who-has 169.254.N1.N2 tell 169.254.N1.N2
…
@MAC > ff:ff:ff:ff:ff:ff ARP who-has 169.254.N1.N2 tell 169.254.N1.N2

Détection d'Adresse Dupliquée

1) Elle a lieu tout au long de la période d'utilisation de l'adresse lien-local (cf. réunion de réseaux sans-fil).
2) Surveillance permanente de **tous** les paquets **ARP**, qui sont toujours envoyés en **broadcast** Ethernet pour les adresses lien-local.
3) Les machines peuvent tenter de conserver leur adresse si par exemple elles ont des connexions TCP en cours.

Détection d'Adresse Dupliquée

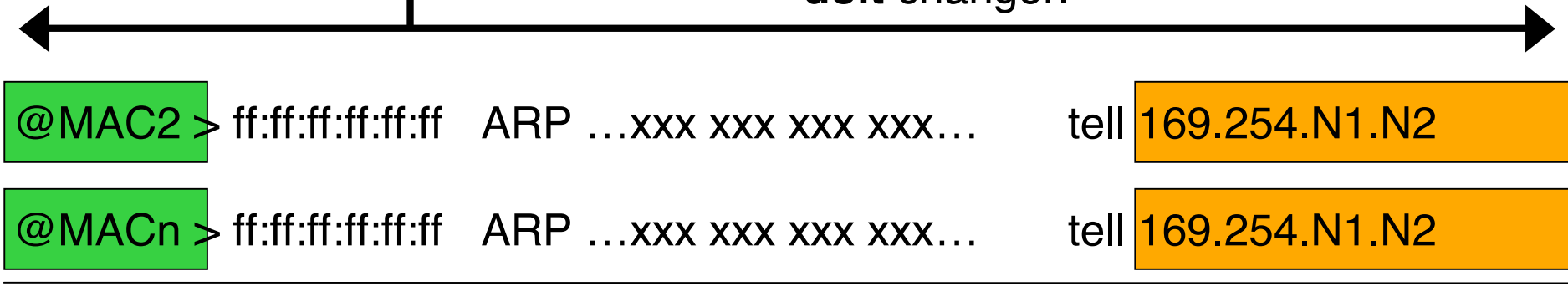


Une machine doit surveiller ARP

Si elle détecte un conflit sur son @IP :

- Choix N° 1 : elle change d'@IP
- Choix N° 2 : elle défend son @IP

Si nouveau conflit avant 10 secondes : elle **doit** changer.



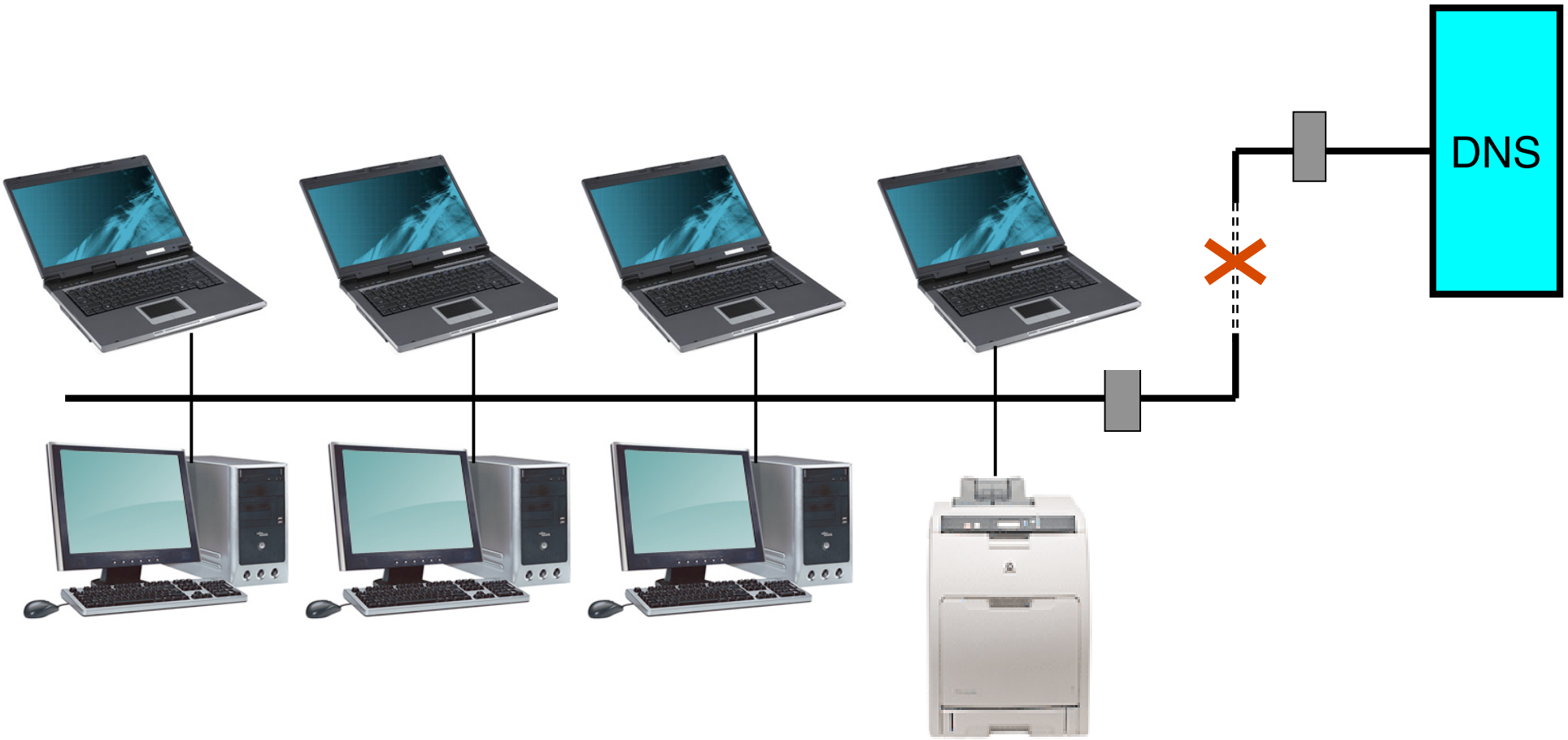
@MAC > ff:ff:ff:ff:ff:ff ARP who-has 169.254.N1.N2 tell 169.254.N1.N2

Autoconfiguration et DHCP

- Sous Mac OS X et Windows, DHCP est toujours tenté en premier et se poursuit pendant l'autoconfiguration :
  - si DHCP échoue on lance l'autoconfiguration,
  - ensuite tentative de DHCP toutes les 5 minutes.
- La commutation entre DHCP et l'autoconfiguration est automatique :
  - déconnexion et reconnexion câble,
  - réseaux sans fil.
- L'autoconfiguration est souvent implémentée dans le client DHCP
  - sous Mac OS X, dans `bootd`,
  - `zcip` est une exception (autoconfiguration seule).

DNS multicast sur le lien local

Sans DNS point de salut …



Résultat : plus rien ne marche !!!

DNS multicast sur le lien-local

Les choses se compliquent un peu car deux propositions s'affrontent :

- LLMNR (*Linklocal Multicast Name Resolution*),
  - soutenu par Microsoft (Bernard Aboba)
  - **draft-ietf-dnsext-mdns-45**
  - 6 octobre 2005
- mDNS (*Multicast DNS*),
  - soutenu par Apple (Stuart Cheshire)
  - **draft-cheshire-dnsext-multicastdns-05**
  - 7 juin 2005

mDNS - LLMNR

Les différences « numériques »

	mDNS	LLMNR
@ multicast IPv4	224.0.0.251	224.0.0.252
@ multicast IPv6	FF02::FB	FF02::1:3
port	5353	5355
TTL - Hop Limit	255	1

TTL : fondamental pour la sécurité,
mais un détail dans ces protocoles.

mDNS - LLMNR

Les différences « profondes »

	mDNS	LLMNR
Origine du Protocole	Stuart Cheshire (Apple)	Groupe IETF DNSEXT
Conception du protocole	Remplacer Appletalk (une des briques)	Pallier le manque de DNS
Domaines résolus	.local.	Tous
Caches distincts des caches DNS	Oui	Oui
Utilisation du multicast	Importante	Faible

LLMNR

LLMNR reste très proche du DNS classique

- **Points communs** :
  - Une question par requête
  - Champ ID copié dans les réponses
  - Champ RCODE utilisé (réponses vides ou négatives)
  - Utilisation TCP possible
  - TTL des enregistrements simples (défaut 30 secondes)

- **Différences** :
  - Requêtes en multicast
  - Indicateur de conflit de nom dans les requêtes
  - Pas de requêtes en unicast UDP

Pas d'implémentation libre **&** draft-ietf-dnsext-mdns-**45 !!!**

mDNS = DNS distribué

Requêtes (et Réponses) en multicast

mDNS

Profite élégamment des avantages du transport par multicast uniquement sur le lien-local des enregistrements normaux du DNS :

- Les champs ID et RCODE non ignorés, pas de SOA.
- Pas de copie des requêtes dans les réponses,
- Plusieurs questions sont possibles dans une requête,
- Réponses *« déjà connues »* incluses dans les requêtes,
- TTL d'un enregistrement à 0 pour indiquer qu'il a été supprimé,
- Utilisation sophistiquée des TTL des enregistrements pour le système de cohérence de caches,
- Surveille les requêtes pour suppression des requêtes dupliquées,
- Surveille les réponses pour suppression des réponses dupliquées.
- **Priorité dans la conception** : la charge réseau (! = Appletalk)

Découverte des services

SLP, SSDP, DNS-SD

Si l'on ne compte que les propositions ayant produit des documents IETF (exclus : Jini, OSGi), on trouve trois candidats :

- **SLP** (*Service Location Protocol)*
  - Une ***Norme*** de l'IETF
- **SSDP** (*Simple Service Discovery Protocol)*
  - Proposé par le Forum UPnP
  - (*Universal Plug and Play Forum)*
  - IETF : **draft-cai-ssdp-v1-03** (1999)
- **DNS-SD** (*DNS-Based Service Discovery)*
  - Proposé par Apple (Stuart Cheshire)

SLP != Simple Lightweight Protocol

Le protocole SLP bien que déjà ancien n'a pas connu un énorme succès sur nos machines jusqu'à maintenant :

- **SLP** est un standard de **l'IETF** :
  - RFC 2165 (v1) , 2608 (v2), 2609, 2926, 3059, 3111, … 4018.
- **SLP est complexe** :
  - basé sur les URLs,
  - trois sortes d'agents : *User Agent, Service Agent, Directory Agent,*
  - 11 types de messages : certains obligatoires d'autres optionnels,
  - emprunte à LDAP son langage des requêtes,
  - etc., etc.
- **SLP** est difficile à embarquer dans les petits équipements.

La découverte des services

- proto : ftp
- host : nom1 - @IP1
- port : 3456
- Options : u=anonymous
  path=/photos/Duchamp

FTP

- proto : ftp
- host : nom2 - @IP2

DNS-SD

DNS-SD n'est pas un protocole qui circule sur nos réseaux

- DNS-SD utilise le DNS traditionnel **ou** mDNS.
  - Il n'utilise rien d'autre !
  - Prolonge les concepts du RFC 2782
  - Utilise les enregistrements DNS SRV et TXT
  - Précise les longueur des champs, des codages, etc. (ex : UTF-8)
  - Spécifie une méthode pour le passage des paramètres des services dans les enregistrements de type TXT
  - Une indirection (PTR) de plus est simplement ajoutée / RFC 2782
- Spécification du protocole **:**
  - **draft-cheshire-dnsext-dns-sd-05**

Enregistrements SRV (RFC 2782)

_Service._Protocole SRV Priorité Poids Port Cible	
Service	Nom du service au sens ***Assigned Numbers*** (RFC 1700)
Protocole	Le nom du procotole IP (**udp** ou **tcp**)
Priorité	Priorité à la plus basse valeur [0-65536] (Comme pour les MX)
Poids	Poids en valeur relative [0-65536] pour une même priorité (équilibrage de charge)
Port	Le port du service
Cible	Nom DNS de la machine cible (!= CNAME)

DNS-SD : principe de base

On fait d'abord une requête de **PTR** sur :

<service> . <domaine> .

On obtient une liste (parfois vide) d'entrées de la forme :

<Instance> . <service> . <domaine> .

Instance ***=*** *un « label » DNS codé en UTF-8* ***(l < 63 octets)***

On fait alors une seconde requête de type **ANY** sur :

<Instance> . <service> . <domaine> .

On obtient alors toutes informations sur cette instance de ce service : nom d'hôte,@IP (A, AAAA), port, priorité, poids, et des informations concaténées dans le champ TXT.

Une instance de service

J'ai « des photos de Duchamp »
Je les partage en ftp

< Une instance de service >

Des photos de Duchamp (portable mémé)

- service : _ftp._udp.
- host : nom - A, AAAA
- port : 3456
- TXT : u=anonymous
  path=/photos/Duchamp

DNS-SD : ordre des champs

Pourquoi avoir choisi :

<Instance> . <Service> . <Domaine>.

Plutôt que :

<Service > . <Instance> . <Domaine>.

- Le client **connaît le service** dont il **cherche les Instances**, et non pas le contraire (***choix dans des menus***),
- Possibilité de déléguer les sous-domaines de services,

  Exemples :

  - `_tcp.mon-domaine.org.`
  - `_ipp._tcp.mon-domaine.org.`
- Compression efficace des paquets contenant des réponses multiples, car la partie <service>.<domaine> est commune.

DNS-SD : exemple réel sur DNS

% **dig _ftp._tcp.dns-sd.org PTR**

```
;; ANSWER SECTION:
_ftp._tcp.dns-sd.org.   60     IN     PTR    Apple\032QuickTime\032Files._ftp._tcp.dns-
        sd.org.
_ftp._tcp.dns-sd.org.   60     IN     PTR
        Microsoft\032Developer\032Files._ftp._tcp.dns-sd.org.
_ftp._tcp.dns-sd.org.   60     IN     PTR
        Restricted,\032Registered\032Users\032Only._ftp._tcp.dns-sd.org.
```

% **dig 'Apple QuickTime Files'._ftp._tcp.dns-sd.org ANY**

```
;; ANSWER SECTION:
Apple\032QuickTime\032Files._ftp._tcp.dns-sd.org.
            60 IN SRV 0 0 21 ftp.apple.com.
Apple\032QuickTime\032Files._ftp._tcp.dns-sd.org.
            60 IN TXT "path=/quicktime"
```

Dépôt des noms de services

- DNS-SD propose que ce soit IANA qui enregistre les noms des services.

  Problème :

  - Les noms de services du document
  - «***list of assigned ports names and numbers***» doivent correspondre à des N° de ports fixes,
  - On ne peut donc pas demander à IANA un nom de service sans numéro de port.
  - IANA ne gère pas les options des enregistrements TXT de DNS-SD.
- En attendant que IANA s'en occupe (un jour ?),

  solution provisoire : dépôt sur **`www.dns-sd.org.`**

DNS-SD : infos sur les domaines

Pseudo-service et meta-requêtes	
_services._dns-sd._udp. ***<domaine>***	Liste des services disponibles sur le domaine (PTRs)
b._dns-sd._udp***.<domaine>***	Liste des domaines recommandés pour la découverte des services
db._dns-sd._udp***.<domaine>***	Le domaines recommandé pour la découverte des services
r._dns-sd._udp ***.<domaine>***	Liste des domaines recommandés pour l'enregistrement des services,
dr._dns-sd._udp ***.<domaine>***	Le domaine recommandé pour l'enregistrement des services
lb._dns-sd._udp ***.<domaine>***	Domaine par défaut passé aux applications par héritage

Implémentations

Implémentations de Zeroconf

Les trois classiques :

Bonjour *Apple*

mDNSResponder : licence APSL

Howl *Porchdog software*

Ajouts à mDNSResponder

Avahi *freedesktop.org*

licence LGPL/GPL *(ils cherchent un logo …)*

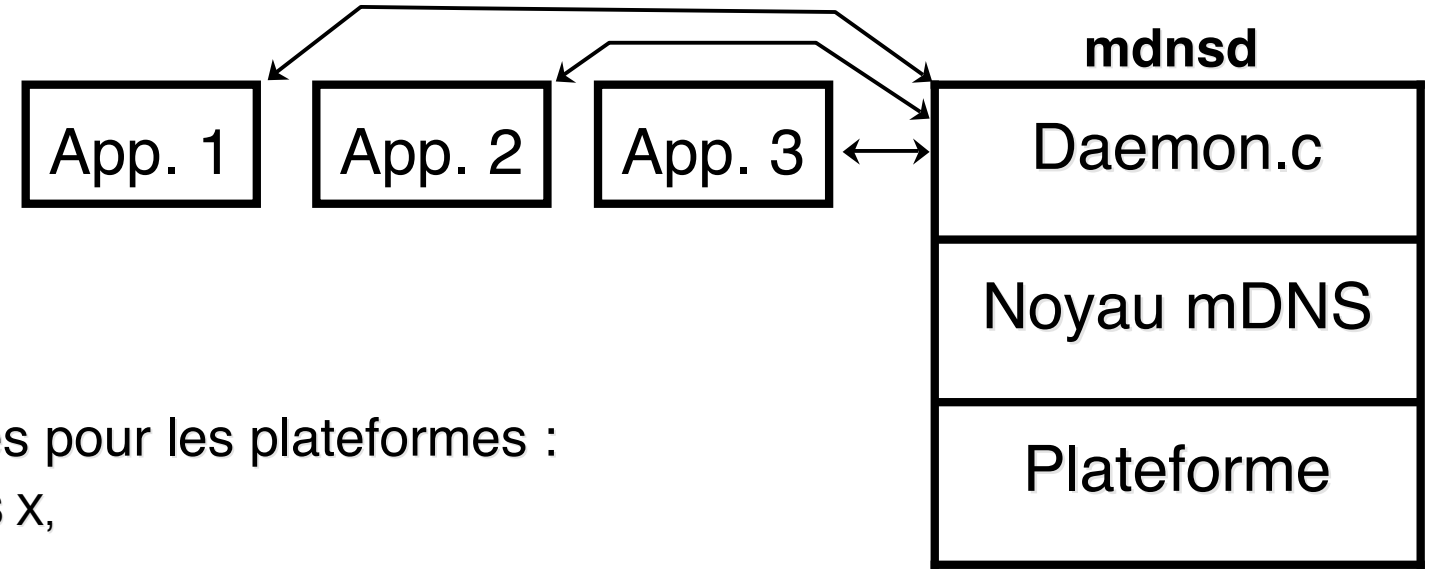
Pour tous les goûts :

JmDNS, PyZeroconf, PyRendezous, etc.

Et les vieux :

Liaison, mdnsd, tmdns …

mDNSResponder



- Sources disponibles pour les plateformes :
  - Mac OS 9, Mac OS X,
  - Windows,
  - Systèmes POSIX : Linux, Solaris, FreeBSD, etc.,
  - Vxworks.
- Support IPv4 et IPv6 (sauf Mac OS 9)
- Mac OS X / POSIX,
  - un démon : **mDNSResponder / mdnsd.**
- Programmes en ligne de commande :
  - mDNSResponder, dns-sd, mDNSNetmonitor, exemples, etc.

Wide Area Bonjour

Nouveauté de la version Mac OS X 10.4 (Tiger),

DNS-SD sur du DNS classique avec des mises à jour de serveurs et une portée mondiale.

Trois nouvelles propositions :

- DNS-LLQ (*DNS Long-Lived Queries*),
- DNS-UL (Dynamic DNS Update Leases),
- NAT-PMP (NAT Port Mapping Protocol).

Pour en savoir plus …

- `for truc in` **zeroconf**
  dotlocal
  multicastdns
  dns-sd

  `do`

  `http://`[**www.$truc.org**]

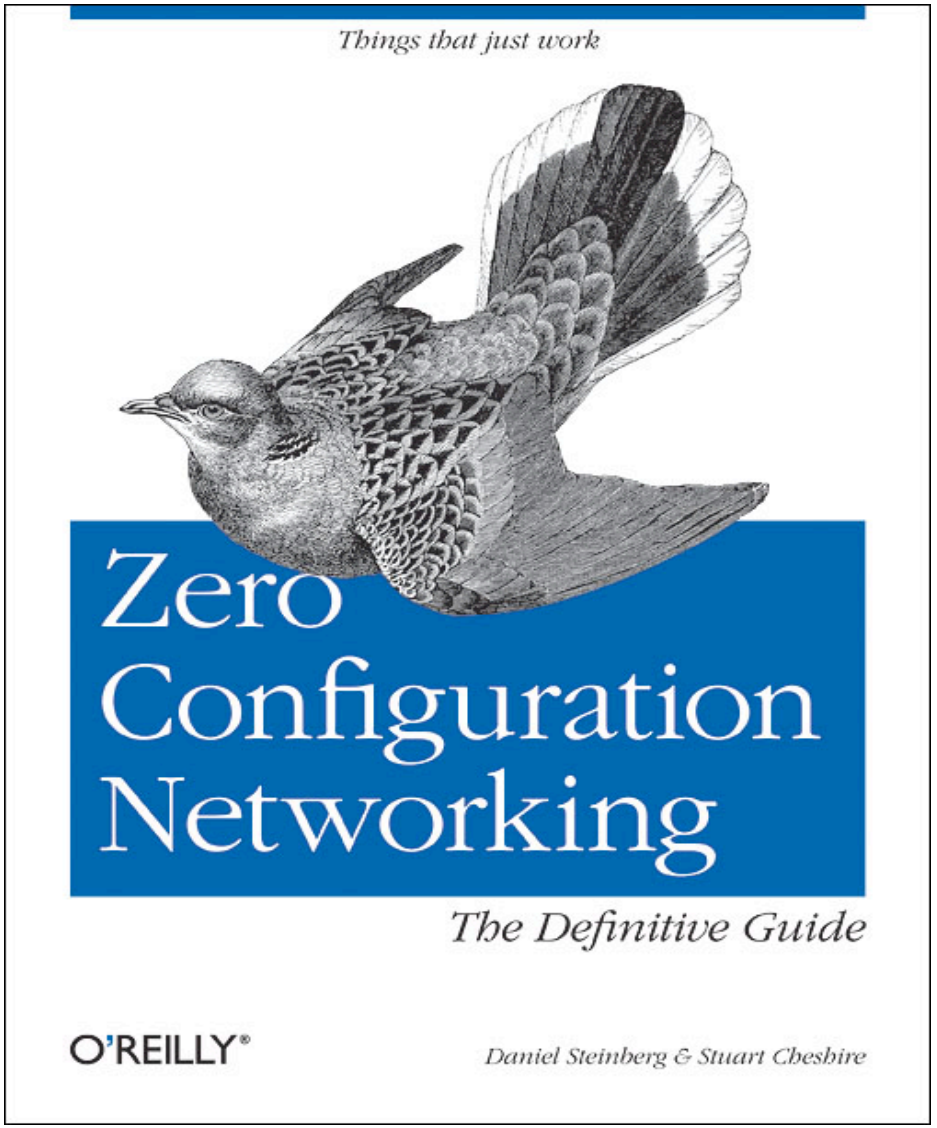
  `done`

- **Wikipedia**, entrée « *Zeroconf* »

- Le site développeurs Apple, rubrique « *Bonjour* ».

- Le livre qui paraîtra en …

  décembre 2005 !



THE END

Des questions ?

Ou une toute petite démo ?