# Démarrage à partir du réseau

Matthieu Herrb

LAAS-CNRS

12 octobre 2006

# Plan

# Pourquoi démarrer du réseau ?

## Installation

- alternative au boot sur CD ou disquette
- toujours disponible
- pas de limite de taille du média

## Dépannage

- Similaire à une installation
- N’utilise pas les disques de la machine
- Toujours disponible
- Partage ressources avec installation

# Pourquoi démarrer du réseau (2) ?

## Client Léger

- Pas de disque local
- Diminue coût, consommation, bruit
- Configurations centralisées

## Équipements réseau

- Pas de disque
- Pas de pièce mobile (fiabilité)
- Configurations centralisées
- Remplacé par une mémoire flash locale...

# Protocoles

Apparus avec le stations de travail dans les années 80.

- MOP (DEC)
- RARP (RFC903) + bootparams (Sun)
- TFTP (RFC 783, 1350, 2347)
- BOOTP (CMU RFC 951 )
- DHCP (RFC 2131, 2132, 3315)
- PXE (Intel)
- BINL (Boot Information Negotiation Layer - Microsoft)
- NetBoot (Apple)
- Zéroconf / Rendez-vous / Bonjour (RFC 3927)
- HTTP
- ...

# Principe du démarrage d’un ordinateur

- Boot primaire ROM
- Master Boot Record (secteur d’amorçage du disque - PC)
- Boot secondaire (Disque ou Réseau)
- Chargement du noyau en mémoire
- Montage du système de fichiers racine
- Scripts de boot $\rightarrow$ démarrage des services (démons)

# BOOTP : protocole

| op(1) | htype(1) | hlen(1) | hops(1) |
|---|---|---|---|
| xid(4) | | | |
| secs(2) | | flags(2) | |
| ciaddr(4) | | | |
| yiaddr(4) | | | |
| siaddr(4) | | | |
| giaddr(4) | | | |
| chaddr(16) | | | |
| sname(64) | | | |
| file(128) | | | |
| **vendor options**(64) | | | |

## BOOTP

- UDP
- port client : 68
- port serveur : 67
- htype=1 : ethernet
- hlen=6 : ethernet
- hops=0

# TFTP

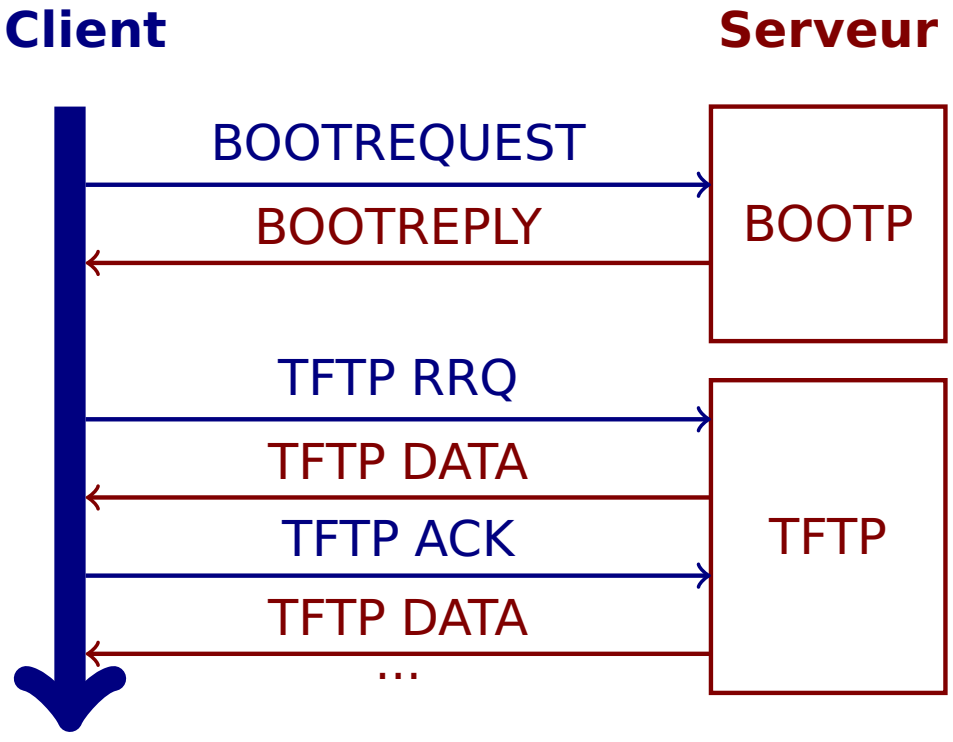
**T**rivial **F**ile **T**ransfer **P**rotocol

- UDP, port 69
- mode **netascii** ou **octet** (binaire)
- fenêtre réduite à un paquet

## Types de paquets TFTP

| opcode | operation |
|---|---|
| 1 | Read request (RRQ) |
| 2 | Write request (WRQ) |
| 3 | Data (DATA) |
| 4 | Acknowledgment (ACK) |
| 5 | Error (ERROR) |

# BOOTP + TFTP ensemble



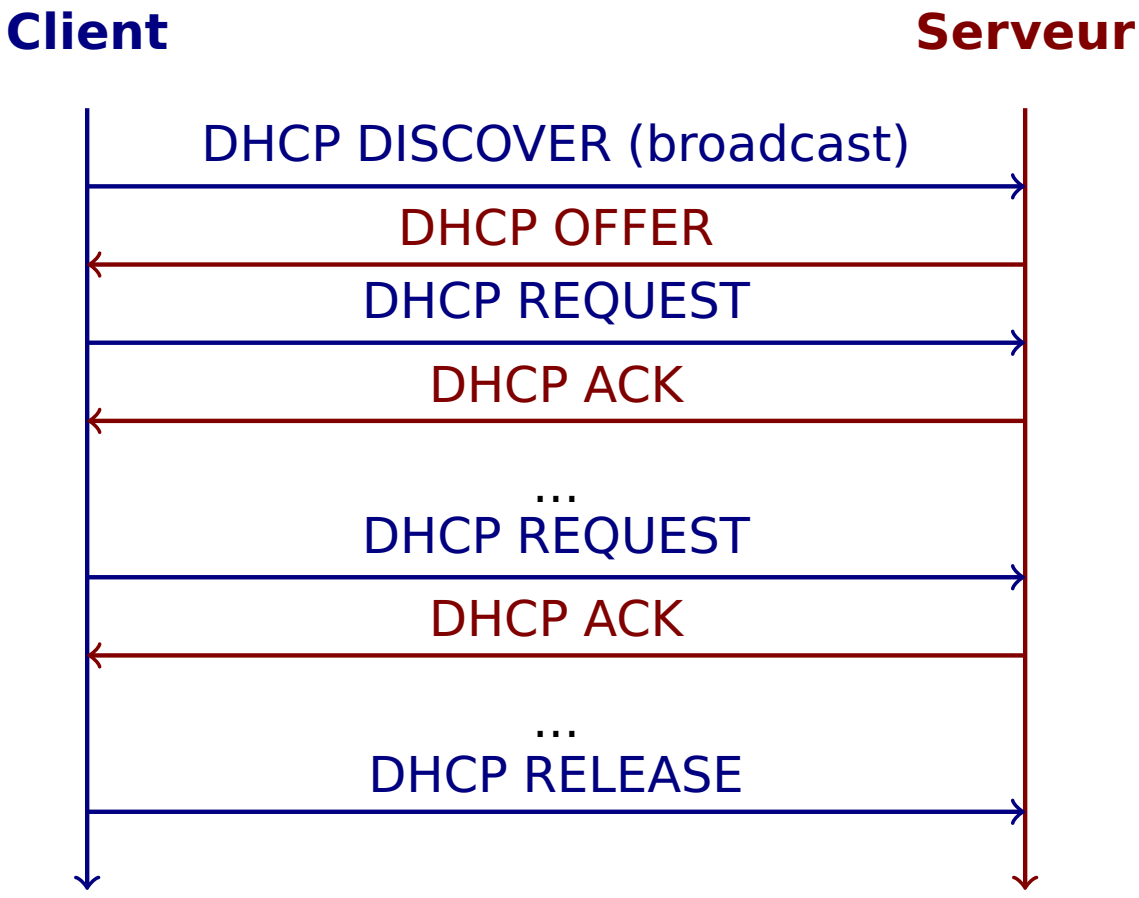

- Obtenir mon adresse IP et celle du serveur TFTP
- Télécharger le boot secondaire
- Exécuter le boot secondaire..

# Boot secondaire classique

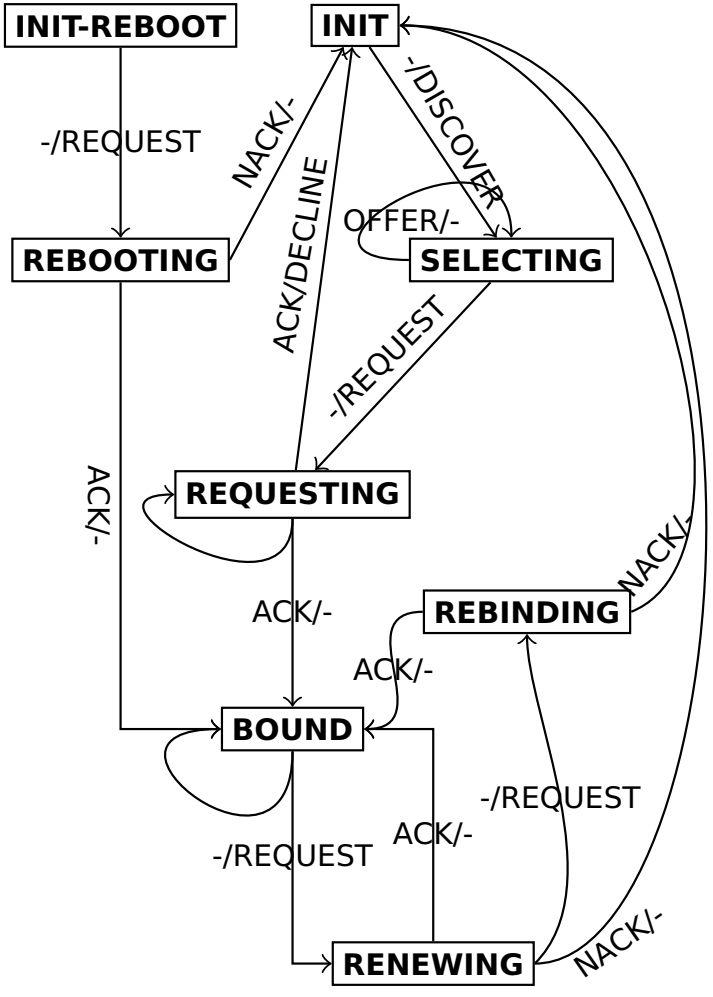
- obtenir les autres informations nécessaires (BOOTP / BOOTPARAMS)
  - serveur NFS
  - nom du noyau
  - taille et emplacement du swap
- montage du système de fichier racine et chargement du noyau (NFS)
- le boot secondaire passe la main au noyau

# DHCP

Dynamic Host Configuration Protocol



# DHCP (2)


INIT-REBOOT
INIT
-/DISCOVER
NACK/-
-/REQUEST
ACK/DECLINE
OFFER/-
REBOOTING
SELECTING
-/REQUEST
ACK/-
REQUESTING
NACK/-
ACK/-
REBINDING
ACK/-
BOUND
-/REQUEST
ACK/-
-/REQUEST
RENEWING
NACK/-

# DHCP - Options (RFC 2132)

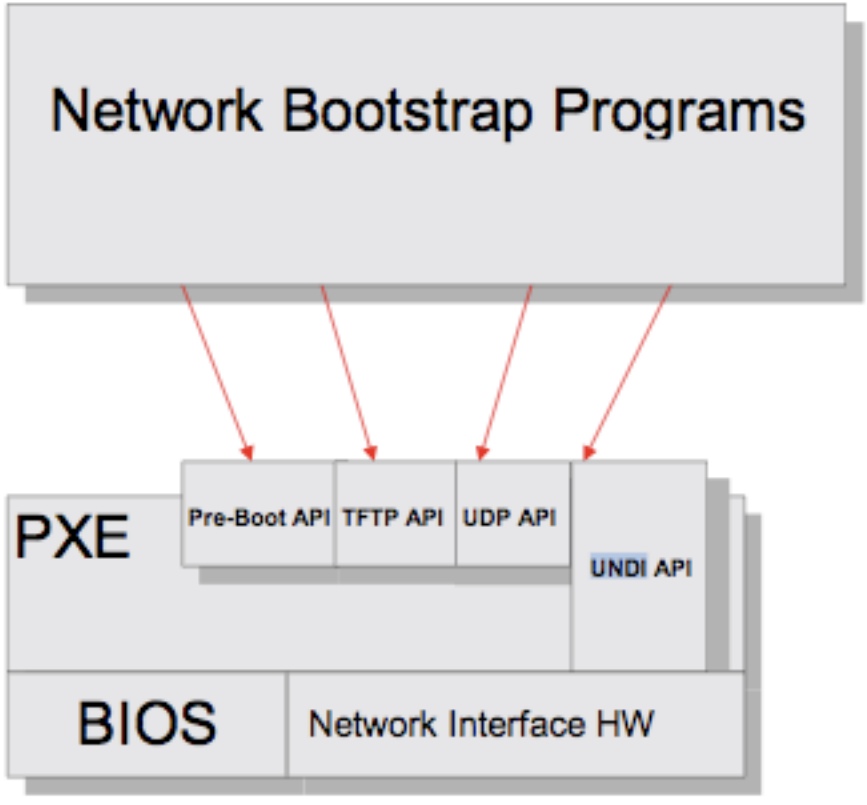
Stockées dans les vendor options des paquets. Plusieurs REQUEST si nécessaire.

- subnet mask
- timezone (offset)
- routeurs
- serveurs de temps
- serveurs DNS
- serveurs de Log
- host name
- domain name
- swap server
- root file system
- NIS domain, NIS server
- ...

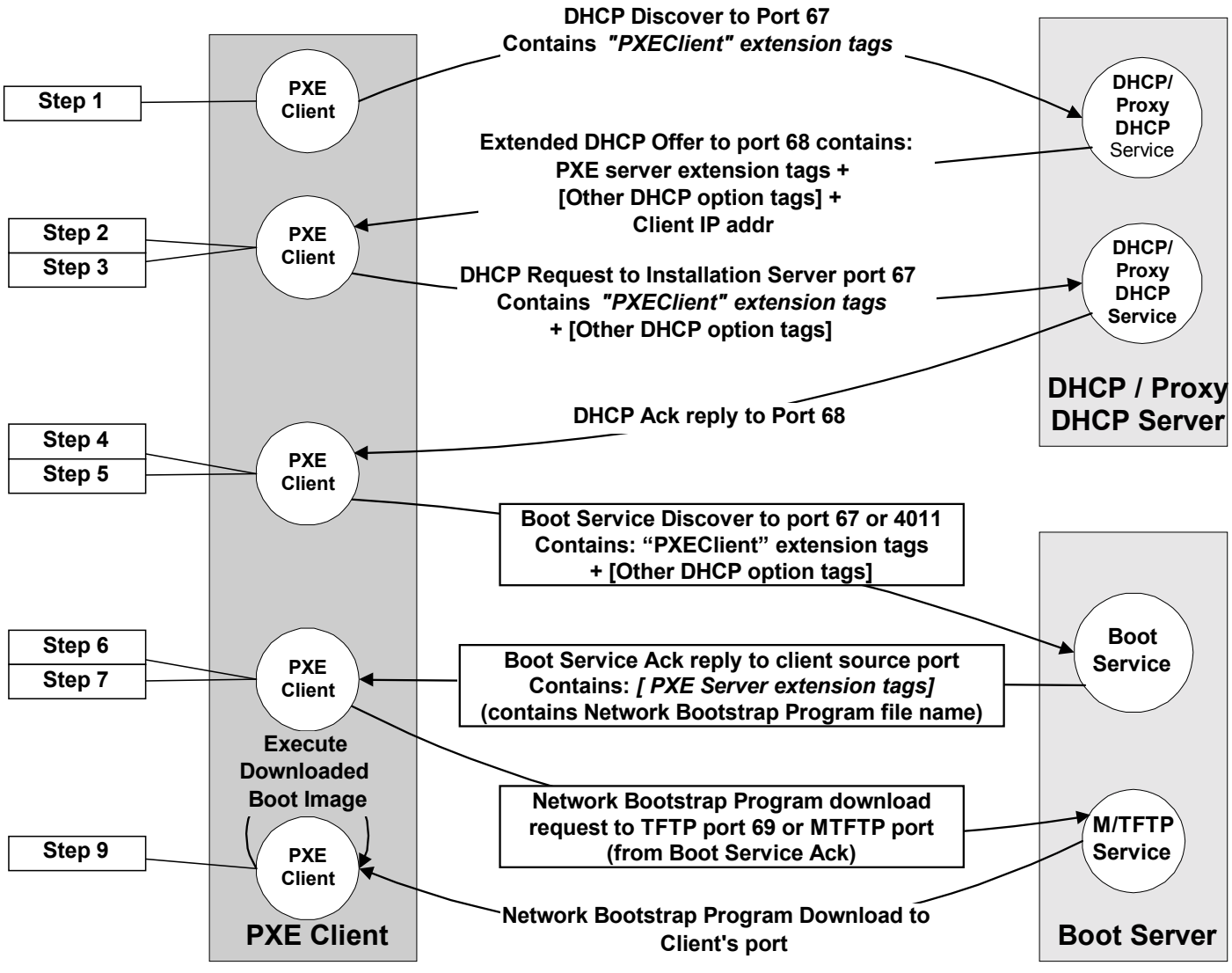
# PXE

**P**reboot e**X**ecution **E**nvironment

- Proposé par Intel - architectures x86
- Extension du BIOS sur les cartes réseau
- Utilise DHCP avec extensions & TFTP
- Supporté par la plupart des machines modernes avec carte réseau intégrée



# Séquence de boot PXE



# NetBoot

Boot réseau à la sauce Apple

- BOOTP/DHCP avec Options Apple
  TFTP + NFS, AFP ou HTTPS
- serveur fourni avec Mac OS X serveur
  (System Image Utility)
- récupère une image disque complète
  (système de fichiers + noyau)
- `http://images.apple.com/server/pdfs/Network_Install_TB_v10.4.pdf`

# Implémentations

## Coté client

- PC :
  - BIOS : PXE, Floppy : etherboot
  - NTLDR, PXELinux, PXEGrub, pxeboot (BSD), ...
- Mac, stations de travail, équipements réseau :
  - clients BOOTP/DHCP, TFTP en ROM
  - protocoles spécifiques (MOP, RARP, Bootparams)

## Coté serveur

- RIS
- Apple NetBoot Server
- ISC DHCP + tftp

# Etherboot

- image disque (disquette, clé usb) qui gère le boot réseau
- utile sur les machines sans BIOS PXE
- `http://www.etherboot.org/`
- `http://www.rom-o-matic.net/` pour générer une image avec le driver pour une carte réseau donnée.
- Variantes :
  - boot secondaire pour grub
  - ROM pour émulateurs (VMWare, Bochs, Qemu)

# PXELinux

- variante de SYSLINUX pour boot réseau (PXE)
- `http://syslinux.zytor.com/pxe.php`
- le BIOS PXE récupère `pxelinux.0` par TFTP
- pxelinux utilise TFTP pour :
  - charger un fichier pxelinux.cfg (par adresse MAC ou adresse IP)
  - charger un noyau Linux (avec initrd) et lui passer les paramètres définis par `pxelinux.cfg`

# Grub

**GR**and **U**nified **B**ootloader

- `http://www.gnu.org/software/grub/grub-legacy.en.html`
- Boot loader générique utilisé entre autres par Linux, Solaris 10 (06/06),...
- Images secondaires pour boot réseau :
  - `pxegrub` - PXE
  - `nbgrub` - etherboot
- Chargent le fichier de configuration (`grub.conf`) et le noyau par TFTP
- Supporte également RARP
- Ne supporte pas toutes les cartes réseau

# Serveur DHCP : ISC DHCPD

- `http://www.isc.org/index.pl?/sw/dhcp/`
- Le plus répandu des serveurs DHCP Open-Source pour Unix
- Distribue des adresses IP dynamiques ou statiques
- Supporte toutes les extensions spécifiques des vendeurs
- Configuration via `/etc/dhcpd.conf`

# Exemple de /etc/dhcpd.conf

```
shared-network LOCAL-NET {
        subnet 10.0.1.0 netmask 255.255.255.0 {
                option domain-name-servers 10.0.1.254;
                option routers 10.0.1.254;
                range 10.0.1.1 10.0.1.200;
        }

        host robitop {
                hardware ethernet 00 :0d :56 :ea :39 :f2;
                next-server 10.0.1.254;
                fixed-address 10.0.1.253;
                filename "pxegrub";
        }
}
```

# RIS

**R**emote **I**nstallation **S**ervice

- Service d'installation à distance pour Windows 2000/XP
- Basé sur PXE + TFTP + BINL
- Permet de gérer le boot de n'importe quel client PXE
  `http://syslinux.zytor.com/ris.php`
- Serveur RIS sur Linux :
  `http://oss.netfarm.it/guides/pxe.php`

Voir aussi présentation suivante...

# Sécurité

- pas d'authentification
- UDP $\longrightarrow$ spoofable
- adresse MAC $\longrightarrow$ forgeable
- broadcast $\longrightarrow$ un seul serveur par LAN (DoS)
- DHCP distribue des paramètres sensibles (route, serveurs d'authentification, ...)

$\Rightarrow$ Nécessite un réseau local physiquement protégé.

Permet aussi de faire des images de disques piratés en vue d'analyse future (CERT, services de police/justice). Cf formation A2IMP...

# Conclusion

Boot réseau : l'un des couteaux suisses de l'administration système
Infrastructure :

- serveur DHCP
- serveur TFTP
- serveur NFS (Unix)
- tcpdump ou ethereal

**Évolutions :** Utilisation de HTTP(s) + scripts CGI/SOAP/...
$\longrightarrow$ solutions propriétaires et fermées : - (

Questions ?