istic Informatique Électronique

Architecture Réseaux Entreprises (ARES)

Services réseau essentiels

Brice - Ekane (brice.ekane@univ-rennes.fr)

ISTIC Rennes - France

2025-2026

git clone https://github.com/bekane/ares-2025.git

Plan du module

Outline for section 1

Objectifs

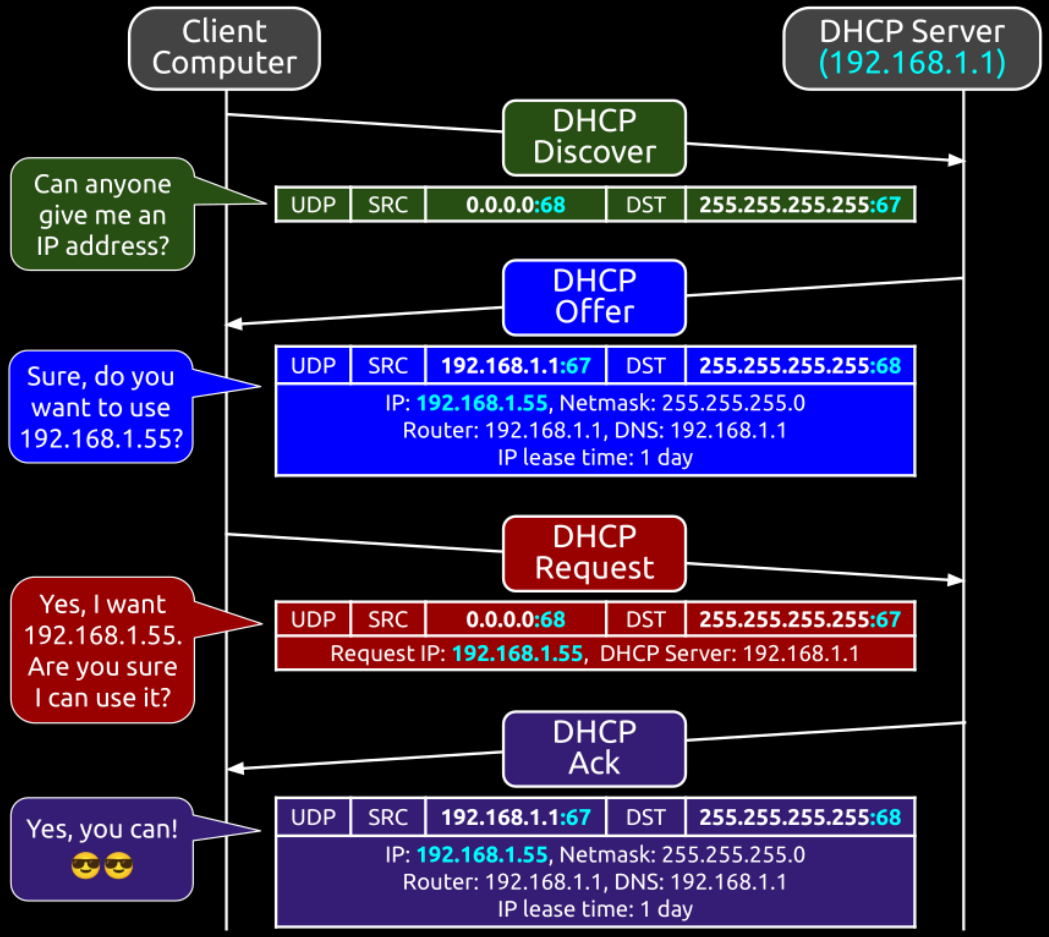
- **Comprendre** : rôle fondamental de DHCP, DNS dans l'infrastructure.

Outline for section 2

Sans IP, pas de réseau

- **Problème** : une machine sans IP ne peut pas sortir de son segment local.
- **Broadcast de découverte** : `255.255.255.255` $\rightarrow$ seul moyen d'atteindre un serveur DHCP inconnu.
- **DORA en 4 temps** :
  1. Discover – « Qui peut me donner une IP ? »
  2. Offer – « Je t'offre X.X.X.X »
  3. Request – « Je veux X.X.X.X »
  4. Ack – « C'est à toi »
- **DHCP Relay** : transmet le Discover d'un VLAN à un serveur central.

DHCP - DORA



Implémentations de serveurs DHCP

Plusieurs solutions existent

- **ISC DHCP** : historique, très répandu, mais considéré comme legacy.
- **Dnsmasq** : léger, simple à configurer, combine DNS et DHCP.
- **Kea (ISC)** : successeur moderne d'ISC DHCP, modulaire, API REST.
- **systemd-networkd** : service intégré au système.
- **dhcpd intégré aux routeurs/box** : version simplifiée, souvent propriétaire.
- ...

dnsmasq

Qu'est-ce que dnsmasq ?

- Service léger qui combine DNS cache et DHCP serveur.
- Utilisé dans les réseaux locaux, routeurs et environnements virtualisés.
- Facile à configurer.
- Polyvalent : brique technique dans des environnements cloud, virtualisation et conteneurs.

dnsmasq - Installation (exemple Debian/Ubuntu)

```
sudo apt update
sudo apt install dnsmasq
```

dnsmasq - Logs et supervision

- Journal système : `sudo journalctl -u dnsmasq`
- Ou dans `/var/log/syslog` selon la configuration.
- Messages typiques : attribution d'IP, requêtes DNS, erreurs.

dnsmasq - Exemple de configuration

```
# écouter sur l'interface lan eth0
interface=eth0

# Plage d'adresses et durée
dhcp-range=192.168.1.50,192.168.1.150,12h


# Masque de sous-réseau (option 1)
dhcp-option=1,255.255.255.0

# définir la passerelle par défaut
dhcp-option=3,192.168.1.1

# Broadcast address (option 28)
dhcp-option=28,192.168.1.255

# définir une option DNS
dhcp-option=6,8.8.8.8,8.8.4.4
```

Options DHCP courantes (dnsmasq)

Option	Nom	Exemple dnsmasq
1	Masque de sous-réseau	`dhcp-option=1,255.255.255.0`
3	Passerelle (routeur)	`dhcp-option=3,192.168.1.1`
6	DNS servers	`dhcp-option=6,8.8.8.8,8.8.4.4`
15	Nom de domaine	`dhcp-option=15,example.com`
28	Adresse de broadcast	`dhcp-option=28,192.168.1.255`
42	Serveur NTP	`dhcp-option=42,192.168.1.100`
51	Durée du bail (lease time)	`dhcp-option=51,3600`
66	Nom du serveur TFTP	`dhcp-option=66,"tftp.local"`
67	Fichier de boot (PXE)	`dhcp-option=67,"pxelinux.0"`
119	Domain search list	`dhcp-option=119,corp.local`
121	Routes statiques classless	`dhcp-option=121,192.168.2.0/24,192.168.1.1`

Attribuer des adresses IP statiques

Configuration des baux statiques

- Vous pouvez assigner une adresse IP fixe à un périphérique spécifique en fonction de son adresse MAC.
- Ajouter cette configuration dans le fichier `dnsmasq.conf` :
  - `dhcp-host=00:11:22:33:44:55,192.168.1.10`
- Cela associe l'adresse MAC `00:11:22:33:44:55` à l'adresse IP `192.168.1.10`.

Sécuriser le service DHCP

Limitation de la portée du DHCP

- Limiter les interfaces sur lesquelles le service DHCP fonctionne :
  - `interface=eth0`
- Vous pouvez spécifier plusieurs interfaces si nécessaire :
  - `interface=eth0,eth1`
- Cette configuration empêche le DHCP de répondre sur des interfaces non autorisées.

DHCP `authoritative`

Deux modes possibles

- **Authoritative** :
  - Le serveur déclare être l'**autorité unique** sur le réseau.
  - Répond rapidement aux clients avec des baux corrects.
  - Force la réattribution si le client arrive avec une IP invalide.

- **Non-authoritative** :
  - Le serveur reste **passif**.
  - Si le client demande une IP douteuse, il peut attendre ou être ignoré.
  - Utile si **plusieurs DHCP coexistent**.

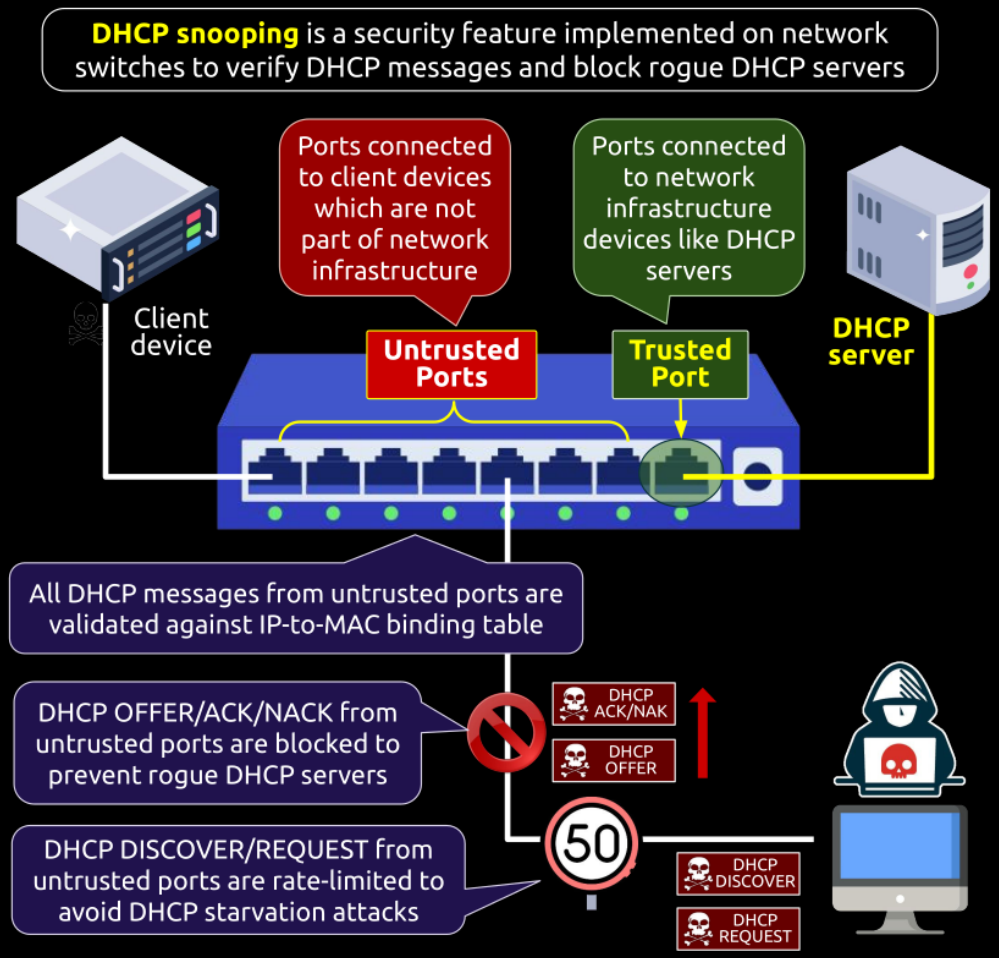
Exemple dnsmasq

```
dhcp-authoritative
```

DHCP Snooping et `dnsmasq`

- **DHCP Snooping** = fonction de sécurité d'un switch (L2).
- Permet de bloquer les **DHCP rogue** (faux serveurs DHCP).
- Maintient une table IP $\leftrightarrow$ MAC $\leftrightarrow$ Port.
- `dnsmasq` = serveur DHCP/DNS, il ne fait pas de snooping.

DHCP Snooping et dnsmasq



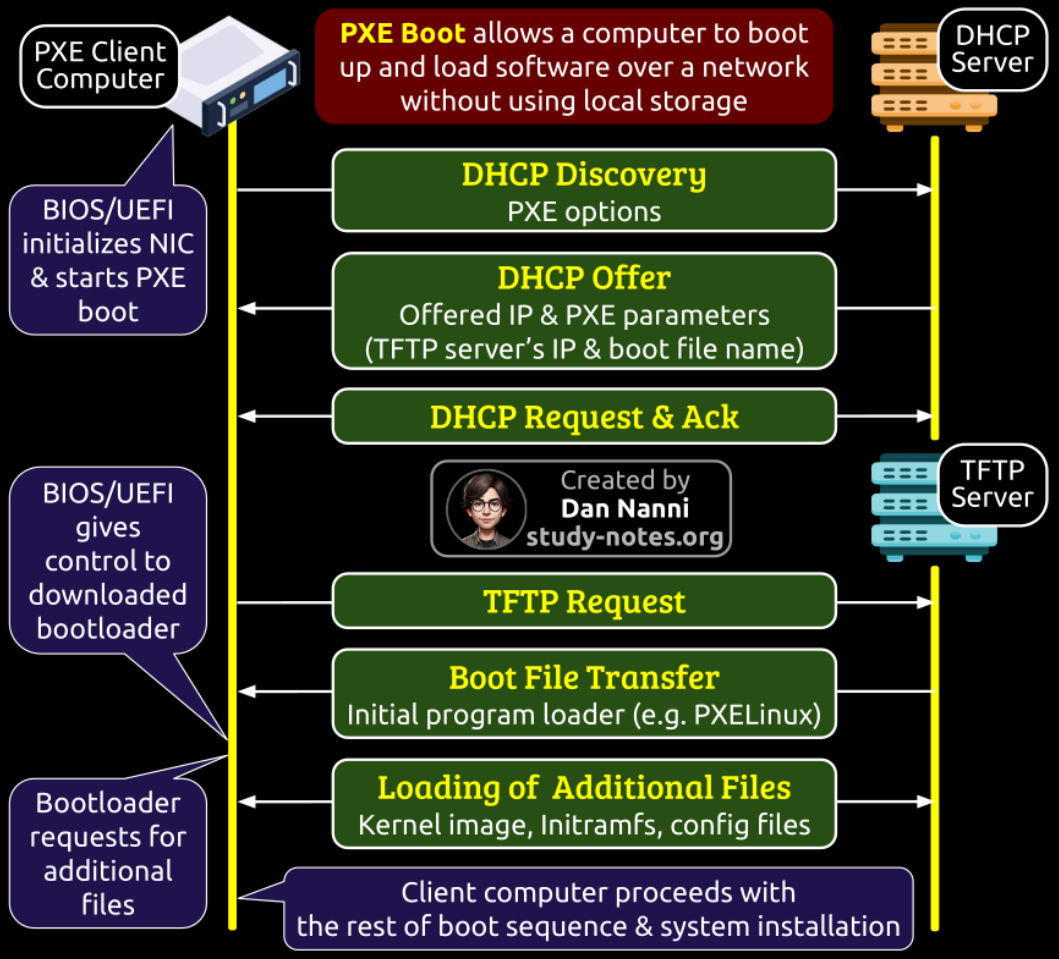
©Dann Nanni

PXE Boot avec `dnsmasq`

Principe

- **PXE** (Preboot eXecution Environment) permet de démarrer une machine via le réseau.
- `dnsmasq` fournit un service léger combinant **DHCP**, **TFTP**.

PXE Boot - Étapes du PXE Boot



PXE Boot avec dnsmasq

Exemple de configuration

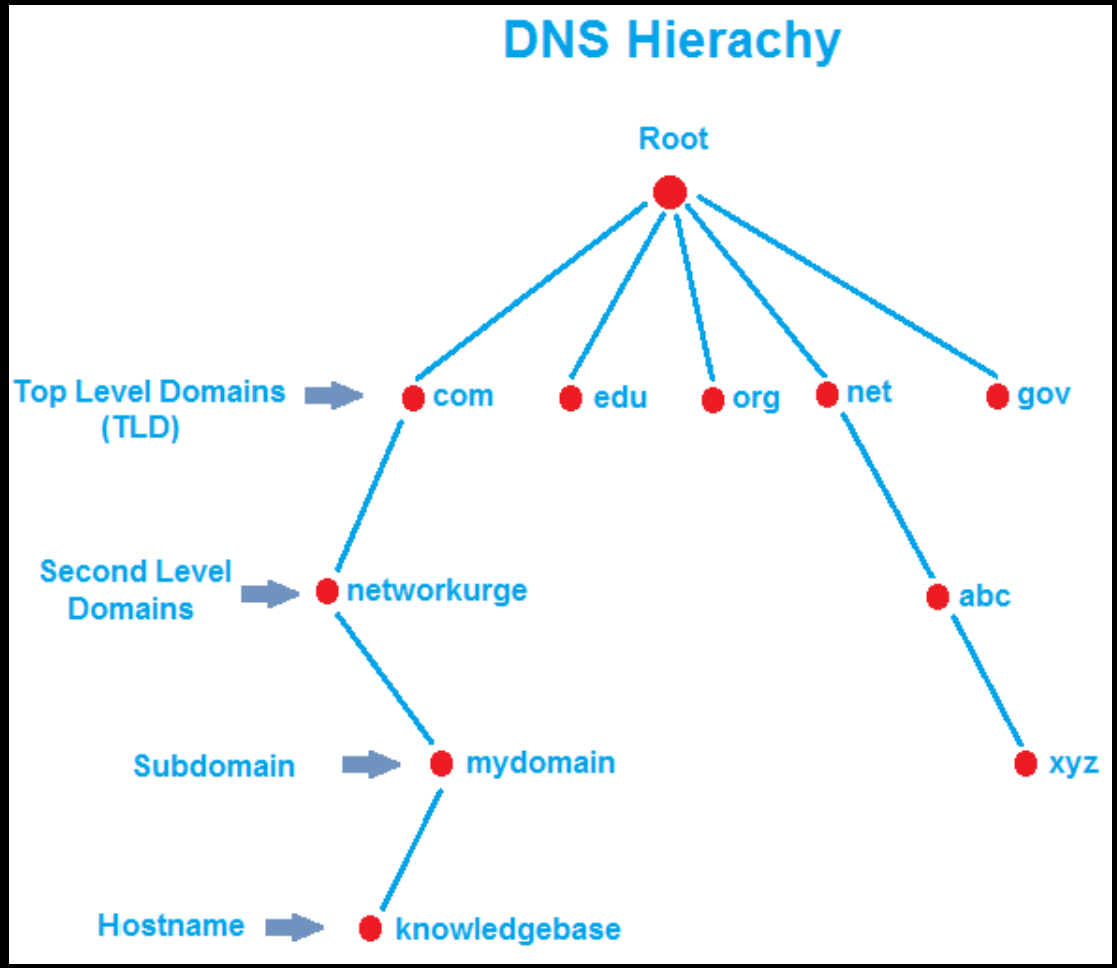
```
dhcp-range=192.168.1.50,192.168.1.150,12h
dhcp-boot=pxelinux.0
enable-tftp
tftp-root=/srv/tftp
```

Outline for section 3

Hiérarchie et requêtes

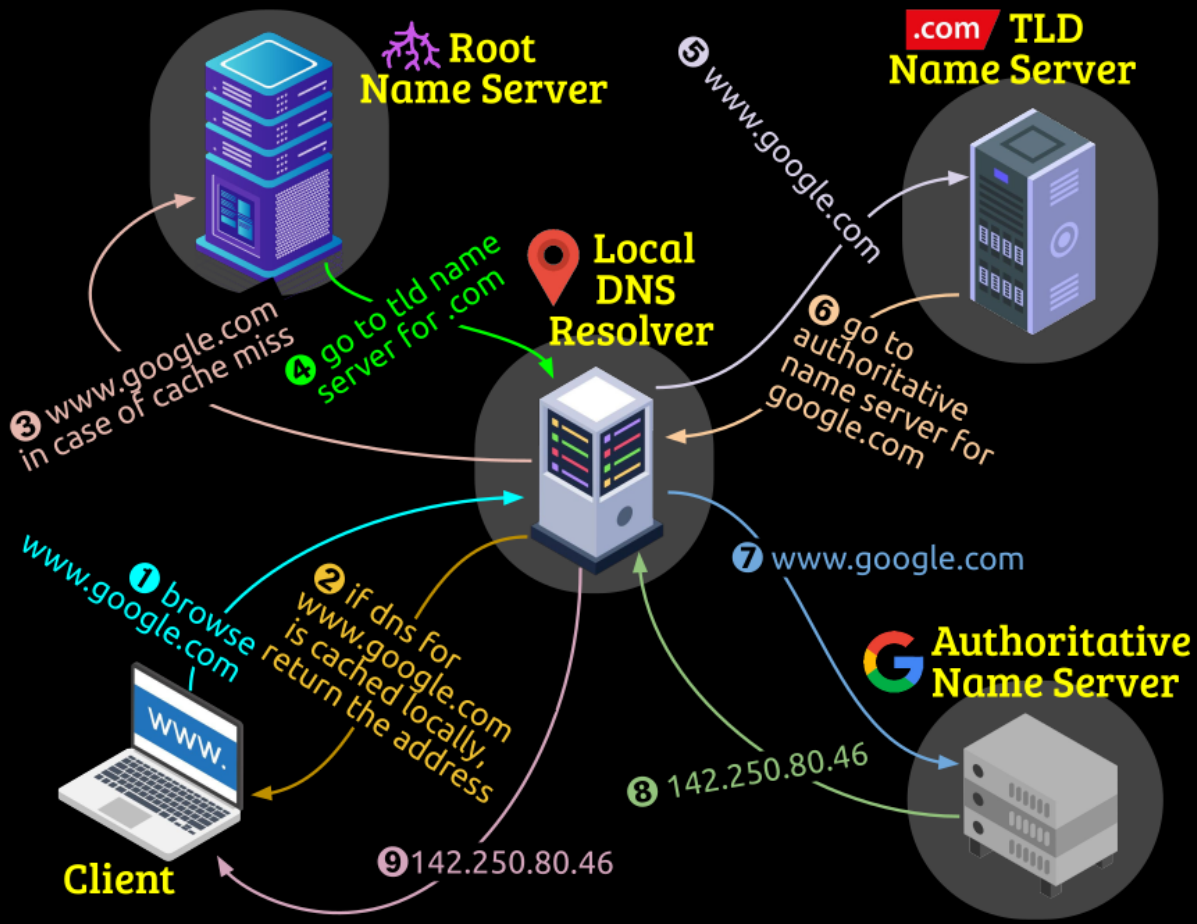
- **Hiérarchie** : délégation par zones (`.`, `.com`, `google.com`) $\rightarrow$ scalabilité.
- **Requêtes** :
  - *Récursive* : le serveur local fait tout.
  - *Itérative* : le client relance vers chaque serveur indiqué.
- **Enregistrements clés** : A, AAAA, CNAME, MX, PTR (résolution inversée).

Hiérarchie

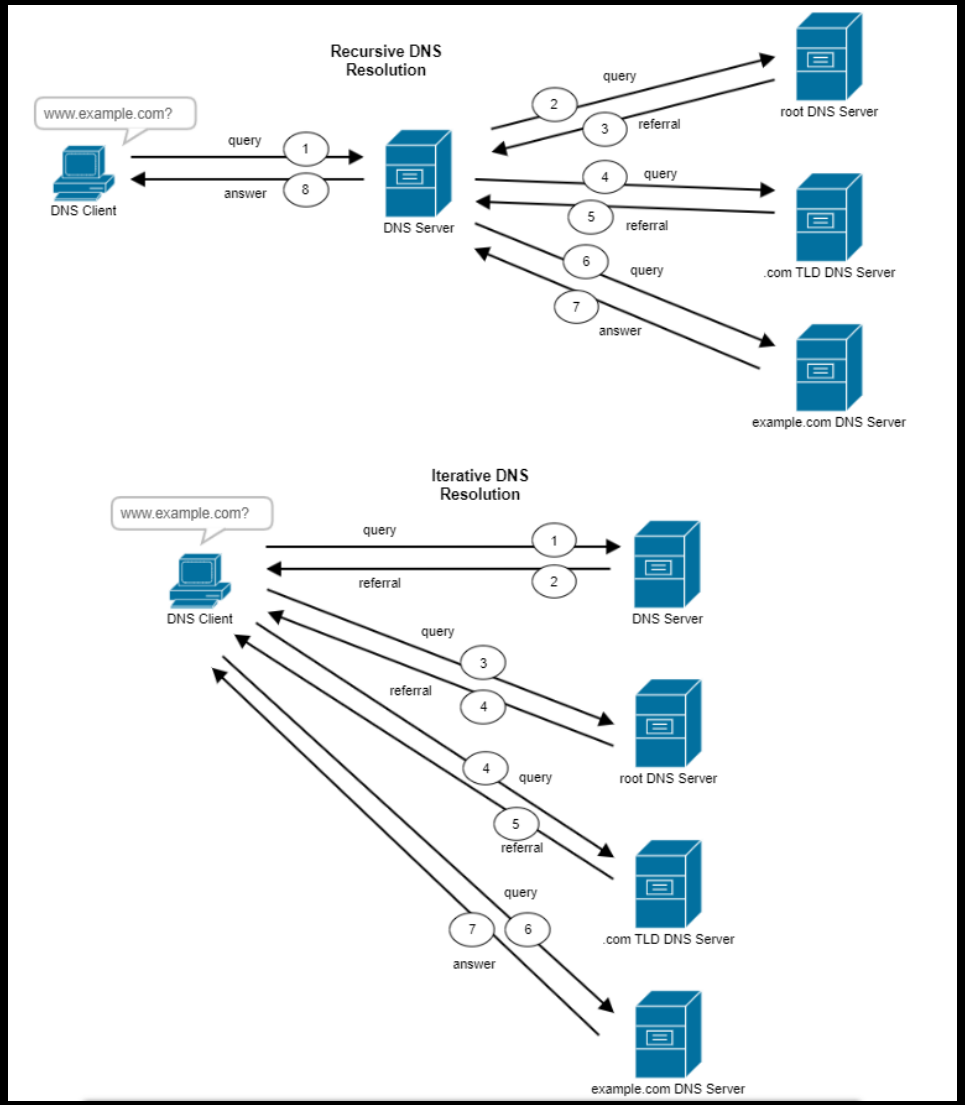


https://www.networkurge.com/2017/11/how-dns-works.html

DNS - Fonctionnement

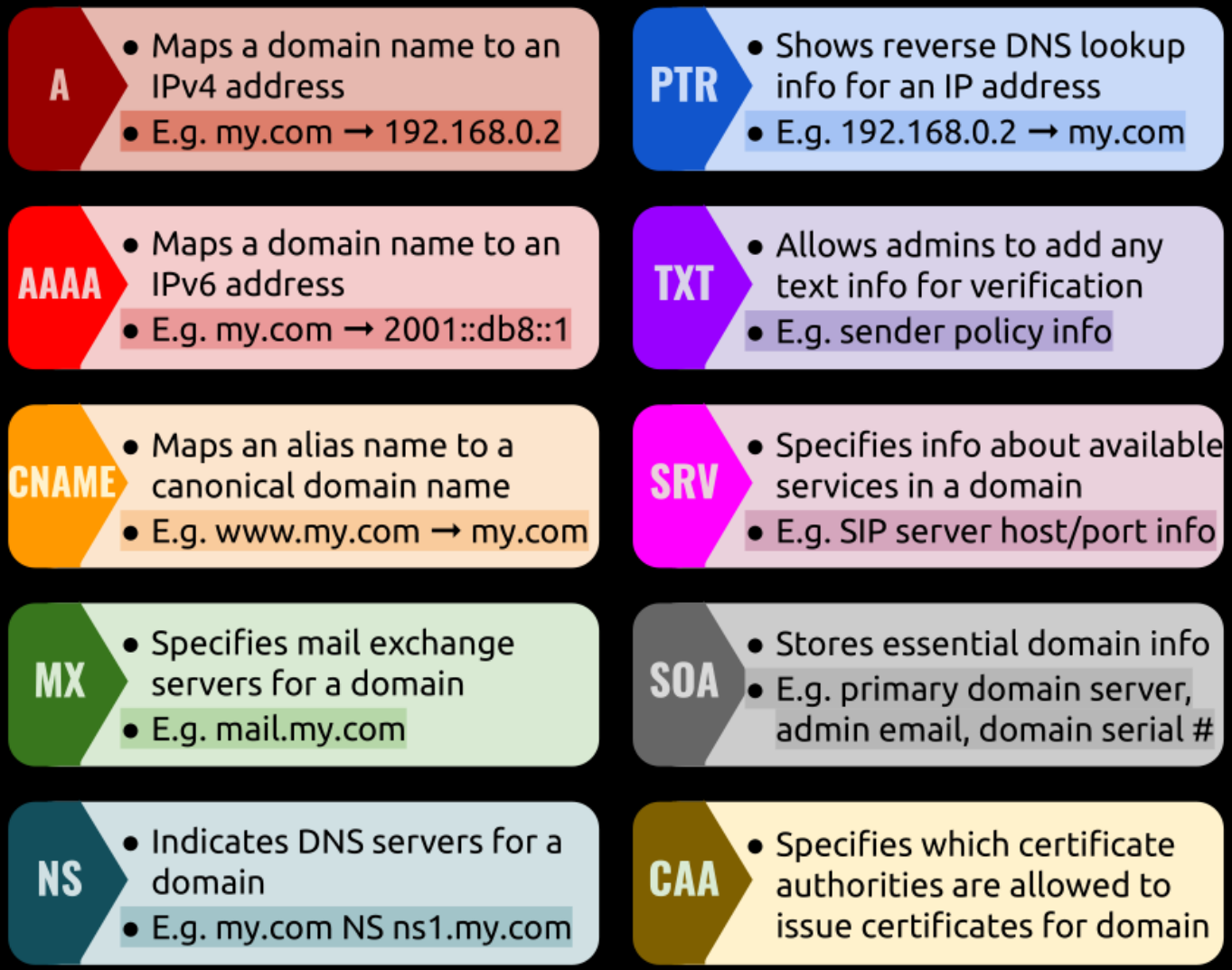


DNS - Récursive vs Itérative



https://geekmungus.co.uk/?p=3771

Enregistrements DNS principaux



dnsmasq vs Bind9 : comparaison de la notation

Type	dnsmasq	Bind9
A	`address=/www.ex.com/192.0.2.10`	`www IN A 192.0.2.10`
AAAA	`address=/www.ex.com/2001:db8::10`	`www IN AAAA 2001:db8::10`
CNAME	`cname=blog.ex.com,www.ex.com`	`blog IN CNAME www`
MX	`mx-host=ex.com,mail.ex.com,10`	`@ IN MX 10 mail.ex.com.`
PTR	`ptr-record=10.2.0.192.in-addr.arpa,www.ex.com`	`10 IN PTR www.ex.com.`
TXT	`txt-record=ex.com,"v=spf1 -all"`	`@ IN TXT "v=spf1 -all"`
SRV	`srv-host=_sip._tcp.ex.com,sip1.ex.com,5060,10,60`	`_sip._tcp IN SRV 10 60 5060 sip1.ex.com.`
NS	*pas supporté nativement*	`@ IN NS ns1.ex.com.`

dnsmasq = parfait comme résolveur/cache DNS + DHCP + services locaux vs. Bind9 = standard production

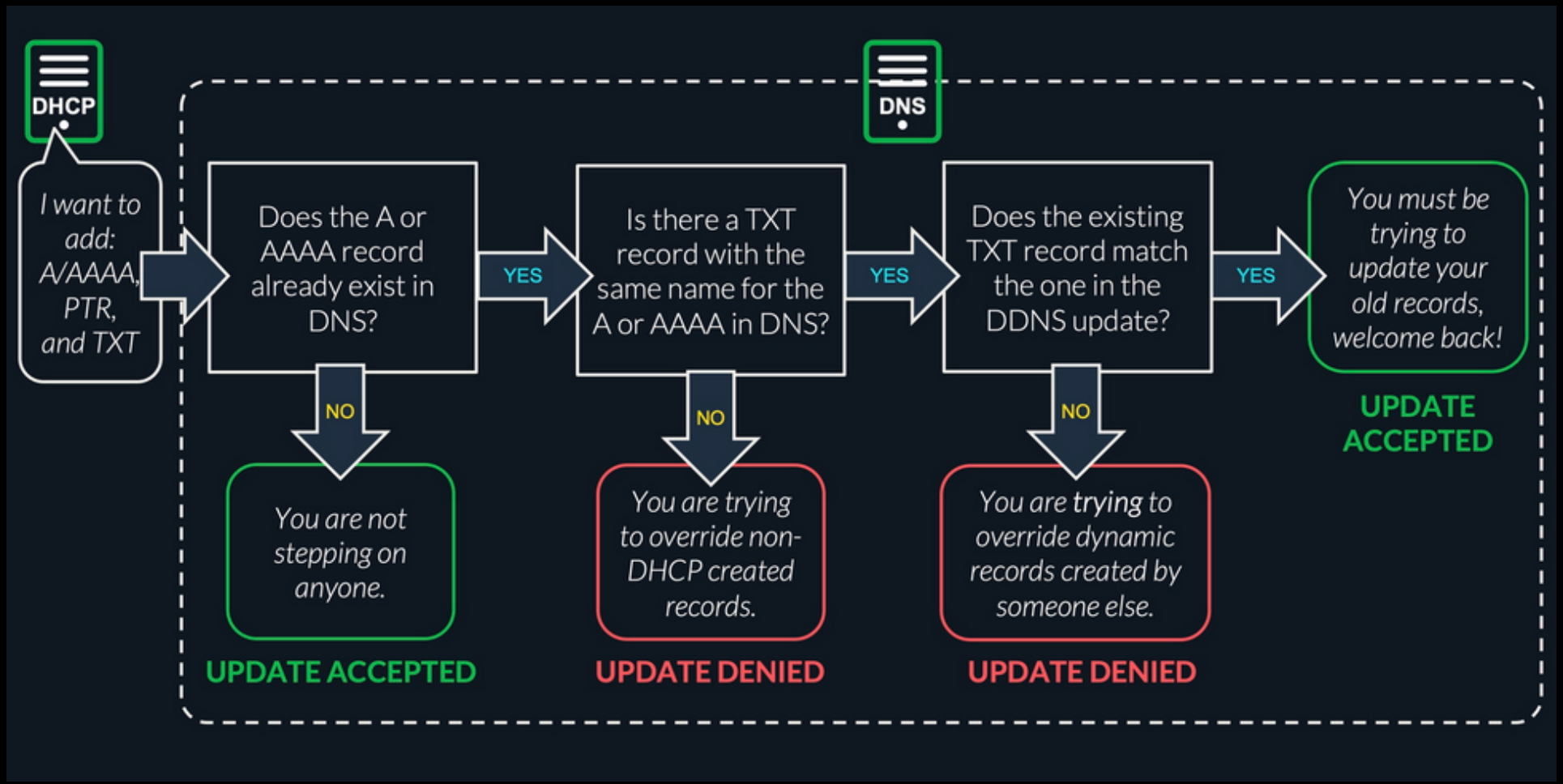
dnsmasq - exemples

```
   # Activer le service DHCP sur le réseau local
interface=eth0
dhcp-range=192.168.1.50,192.168.1.150,12h

# Passerelle par défaut
dhcp-option=3,192.168.1.1

# DNS à annoncer aux clients
dhcp-option=6,192.168.1.1,8.8.8.8

# Activer le cache DNS
cache-size=1000

# Domaine local
domain=exemple.com

# Ne pas forwarder noms incomplets
domain-needed
bogus-priv

# DNS amont
server=8.8.8.8

# A & AAAA records
address=/www.exemple.com/192.0.2.10
address=/www.exemple.com/2001:db8::10

# CNAME (alias)
cname=blog.exemple.com,www.exemple.com
```

Dynamic DNS (DDNS)

- **Problème** : IP attribuée dynamiquement $\rightarrow$ risque d'info obsolète dans DNS.
- **Solution** : DHCP informe DNS après attribution (mise à jour A et PTR).
- **Implémentations** :
  - `dnsmasq` : intègre DHCP + DNS.
  - `isc-dhcp-server` + Bind : mise à jour sécurisée via DDNS Update.

Dynamic DNS (DDNS)



from: https://www.dnsinsecurity.com/blog/ddns-update-security

Outline for section 4

Synthèse

- DHCP, DNS, DDNS = fondations automatiques du réseau.
- Prochaine étape : sécuriser avec VPN (WireGuard).

Ressources

- Lire : RFC 1035 (DNS), RFC 2131 (DHCP), RFC 1027 (Proxy ARP).
- Préparer la prochaine séance : VPN et sécurité avec WireGuard.