Serveur DDNS / DHCP

Sujet du projet ?

« Notre réseau est équipé d'un serveur DNS primaire/secondaire fonctionnel. Cependant, l'adressage est statique.
Nous vous demandons de mettre en place un serveur DHCP qui permettra d'assurer la configuration automatique des paramètres TCP/IP des hôtes qui se connecteront sur le réseau.
Par ailleurs, un second serveur dhcp assurera une tolérance de panne. »

Structurons notre démarche :

*** Création du serveur Primaire**

- Service DHCP
- Service DynDNS

**** Serveur secondaire**

- Service DHCP failover
- DNS secondaire

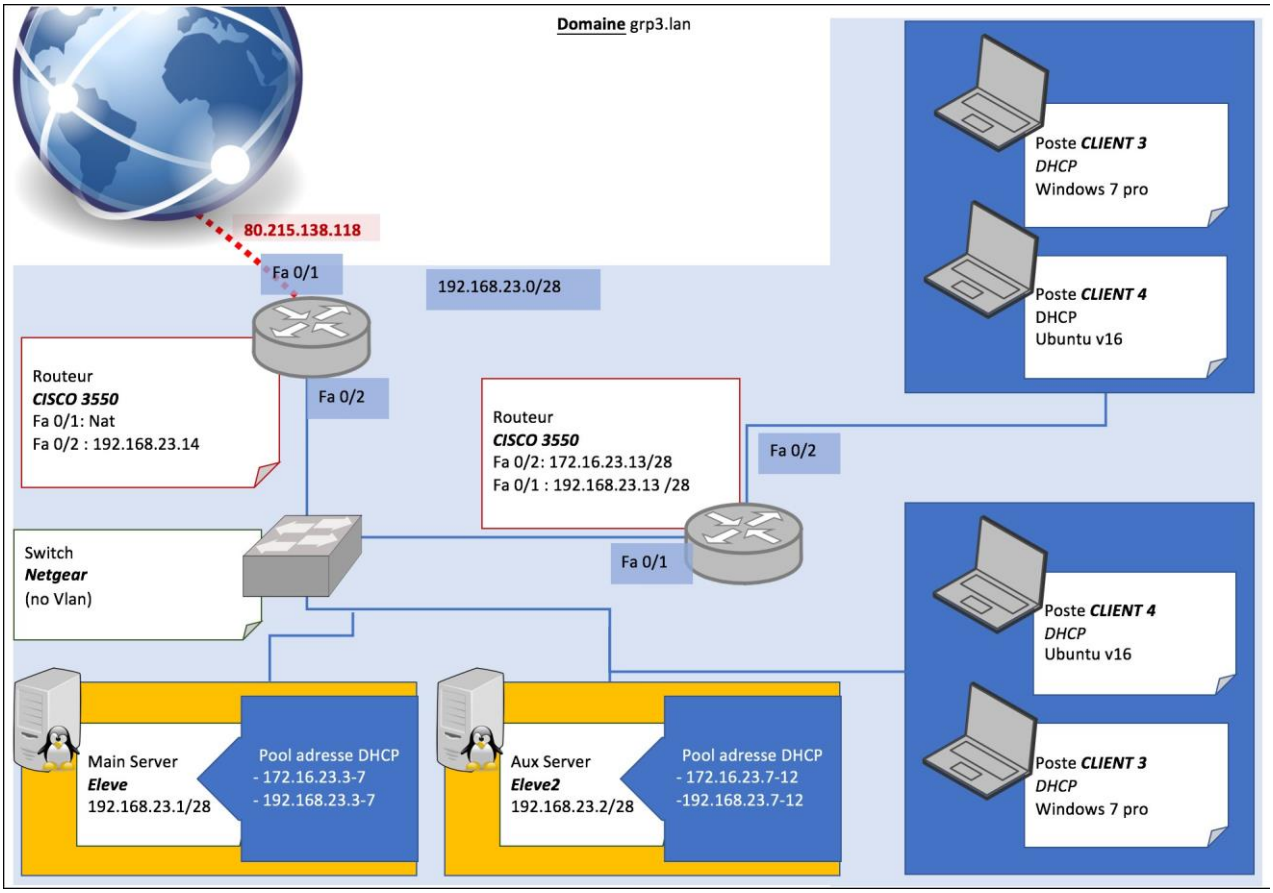
**** Routeur**

- Création de l'architecture (schéma)
- Configuration router1 & routeur 2
- ⚠ Dhcp relay

\+ configuration PC Fedora / MacOS / Windows 7

\+ **PROBLÈMES RENCONTRÉS**

Schema de Production



Configuration du serveur DNS primaire et secondaire

Créer deux machines dans le même lan et configurer les adresses : 192.168.23.1 pour le primaire et 192.168.23.2 pour le secondaire.

On retiendra donc que pour la suite on:

PC1 & PC2 : 172.16.23.x et 172.16.23.y

PC 3 & PC4 : 192.168.23.x et 192.168.23.y

DNSDHCP Main : 192.168.23.1

DNSDHCP Aux : 192.168.23.2

Configuration communes aux deux machines

Installer ***bind*** avec la commande

```
yum install bind-chroot
```

Dans **/etc/selinux/config** vérifiez que selinux est désactivé :

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

vi /etc/sysconfig/network-scripts/ifcfg-enp0s3

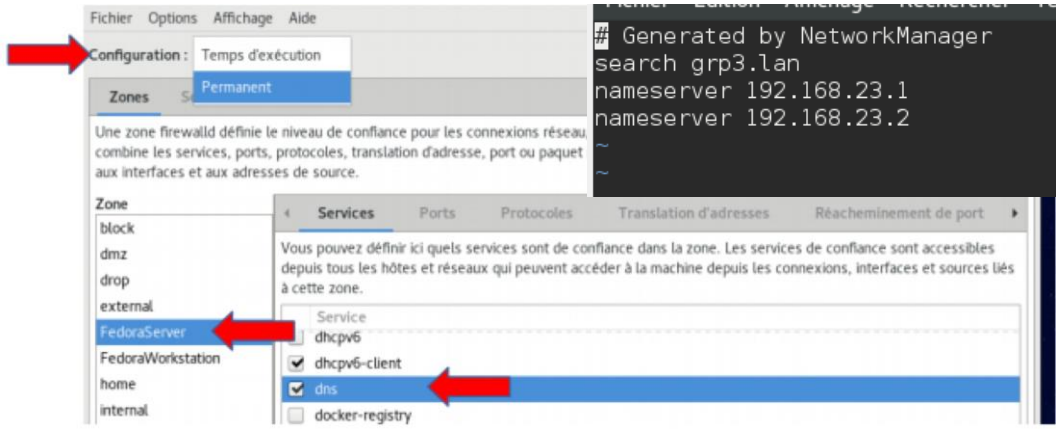
➤et renseigner ces informations (ip différente

```
HWADDR="08:00:27:3B:7D:F4"
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="enp0s3"
UUID="52d0d6f3-9ae5-496f-ae89-4bea23e5212a"
ONBOOT="yes"
PEERDNS="yes"
PEERROUTES="yes"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
IPADDR="192.168.23.1"
DOMAIN="grp3.lan"
DNS1="192.168.23.1"
DNS2="192.168.23.2"
~
~
~
```

Finissons par démarrer le service **named** au démarrage avec la commande

systemctl enable named

➤ Désactiver le firewall par défaut avec la commande systemctl stop firewall ou aller dans les configurations du firewall (s'il est installé)



➤ Ou par interface graphique :

Configuration communes aux deux machines

Aller dans le fichier **/etc/named.conf** et renseigner ces informations :

```
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 192.168.23.1; };
        listen-on-v6 port 53 { ::1; };
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        forwarders { 8.8.8.8; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation no;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
```


```
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation no;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
```


```
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named.conf.local";
include "/etc/rndc.key";
```

➤ Créer le fichier **named.conf.local**

/etc/named.conf.local

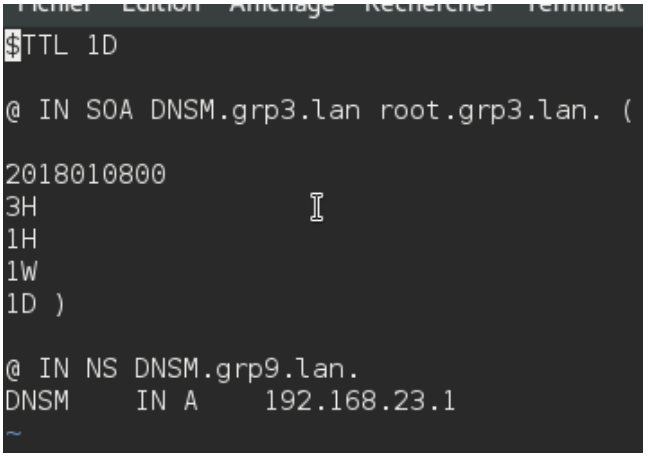
et le compléter de la façon suivante :

```
zone "grp3.lan" {
        type master;
        file "db.grp3.lan";
        allow-update { key pti; };
};

zone "23.168.192.in-addr.arpa" {
        type master;
        file "rev.grp3.lan";
        allow-update {key pti; };
};
```

Créer deux fichiers : un pour la recherche directe, un autre pour la recherche inversée.

Réciproquement :

➤ db.grp3.lan



➤rev.grp3.lan.

On teste ensuite les deux fichiers avec les commandes

```
named-checkzone grp3.lan db.grp3.lan
named-checkzone grp3.lan rev.grp3.lan
```

Si les informations ont bien été tapées, la réponse doit être « ok ».

⚠ Pensez à redémarrer

```
# systemctl restart named.service
# rndc reload
```

⚠ et recharger

Configuration du serveur DNS secondaire :

➤ Dans **/etc/named.conf.local**, renseignez les informations de sorte à ce que la machine sache qu'elle sert de DNS secondaire et qu'elle ait connaissance du DNS primaire

```
zone "grp3.lan" {
        type master;
        file "db.grp3.lan";
        allow-update { key pti; };
};

zone "23.168.192.in-addr.arpa" {
        type master;
        file "rev.grp3.lan";
        allow-update {key pti; };
};
```

Donnez les droits d'écriture aux utilisateurs du groupe dans le répertoire **/var/named** avec la commande

```
chmod g+w /var/named
```

Relancer le service named du serveur primaire puis secondaire.

```
systemctl restart named.service
```

Le serveur secondaire récupère ainsi db et rev du serveur primaire.

Configuration DHCP

Installer les paquets DHCP sur le serveur : **dhcp**

⚠ Pour que le serveur DHCP prenne le dessus sur le serveur DNS et puisse prendre contrôle sur la zone, on commence par créer une clé qui permettra d'authentifier les transactions. Le serveur DHCP connaîtra cette clé et l'utilisera.

Pour se faire, on saisit la commande suivante :

```
dnssec-keygen -a HMAC-MD5 -b 128 -n USER pti
```

➤ Une fois cette clé créée on l'extrait : `vi Kpti.+157+51860.private`

Copier la clé qui est sous cette forme : **UNkdNYUxlZD7zEu2tp1B8g==**
Et la coller dans le fichier **/etc/rndc.key** à la place de la clé existante

Mettre **named** en tant que groupe du fichier **rndc.key** puis modifier les droits du fichier de sorte à ce que le groupe **named** puisse lire et que le propriétaire puisse lire et écrire.

```
chown -R named named/
```

Également **named** le propriétaire du répertoire **/var/named**.

⚠ Appliquez la modification de manière récursive.

Tentons de faire ressembler le fichier /etc/named.conf comme ci-dessous

```
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 192.168.23.1; };
        listen-on-v6 port 53 { ::1; };
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        forwarders { 8.8.8.8; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation no;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
```


```
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation no;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
```


```
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named.conf.local";
include "/etc/rndc.key";
```

➤ Il est temps de s'occuper des zones inversée et direct, dans le fichier **/etc/named.conf.local** renseigner ces informations :

```
zone "grp3.lan" {
        type master;
        file "db.grp3.lan";
        allow-update { key pti; };
};

zone "23.168.192.in-addr.arpa" {
        type master;
        file "rev.grp3.lan";
        allow-update {key pti; };
};
```

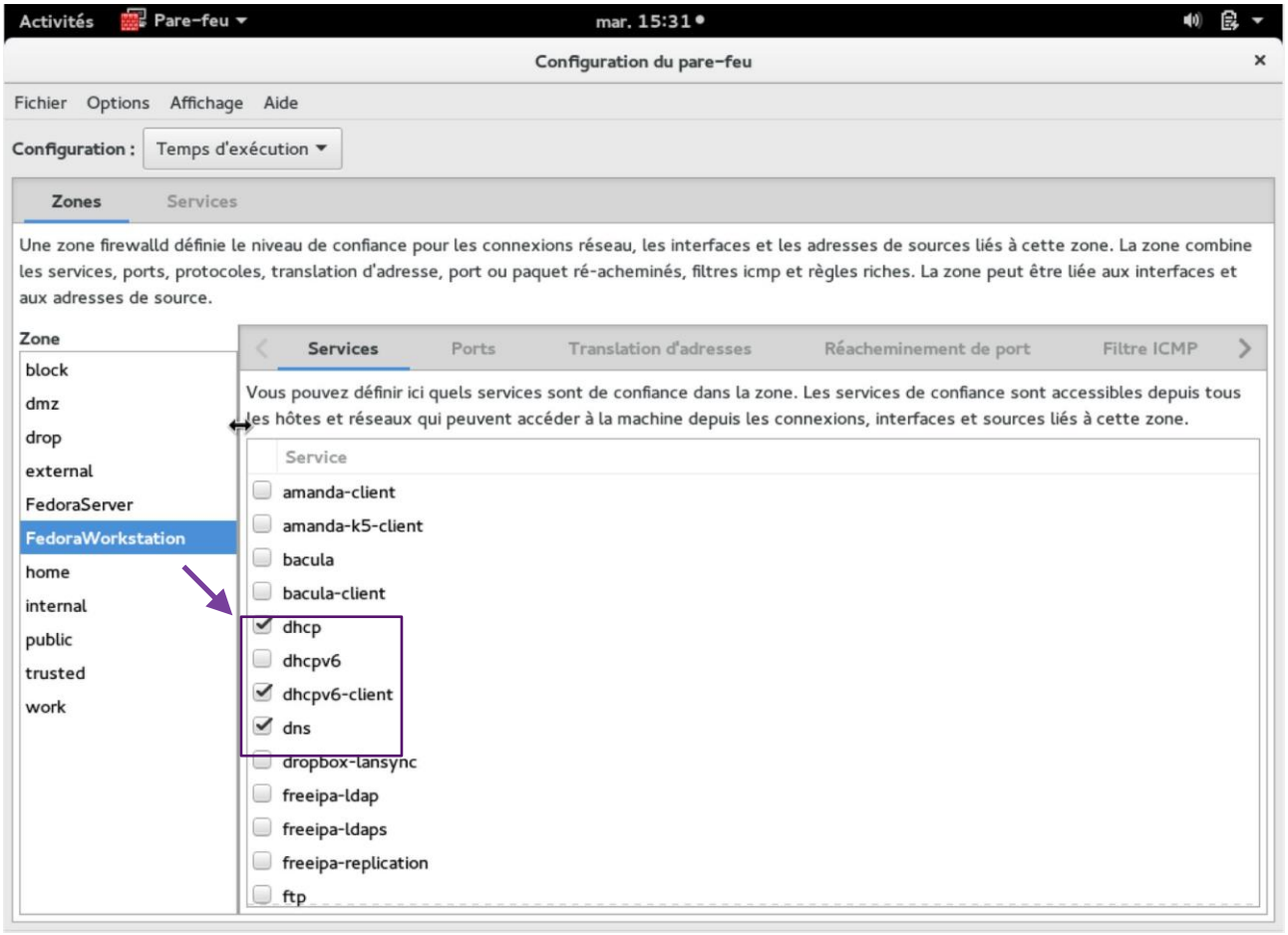
➤ redémarre le service **named**

➤ On va passer ensuite à la configuration du fichier **/etc/dhcpd.conf :**

```
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp/dhcpd.conf.example
#   see dhcpd.conf(5) man page

server-identifier 192.168.23.1;
authoritative;
ignore declines;
deny duplicates;
option domain-name-servers 192.168.23.1;
option domain-name "grp3.lan";
ddns-update-style interim;
ddns-updates on;

#gestion du réseau 192.168.23.0
subnet 192.168.23.0 netmask 255.255.255.240 {
        range 192.168.23.3 192.168.23.12;
        option routers 192.168.23.14;
        option subnet-mask 255.255.255.240;
        option broadcast-address 192.168.23.15;
        default-lease-time 21600;
        max-lease-time 43200;
        ddns-domainname "grp3.lan";
        ddns-rev-domainname "in-addr.arpa";
        include "/etc/rndc.key";

        zone grp3.lan {
        primary 192.168.23.1;
        key pti;
        }

        zone 23.168.192.in-addr.arpa. {
        primary 192.168.23.1;
        key pti;
        }

#ip fixe
host PC1 {
hardware ethernet 00:0C:29:AC:4B:C1;
fixed-address 192.168.23.3;
}


host localhost.localdomain {
hardware ethernet 08:00:27:3B:7D:F4;
fixed-address 192.168.23.1;
}
```

⚠️Relancer après cela le service DHCP qui doit se relancer sans erreurs si aucune faute de frappe n'a été commise.

➤ Sur le serveur DHCP, laisser entrer les trames DHCP :



Routeur Cisco 3550 series

➤Ci-joint la configuration du **routeur1**

```
interface FastEthernet0/1
 no switchport
 no ip address

interface FastEthernet0/2
 no switchport
 ip address 192.168.23.14 255.255.255.240
```

➤ Et voici celle qui complétera le **routeur2**

```
interface FastEthernet0/1
 no switchport
 ip address 192.168.23.13 255.255.255.240
 ip helper-address 172.16.23.13

interface FastEthernet0/2
 no switchport
 ip address 172.16.23.13 255.255.255.240
ip route 0.0.0.0 0.0.0.0 192.168.23.14
```

On pense au dhcp relais, afin que les clients PC1 et PC2 puisse obtenir la configuration envoyé par le serveur DHCP/DNS

⚠**Les Cisco 3550** sont **multilaye**r ils occupent donc le rôle de routeur ET de switch

Il n'est donc pas nécessaire de rajouter un switch supplémentaire/intermédiaire

⚠Notons également que les autres port du switch sont déjà paramètre en

```
switchport mode acess
```

Nous utiliserons donc les **ports 17/18/19** pour branchez nos serveurs et PC 3/4

La nécessité d'indiqué la route par défaut à notre routeur 2 permet d'assurer la communication avec son camarade routeur 1

Côté Client : 3 configuration

Linux (Fedora) : Théorique

Dans /etc/sysconfig/network-scripts/ifcfg-enp0s3

Modifier le Bootproto de static à DHCP

Et le PeerDNS à YES.

Si IPADRR est renseigné, le supprimer.

Renommer la machine sous /etc/hostname puis la redémarrer pour que la modification soit prise en compte.

Relancer le service network du client et faire un Ifconfig afin de vérifier si le client a récupérer une nouvelle adresse.

9. Tester des ping grâce aux noms de machines des clients.

9. Vérifiez dans le fichier **/var/lib/dhcpd/dhcpd.leases** du serveur DHCP si la transaction a bien été effectuée. Vous devriez y retrouver les informations suivantes :

lease 192.168.1.20 {

starts 6 2014/08/23 08:59:31;

.....

set ddns-rev-name = "20.1.168.192.in-addr.arpa";

set ddns-txt = "31b4f876a7536483a1ca7a143980b337d6";

set ddns-fwd-name = "testclient.pti.lan";

client-hostname "testclient";

9. Visualiser le répertoire /var/named, des fichiers temporaires .jnl ont du se créér : **db.pti.lan.jnl, rev.pti.lan.jnl.** Ils contiennent les mises à jours dynamiques du DNS.

9. Effectuer les **ping** avec le nom associé à la nouvelle machine. Testez également la commande **nslookup**

9. Si ce n'est pas le cas, vérifiez que named a bien les droits d'écriture sur /var/named

9. Mettez à jour les fichiers de zones par la commande : **rndc reload**

9. Testez la commande dhclient qui permet à une station cliente d'obtenir une adresse IP: **dhclient eth0** ou de libérer une adresse **dhclient -r eth0**

9. Installez l'analyseur de trame wireshark sur le client et serveur pour visualiser les trames pendant la demande du client : **dnf install wireshark** et **dnf install wireshark-gnome**

9. Lancez wireshark sur un client et sur le serveur et analyser les trames dhcp et dns.

9. Testez le DHCP sur un Client Windows.

    1. Modifiez l'hostname (nom de la machine)du poste, puis redémarrer

    2. Paramétrez le configuration IP de l'interface : cochez "Obtenir une adresse IP automatiquement" et "Obtenir les adresses des serveurs DNS automatiquement".

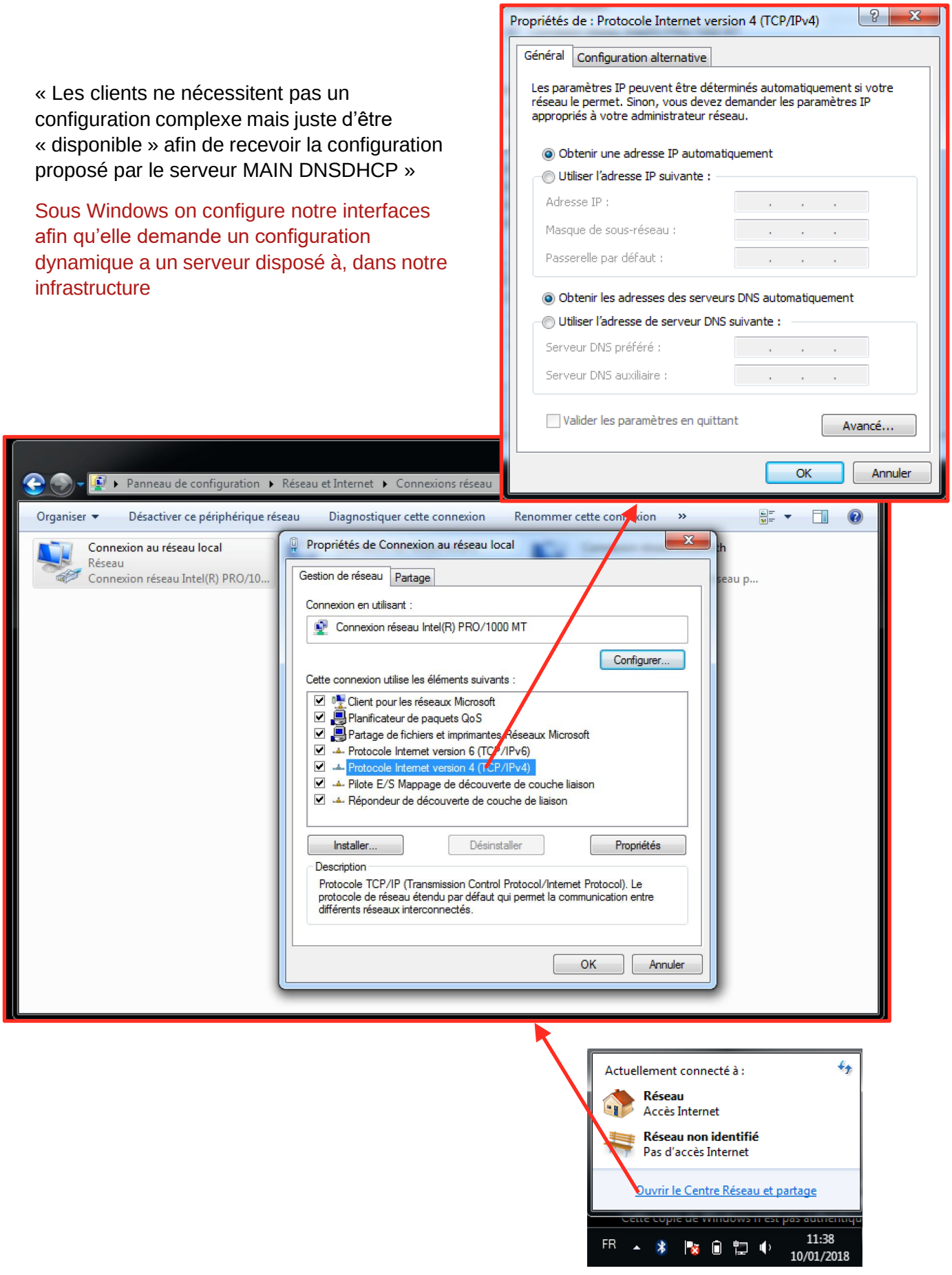
    3. Ouvrir une console puis tapez les commandes permettant de réinitialiser l'adressage TCP-IP : **ipconfig /release**, puis de réattribuer l'adressage IP : **ipconfig /renew**

    4. Effectuer lez commandes des points 13 à 15.

Windows-7

« Les clients ne nécessitent pas un configuration complexe mais juste d'être « disponible » afin de recevoir la configuration proposé par le serveur MAIN DNSDHCP »

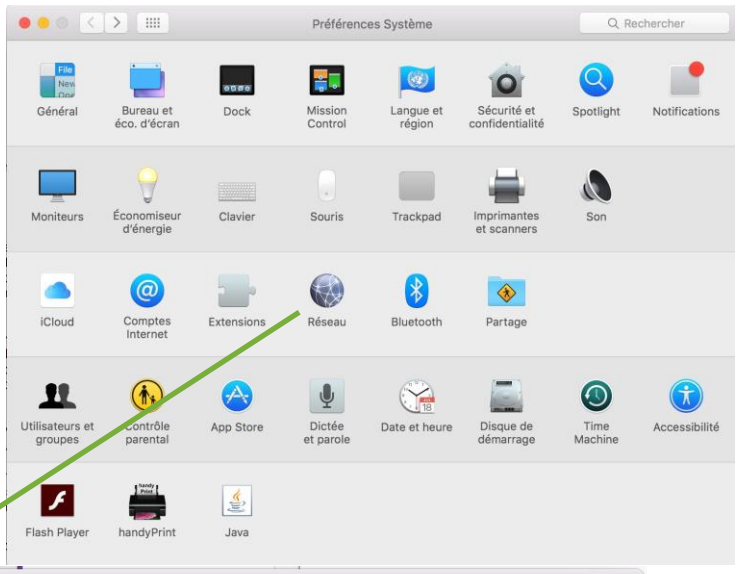
Sous Windows on configure notre interfaces afin qu'elle demande un configuration dynamique a un serveur disposé à, dans notre infrastructure

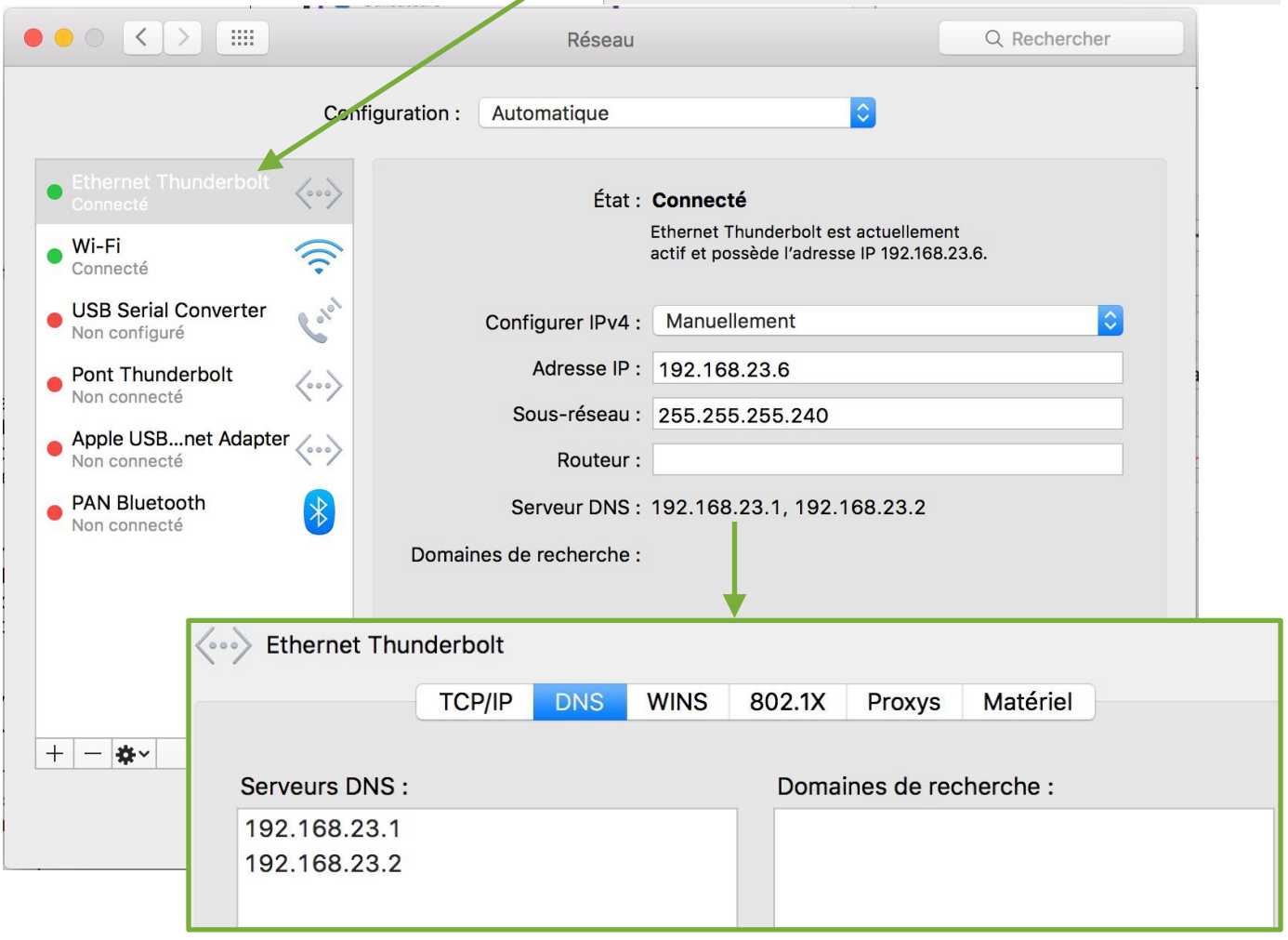


MAC-OS

« Les clients ne nécessitent pas un configuration complexe mais juste d'être « disponible » afin de recevoir la configuration proposé par le serveur MAIN DNSDHCP »

Sous MacOS la configuration ressemble a ceci :





Problèmes rencontrés

1. Routeur 1 & 2 : un des deux port était HS ► changement routeur/switch multilayer ☑
2. Paquets manquants sur les serveurs DNSDHCP1 et DNSDHCP2 : ☐
   - Réinstallation nécéssaire des machines !
3. VM (serveur) accessible depuis l'infra ☑
   - Multiple carte réseau pose pb ► 1 seul carte réseau UP
4. Communication Client/Routeur à travers l'infrastructure
   - Host to Host
   - Configuration « table de routage » des routers 1 & 2 ☐
     - passerelle par défaut
     - Et route du réseau 192.168.23.0 to 172.16.23.0