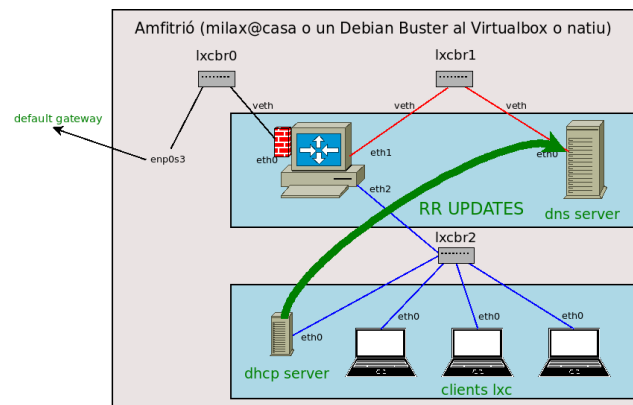


## Pràctica 3, part 3: Servei DNS dinàmic

Fins ara els clients DHCP no tenien nom. Aquests clients poden ser molts i pot ser que d'un *boot* a un altre se'ls assigni una IP diferent i per tant el seu nom no pot ser estàtic (com vàrem fer amb la resta de contenidors).

### Què farem:

- Partirem del laboratori anterior funcionant.
- Configurarem el servi DHCP per a que generi un nom diferent per a cada *lease*.
- Farem que aquest servei notifiqui aquests noms al servei DNS.
- Per a poder fer els *updates* de forma segura usarem una clau criptogràfica simètrica compartida entre els dos servidors.



Els ordinadors de la intranet dels usuaris hauran de tenir un nom dinàmic **assignat pel dhcpd**. Aquest nom dependrà de l'adreça IP assignada. Un cop generat aquest nom dinàmic el dhcpd enviarà un **update** amb el nom i la IP al servidor **bind** (a la zona forward i a la reversa), el qual els guardarà als respectius fitxers binaris de tipus **.jnl**

Aquesta és una pràctica molt utilitzada. Ho podem veure al següent exemple:

```
tracert -m 4 www.telefonica.es
tracert to www.telefonica.es (141.101.90.96), 4 hops max, 60 byte
packets
 1  router (192.168.1.1)  0.486 ms  0.559 ms  0.687 ms
 2  * * *
 3  229.red-81-41-231.staticip.rima-tde.net (81.41.231.229)  ...
 4  230.red-81-41-231.staticip.rima-tde.net (81.41.231.230)  ...
```

Podeu fer la prova usant el servidor web del vostre ISP.

## A) Al contenidor 'dhcp': servei DHCP

### A.1 Generem la clau secreta compartida

Per a que els dos serveis es puguin autenticar i fer els *updates*, la forma més senzilla consisteix en que els dos **comparteixin una clau secreta** simètrica (TSIG).

La clau es genera d'aquesta manera:

```
$ /usr/sbin/dnsssec-keygen -a HMAC-MD5 -b 128 -n USER CLAU_DHCPDNS
```

Posarem la clau guardada en el fitxer generat `.private`<sup>1</sup> a la configuració dels dos servidors amb el següent format:

```
key CLAU_DHCPDNS {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;
    secret "+abcd123.....xyz789==";
};
```

### A.2 Generació de noms dinàmica en el servidor DHCP

En el moment de preparar la oferta de *lease* es generarà un nom amb el format:

**client-1.23.intranet.gsx**

on 1 i 23 són els dos octets de menys pes de l'adreça IP assignada

Això s'aconsegueix modificant el fitxer `/etc/dhcp/dhcpd.conf` adaptant les següents opcions<sup>2</sup> per a la subnet de la intranet<sup>3</sup>:

```
ddns-hostname= pick(option fqdn.hostname, option host-name,
    concat ("prefix-",binary-to-ascii(10,8,"-",
    substring(leased-address,3,1))) );

option host-name = config-option server.ddns-hostname;
```

Tal com està a l'exemple convertiria **10.11.12.13** al nom: **prefix-13**

Les funcions del **dhcp-eval** usades són:

- `pick(...)` : agafa el primer valor no nul
- `concat()`: concatena strings
- `binary-to-ascii(base, #bits, separador, octets)`: passa el vector d'octets a strings numèrics en base 2 a 16
- `substring(cadena, offset, lenght)`: retorna el substring que comença a la posició *offset*
- `config-option`: retorna el valor de la opció especificada

### A.3 Activar l'enviament dels uptades

Al fitxer `/etc/dhcp/dhcpd.conf` a més d'afegir la definició de la clau, cal indicar que s'han de fer **updates** al DNS:

```
ddns-update-style interim;
```

<sup>1</sup> Un cop copiada, els dos fitxers generats es poden eliminar (`.key` i `.private`)

<sup>2</sup> Per més detalls mireu el man `dhcp-eval` (cal el paquet **isc-dhcp-common**)

<sup>3</sup> Aneu amb compte amb el Copy&Paste, els guions i les cometes sovint causen problemes.

```
ddns-updates on;  
deny client-updates;
```

També cal definir cada zona (intranet **forward** i **reverse**) per les quals es faran els *updates*.

Exemple per a la zona forward:

```
zone intranet.gsx {  
    primary $ipNS;  
    key CLAU_DHCPDNS;  
}
```

## B. Al contenidor 'server': servei DNS

### B.1 Permetre la recepció dels uptades

Al fitxer **/etc/bind/named.conf.options** heu d'afegir la definició de la clau simètrica compartida amb el servei dhcp.

Al fitxer **/etc/bind/named.conf.local** cal permetre els *updates* amb aquesta clau a les zones on s'hagi d'actualitzar els noms:

```
allow-update { key CLAU_DHCPDNS; };
```

Els *updates* es guardaran a un fitxer binari del tipus .jnl per a cada zona. Com es va demanar que els fitxers estiguessin a **/etc/bind/** és necessari que el grup bind hi pugui escriure. Així doncs, cal canviar els permisos d'aquest directori.

### B.2 Logging dels uptades

Per a facilitar el seguiment d'aquests *updates* farem que registri els *updates* a un fitxer de log a part del *syslog* general. Assegureu-vos dels permisos/owner del directori i del fitxer.

Per això afegirem al fitxer **/etc/bind/named.conf.options** la següent configuració:

```
logging {  
    category update { update_debug; };  
    channel update_debug {  
        file "/var/log/bind/update_debug.log";  
        severity debug 1;  
        print-category yes;  
        print-severity yes;  
        print-time yes;  
    };  
};
```

Al final de la sessió necessitareu aquest log per al lliurament.



## C. Als contenidors 'client':

- Primer haurem de desactivar que els clients enviïn el seu nom actual als seus DHCPREQUESTS. Assegureu-vos de tenir comentada la línia del fitxer **/etc/dhcp/dhclient.conf**:

```
# send host-name = gethostname();
```

El **dhclient** ara rebrà un *lease* amb la nova IP i el nou nom. Amb aquest nom el **dhclient** no en fa res però convé actualitzar el nou nom al **hostname**. Per aplicar-lo posarem un *script* que ho faci, però sols després del DHCPACK. Per això utilitzarem un *exit-hook*: un script que "s'enganxa" a la sortida del **dhclient**.

- Descarregueu del moodle el fitxer **dhclient-exit-hook.tar** i descomprimiu-lo al directori local.
- Poseu el fitxer descarregat **actualitza\_nom\_local** al directori **/etc/dhcp/dhclient-exit-hooks.d/**  
No importa el permís d'execució però sí el de lectura.
- Abaixeu la **eth0** i torneu-la a aixecar.
- Comproveu visualment que s'ha executat el *exit-hook* tot observant els missatges que aquest escriu per pantalla.

## Proves:

Als clients:

- Comproveu que el contingut del **resolv.conf** sigui correcte.
- Comproveu amb la comanda **hostname** que el nom hagi estat actualitzat.
- Guardau el lloguer obtingut i guardat a **/var/lib/dhcp/...**

Al servidor DNS:

- Comproveu al log que tinguin els *updates* correctes:

```
Added new forward map ...
Added reverse map ...
```

Errors comuns són:

```
unable to add reverse map, timed out, invalid TSIG key, not a zone...
```


- Si cal, proveu de capturar els updates amb el **wireshark/tcpdump**. Exemples:

```
root@server:~/server# tcpdump -i eth0 port 53
root@dhcp:~/dhcp# tcpdump -vi eth0 port 53 | grep update
```

- Comproveu que té els fitxers binaris dels *journal* (**.jnl**). Aquesta informació es copia de forma periòdica del **.jnl** als fitxers amb RR estàtics. Tanmateix, es pot forçar amb:

```
# rndc sync
```

Comproveu ara que els fitxers amb els registres RR incorporen aquesta informació.

- Per a poder comprovar que s'han afegit els updates a la zones useu la comanda **dig** per a fer [dues transferències de zona intranet](#) (la forward i la revers) des del propi server i guardeu-les per a l'entrega. 

### ***Documentació específica:***

- man *dhcp-options* i *dhcp-eval* (cal el paquet **isc-dhcp-common**)
- man *dhcpd.conf* (secció DYNAMIC DNS UPDATE SECURITY o busqueu /ddns)
- [Debian DDNS](#)
- [Zytrax: DDNS with DHCPv4 and DHCPv6](#)
- [IETF secure-ddns-howto.html](#)