Práctica 2

Asignatura: Administración de sistemas 2
Fecha: 22/3/2020
Autor: Diego Marco Beisty, 755232

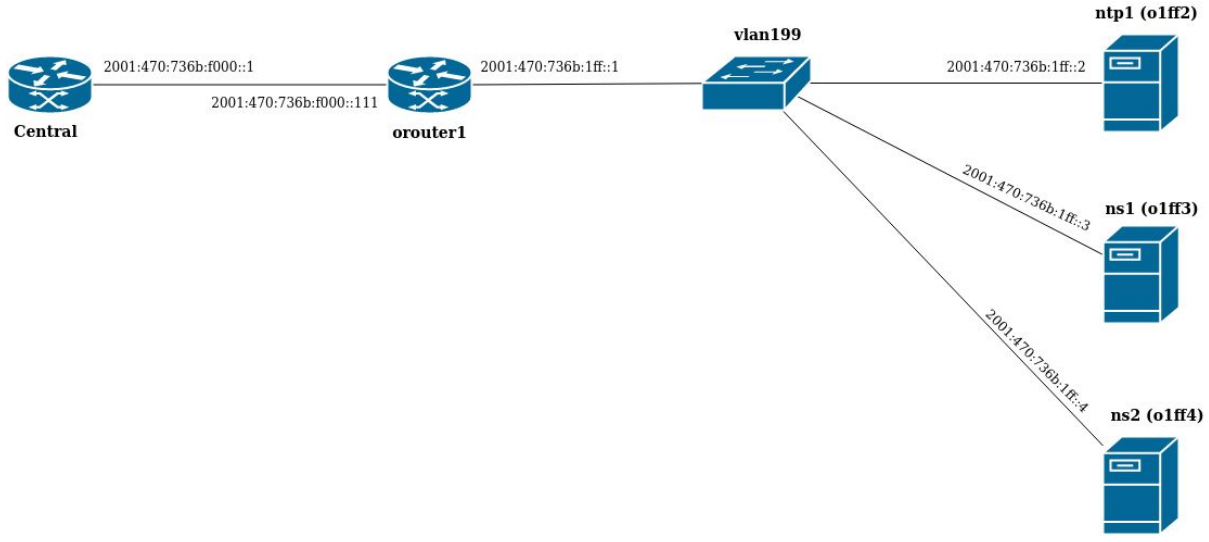
RESUMEN

Respecto a la práctica 1, se han añadido dos nuevas máquinas a la subred interna de la arquitectura. Además se han puesto en marcha 3 nuevos servicios. Un servicio de resolución de nombres, con implementación nsd, autoritario y no recursivo. Otro servicio DNS mediante la implementación unbound, no autoritario, recursivo y con cacheado. Por último un servicio de tiempo NTP.

INTRODUCCIÓN Y OBJETIVOS

Se van a configurar los servicios DNS y ntp en tres máquinas conectadas a la subred interna `2001:470:736b:1ff::/64`. Puesto que van a actuar como servidores, se les va a asignar una ip estática para poder acceder a los servicios de forma estable.
La implementación DNS, nsd, se configurará en dos máquinas para asegurar la persistencia de los datos, siendo una de ellas el master y la otra el slave. Actuarán como servidores autoritarios de la zona directa 1.ff.es.eu.org y la zona inversa `1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.`
El servicio de DNS unbound se configurará en otra máquina permitiendo la resolución recursiva y con cacheado de nombres de dominio y direcciones IP para las máquinas en el rango `2001:470:736b::/48`, es decir, las pertenecientes a la arquitectura de la práctica.
Por último se levantará un servicio ntp para mantener la información de tiempo de todas las máquinas actualizado. Para ello se sincronizará con un servidor de tiempo de stratum 1 y serán las demás máquinas las que actúen como clientes ntp de este servidor, (excepto el router externo).

ARQUITECTURA DE ELEMENTOS RELEVANTES



En el diagrama quedan representados de izquierda a derecha los siguientes elementos:

- El router Central que conecta las MVs a internet.
- orouter1, que está conectado a la subred `2001:470:736b:f000` con Central, y a la subred `2001:470:736b:1ff` con las máquinas servidores, mediante la vlan199.
- o1ff2 (nombre DNS ntp1), es el servidor ntp y DNS recursivo con caché.

- o1ff3 (nombreDNS ns1), es el servidor autoritario DNS primario.
- o1ff4 (nombre DNS ns2), es el servidor autoritario DNS secundario.

COMPREHENSIÓN DE ELEMENTOS RELEVANTES

servicio DNS(nsd)

Este servicio se configura en dos máquinas siendo una la primaria y otra la secundaria, garantizando así la consistencia de los datos internos. Puesto que las escrituras se van a realizar únicamente en el primario, será este en el que se ingresen inicialmente los datos de zona de los cuales va a ser responsable. El servidor secundario realizará periódicamente peticiones al primario para comprobar si necesita actualizar sus datos.
El servidor DNS primario se implementará en la máquina o1ff3. El servicio escuchará en el puerto 53 de la IP `2001:470:736b:1ff::3`. El servidor DNS secundario escuchará en el puerto 53 de la IP `2001:470:736b:1ff::4`.
Respecto a los detalles de configuración, cabe destacar:
En el fichero /var/nsd/etc/nsd.conf se establece una clave privada llamada “mskey” para cifrar la transmisión entre el primario y el secundario. Además en el primario se va a permitir notificar sobre actualizaciones y proveer información de la zona al secundario añadiendo el patrón:

```
pattern:
        name: "tosecondary"
        notify: 2001:470:736b:1ff::4 mskey
        provide-xfr: 2001:470:736b:1ff::4
```

A su vez, en el secundario se añade el patrón toprimary, para poder ser notificado y recibir actualizaciones del primario:

```
pattern:
        name: "toprimary"
        allow-notify: 2001:470:736b:1ff::3 mskey
        request-xfr: AXFR 2001:470:736b:1ff::3 mskey
```

Los ficheros de zona se van a configurar únicamente en el primario. Puesto que el servidor DNS va a resolver peticiones directas e inversas, se va a hacer cargo de dos zonas. La zona directa 1.ff.es.eu.org y la zona inversa
`1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.`

La zona directa está configurada en el fichero /var/nsd/zones/1.ff.es.eu.org.directo.
Cabe destacar que en el registro SOA se ha configurado un nº de serie correspondiente a la fecha actual en el formato AAAMMDDVV siendo VV el número de versión, que aumenta cada vez que se actualiza el fichero. El servidor secundario comprobará si hay nuevas actualizaciones cada 6 horas. Si el servidor primario falla, el servidor secundario intentará comunicarse con él cada 1 hora y además si ha pasado una semana desde que ha caido el servidor primario, el secundario dejará de servir información a los clientes DNS.

```
$ORIGIN 1.ff.es.eu.org.
@     IN    SOA   ns1.1.ff.es.eu.org.  a755232.1.ff.es.eu.org. (
                    2020031101          ; numero serie
                    21600               ; Refresca cada 6 horas
                    3600                ; Reintenta cada 1 hora
                    604800              ; Expira despues de 1 semana
                    86400 )             ; TTL minimo cliente de 1 dia
```

Respecto a los registros directos AAAA y CNAME se presentan a continuación:

```
            IN    NS    ns1.1.ff.es.eu.org.
            IN    NS    ns2.1.ff.es.eu.org.
ns1         IN    AAAA  2001:470:736b:1ff::3
ns2         IN    AAAA  2001:470:736b:1ff::4
ntp1        IN     AAAA    2001:470:736b:1ff::2
router1     IN    AAAA  2001:470:736b:f000::111
otro_servidor     IN    AAAA    2001:470:736b:1ff::f
o1ff3       IN    CNAME   ns1
o1ff4       IN    CNAME   ns2
```

La zona inversa queda configurada en el fichero 1.ff.es.eu.org.inverso y en ella se resuelven las direcciones IP que identifican a las máquinas ns1, ns2 y router1:

```
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f    IN    PTR   ns1.1.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f    IN    PTR   ns2.1.ff.es.eu.org.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f    IN    PTR
router1.1.ff.es.eu.org.
```

Este servicio se inicia en ambas máquinas cuando arranca el sistema añadiendo en el fichero /etc/rc.conf.local la línea: `nsd_flags="".`

Modificación fichero de zona

Para añadir el dominio “otro_servidor“en la zona directa del servidor master, se han realizado los siguientes pasos. Primero se ha añadido la línea en el fichero de zona directa:

```
otro_servidor     IN     AAAA     2001:470:736b:1ff::f
```

Después se ha modificado el número de serie del fichero para indicar que se ha realizado una actualización de la zona. A continuación se ha hecho `nsd-control write` para escribir los cambios en disco y que se mande un notify al secundario indicándole que existe una versión más reciente del fichero de su fichero de zona. Por último, desde el servidor secundario fuerzo una transferencia de zona mediante el comando `nsd-control transfer zone` y de esta forma quedan los cambios actualizados en ambos servidores.

Servicio DNS (unbound)

Este servicio se configura en la máquina o1ff3 y va a permitir resolver de forma recursiva las peticiones de las demás máquinas que se van a configurar como clientes DNS añadiendo en /etc/resolv.conf:

```
lookup file bind
nameserver 2001:470:736b:1ff::2
```
Esto indica que cualquier resolución de nombres de dominio se va a redirigir al servidor unbound.
La configuración del servidor unbound se va a hacer en el fichero /var/unbound/etc/unbound.conf. Se ha dado acceso al servidor a todas las máquinas de prefijo `2001:470:736b::/48` y además todas las peticiones entrantes se van a redirigir a los servidores recursivos `2001:470:20::2 y 2001:4860:4860::8888`.
Para poder ejecutar este servicio al arrancar la máquina ,se ha modificado el fichero /etc/rc.conf.local añadiendo unbound_flags="".

servicio ntp

ntp es un servicio distribuido jerárquico que sincroniza la hora exacta entre las máquinas de las distintas capas o estratos que conforman su arquitectura.
Se ha decidido sincronizar el reloj local del servidor o1ff2 con cuatro servidores ntp de distintos estratos para proveer de información sobre el tiempo al resto de máquinas que conforman la arquitectura de esta práctica.
Por lo tanto el resto de máquinas o1ff3 y o1ff4, excepto orouter1, actuarán como clientes ntp sincronizandose con o1ff2 para obtener la hora actual.

Configuración servidor ntp o1ff2:

- Fichero /etc/ntpd.conf

```
listen on ::1
listen on 2001:470:736b:1ff::2
server 2001:470:0:50::2
server 2001:470:0:2c8::2
server prometeo.cps.unizar.es
server ntp.unizar.es
```

Aquí se puede observar como el servidor ntp o1ff2 permite sincronizar a todos las máquinas que accedan a la dirección `2001:470:736b:1ff::2` y también a sí misma en la dirección `::1.`
Además se sincroniza dos servidores de stratum 1: `2001:470:0:50::2 y 2001:470:0:2c8::2,` un servidor de stratum 2: `prometeo.cps.unizar.es` y un servidor de stratum 4: `ntp.unizar.es`

Configuración clientes ntp o1ff3 y o1ff4:

- Fichero /etc/ntpd.conf

```
server ntp1.1.ff.es.eu.org
```

Por último para poder ejecutar este servicio desde el arranque del sistema, se va a añadir en el fichero /etc/rc.conf.local de todas las máquinas, tanto servidor ntp como clientes, la línea ntpd_flags=-s.

Tras este cambio, se ejecutará ntpd con la opción -s en el arranque, que permitirá al demonio ntpd actualizar inmediatamente la hora local con alguno de sus servidores de referencia si este reloj local tiene un desfase de más de 180 segundos. Esto evitará correcciones de tiempo muy largas.

VALORES NUMÉRICOS REGISTRO SOA

Número de serie: Es el número de versión del archivo de zona y se modifica cada vez que se actualiza el archivo. Permite saber quién tiene la versión más reciente del archivo y de esta forma cuando la máquina secundaria detecte que el fichero de zona del primario tiene un número de serie superior al suyo, le pedirá una copia de esta nueva versión para poder actualizar su zona.

refresh: Indica la frecuencia en segundos con la que el servidor secundario comprobará si el número de serie de la zona del primario es superior al suyo. De esta forma sabrá que tiene que actualizar su zona.

retry: Es la frecuencia en segundos con la que va a intentar contactar el secundario con el primario desde que se da cuenta de que este no responde.

Expire: Indica el tiempo que el servidor secundario mantendrá su archivo de zona como válido mientras el primario está caído. Una vez pasado este tiempo no proveerá servicio a los clientes DNS pero sí intentará contactar con el primario hasta que este le responda. Este campo permite controlar el tiempo durante el cual consideramos que los datos seguirán siendo válidos hasta que el sistema vuelva a ser estable.

Mínimum: Este campo se utiliza para establecer el tiempo máximo que otros servidores DNS pueden mantener los datos solicitados del archivo de zona en sus cachés. De esta forma si el servidor DNS autoritario actualiza sus datos de forma regular, se configurará un tiempo menor que si no actualiza con regularidad su información interna. Este campo permite además al servidor regular el tráfico de peticiones que recibe.

PROBLEMAS ENCONTRADOS

He tenido varios pequeños problemas sintácticos al añadir las direcciones ip en el fichero de zona inversa al no calcular bien el número de ceros a añadir.

ANEXO

VERIFICACIÓN

Servicio nsd:

- Para comprobar que tanto el fichero de configuración nsd.conf como los ficheros de zona eran correctos, se ha usado los comandos :

```
nsd-checkconf
nsd-checkzone
```

- Se ha verificado en el fichero nsd.log que primario y secundario se comunican.

```
doas tail -f /var/log/nsd.log
```

stdout secundario:

```
[2020-03-22 23:46:37.605] nsd[30174]: notice: nsd starting (NSD 4.1.25)
[2020-03-22 23:46:37.728] nsd[51264]: notice: nsd started (NSD 4.1.25), pid
83257
[2020-03-22 23:46:39.463] nsd[83803]: info: notify for 1.ff.es.eu.org. from
2001:470:736b:1ff::3 serial 2020031104
[2020-03-22 23:46:42.471] nsd[83803]: info: notify for
1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. from 2001:470:736b:1ff::3 serial
2020031102
```

- Para comprobar el funcionamiento del servicio de nombres tanto del primario como se secundario, se ha ejecutado para todos los nombres de dominio configurados:

```
#Comprobar resolución directa de primario
dig -6 @2001:470:736b:1ff::3 AAAA router1.1.ff.es.eu.org

#Comprobar resolución inversa de primario
dig -6 @2001:470:736b:1ff::3 -x 2001:470:736b:1ff::1

#Comprobar resolución directa de secundario
dig -6 @2001:470:736b:1ff::4 AAAA router1.1.ff.es.eu.org

#Comprobar resolución inversa de secundario
dig -6 @2001:470:736b:1ff::4 -x 2001:470:736b:1ff::1
```

Servicio unbound:

- Desde todas las máquinas se ha ejecutado el comando `dig moodle2.unizar.es` para comprobar que se resuelve el nombre de dominio y además a partir de la segunda petición se reduce drásticamente el tiempo de resolución debido al caché del servidor recursivo.
  Tras ejecutar una vez el comando

```
;; ANSWER SECTION:
moodle2.unizar.es.    86400   IN      CNAME
alojamiento02.unizar.es.
alojamiento02.unizar.es. 21599  IN    A     155.210.11.79
;; Query time: 215 msec
```

  Tras ejecutar dos veces el comando

```
;; ANSWER SECTION:
alojamiento02.unizar.es. 21386  IN    A     155.210.11.79
;; Query time: 1 msec
```

  Se observa que el tiempo de respuesta se ha reducido de 215ms a 1ms.

Servicio ntp:

- Se ha comprobado la sincronización del servidor ntp o1ff2 con los servidores de stratum 1, 2 y 4 de los que obtiene la información mediante el comando `ntpctl -sa.`

```
1/4 peers valid, clock synced, stratum 2

peer
wt tl st  next  poll       offset     delay      jitter
2001:470:0:50::2
     1  2  -  225s  300s         ---- peer not valid ----
2001:470:0:2c8::2
*  1 10  1   10s   34s     -0.062ms   122.294ms  0.147ms
155.210.152.180 prometeo.cps.unizar.es
   1  2  - 5s   15s              ---- peer not valid ----
155.210.12.9 ntp.unizar.es
   1  2  - 5s   15s              ---- peer not valid ----
```

  Se recibe respuesta únicamente del servidor 2001:470:0:2c8:::2 del cual se puede observar un offset relativamente pequeño

- Se ha comprobado la sincronización de los clientes ntp o1ff3 y o1ff4 con el servidor ntp o1ff2 mediante el comando `ntpctl -sa.`

```
wt tl st  next  poll       offset     delay      jitter
2001:470:736b:1ff::2 ntp1.1.ff.es.eu.org
     1  6  2    1s    5s    170.847ms  0.428ms    0.043ms
```

- Se ha comprobado también que funciona el servidor ntp comparando su reloj con el de Central, mediante el comando `ntpdate -q 2001:470:736b:1ff::2.`
  `server 2001:470:736b:1ff::2, stratum 2, offset 0.000972, delay 0.04196`
  `23 Mar 00:21:24 ntpdate[54342]: adjust time server 2001:470:736b:1ff::2 offset 0.000972 sec`

FICHEROS DE CONFIGURACIÓN

/var/nsd/etc/nsd.conf (primario)

```
 server:
      #El servidor no responde a peticiones de version
      hide-version: yes
      #Nivel de verbosidad en los logs (0 default,1,2,3)
      verbosity: 1
      ip-address: 2001:470:736b:1ff::3 #Asociar @IP a NSD
                  database: "/var/nsd/db/nsd.db"
                  #NSD se queda con los privilegios del grupo _nsd
                  username: _nsd
                  logfile: "/var/log/nsd.log"
                  pidfile: "/var/nsd/run/nsd.pid"
      port: 53
      server-count: 1 #CPUs a utilizar
      ip6-only: yes
      tcp-count: 60 #Maximo numero de conexiones TCP concurrentes
      zonesdir: "/var/nsd/zones"

   #permitir control local del demonio con el comando nsd-control
 remote-control:
      control-enable: yes
      control-interface: ::1
      control-port: 8952
      server-key-file: "/var/nsd/etc/nsd_server.key"
      server-cert-file: "/var/nsd/etc/nsd_server.pem"
      control-key-file: "/var/nsd/etc/nsd_control.key"
      control-cert-file: "/var/nsd/etc/nsd_control.pem"
   #Clave secreta que NSD usa para ejecutar transferencias entre
   #primario y secundario de forma segura.
   #TSIG(Transaction SIGnature)
 key:
      name: "mskey"
      algorithm: hmac-sha256
      secret: "bWVrbWl0YXNkaWdvYXQ="
```

```
  pattern:
     name: "tosecondary"
     #notifica al secundario de actualizaciones
     notify: 2001:470:736b:1ff::4 mskey
     #provee informacion de la zona al secundario
     provide-xfr: 2001:470:736b:1ff::4 mskey

   #zona directa "1.ff.es.eu.org"
   zone:
     name: "1.ff.es.eu.org"
     zonefile: "1.ff.es.eu.org.directo"
     include-pattern: "tosecondary"

   #zona inversa "1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
   zone:
     name: "1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
     zonefile: "1.ff.es.eu.org.inverso"
     include-pattern: "tosecondary"
```

Fichero de zona directa 1.ff.es.eu.org.directo

```
$ORIGIN 1.ff.es.eu.org.
@     IN    SOA   ns1.1.ff.es.eu.org.  a755232.1.ff.es.eu.org. (
                        2020031101       ; numero serie
                        21600            ; Refresca cada 6 horas
                        3600             ; Reintenta cada 1 hora
                        604800           ; Expira despues de 1 semana
                        86400 )          ; TTL minimo cliente de 1 dia

            IN    NS    ns1.1.ff.es.eu.org.
            IN    NS    ns2.1.ff.es.eu.org.
ns1         IN    AAAA  2001:470:736b:1ff::3
ns2         IN    AAAA  2001:470:736b:1ff::4
ntp1        IN     AAAA    2001:470:736b:1ff::2
router1     IN    AAAA  2001:470:736b:f000::111
otro_servidor     IN    AAAA    2001:470:736b:1ff::f
o1ff3       IN    CNAME   ns1
o1ff4       IN    CNAME   ns2
```

Fichero zona inversa 1.ff.es.eu.org.inverso

```
$ORIGIN 1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
@     IN    SOA   ns1.1.ff.es.eu.org.  a755232.1.ff.es.eu.org. (
                        2020031101       ; numero serie
                        21600            ; Refresca cada 6 horas
                        3600             ; Reintenta cada 1 hora
                        604800           ; Expira despues de 1 semana
                        86400 )          ; TTL minimo cliente de 1 dia
      IN    NS    ns1.1.ff.es.eu.org.
      IN    NS    ns2.1.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f   IN    PTR   ns1.1.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f   IN    PTR   ns2.1.ff.es.eu.org.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f   IN    PTR
router1.1.ff.es.eu.org.
```

/var/nsd/etc/nsd.conf (secundario)

```
server:
      #El servidor no responde a peticiones de version
      hide-version: yes
      #Nivel de verbosidad en los logs (0 default,1,2,3)
      verbosity: 1
      ip-address: 2001:470:736b:1ff::4 #Asociar @IP a NSD
            database: "/var/nsd/db/nsd.db"
            #NSD se queda con los privilegios del grupo _nsd
            username: _nsd
            logfile: "/var/log/nsd.log"
            pidfile: "/var/nsd/run/nsd.pid"
      port: 53
      server-count: 1 #CPUs a utilizar
      ip6-only: yes
      tcp-count: 60 #Maximo numero de conexiones TCP concurrentes
      zonesdir: "/var/nsd/zones"

#permitir control local del demonio con el comando nsd-control
remote-control:
      control-enable: yes
      control-interface: ::1
      control-port: 8952
      server-key-file: "/var/nsd/etc/nsd_server.key"
      server-cert-file: "/var/nsd/etc/nsd_server.pem"
      control-key-file: "/var/nsd/etc/nsd_control.key"
      control-cert-file: "/var/nsd/etc/nsd_control.pem"

#Clave secreta que NSD usa para ejecutar transferencias entre
#primario y secundario de formasegura. TSIG(Transaction SIGnature)
```

```
key:
      name: "mskey"
      algorithm: hmac-sha256
      secret: "bWVrbWl0YXNkaWdvYXQ="

pattern:
      name: "toprimary"
      allow-notify: 2001:470:736b:1ff::3 mskey #Permite ser
notificado por primario
      request-xfr: AXFR 2001:470:736b:1ff::3 mskey #Pide
actualizaciones al primario

#zona directa "1.ff.es.eu.org"
zone:
      name: "1.ff.es.eu.org"
      zonefile: "1.ff.es.eu.org.directo"
      include-pattern: "toprimary"


#zona inversa "1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
zone:
      name: "1.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa"
      zonefile: "1.ff.es.eu.org.inverso"
      include-pattern: "toprimary"
```

Fichero /var/unbound/etc/unbound.conf

```
server:
      interface: 0.0.0.0
      interface: ::0
      verbosity: 1
      hide-identity: yes
      hide-version: yes
      access-control: 2001:470:736b::/48 allow
      access-control: ::1 allow

remote-control:
      control-enable: yes
      control-use-cert: no

# Use an upstream forwarder (recursive resolver) for specific zones.
# Example addresses given below are public resolvers valid as of
2014/03.
#
forward-zone:
      name: "."                              # use for ALL queries
```

```
      forward-addr: 2001:470:20::2          # he.net v6
      forward-addr: 2001:4860:4860::8888    # google.com v6
      forward-first: yes             # try direct if forwarder fails
```

Fichero etc/resolv.conf

```
      lookup file bind
      nameserver 2001:470:736b:1ff::2
```

FIchero /etc/ntpd.conf (servidor ntp)

```
      listen on ::1
      listen on 2001:470:736b:1ff::2

      server 2001:470:0:50::2
      server 2001:470:0:2c8::2
      server prometeo.cps.unizar.es
      server ntp.unizar.es
```

Fichero /etc/ntpd.conf (cliente ntp)

```
      server ntp1.1.ff.es.eu.org
```

SCRIPTS USADOS

Se han guardado en dos scripts llamados define.sh y undefine.sh el conjunto de instrucciones necesarias para realizar la puesta en marcha y parada de todas las máquinas. Se pretende para la siguiente práctica, mejorar los scripts y pasarlos a ruby.

Fichero define.sh

```
#!/bin/bash
maquinas=( "orouter1.xml" "o1ff2.xml" "o1ff3.xml" "o1ff4.xml" )
for vm in "${maquinas[@]}";do
    sudo virsh define /misc/alumnos/as2/as22019/a755232/$vm
done
sudo virsh list --all
virt-manager
```

Fichero undefine.sh

```
#!/bin/bash
read -p "HAS APAGADO TODAS LAS MAQUINAS?? [yes|no]: " response
if [ $response = "yes" ];then
      maquinas=( "orouter1" "o1ff2" "o1ff3" "o1ff4" )
      for vm in "${maquinas[@]}";do
            sudo virsh undefine $vm &> /dev/null
      done
       pkill virt-manager
       sudo virsh list --all
```

```
else
    echo "Abortando..."
fi
```