# Documento para apuntes de DPL

teoria y practica

udp = port 53
direcciones recursivas 8.8.8.8 google 1.1.1.1 cloudfare, las recursivas no se repiten

direcciones ip de los 13 servidores raiz 1 es 192.58.128.30

options:
options esta en /etc/bind/named.conf.options
para que sea recursivo tienes que poner; aw
forward only = evita que sea recursivo
forwarders {
servidores recursivos que resolverán la llamada
	8.8.8.8;(es un ejemplo)
}

## Preguntas

como sabe que el de google no es autoritativo?

pese al tiempo que queda de clase habrá recuperación o este examen es un all in? all in

¿Dónde ponemos los certificados del profe una vez descargados?

¿Por qué pone @1.1.1.1 en el dig?
si creen que una respuesta esta mal corrijanla

# QUE ENTRA EN EL EXAMEN

certificado digital, https, DNS

**HTTPS**: ENCRIPTACIÓN + hash, puerto bien conocido(el 443), certificado digital, proteger información

**DNS**: puerto bien conocido (el 53), estructura del espacio de nombres, peticiones recursivas vs iterativas, servidores autoritarios (concepto), solicitudes recursivas + forward only (configuración), apuntes

PARA SERVIDORES AUTORITATIVOS:

**dig**: STATUS:NOERROR -> respuesta positiva
STATUS:NXDOMAIN-> respuesta negativa
STATUS: SERVERFAIL-> error de algún tipo

flags: qr rd ra aa
rd = recursive desired
ra = recursividad available
rr = NS(devuelve nombre de dominio), MX(devuelve nombre de dominio), A(devuelve IPV4), AAAA(devuelve IPv6)

Resolutor → forwarder →8.8.8.8
/etc/resolv.conf
nameserver = ip de tu servidor (configurar en maquina virtual)
curl https://www.angelmelchor.pro (muestra el contenido)
curl -I(es una i mayus.) https://www.angelmelchor.pro (muestra la cabecera)

El certificado va vinculado a un nombre de dominio, en caso de solo tener su ip usar:
~$ curl -v https://80.240.126.170

y te saldrá algo como esto

```
*   Trying 80.240.126.170:443...
* Connected to 80.240.126.170 (80.240.126.170) port 443
…..
* ALPN: server accepted http/1.1
* Server certificate:
*  subject: CN=www.angelmelchor.pro
*  start date: Dec 25 12:18:25 2025 GMT
*  expire date: Mar 25 12:18:24 2026 GMT
*  subjectAltName does not match 80.240.126.170
* SSL: no alternative certificate subject name matches target host name '80.240.126.170'
* Closing connection
* TLSv1.2 (OUT), TLS alert, close notify (256):
curl: (60) SSL: no alternative certificate subject name matches target host name
'80.240.126.170'
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

Para agregar una IP a tu máquina → ip addr add 172.17.0.7/24 dev enp0s3

**se necesita para el examen**: el nginx, bind9 y dig
10 preguntas https y 7 preguntas dns
Descargar certificados del profe
Guardar respuestas con capturas y/o textos

en el servidor web configurar el puerto bien conocido (https)(443)
poner en el listen 443 ssl;
certificados digitales

Aquí tienes los pasos exactos para **Nginx**:

## 1. Dónde poner los archivos

Al igual que en Apache, lo mejor es ser ordenado:

- **Certificado:** `/etc/ssl/certs/examen.crt`
- **Clave privada:** `/etc/ssl/private/examen.key`

Bash
sudo cp examen.crt /etc/ssl/certs/
sudo cp examen.key /etc/ssl/private/

## 2. Configurar el bloque de servidor (VirtualHost)

En Nginx, los sitios se configuran en `/etc/nginx/sites-available/`. Probablemente tengas uno llamado `default`. Edítalo (`sudo nano /etc/nginx/sites-available/default`) y busca o crea la sección para el puerto **443**:

Nginx
server {
    listen 443 ssl;
    listen [::]:443 ssl;

    server_name www.examen.lan; **# El nombre que configuraste en el DNS**(curl -v https://80.240.126.170 **CN de lo que te devuelva la petición)**

    root /var/www/html;
    index index.html;

    **# --- CONFIGURACIÓN SSL PARA EL EXAMEN ---**
    ssl_certificate         /etc/ssl/certs/examen.crt;
    ssl_certificate_key     /etc/ssl/private/examen.key;


    }
}

# Servidor DNS a modificar : archivo que se encuentra en /etc/bind/named.conf.options

```
options {
    directory "/var/cache/bind";

    // Habilitar recursividad (obligatorio para que funcione el reenvío)
    recursion yes;              // [cite: 473]
    allow-query { any; };       // Permite consultas de cualquiera [cite: 474]

    // --- LA CLAVE DEL EXAMEN ---
    // Esto evita que tu servidor intente contactar con los Root Servers reales
    forwarders {
        192.168.X.1;  // <--- AQUÍ PONES LA IP DEL ROUTER DEL PROFESOR
    };

    // "forward only" asegura que SI EL ROUTER FALLA, NO intente salir a buscar raíces
(que no tienes)
    forward only;               // [cite: 474]

    dnssec-validation auto;     // RECOMENDACIÓN: Desactívalo si no hay internet real, evita
líos de llaves.
    listen-on-v6 { any; };
};
```