

GUÍA MAESTRA TOTAL: SERVICIOS EN RED (DNS + HTTPS)

Asignatura: Despliegue de Aplicaciones (DPL) **Tipo de Examen:** All-in (Práctico + Teórico, sin recuperación) **Herramientas:** Bind9, Nginx, OpenSSL, Curl, Dig

1. CONCEPTOS TEÓRICOS

DNS (Domain Name System)

Sistema encargado de traducir nombres de dominio (www.google.com) a direcciones IP (142.250.200.14).

- **Puerto:** 53
- **Protocolo:** UDP (por defecto) y TCP (respuestas grandes o transferencias de zona).
- **Espacio de nombres:** Jerárquico (. > TLD > Dominio > Host).
- **Servidores raíz:** 13 servidores lógicos (A–M).

Tipos de consultas:

1. **Recursiva:** El cliente delega todo el trabajo al servidor ("Dámelo hecho").
2. **Iterativa:** El servidor responde con referencias a otros servidores ("Pregunta a aquél").

Tipos de servidores:

- **Autoritativo:** Tiene los datos originales de la zona (flag `aa` en dig).
- **Recursivo (Resolver):** Busca respuestas por el cliente y las cachea (ej: 8.8.8.8).

HTTPS (HTTP Secure)

HTTP funcionando sobre SSL/TLS.

- **Puerto:** 443 (TCP).
 - **Objetivos de seguridad (CIA):**
 1. **Confidencialidad:** Cifrado.
 2. **Integridad:** Hash.
 3. **Autenticación:** Certificados digitales.
-

2. CHECKLIST DE PREPARACIÓN

(Ejecutar nada más empezar el examen)

1. Instalar paquetes

Bash

```
sudo apt update  
sudo apt install bind9 bind9utils bind9-doc nginx curl -y
```

2. Backups de configuración

Bash

```
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options.original  
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default.original
```

3. Snapshot (si usas Máquina Virtual) Crear una instantánea llamada "Limpia" antes de configurar nada.

4. Liberar puertos 80/443

Bash

```
sudo systemctl stop apache2
```

3. MÓDULO DNS: BIND9

Objetivo: Configurar un servidor DNS Forwarder que solo reenvíe consultas al DNS del profesor y no salga a internet por su cuenta.

Configuración principal Archivo: `/etc/bind/named.conf.options`

C

```
options {  
    directory "/var/cache/bind";  
  
    // Habilitar recursividad  
    recursion yes;  
    allow-query { any; };  
  
    // IP del router / DNS del profesor  
    forwarders {  
        192.168.X.X;  
    };  
  
    // CRÍTICO: Si el profe falla, no buscar en raíces  
    forward only;
```

```
dnssec-validation no;  
  
listen-on-v6 { any; };
```

Aplicar cambios

```
Bash  
sudo named-checkconf  
sudo systemctl restart bind9
```

Diagnóstico con DIG Sintaxis: `dig @SERVIDOR_DNS DOMINIO TIPO`

- **STATUS: NOERROR** → Dominio resuelto correctamente.
 - **STATUS: NXDOMAIN** → Dominio inexistente.
 - **STATUS: SERVFAIL** → Error del servidor.
 - **FLAG: aa** → Respuesta autoritativa (El servidor es el dueño).
 - **FLAG: ra** → Recursividad disponible.
 - **FLAG: rd** → Cliente pidió recursividad.
-

4. MÓDULO HTTPS: NGINX

Objetivo: Configurar un servidor web seguro con certificados proporcionados.

1. Ubicación correcta de certificados

```
Bash  
# Mover archivos  
sudo cp examen.crt /etc/ssl/certs/  
sudo cp examen.key /etc/ssl/private/  
  
# Asegurar clave privada  
sudo chmod 600 /etc/ssl/private/examen.key
```

2. Configurar VirtualHost Archivo: `/etc/nginx/sites-available/default`

```
Nginx  
server {  
    listen 443 ssl;  
    listen [::]:443 ssl;  
  
    # EL NOMBRE DEBE COINCIDIR CON EL CERTIFICADO
```

```
server_name www.examen.lan;  
  
root /var/www/html;  
index index.html;  
  
# Rutas a certificados  
ssl_certificate    /etc/ssl/certs/examen.crt;  
ssl_certificate_key /etc/ssl/private/examen.key;  
}
```

Aplicar cambios

Bash

```
sudo nginx -t  
sudo systemctl restart nginx
```

5. EL TRUCO DEL ARCHIVO HOSTS

El problema: El certificado está emitido para un nombre, no para una IP. Si usas la IP en el comando curl, fallará con Error 60.

La solución:

Ver el nombre real del certificado:

Bash

```
openssl x509 -in /etc/ssl/certs/examen.crt -noout -subject  
# Salida esperada ejemplo: subject=CN = www.examen.lan
```

1.

Editar /etc/hosts:

Bash

```
sudo nano /etc/hosts
```

2. Añadir la línea al final: **192.168.X.X www.examen.lan**

Probar correctamente:

Bash

```
curl -v https://www.examen.lan
```

3.

6. RESOLUCIÓN DE PROBLEMAS

Nginx no arranca

- *Causa:* Error de sintaxis (falta ; o }) o ruta de clave mal.
- *Solución:* `sudo nginx -t`

Error SSL: subject name mismatch

- *Causa:* Acceso por IP en lugar de por nombre.
- *Solución:* Configurar `/etc/hosts` como se indica en el punto 5.

DIG: Connection timed out

Solución: Verificar estado y puertos.

Bash

```
sudo systemctl status bind9  
sudo ss -tulpen | grep 53
```

-

7. SIMULACRO DE EXAMEN (Preguntas rápidas)

P1: ¿Puerto y protocolo DNS? R: 53 / UDP (y TCP para paquetes grandes).

P2: ¿Cómo saber si una respuesta es autoritativa? R: Si aparece la Flag `aa` en la respuesta de `dig`.

P3: ¿Para qué sirve forward only? R: Obliga al servidor a usar solo los reenviadores (IP del prove) y no salir a internet por su cuenta si estos fallan.

P4: Principios de HTTPS R: Confidencialidad (Encriptación), Integridad (Hash), Autenticación (Certificado).

8. HOJA DE REFERENCIA RÁPIDA

Rutas importantes

- DNS Config: `/etc/bind/named.conf.options`
- Nginx Config: `/etc/nginx/sites-available/default`
- Hosts: `/etc/hosts`
- Resolver: `/etc/resolv.conf`
- Certificados: `/etc/ssl/certs/`
- Claves: `/etc/ssl/private/`

Comandos esenciales

- Verificar DNS: `sudo named-checkconf`
- Verificar Nginx: `sudo nginx -t`
- Reiniciar DNS: `sudo systemctl restart bind9`
- Reiniciar Nginx: `sudo systemctl restart nginx`
- Ver puertos: `sudo ss -tulpen`
- Leer certificado: `openssl x509 -in cert.crt -noout -subject`
- Curl detallado: `curl -v https://dominio`
- Curl inseguro: `curl -k https://dominio`