# Redes de Datos
# Laboratorio 2 – Domain Name System

**Universidad ORT Uruguay**

**Curso 2025**

En este laboratorio, analizaremos cómo se resuelve la búsqueda de nombres de dominio mediante el *sistema de nombres de dominio* (Domain Name System, DNS).

Previo a comenzar esta parte, se debe verificar que la VM se encuentre funcionando tal cual se explicó anteriormente. En esta sección del obligatorio se trabajará con la funcionalidad `nslookup`, que permite realizar consultas DNS a pedido del usuario. Para ello primero se debe configurar el servidor que utiliza `nslookup` para que utilice el servidor DNS local que provee la VM.

```
C:\Users\Usuario> nslookup
 Servidor predeterminado: 8.8.8.8 (depende de la máquina)
 Address: 8.8.8.8  (depende de la máquina)

> server 192.168.56.2
 Servidor predeterminado: 192.168.56.2
 Address: 192.168.56.2

> set nosearch
```

Luego de esto, las consultas DNS que se realicen con esta instancia de nslookup, se ejecutarán contra el servidor instalado en la VM. El comando `set nosearch` es para evitar que el `nslookup` realice búsquedas adicionales con el nombre de dominio por defecto de su máquina como sufijo. De este modo se garantiza de que todas las consultas sean absolutas. Otra forma de lograr esto es indicando con `.` el final del nombre a buscar. En el apéndice se brindan algunos comandos útiles de `nslookup`.

## Consultas al DNS local

Inicie el analizador de tráfico Wireshark. Para esta parte de la práctica se debe capturar el tráfico de la interfaz “Virtual Box host-only network”.

1. Comience la captura y realice, desde su máquina host, una consulta DNS por un registro A usando el comando nslookup.
2. Observe el intercambio entre la máquina host y el servidor DNS local de la máquina virtual.
3. ¿Se resuelve la consulta? ¿Cuánto demora el proceso?
4. Si repite la misma consulta, ¿se logra resolver en menos tiempo? ¿Por qué?

## Resolución del DNS global

En esta segunda parte, es importante capturar el tráfico en 2 interfaces al mismo tiempo: la interfaz local “Virtual Box host-only network” y la interfaz que esté usando la PC para salir a Internet (puede elegir varias interfaces usando CTRL). La idea es ahora observar las consultas adicionales que realiza el DNS local de la VM para resolver la consulta inicial, actuando de manera recursiva.

1. Ingrese como administrador (`redes`, password `redes`) y utilice el comando:

   ```
   $> sudo systemctl restart named
   ```

   Esto permite reiniciar el DNS local y en particular borrar el caché. Puede repetir este comando las veces que lo necesite.

2. Realice nuevamente, desde la máquina host, una consulta DNS por un registro A usando el comando nslookup. Elija un sitio que no haya sido utilizado recientemente (o borre el caché) tratando de comenzar el intercambio de tráfico contra algún root servers.

3. Analice en wireshark el intercambio requerido para resolver la consulta. Identifique en particular:

   *a*) El root-server utilizado.

   *b*) Todos los servidores de nombres de dominio por los que pasa la consulta.

   *c*) Cómo se produce la redirección de un servidor al siguiente (registros NS).

   *d*) Si el servidor final contesta de manera autoritativa al DNS local.

   Puede ser necesario aplicar filtros en Wireshark para lograr reducir la cantidad de paquetes visualizados (por ejemplo `tcp.port==53 || udp.port==53`). Tener en cuenta que existe una gran cantidad de tráfico que se cursa habitualmente por la conexión utilizada por el PC para acceder a Internet.

4. Reinicie la captura de Wireshark (puede guardar la anterior si así lo desea). Realice la misma consulta DNS y analice nuevamente el intercambio en Wireshark. ¿El servidor contesta de caché? ¿Cómo distingue si la respuesta es de caché o no? Detalle las diferencias con el caso anterior. Indique al menos 2 (dos) formas de darse cuenta.

5. ¿Cuál es el comando para encontrar los servidores autoritativos del dominio `com.uy`? Realice la consulta y verifique cuáles son.

6. Realice una consulta no recursiva, usando el registro A, correspondiente a un dominio por el cual no haya consultado anteriormente. Indique el comando utilizado y la salida obtenida. ¿Puede obtener la respuesta? ¿Por qué?

7. Vuelva a realizar la consulta pero en modo recursivo. Indique el comando utilizado y la salida obtenida. ¿Puede obtener la respuesta ahora? ¿Por qué?

8. Haga una consulta correspondiente a `www.yahoo.com` y repita inmediatamente la misma consulta. Detalle las consultas y las salidas obtenidas. Compare las respuestas y explique las diferencias. ¿Cuál es la funcionalidad de esto? ¿Es realmente efectivo? ¿Existen soluciones con mejores resultados?, indicar.

## Consultas al servidor local

1. Obtenga la dirección IP asociada al nombre `www.lab.ort.edu.uy`. ¿Quién responde a esta consulta de manera autoritativa?

2. Busque cómo es posible obtener todos los dominios asociados a la dirección IP `192.168.56.2`.

3. ¿Cuál es el registro por el que se debe preguntar para conocer el servidor al cual podemos entregar correos para el dominio `lab.ort.edu.uy`? Realice la consulta.

## Apéndice: comandos de nslookup

```
> <nombre de dominio>           (realiza una consulta por el nombre de dominio
                                 dado al servidor por defecto)
> <nombre de dominio> <IP>      (realiza una consulta por el nombre de dominio
                                 al servidor situado en IP)
> server <IP DNS local>         (setea el servidor por defecto)
> <IP>                          (realiza una búsqueda reversa en el árbol usando PTR)
> set type=X                    (setea el tipo de registro a buscar, A, MX, etc.)
> set nosearch                  (evita que agregue sufijos al dominio)
> set debug                     (agrega información de debug a la salida)
> set [no]recurse               (permite hacer o evitar las consultas recursivas)
> set all                       (muestra la configuración actual)
```