

# Laboratorio No. 5 - Bases de datos y protocolos de la red

Julian Bojaca

Michael Perilla

## Objetivo

---

- Continuar el aprendizaje de instalación de software base y la operación de los protocolos de la red.

## Herramientas a utilizar

---

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• Computadores</li><li>• Acceso a Internet</li></ul> | <ul style="list-style-type: none"><li>• Software de virtualización</li><li>• Wireshark</li></ul> |
|--|--|

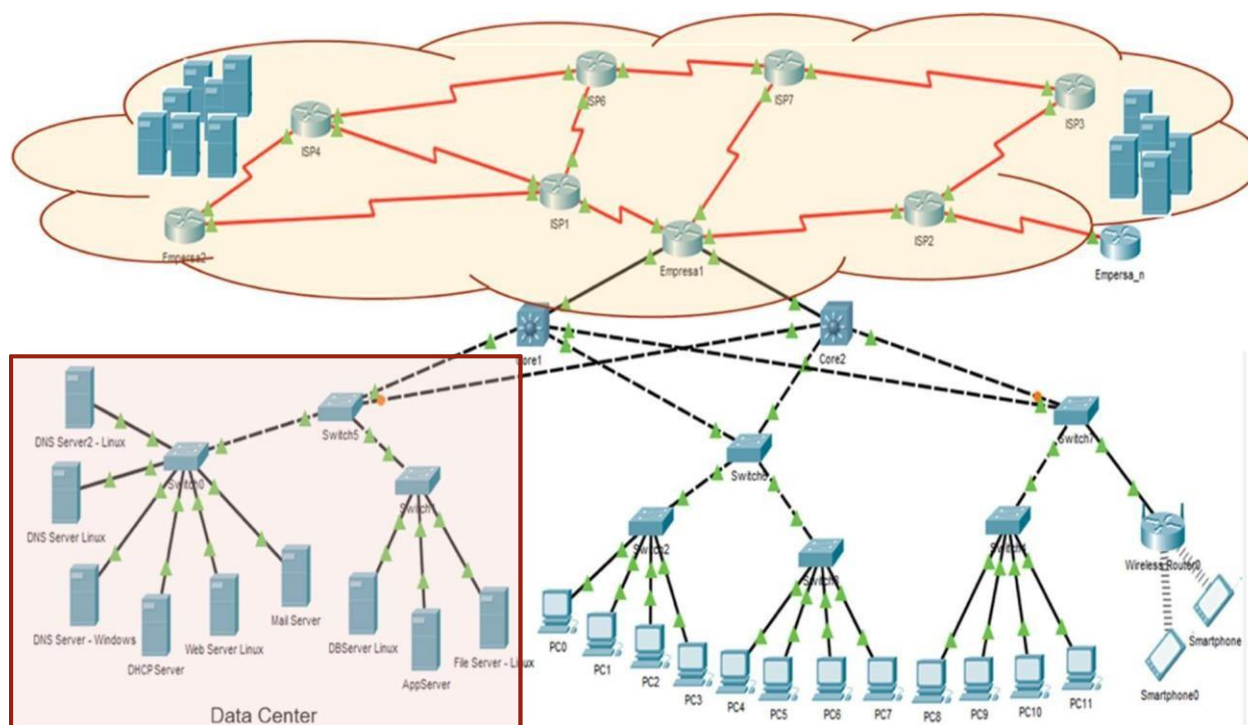
## Marco teorico

- telnet : es una herramienta que ha sido utilizada durante décadas por los administradores de sistema informáticos en el ámbito de las redes. Las conexiones remotas no son algo precisamente nuevo, ya desde las primeras redes y con sistemas sin escritorio se utilizaban herramientas como Telnet para conectarnos a servidores y equipos conectados a una red, tanto de forma remota como interna.
- Wireshark : La herramienta intercepta el tráfico y lo convierte en un formato legible para las personas. Esto hace que sea más fácil identificar qué tráfico está cruzando la red, con qué frecuencia y la latencia que hay entre ciertos saltos. Si bien Wireshark admite más de 2.000 protocolos de red, muchos de ellos inusuales o antiguos, los profesionales encuentran una gran utilidad en el análisis de identidades IP. La mayoría de los paquetes son TCP, UDP e ICMP.
- DNS : El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet. Las personas acceden a la información en línea a través de nombres de dominio como nytimes.com o espn.com. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet. Cada dispositivo conectado a Internet tiene una dirección IP única que otros equipos pueden usar para encontrarlo. Los servidores DNS suprimen la necesidad de que los humanos memoricen direcciones IP tales como 192.168.1.1 (en IPv4) o nuevas direcciones IP alfanuméricas más complejas, tales como 2400:cb00:2048:1::c629:d7a2 (en IPv6).

- HTTP : nos permite realizar una petición de datos y recursos, como pueden ser documentos HTML. Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web. Así, una página web completa resulta de la unión de distintos sub-documentos recibidos, como, por ejemplo: un documento que especifique el estilo de maquetación de la página web (CSS), el texto, las imágenes, vídeos, scripts, etc...

## Introducción

Seguimos trabajando sobre una infraestructura de una empresa, la cual normalmente cuenta con varios servicios de infraestructura TI. En ella se encuentran estaciones de usuario alámbricas e inalámbricas y servidores (físicos y virtualizados), todos estos conectados a través de switches (capa 2 y 3), equipos inalámbricos y routers que lo conectan a Internet. También es común contar con infraestructuras en la nube desde donde se provisionan recursos según las necesidades de la organización. Dentro de los servidores se pueden encontrar servicios web, DNS, correo, base de datos, almacenamiento y aplicaciones, entre otros. Recordemos la configuración que estamos usando de base:



En este parte del laboratorio nos enfocaremos en seguir alistando nuestros servidores.

# Revisión de protocolos de red

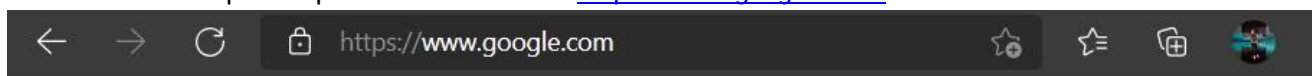
## 1. Revisión de mensaje DNS

Usando el software Wireshark realice una consulta a la página <http://www.google.com/>, filtre los mensajes DNS y revise la resolución de nombre. Identifique los campos y explique sus partes.

Le damos al tipo de internet que tenemos en mi caso es Ethernet

Conexión de área local* 12	—
Conexión de área local* 11	—
Conexión de área local* 10	—
Conexión de red Bluetooth	—
Wi-Fi	—
Ethernet	✓
Conexión de área local* 4	—
Conexión de área local* 3	—
Adapter for loopback traffic capture	✓
OpenVPN TAP-Windows6	—
Conexión de área local	—

Buscamos la ruta que nos pidan en este caso es <http://www.google.com/>



Primero filtramos DNS



Luego nos mostrara todos los dns que encuentre

Time	Source	Destination	Protocol	Length	Info
4615	37.764944	192.168.0.20	DNS	86	Standard query 0x8f95 A encrypted-tbn0.gstatic.com
4616	37.774789	190.157.8.101	DNS	102	Standard query response 0x8f95 A encrypted-tbn0.gstatic.com A 142.250.78.174
4689	37.974834	192.168.0.20	DNS	85	Standard query 0x341c A lhs.googleusercontent.com
4701	37.988758	190.157.8.101	DNS	130	Standard query response 0x341c A lhs.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 142.250.78.129
4801	38.381910	192.168.0.20	DNS	77	Standard query 0x9a54 A fonts.gstatic.com
4811	38.395065	190.157.8.101	DNS	129	Standard query response 0x9a54 A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 142.250.78.99
5318	39.625340	192.168.0.20	DNS	73	Standard query 0x7f81 A id.google.com
5320	39.638343	190.157.8.101	DNS	89	Standard query response 0x7f81 A id.google.com A 142.250.78.67
7424	49.003298	192.168.0.20	DNS	81	Standard query 0xb9e8 A www.escuelaing.edu.co
7442	49.034404	192.168.0.20	DNS	81	Standard query 0xb9e8 A www.escuelaing.edu.co
7459	49.079976	190.157.8.101	DNS	213	Standard query response 0xb9e8 A www.escuelaing.edu.co CNAME stark-cherimoya-jg38tzhuy4qth9c744i6vz0y.herokudns.com A 54.237.133.81
7476	49.095792	190.157.8.101	DNS	213	Standard query response 0xb9e8 A www.escuelaing.edu.co CNAME stark-cherimoya-jg38tzhuy4qth9c744i6vz0y.herokudns.com A 18.205.222.128
7477	49.096122	192.168.0.20	DNS	89	Standard query 0xcfd9 A nav.smartscreen.microsoft.com

7424 49.003298	192.168.0.20	190.157.8.101	DNS	81 Standard query 0xb9e8 A www.escuelaing.edu.co
----------------	--------------	---------------	-----	--

- El primer numero es 7424 este es el numero que el ocupa
- Luego sale 49.003298 este es el tiempo que se demoro en encontrarla
- El 192.168.0.20 es la ip es la fuente
- El 190.157.8.101 es la ip del destinatario
- Luego el DNS es el protocolo este puede variar, pero por el momento solo es DNS
- EL 81 es el tamaño de la longitud
- Por ultimo nos queda la información que dice si es estándar o no en este caso si y mas cosas

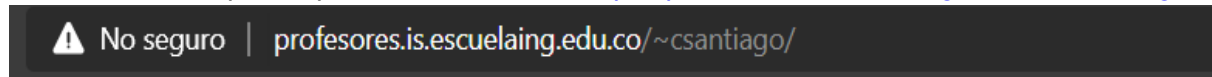
## 2. Revisión de mensaje HTTP

Usando el software Wireshark realice una consulta a la página <http://profesores.is.escuelaing.edu.co/~csantiago/>, filtre los mensajes GET y revise en encabezado del mensaje HTTP. Identifique los campos y explique sus partes.

Le damos al tipo de internet que tenemos en mi caso es Ethernet

Conexión de área local* 12	—
Conexión de área local* 11	—
Conexión de área local* 10	—
Conexión de red Bluetooth	—
Wi-Fi	—
Ethernet	✓
Conexión de área local* 4	—
Conexión de área local* 3	—
Adapter for loopback traffic capture	✓
OpenVPN TAP-Windows6	—
Conexión de área local	—

Buscamos la ruta que nos piden en este caso es <http://profesores.is.escuelaing.edu.co/~csantiago/>



Filtramos



No.	Time	Source	Destination	Protocol	Length	Info
11607	48.169838	192.168.0.20	45.239.88.86	HTTP	677	GET /~csantiago/ HTTP/1.1
11630	48.249798	45.239.88.86	192.168.0.20	HTTP	241	HTTP/1.1 304 Not Modified

Si le damos al alguno nos mostrara mas información

Tenemos la cantidad de frames 11607

Los bytes 677

La ip 192.168.0.20

Etc...

> Frame 11607: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface \Device\NPF_{A1776738-4369-420F-B51E-00F1A3214C94}, id 0		
> Ethernet II, Src: CompalIn_76:aa:62 (08:97:98:76:aa:62), Dst: Technico_d6:f5:a0 (e4:bf:fa:d6:f5:a0)		
> Internet Protocol Version 4, Src: 192.168.0.20, Dst: 45.239.88.86		
> Transmission Control Protocol, Src Port: 52722, Dst Port: 80, Seq: 1, Ack: 1, Len: 623		
> Hypertext Transfer Protocol		
0000	e4 bf fa d6 f5 a0 08 97 98 76 aa 62 08 00 45 00	.....-v-b--E-
0010	02 97 5a 4a 40 00 80 06 00 00 c0 a8 00 14 2d ef	..ZJ@.....
0020	58 56 cd f2 00 50 53 8b 02 4e 06 96 b2 1f 50 18	XV---PS- -N---P-
0030	fa f0 49 8b 00 00 47 45 54 20 2f 7e 63 73 61 6e	..I---GE T /~csan
0040	74 69 61 67 6f 2f 20 48 54 54 50 2f 31 2e 31 0d	tiago/ H TTP/1.1-
0050	0a 48 6f 73 74 3a 20 70 72 6f 66 65 73 6f 72 65	-Host: p rofessore
0060	73 2e 69 73 2e 65 73 63 75 65 6c 61 69 6e 67 2e	s.is.esc uelaing.
0070	65 64 75 2e 63 6f 0d 0a 43 6f 6e 6e 65 63 74 69	edu.co-- Connecti

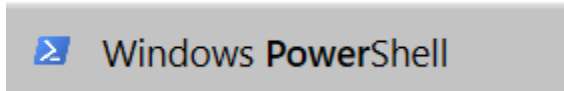
**NOTA:** No hacer este punto en caso de estudiantes trabajando solos.

### 3. Conexión HTTP

- Desbloquee el uso del protocolo TELNET en su computador.

[https://www.youtube.com/watch?v=jqLfTaFO6mM&ab\\_channel=SmythSysITConsulting](https://www.youtube.com/watch?v=jqLfTaFO6mM&ab_channel=SmythSysITConsulting)

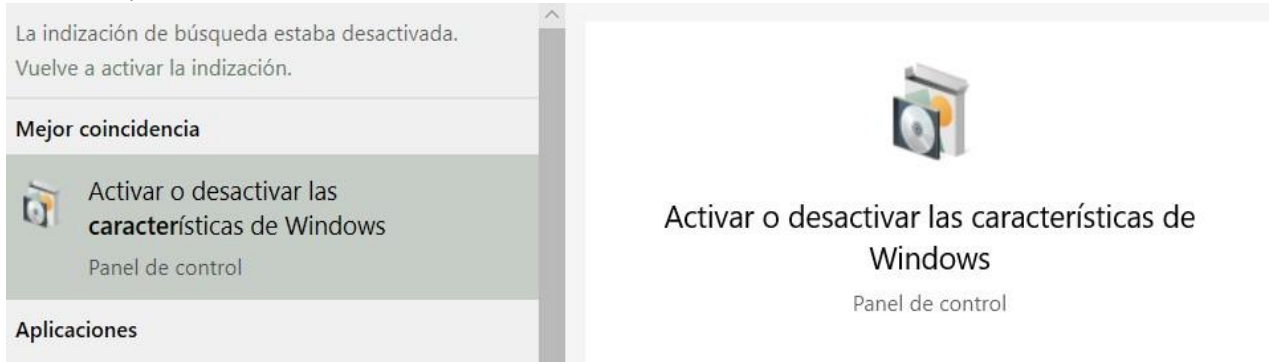
abrimos Windows PowerShell



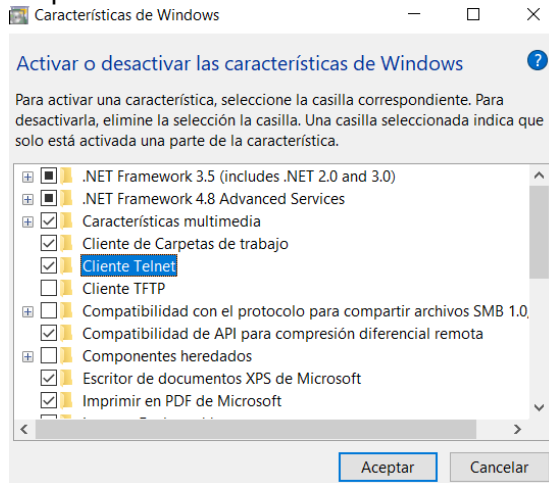
Y cololamos este comando: `dism /online /enable-feature /featurename: telnetclient`

También se puede de otra manera

Buscamos y abrimos Activar o desactivar las características de Windows



Se nos abrirán varias carpetas ya solo buscamos la que dice Cliente Telnet y la activamos y le damos aceptar



Y se pondrá a cargar y lo activara



- Realice captura de los paquetes cuando usa los protocolos TELNET y HTTP y muestre los mensajes de la capa de aplicación generados en las siguientes consultas:
  - Capture la siguiente página web <http://profesores.is.escuelaing.edu.co/~csantiago/RECO/index.html> usando los protocolos:
    - Telnet
      - Telnet profesores.is.escuelaing.edu.co 80
      - **GET** path/archivo. Ej **GET** /index.html.
      - Descargue el archivo tipo PDF prueba.pdf.
      - Descargue el archivo tipo imagen network.png.
    - HTTP
      - Use el browser para mirar las mismas páginas que consultó a través de TELNET
- Presente y explique el resultado de la captura.
- Qué diferencia encuentra entre los archivos descargados con el protocolo TELNET y con el browser?

#### 4. Revisión de frames Ethernet

Usando el software Wireshark realice una consulta a la página <http://profesores.is.escuelaing.edu.co/~csantiago/>, filtre los mensajes GET y revise en encabezado del frame Ethernet. Identifique los campos y explique sus partes.

## Instalación de software base

---

Otro elemento importante en una infraestructura computacional básica son los motores de base de datos. Estos motores pueden estar alojados dentro del datacenter de la empresa o un un servidor ubicado en la nube. En ellos se almacenan los datos estructurados de la organización y son usados desde diferentes aplicativos que soportan su operación.

En los mismos grupos en los que se realizó todo este laboratorio, realice las siguientes actividades:

### 1. Oracle - Solaris

Para todos los grupos

- a. Instale el motor de base de datos Oracle sobre una máquina virtual con sistema operativo Solaris.
- b. Cree un usuario, uno por cada estudiante del grupo. Use los nombres de los estudiantes como nombre de usuario. En caso de grupos de un estudiante, crear al menos dos usuarios.
- c. Cree una bases de datos para manejar la lista de películas/series/programas de TV/etc de cada estudiante, en dicha lista se debe indicar tipo de registro (película/serie/etc), en qué proveedor lo encuentra (TV Terrestre, TV cable - Proveedor, Empresa de entretenimiento por Internet, etc), canal (si aplica) adicionalmente, deberá indicar una programación tentativa para el próximo mes en donde verá los programas indicados. La base de datos debe tener al menos 3 tablas. Cada estudiante debe tener acceso sólo a la base de datos de cada uno.
- d. Inserte datos en las bases de datos.

## 2. PostgreSQL - Linux

Grupo de dos o tres estudiantes

- a. Instale el motor de base de datos PostgreSQL sobre una máquina virtual con sistema operativo Linux Slackware.
- b. Cree un usuario por cada estudiante del grupo. Use los apellidos de los estudiantes como nombre de usuario
- c. Cree una base de datos para manejar el plan de estudios para los semestres que le faltan para terminar la carrera. De cada materia se deberá tener información general como nombre, nemónico, número de créditos, semestre al que pertenece y línea. La base de datos debe tener al menos 3 tablas. Cada estudiante debe tener acceso sólo a la base de datos de una empresa de eventos.
- d. Inserte datos en las bases de datos

## 3. Microsoft SQLServer - Windows Server

Para el grupo de tres estudiantes repita el ejercicio del punto 1 sobre el sistema operativo Windows Server. La base de datos que debe crear debe permitir gestionar los lugares del mundo que quieren visitar, incluyendo destino, tiempo estimado de viaje, días de viaje, condiciones climáticas, tipo de ropa a llevar, tipo de planes a realizar y costos generales. Mínimo 3 tablas.

## 4. Otras configuraciones de motores de bases de datos

1. En los servidores en los que instaló los motores de bases de datos, configure el sistema operativo de tal manera que los motores de base de datos suban automáticamente cuando arranque el sistema operativo.
2. Usando un cliente de conexión a motores de base de datos (Ej. DBeaver), conéctese a sus bases de datos desde una máquina remota y vea el contenido de las tablas.

Muestre los resultados a su profesor.

## Conclusión

Este laboratorio aprendimos a usar una extensión que tenia el pc tenia desactivada y que ayuda a conectarse a otros pc, también vimos mas funciones de WIRESHARK y que es una herramienta muy útil para entender mas todo lo que tiene que ver con conexión.

También vimos el modo correcto de activar las bases de datos en varios sistemas operativos y sus funciones.

## Bibliografía:

<https://www.profesionalreview.com/2019/01/20/telnet-que-es/> (TELNET)

<https://cso.computerworld.es/tendencias/que-es-wireshark-asi-funciona-la-nueva-tendencia-esencial-en-seguridad> (WIRESHARK)

<https://developer.mozilla.org/es/docs/Web/HTTP/Overview> (http)

[https://www.youtube.com/watch?v=jqLftaFO6mM&ab\\_channel=SmythSysITConsulting](https://www.youtube.com/watch?v=jqLftaFO6mM&ab_channel=SmythSysITConsulting) (activar TELNET)