Universidad de los Andes
Facultad de Ingeniería

**Departamento de Ingeniería de Sistemas y Computación**
**Infraestructura de Comunicaciones**

ABET Engineering Accreditation Commission

**Profesor Carlos Lozano**
**calozanog@uniandes.edu.co**

**Asist. De laboratorio: Nathalia Quiroga**
**n.quiroga@uniandes.edu.co**

**Laboratorio #2**

# ANÁLISIS DE PROTOCOLOS DE LA CAPA DE APLICACIÓN

## 1. OBJETIVO (S)

El objetivo de este laboratorio es comprender el funcionamiento de algunos de los protocolos utilizados por los servicios que se prestan en una red de computadoras. Para tal fin se realizará monitoreo y análisis del tráfico de red utilizando la herramienta Wireshark.

Al finalizar la práctica el estudiante estará en la capacidad de:

- Comprender el funcionamiento de los protocolos de la capa de aplicación en la pila de protocolos de Internet.
- Explorar cómo operan y trabajan en forma conjunta protocolos como DNS, RTMP, HTTP, HTTPS y FTP para prestar servicios sobre una red de datos
- Identificar el esquema de encapsulado de datos en la pila de protocolos de Internet
- Identificar y establecer diferencias entre la funcionalidad de diferentes protocolos y servicios de red
- Utilizar el analizador de protocolos Wireshark para el análisis de servicios de red.

## 2. LECTURAS PREVIAS

- Sección - 2.2 Principles of Network Applications. Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th edición.
- Sección - 2.3 Principles of Network Applications. Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th edición.
- Capitulo 4 Network Analysis Using Wireshark. Yoram Orzach. Packt Publishing.

## 3. INFORMACIÓN BÁSICA

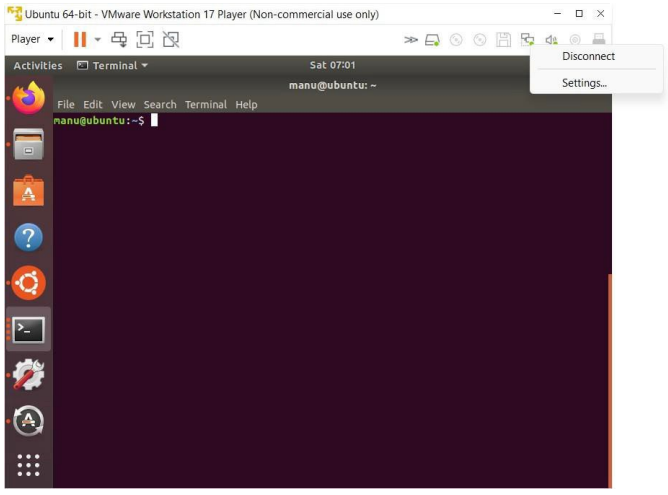
Durante el desarrollo de este laboratorio usted trabajará con un ambiente virtualizado y utilizará herramientas de software de análisis de protocolos para comprender la operación de los diferentes protocolos y mecanismos de intercambio de paquetes en una red de datos.

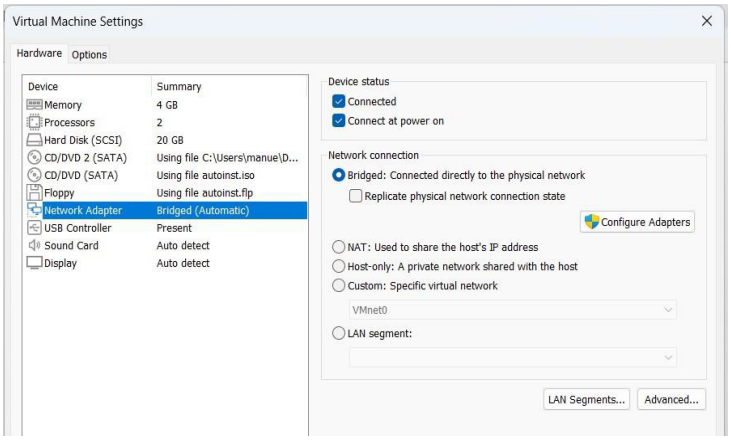
Se recomienda leer la guía completamente antes de iniciar a resolver las actividades propuestas, con el objetivo de tener presente las actividades y los entregables a desarrollar.

## 4. CONFIGURACIÓN DE RED PARA MÁQUINAS VIRTUALES

Es posible configurar la conexión de red de una máquina virtual (VM) de varias formas, para este laboratorio son importantes NAT y Bridge.

Para cambiar la configuración de red en VMware, en la barra superior dé click derecho al botón Network Adapter, diríjase a la configuración y seleccione la configuración en la sección Network connection, no olvide aplicar los cambios en la barra inferior de la ventana.




## 5. NAT

NAT proporciona a una máquina virtual acceso a los recursos de red con la dirección IP del equipo host, es decir, permite que la VM acceda a redes externas a través de la IP del host.

La VM obtene una dirección privada, cuando esta quiere comunicarse con una red externa (como internet), se traduce la IP privada de la VM a la IP pública del host. Las respuestas externas llegan a la IP pública del host y esas respuestas se traducen de vuelta a la IP privada de la VM.

## 6. BRIDGE

El modo Bridge hace que la máquina virtual se comporte como una nueva máquina física, puede asignar IPs de forma automática dentro del rango de la red del host que usualmente es 192.168.1.1 – 192.168.1.254, aunque usualmente se asignan IPs fijas.

La VM se comporta como otro dispositivo en la red local y obtiene una dirección IP del mismo servidor DHCP que el host (o utiliza una dirección estática), cualquier dispositivo en la red puede comunicarse directamente con la VM sin necesidad de traducir direcciones.

# 7. PROCEDIMIENTO

Este laboratorio presenta una topología de red local en pequeña escala, donde se integran equipos de cómputo que ofrecen el servicio de nombres de dominio, un servicio web, un servicio de transmisión de video, un servicio de voz por IP y un servicio de transferencia de archivos. Deben desplegar los servicios de red mencionados y garantizar la conectividad y operación de cada uno de los servicios.

Como se mencionó anteriormente, se utilizará esta infraestructura para realizar un monitoreo del tráfico y el análisis de protocolos utilizando la herramienta de análisis de paquetes Wireshark.

**¡RECORDATORIO! LAS SIGUIENTES HERRAMIENTAS SON SÓLO RECOMENDACIONES, USTEDES PUEDEN USAR OTROS RECURSOS, TUTORIALES ETC.**

## 7.1 Servidor WEB

- Utilice Apache2 como servidor web sobre Ubuntu.
- Cree una página web personalizada (sencilla “Hello world”) alojada localmente.
- Para habilitar HTTPS, genere un certificado autofirmado con OpenSSL y configúrelo en Apache.
- Verifique que los puertos 80 y 443 o Apache estén **permitidos en el firewall (UFW)**
- **Cuando tenga el DNS:** Asegúrese de que el DNS esté configurado y resolviendo correctamente la URL del servidor web, la url debe ser web.labredesXY.com. Donde “X” es el número de grupo y “Y” la sección.
- Se espera que el sitio sea accesible tanto por IP como por url (HTTP y HTTPS).

## 7.2 Servidor FTP

- Use ProFTPD como servidor FTP.
- Cree usuarios locales con acceso a carpetas específicas y necesarias.
- Reinicie el servicio y compruebe que el servidor esté funcionando con la aplicación FileZilla.
- Las pruebas deben incluir descarga y subida de archivos usando FileZilla u otro cliente gráfico.
- **Cuando tenga el DNS**: Asegúrese de que el DNS esté configurado y resolviendo correctamente la URL del servidor ftp, la url debe ser ftp.labredesXY.com. Donde “X” es el número de grupo y “Y” la sección.

## 7.3 Servidor RTMP

- Instale Nginx.
- Permitir el tráfico por el firewall a Nginx HTTP.
- Instale libnginx-mod-rtmp
- Edite nginx.conf, con el puerto usual 1935
- Permita el tráfico del **puerto 1935/TCP** en el firewall.
- Instale **OBS Studio** en la máquina emisora y configure la URL del servidor como rtmp://<IP>/key-personal y el stream key.
- Transmita una fuente de video (puede ser captura de escritorio).
- Desde otra máquina (cliente), visualice la transmisión usando **VLC Media Player** con la URL rtmp://<IP>/live/<streamkey>.

## 7.4 Servidor VoIP

- Utilice Asterisk como central telefónica IP, instale y configure el cliente.
- Configure los usuarios (al menos 2 usuarios) SIP
- El puerto usual es el 5060, y autenticación básica (username, secret).
- Definir las extensiones de llamada.
- Utilice el CLI de Asterisk (asterisk -r) para validar la carga de configuraciones (sip reload, sip show peers).
- Use **Zoiper** y conéctelo al servidor.
- La llamada debe funcionar entre dos clientes conectados a la red.

## 7.5 Servidor DNS

- Instale **BIND9** y sólo use **IPv4**.
- Recuerde crear que hay 2 zonas: inversa y directa que ustedes deben configurar,
- **Añada los registros para los siguientes servicios**: WEB, FTP y DNS.
    - dns.labredesXY.com

- web.labredesXY.com
- ftp.labredesXY.com

- Donde “X” es el número de grupo y “Y” la sección.
- Valide la configuración con named-checkzone.
- Configure las demás VMs para que usen este DNS, y pruebe con **nslookup** desde los clientes.

# 8. PRUEBAS DE CONECTIVIDAD USANDO WIRESHARK Y CMD.

**CAPTURA DE TRÁFICO = CAPTURA DE WIRESHARK**

## 8.1 Prueba ping

Con la finalidad de verificar la conectividad de los dispositivos en la red, y de analizar el tráfico generado por esta prueba se propone la realización de las siguientes actividades.

1. Realice pruebas de conectividad desde el Cliente al Servidor seleccionado para prestar el servicio de DNS en la red, para esta prueba utilice la dirección IP del servidor. Guarde en un archivo la captura del tráfico con el nombre **Ping_DNS_IP.pcap**.
2. Realice pruebas de conectividad desde el Cliente al Servidor seleccionado para prestar el servicio de transferencia de archivos, para esta prueba utilice la dirección IP del servidor. Guarde en un archivo la captura del tráfico con el nombre **Ping_FTP_IP.pcap**.
3. Abra cada uno de los archivos .pcap y en el cuadro de filtro en la interfaz de Wireshark escriba ICMP y haga click en el botón Apply; a continuación, identifique la siguiente información y consígnela en una tabla en el documento de reporte:
   - Dirección IP de origen del paquete generado por el comando request
   - Dirección IP de destino del paquete generado por el comando request
   - Dirección IP de origen del paquete generado por el comando reply
   - Dirección IP de destino del paquete generado por el comando reply
   - Dirección MAC del equipo Cliente
   - Dirección MAC del equipo Servidor

## 8.2 Análisis de tráfico del Servicio DNS

Como se evidenció en los anteriores laboratorios el servicio DNS es un servicio que realiza la traducción entre los nombres de los dominios y las direcciones IP – y viceversa- con la finalidad de que se pueda establecer un proceso de comunicación con un dispositivo destino accediendo al mismo por su nombre.

Durante esta práctica de laboratorio usted generará tráfico correspondiente al servicio DNS y este será capturado utilizando la herramienta Wireshark.

1. Realice pruebas de conectividad desde el Cliente al Servidor seleccionado como Servidor Web en la red utilizando su dirección IP. Guarde en un archivo la captura del tráfico con el nombre **Ping_WEB_IP.pcap**.

2. En la consola de comandos del equipo Cliente digite el comando ipconfig /displaydns.

3. Borre el registro caché del DNS. Para este fin en la consola de comando del equipo Cliente digite el comando ipconfig /flushdns. Verifique que la caché del DNS se vació usando nuevamente el comando ipconfig /displaydns.

4. Realice nuevamente pruebas de conectividad desde el Cliente al Servidor seleccionado como Servidor Web en la red, pero esta vez utilizando su dirección URL (web.labredesZX.com). Guarde en un archivo la captura del tráfico con el nombre **Ping_WEB.pcap**.

5. Abra cada uno de los archivos. pcap y en el cuadro de filtro en la interfaz de Wireshark escriba DNS y haga click en el botón Apply; a continuación, identifique la siguiente información y consígnela en el documento de reporte:

    - Identifique la información de la capa de aplicación que aparecen en los paquetes capturados que estén relacionados con el servicio DNS, en las pruebas realizadas.

    - Identifique el protocolo de la capa de transporte generado por las peticiones al servidor DNS.

    - Identifique los puertos utilizados por el servicio de DNS

    - Complete la tabla generada en el punto anterior con los datos del Servidor Web.

## 8.3 Análisis de tráfico del Servicio FTP

El protocolo de transferencia de archivos (FTP) se utiliza para transferir archivos desde un dispositivo de red hasta otro. Verifique el correcto funcionamiento para descargar y cargar archivos del servidor antes de iniciar el trabajo propuesto.

1. Borre el registro caché del DNS.

2. En la maquina Cliente, acceda al programa cliente FTP y conéctese al servidor FTP, utilice la dirección IP del servidor o su URL (ftp.labredesZX.com). Recuerde que para acceder al servicio debe autenticarse con un usuario valido.

3. Una vez conectado al servidor FTP descargue un archivo. Guarde en un archivo la captura del tráfico generado hasta este punto con el nombre **FTP_download.pcap**.

4. Cargue un archivo en el servidor FTP, específicamente en el directorio asignado al usuario. Guarde en un archivo la captura del tráfico generado hasta este punto con el nombre **FTP_upload.pcap**.

5. Abra cada uno de los archivos. pcap y realice primero un filtro en la interfaz de Wireshark para el protocolo FTP y haga click en el botón Apply; a continuación, identifique la siguiente información y consígnela en el documento de reporte:

    - Identifique la información de la capa de aplicación que aparecen en los paquetes capturados que estén relacionados con el servicio de transferencia de archivo, en las pruebas realizadas.
    - Identifique el protocolo de la capa de transporte generado por las peticiones al servidor FTP.
    - Identifique los puertos utilizados por el servicio de FTP.

## 8.4 Análisis de tráfico del Servicio Web

El servidor web es uno de los servicios de red más populares que utiliza un modelo cliente/servidor. Se utilizan principalmente los protocolos HTTP y HTTPS. Verifique que tiene conectividad con el servidor y que su servicio web funciona correctamente accediendo desde el navegador de la máquina Cliente.

1. Borre el registro caché del DNS.
2. Utilizando el navegador de la máquina cliente conéctese al sitio web configurado en su servidor utilizando el protocolo HTTP. Guarde en un archivo la captura del tráfico generado con el nombre **HTTP_view.pcap**.
3. Abra el archivo **HTTP_view.pcap** y realice primero un filtro en la interfaz de Wireshark para el protocolo HTTP y haga click en el botón Apply; a continuación, identifique la siguiente información y consígnela en el documento de reporte:

    - Identifique la información de la capa de aplicación que aparecen en los paquetes capturados que estén relacionados con el servicio web.
    - Identifique el protocolo de la capa de transporte generado por las peticiones al servidor web.
    - Identifique los puertos utilizados por el servicio web.

## 8.5 Análisis del protocolo HTTPS realizando navegación en el sitio de YouTube

Esta prueba puede realizarse desde cualquier equipo que posea conexión a internet, sea un equipo personal o un equipo del laboratorio

4. Cierre todas las aplicaciones que consuman recursos de red (Navegadores Web, Clientes de Correo Electrónico, Clientes de Mensajería Instantánea, entre otros).
5. Borre el registro caché del DNS.
6. Si utiliza el equipo de laboratorio Windows 10, debe hacer su captura de tráfico usando la interfaz nombrada como Ethernet. Si usa algún un equipo personal identifique la interfaz de conexión a

internet y selecciónela para hacer su captura.

7. Utilizando el navegador conéctese al sitio web https://www.youtube.com/. Es altamente recomendado tener solamente una única pestaña activa en el navegador con la finalidad de poder realizar la captura de tráfico con la menor interferencia posible.

8. Inicié sesión en YouTube con su cuenta de Gmail (de ser posible), navegué por diferentes canales y coloqué comentarios en algunos videos. Guarde en un archivo la captura del tráfico generado con el nombre **YouTube_view.pcap**.

9. Abra una nueva pestaña del navegador, y visite lo sitios web: https://www.elespectador.com, https://www.eltiempo.com/, https://www.uniandes.edu.co/, y https://www.bancolombia.com/. Guarde en un archivo la captura del tráfico generado con el nombre **HTTPS_view.pcap**.

10. Abra cada uno de los archivos .pcap y realice primero un filtro en la interfaz de Wireshark por el puerto 443 mediante la siguiente instrucción tcp.port==443 y haga click en el botón Apply; a continuación, identifique la siguiente información y consígnela en el documento de reporte:

    - Identifique la información de la capa de aplicación que aparecen en los paquetes capturados que estén relacionados con la navegación segura.
    - Identifique el protocolo de la capa de transporte generado por las peticiones al servidor web seguro.
    - Identifique los puertos utilizados por el servicio web seguro

## 8.6 Análisis del protocolo VoIP

1. Cierre todas las aplicaciones que consuman recursos de red (Navegadores Web, Clientes de Correo Electrónico, Clientes de Mensajería Instantánea, entre otros).

2. Inicie una llamada entre dos clientes

3. Guarde en un archivo la captura del tráfico generado con el nombre **VoIP_view.pcap**

4. Abra el archivo .pcap y realice un filtro en la interfaz de Wireshark para distinguir los paquetes provenientes del protocolo

    - Identifique la información de la capa de aplicación que aparece en los paquetes capturados
    - Identifique el protocolo de la capa de transporte utilizado para realizar la llamada
    - Identifique los puertos utilizados

## 8.7 Análisis del protocolo RTMP

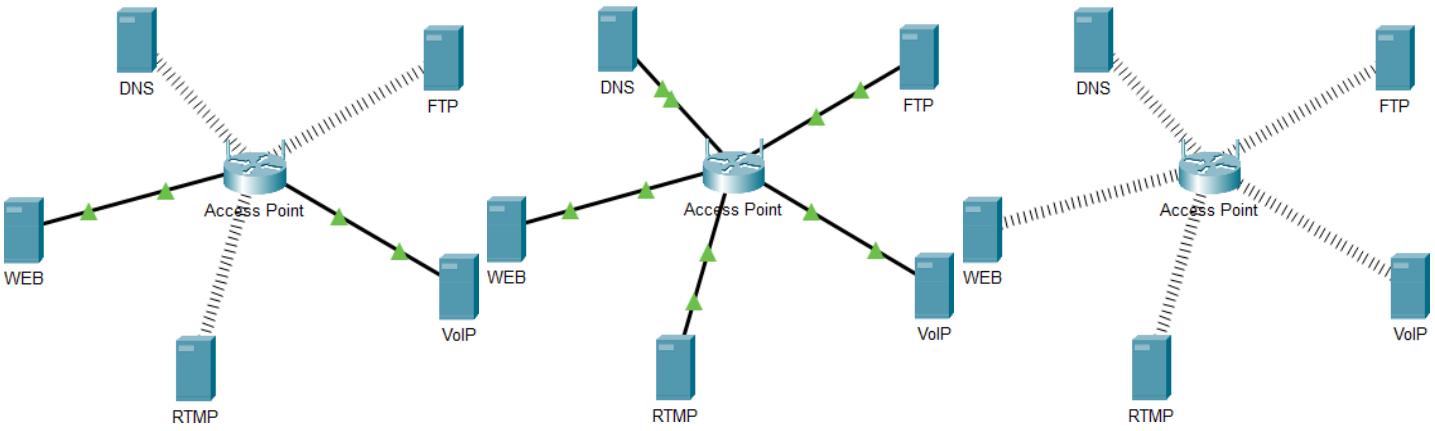
5. Cierre todas las aplicaciones que consuman recursos de red (Navegadores Web, Clientes de Correo Electrónico, Clientes de Mensajería Instantánea, entre otros).

6. Inicie una transmisión a través del servidor
7. Guarde en un archivo la captura del tráfico generado con el nombre **RTMP_view.pcap**
8. Abra el archivo .pcap y realice un filtro en la interfaz de Wireshark para distinguir los paquetes Provenientes del protocolo
    - Identifique la información de la capa de aplicación que aparece en los paquetes capturados
    - Identifique el protocolo de la capa de transporte utilizado para realizar la llamada
    - Identifique los puertos utilizados

## 9. TOPOLOGÍA

Se deben sustentar todos los servicios funcionando, bajo las siguientes consideraciones:

- Las VMs de los servicios deben estar en bridge
- Pueden estar conectados vía Ethernet o Wireless al Access Point como muestran los ejemplos de la imagen (no debe ser exactamente como la imagen, pueden elegir conectar sus servicios de la forma que quieran)
- Si el asistente o uno de los monitores no puede verificar el funcionamiento de la topología, el informe no será revisado.



## 10. ENTREGABLES

El entregable para este laboratorio es:

1. Informe en formato .pdf con:
    - Evidencia pertinente de los resultados de la realización de las actividades de laboratorio con sus respectivos títulos y descripciones.
    - Enlace de descarga para obtener las capturas de tráfico que obtuvo durante la práctica.

Este documento debe ser entregado utilizando el enlace habilitado en Bloque Neón para tal fin.

---

## HISTORIAL DE CAMBIOS

**Registro de cambios**

| Fecha | Autor(es) | Versión | Referencia de cambios |
|---|---|---|---|
| 01/02/2025 | **Nathalia Quiroga** n.quiroga@uniandes.edu.co | 2 | Actualización y cambio de las guías |
| 01/02/2025 | **Manuela Pacheco Malagón** m.pachecom2@uniandes.edu.co | 1.8 | Actualización del laboratorio |
| 24/08/2023 | **Nathalia Quiroga Alfaro** n.quiroga@uniandes.edu.co | 1.7 | Actualización del laboratorio |
| 27/02/2023 | **Nicolás Segura Castro** n.segura@uniandes.edu.co | 1.6 | Actualización del laboratorio |
| 20/02/2022 | **Ramón Alejandro Arias** ra.ariasr@uniandes.edu.co | 1.5 | Ajustes del laboratorio |
| 05/02/2021 | **Arnold Andres Lara** a.larav@uniandes.edu.co | 1.4 | Ajustes de redacción y actualización del laboratorio |
| 05/09/2020 | **Arnold Andres Lara** a.larav@uniandes.edu.co | 1.3 | Ajustes de redacción por cambios de topologías y recursos del laboratorio. |
| 15/01/2020 | **Arnold Andres Lara** a.larav@uniandes.edu.co | 1.2 | Ajustes de redacción y actualización del laboratorio |
| 08/07/2019 | **Jonatan Legro Pastrana** j.legro@uniandes.edu.co | 1.1 | Recopilación de versiones anteriores y actualización. |