**Gestión y Monitoreo de las Redes**

¡Bienvenido a clase!

1. Introducción a la Gestión y Monitoreo de las Redes

**¡Te damos la bienvenida!**

**Gestión y Monitoreo de redes**

Iniciaremos  nuestro estudio de la **Gestión y Monitoreo de Redes**, explorando los conceptos y fundamentos de las redes de comunicación, tales como los modelos de **comunicación OSI y TCP/IP.** Continuaremos analizando las estructuras y principales funciones del modelo OSI  y los diferentes protocolos asociados a este modelo, comenzando por las capas que operan en los niveles más bajos de la jerarquía hasta la más alta, la capa de aplicación. Con especial énfasis en las **Redes de Área Local (o LANs) y el estándar Ethernet.**

Seguiremos examinando el **Protocolo de Internet (o IP)**, que constituye el núcleo de las redes TCP/IP. En particular, revisaremos la estructura de los paquetes, la entrega de paquetes y el direccionamiento. Estudiaremos otros protocolos de comunicación, como lo son **DHCP**, para la entrega dinámica de parámetros de red, NAT para la resolución de direcciones IP, y **UDP y TCP** para el manejo de la comunicación entre procesos ejecutándose en los entes finales de la comunicación.  Nos enfocaremos no sólo en **IPv4**, que constituye la versión más antigua del protocolo, sino también en **IPv6** la propuesta para la generación siguiente de IP.

Es bien conocido el auge de las redes inalámbricas, que aunque siguen los principios y conceptos abordados anteriormente, tienen sus peculiaridades, que abordaremos en esta propuesta educativa. Analizaremos, en particular, a las **redes IEEE 802.11 o redes Wi-Fi**.

Para finalizar te presentamos un compendio de consideraciones que debemos tomar en cuenta a la hora de diseñar, configurar e instalar una red sea cableada o inalámbrica. Y seguidamente estudiaremos el  uso del **solucionador de problemas de Windows y el Network Manager** con el fin de diagnosticar y resolver incidentes que se pueden  presentar en las redes de comunicación.

Después de haber culminado exitosamente el curso de Gestión y Monitoreo de Redes  habrás desarrollado las siguientes capacidades:

# Antes de Comenzar

# Gestión y Monitoreo de redes

#### ¿Qué necesitas?

Experiencia en el manejo  de software como usuario, tales como: procesador de palabras y hoja de cálculo. Conocimiento básico de la estructura de un computador y sus componentes en Windows y Linux, así como también manejo básico de la interfaz gráfica y la interfaz de línea de comando en ambos sistemas operativos. Experiencia en la navegación por Internet y muchas ganas de aprender.

#### Objetivos de aprendizaje

1. **Interpretar los conceptos, características, protocolos y modelos de las redes** de comunicación en el contexto de las comunicaciones actuales.
2. **Usar los elementos de TCP/IP** en el diseño de una red de mediana complejidad.
3. **Usar los elementos del estándar IEEE 802.11 (Wi-Fi)** en el diseño de una red de mediana complejidad.
4. **Desarrollar una configuración para una red TCP/IP** siguiendo un conjunto de buenas prácticas.
5. **Configurar red IEEE 802.11 (Wi-Fi)** siguiendo un conjunto de buenas prácticas.
6. **Resolver incidentes relacionados a las redes Ethernet, TCP/IP y Wi-Fi** de mediana complejidad.

2. Objetivos y expectativas

3. Conoce al equipo de instrucción

UNIDAD 1: Modelos de Redes, Transmisión de Bits y Control de Acceso al Medio (Ethernet)

1. UNIDAD 1: Introducción
2. Lección 1: Introducción a la Redes de Comunicaciones

**Unidad 1**

**Modelos de Redes, Transmisión de Bits y Control de Acceso al Medio (Ethernet)**

Te damos la bienvenida al mundo de las Redes de Comunicación. Comenzamos nuestra trayectoria con una introducción a los elementos que componen un sistema de comunicación, lo cual es importante a la hora de diseñar, implementar y manejar cualquier red de datos. Abordaremos algunas definiciones básicas, así como también una clasificación de estos sistemas de acuerdo a ciertos aspectos, tales como: la cobertura geográfica y su topología. Así mismo, veremos la importancia de los estándares que permiten la interconexión de equipos de diferentes fabricantes.

Dada la complejidad de las redes de comunicación, se han definidos modelos jerárquicos que dividen las tareas en capas o niveles. En nuestro recorrido exploremos los más utilizados hoy en día, como son el Modelo OSI y el Modelo TCP/IP. Abordamos la filosofía de ambos, dividiendo el problema de la comunicación de datos en una serie de capas que van desde el nivel de abstracción más bajo (la capa física) hasta el nivel más alto (la capa de aplicación).

Ethernet es el estándar para redes de área local más usado en el mercado. En esta unidad dedicamos un tiempo en analizar esta tecnología, incluyendo los detalles de la capa física y la capa de acceso al medio. Igualmente, practicaremos con algunos comandos y utilidades de nuestro sistema operativo para ir configurando y manejando nuestra red.

Un aspecto importante de las redes es su rendimiento, durante nuestra aventura de aprendizaje, iremos conociendo algunos parámetros de rendimiento de la red y cómo manejarlos a través de ciertas utilidades y herramientas.

Finalmente, consolidaremos todos estos conceptos revisando los diferentes medios para establecer la conexión entre computadores, ya sea a través de medios cableados o inalámbricos.  Por último, revisaremos los diferentes dispositivos de interconexión de datos, tales como: repetidores, concentradores y conmutadores.

Al finalizar esta unidad estarás en la capacidad de:

**Objetivos de aprendizaje**

1. **Diferenciar los componentes de una red** con la finalidad de definir y manejar un sistema de comunicación.
2. **Usar comandos y herramientas** para realizar actividades de diagnóstico básicas del estado, velocidad y calidad de una red determinada.
3. **Diferenciar los distintos medios de transmisión**, con especial énfasis en las redes Ethernet.
4. **Diferenciar los diversos equipos de interconexión** que pueden ser usados en la implementación de una red de datos.

2.1. Video 1: Definiciones Fundamentales

2.2. Actividad 1

2.3. Video 2: Modelos de Referencia: OSI y TCP/IP

2.4. Actividad 2

2.5. Taller

# Aprende haciendo

# Instalando Wireshark

¡Bienvenido a tu primera aventura en el fascinante mundo de las redes de computadoras!. A continuación vamos a consolidar nuestros conocimientos instalando **Wireshark**, una herramienta que nos permitirá capturar y analizar la información que pasa a través de la red.

1. **Descarga** el archivo de instalación de **Wireshark** del sitio oficial de la herramienta [https://www.wireshark.org/#download.](https://www.wireshark.org/#download)
2. Haz **doble clic** en el archivo descargado para  iniciar la instalación de **Wireshark**. Acepta las opciones por defecto, hasta finalizar la instalación. A continuación algunas imágenes del proceso de instalación.  
   Imagen que contiene captura de pantalla

   Descripción generada automáticamente
3. Después de extraer los archivos y como parte de la instalación, se instala **WinPcap** que es una herramienta que usa **Wireshark** para capturar puertos USB.
4. **Haz clic en Finish**. Se realiza la extracción y luego la instalación.

Ahora que tenemos instalado el Wireshark, podemos empezar a analizar la red que tengas disponible. Para ello, realizamos las actividades que se describen a continuación.

### Actividades:

1. **Ejecuta la aplicación Wireshark**. La aplicación va a empezar a capturar paquetes desde todas las interfaces de red disponibles. **Al transcurrir un tiempo** empiezan a aparecer los datos
2. **Elegimos una interfaz de red**, haciendo clic en la misma. En este caso elegiremos la interfaz Wi-Fi, pero podemos utilizar cualquiera que tenga algún flujo de datos.  
   Imagen que contiene captura de pantalla

   Descripción generada automáticamente
3. **Inicia la captura** haciendo clic en el ícono con forma de aleta de tiburón debajo de la palabra “File”.
4. Ahora **visita diferentes páginas** desde tu navegador, generando un tráfico que pueda ser capturado (algunos sitios están protegidos y no muestran el protocolo HTTP):
   * Reproduce música con Spotify.
   * Inicia la reproducción de algún vídeo de Youtube.
   * Busca en Google: “Tutoriales Wireshark”.
   * Abre tu cliente de correo electrónico.
5. Mientras navegas, **Wireshark** está capturando todo el tráfico que pasa por la interfaz que elegiste para capturar. Detén el proceso de captura haciendo clic en el cuadro que está al lado de la aleta de tiburón.
6. **Elige el tráfico del protocolo ARP**. Para ello usa las facilidades de filtrado de la herramienta. Haciendo clic en el ícono que está debajo de la aleta de tiburón (“Manage saved bookmarks”) se abre una serie de opciones de filtrado ya predefinidas.  
   Imagen que contiene captura de pantalla

   Descripción generada automáticamente  
   Elige el filtro ARP (“**Ethernet type 0x0806 (ARP): eth.type==0x0806**”)  
   Imagen que contiene captura de pantalla

   Descripción generada automáticamente  
   Wireshark muestra sólo los paquetes que cumplen con el criterio de filtro. En este caso, sólo el tráfico del protocolo **ARP**.  
   Imagen que contiene captura de pantalla

   Descripción generada automáticamente  
   Cuando seleccionamos un paquete (Frame), podemos observar que tiene **dos encabezados**, ya que es un PDU de la capa de enlace de datos. Describe cada uno de ellos.
7. **Elige el filtro TCP** (“TCP only:tcp”)  
   Wireshark muestra sólo los paquetes que cumplen con el criterio de filtro. En este caso, sólo el tráfico del protocolo **TCP**.  
   Cuando eliges un paquete (Frame), podemos observar que existen **tres encabezados**, ya que es un PDU de la capa de transporte. Describe cada uno de ellos.
8. **Vamos ahora a observar el tráfico** **HTTP**, para ello escribe directamente “**HTTP**” en la barra de filtro.  
   Wireshark mostrará sólo los paquetes que cumplen con el criterio de filtro. En este caso, sólo el tráfico del protocolo **HTTP**.  
   Cuando escoges un paquete (Frame), puedes observar que tiene **cuatro encabezados**, ya que es un PDU de la capa de aplicación. Describe cada uno de ellos.

Por ahora nos despedimos, invitándote a continuar con las actividades que te ofrecemos para consolidar los conocimientos adquiridos.

# Cápsula de conocimiento

# La Pila de Protocolos de TCP/IP

¡Hola! Seguimos conociendo definiciones fundamentales para la gestión de redes. En esta ocasión estudiaremos la pila de protocolos TCP/IP.

La mayoría de los conjuntos de protocolos de red se estructuran como series de capas, que en ocasiones se denominan **pila de protocolos**. Cada capa está diseñada para una finalidad específica. Cada capa existe tanto en los sistemas de **envío** como en los de **recepción**. Una capa específica de un sistema envía o recibe exactamente el mismo objeto que envía o recibe el proceso equivalente de otro sistema. Estas actividades tienen lugar independientemente de las actividades de las capas por encima o por debajo de la capa que se está considerando. Básicamente, cada capa de un sistema actúa independientemente de las demás capas del mismo sistema y cada capa a su vez actúa en paralelo con la misma capa en otros sistemas.

La **familia de protocolos de Internet**, es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

En ocasiones se le denomina **conjunto de protocolos TCP/IP**, en referencia a los dos protocolos más importantes que la componen, que fueron de los primeros en definirse, y que son los dos más utilizados de la familia:

1. **TCP:** Protocolo de Control de Transmisión.
2. **IP:** Protocolo de Internet.

Existen diferentes protocolos en este conjunto que llegan a ser más de cien, entre ellos se encuentran:

* **ARP:** protocolo de resolución de direcciones, para encontrar la dirección física (MAC) correspondiente a una determinada IP.
* **FTP:** protocolo de transferencia de archivos, popular en la transferencia de archivos.
* **HTTP:** protocolo de transferencia de hipertexto, que es popular porque se utiliza para acceder a las páginas web.
* **POP:** protocolo de oficina de correo, para correo electrónico.
* **SMTP:** protocolo para transferencia simple de correo, para el correo electrónico.
* **TELNET:** (Telecommunication Network), protocolo para acceder a equipos remotos.
* **TCP/IP:** fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

La familia de protocolos de Internet puede describirse por analogía con el modelo **OSI** (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel resuelve una serie de tareas relacionadas con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería. El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de computadoras. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa. Sirve de ayuda entender el OSI, antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el OSI.

### El modelo OSI

El **modelo de Interconexión de Sistemas Abiertos** (ISO/IEC 7498-1), más conocido como “**Modelo OSI**”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO). ​ La Unión Internacional de Telecomunicaciones (UIT) lo publicó en 1983 y, desde 1984, la Organización Internacional de Normalización (ISO) también lo ha divulgado como su estándar.​ Su desarrollo comenzó en 1977.

El Modelo de Referencia OSI constituye un armazón para los estándares desarrollados o a desarrollarse destinados a soportar la interconexión de sistemas. Tiene la finalidad de permitir la comunicación entre equipos de diferentes vendedores y fabricantes alrededor del mundo. En la figura siguiente puede observarse una comparación entre los modelos OSI y TCP.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

La figura muestra las capas de protocolo TCP/IP y los equivalentes del modelo OSI. También se muestran ejemplos de los protocolos disponibles en cada nivel de la pila del protocolo TCP/IP. Cada sistema que participa en una transacción de comunicación ejecuta una única implementación de la pila del protocolo.

## Modelo de arquitectura del protocolo TCP/IP

### Capa de Acceso a la Red

Realiza las funciones de las **capa de red física y la capa de enlace de datos del modelo OSI**. En cuanto a la capa física, especifica las características del hardware que se utilizará para la red. Por ejemplo, las caracterìsticas fìsicas del medio de comunicaciòn. La capa física de TCP/IP describe los estándares de hardware como IEEE 802.3, la especificación del medio de red Ethernet, y RS-232, la especificación para los conectores estándar. En relación con las funciones de la capa de enlace de datos, identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. Esta capa también proporciona control de errores y estructuras. Algunos ejemplos de protocolos de capa de enlace de datos son las estructuras Ethernet IEEE 802.2 y Protocolo punto a punto (PPP).

### Capa de Internet

La capa de Internet, también conocida como **capa de red o capa IP**, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

***Protocolo IP***

El protocolo IP y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

* **Direcciones IP:** Las convenciones de direcciones IP forman parte del protocolo IP. Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo de Internet (Internet Protocol). Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.  Existen actualmente dos formatos de direcciones IPv4 e IPv6.
* **Comunicaciones de host a host:** El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
* **Formato de paquetes:** el protocolo IP agrupa paquetes en unidades conocidas como datagramas.
* **Fragmentación:** Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

**Protocolo ARP**

El protocolo de resolución de direcciones (ARP) se encuentra conceptualmente entre  la capa de enlace de datos  y la de Internet. ARP ayuda al protocolo IP a dirigir los datagramas al sistema receptor adecuado asignando direcciones Ethernet (de 48 bits de longitud) a direcciones IP conocidas (de 32 bits de longitud).

***Protocolo ICMP***

El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red. ICMP registra:

* **Paquetes sueltos:** Paquetes que llegan demasiado rápido para poder procesarse.
* **Fallo de conectividad:** No se puede alcanzar un sistema de destino.
* **Redirección:** Redirige un sistema de envío para utilizar otro enrutador.

### Capa de transporte

La **capa de transporte TCP/IP** garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como **transmisión de punto a punto**. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

***Protocolo TCP***

TCP permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

* Punto de partida, que abre la conexión.
* Transmisión completa en orden de bytes.
* Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

TCP confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción. Por tanto, el protocolo TCP se considera un protocolo fiable orientado a la conexión.

***Protocolo SCTP***

SCTP es un protocolo de capa de transporte fiable orientado a la conexión que ofrece los mismos servicios a las aplicaciones que TCP. Además, SCTP admite conexiones entre sistema que tienen más de una dirección, o de**host múltiple**. La conexión SCTP entre el sistema transmisor y receptor se denomina asociación. Los datos de la **asociación** se organizan en bloques. Dado que el protocolo SCTP admite varios hosts, determinadas aplicaciones, en especial las que se utilizan en el sector de las telecomunicaciones, necesitan ejecutar SCTP en lugar de TCP.

***Protocolo UDP***

UDP proporciona un servicio de entrega de datagramas. UDP no verifica las conexiones entre los hosts transmisores y receptores. Dado que el protocolo UDP elimina los procesos de establecimiento y verificación de las conexiones, resulta ideal para las aplicaciones que envían pequeñas cantidades de datos.

### Capa de aplicación

La capa de aplicación define las aplicaciones de red y los servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos. Existen varios protocolos de capa de aplicación. En la siguiente lista se incluyen ejemplos de protocolos de capa de aplicación:

* Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.
* Comandos UNIX "r", como rlogin o rsh.
* Servicios de nombres, como NIS o el sistema de nombre de dominio (DNS).
* Servicios de directorio (LDAP).
* Servicios de archivos, como el servicio NFS.
* Protocolo simple de administración de red (SNMP), que permite administrar la red.
* Protocolo RDISC (Router Discovery Server) y protocolos RIP (Routing Information Protocol).

### Encapsulado de datos y la pila de protocolo TCP/IP

El paquete es la unidad de información básica que se transfiere a través de una red. El paquete básico se compone de un encabezado con las direcciones de los sistemas de envío y recepción, y un cuerpo, o **carga útil**, con los datos que se van a transferir. Cuando el paquete se transfiere a través de la pila de protocolo TCP/IP, los protocolos de cada capa agregan o eliminan campos del encabezado básico. Cuando un protocolo del sistema de envío agrega datos al encabezado del paquete, el proceso se denomina **encapsulado de datos.** Asimismo, cada capa tiene un término diferente para el paquete modificado, como se muestra en la figura siguiente.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

Hasta aquí hemos visto un resumen de la Pila de protocolos TCP/IP, la cual constituye la base para el recorrido que haremos al interesante mundo de las redes, el cual ha devenido en pilar fundamental de la computación moderna.

2.6. Lectura: La Pila de Protocolos de TCP/IP

3. Lección 2: Transmisión de los Datos

3.1. Video 1: ¿Cómo se Transmiten los Datos?

3.2. Actividad 1

3.3. Lectura: Unidades de Transmisión: Hertz a Bytes

3.4. Lectura: Medios de Transmisión

3.5. Video 2: Ethernet-Opciones de la Capa Física

3.6. Actividad 2

3.7. Taller

3.8. Ejercicio

4. Lección 3: Control de Acceso al Medio

5. UNIDAD 1: Prueba

UNIDAD 2: Protocolo de Internet (IP)

UNIDAD 3: Transporte y Aplicaciones de Red

UNIDAD 4: Redes Inalámbricas

UNIDAD 5: Troubleshooting, Monitoreo y Gestión

EVALUACIÓN FINAL