**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/" \l "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.

CAPAS DE MODELO OSI

* 1. Lectura: La Pila de Protocolos de TCP/IP

# 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.

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

# Cápsula de conocimiento

# Unidades de Transmisión: Hertz a Bytes

¡Hola! Con esta lectura vas a seguir profundizando en los aspectos más importantes sobre la transmisión de datos. En tal sentido, vamos a comprender cómo se realiza el cálculo de la   cantidad de datos a transmitir, a  través de un ancho de banda previamente determinado.

Cuando hablamos de comunicación de datos, nos preguntamos **¿Cuántos bits podemos enviar en un segundo, dadas las limitaciones intrínsecas del medio de transmisión?** Esto es análogo a preguntarse cuántos vehículos pueden ir por una determinada autopista a una velocidad promedio de 100 km/h, que es la velocidad máxima permitida. En este caso el número de canales presente en la autopista juega un factor importante para determinar dicho valor.

Para poder explicar la transmisión de bits por un medio físico es importante conocer  un concepto que es el **ancho de banda**. La definición de este concepto puede ser ambigua, ya que depende del contexto en que estemos hablando. Aquí  proporcionamos un par de definiciones relevantes para la gestión de redes.

El **ancho de banda** es el rango de frecuencias que un canal puede pasar, medidos en **Hertz** (ciclos por segundo), por ejemplo, el ancho de banda de un canal de voz es 3100 Hz.

Por otra parte, el **ancho de banda** también se asocia al número de bits por segundo que un canal, enlace o red puede transmitir (es decir, la velocidad de transmisión de un canal o enlace). Por ejemplo, el máximo ancho de banda de un red Gigabit Ethernet es un gigabit por segundo (1.000.000.000 bits por segundo).

Básicamente existe una relación entre ambos anchos de banda y dicha relación está muy ligada a los mecanismos de compartición del canal que se usan para transmitir la información por el medio. Dado lo extenso y complejo del tema, vamos a  introducir dos teorías desarrolladas en esta área.

## Canal de Nyquist o el Ancho de Banda de Nyquist

El siguiente teorema fue establecido por Harry Nyquist de los Laboratorios de Teléfonos Bell, para definir la máxima capacidad de un canal asumiendo que este está libre de errores:

Tasa de bits = 2 x ancho de banda x *log2* L

Donde el ancho de banda, medido en Hertz, es el ancho de banda del canal y L es el número de niveles de la señal usados para representar los datos. La tasa de bits es medida en bits por segundo.

Utilicemos un caso muy simple para ilustrar el teorema y asumamos que empleamos un nivel de voltaje para representar un 1 binario y otro nivel para representar un 0 binario, en un canal de 4000 Hertz. La máxima tasa de bits teórica se calcula seguidamente:

L =2 sólo utilizamos 2 niveles de la señal, un nivel para representar el 1 y otro nivel para representar el 0.

Tasa de bits = 2 x 4000 x *log2* 2 = 8000 bps

## Capacidad del Canal según Shannon

La transmisión a través de un canal está expuesta a muchos factores que pueden afectar el envío de los datos. Por ejemplo, una señal que viaja por un canal se **atenúa** a medida que recorre el medio y esto puede hacer que algunos de los bits cambien su valor, por ejemplo, lo que es un 1 termine siendo un cero y viceversa. Otro de los factores es el ruido, una señal debería tener más potencia que el ruido presente en el canal, para que no se **distorsione**. En general, las señales viajan a través de medios de transmisión que no son perfectos.

Claude Shannon desarrolló una fórmula para estimar la capacidad teórica de un canal con ruido. La capacidad de Shannon se calcula de la siguiente manera:

Capacidad = ancho de banda X *log2* (1 +SNR)

Donde la capacidad viene expresada en bits por segundo y el ancho de banda del canal en Hertz. SNR es la relaciòn señal/ruido  y se estima de la siguiente forma:

SNR= promedio de la potencia de la señal / promedio de la potencia del ruido

Por ejemplo, si la potencia de la señal a ruido es 3162 y el ancho de banda del canal es 3000 Hz, la capacidad máxima teórica del canal se estima como sigue:

Capacidad = 3000 *log2* (1 + 3162) = 3000 x 11,62 = 34.860 bps

## Medidas de Rendimiento

A parte del ancho de banda, existen otras medidas que son utilizadas para estimar el rendimiento de la red. A continuación analicemos las más comunes.

### Throughput

Es una medida de cuántos bits pueden ser efectivamente enviados por la red. Aunque el **throughput** puede parecer semejante al ancho de banda en bits por segundo, no lo es. Una determinada red puede tener un máximo ancho de banda de 100 Mbps, mientras que la tasa de datos efectiva sea la mitad, es decir, 50 Mbps. Diferentes factores pueden influir en el throughput de la red incluyendo los mecanismos y procedimientos usados en las capas superiores del modelo OSI, los cuales pueden retardar el envío efectivo de los datos.

### Latencia (Retardo)

Es el tiempo que toma un mensaje en llegar completamente a su destino y está constituido por el retardo de transmisión, el retardo de propagación, el retardo en cola y el tiempo de procesamiento. Recordemos que en una transmisión se envía un mensaje; el **tiempo de transmisión** es aquel medido desde que el primer bit del mensaje sale del emisor hasta que el último llega al receptor. La forma de calcular dicho tiempo es la siguiente:

**Tiempo de transmisión = tamaño del mensaje / Ancho de Banda**

Por otra parte, el tiempo de propagación está ligado al medio de transmisión y mide el tiempo que un bit necesita en viajar del destino al fin. El mismo se calcula de la siguiente manera:

**Tiempo de propagación = Distancia / Velocidad de propagación**

La velocidad de propagación de las señales electromagnéticas está asociada al medio y la frecuencia de la señal.

En su viaje de la fuente al destino, un mensaje puede ser **encolado** en espera de ser despachado bien en los dispositivos finales o intermedios. El tiempo en cola va a depender del tráfico en la red, por lo tanto, no es fijo.

Finalmente, cada dispositivo puede tomar un tiempo en procesar cada mensaje, sin embargo, este tiempo suele ser muy pequeño en comparación a los otros tiempos discutidos anteriormente.

Para ilustrar lo anteriormente dicho, podemos calcular la **latencia** en el siguiente caso, donde una trama de 5 millones de bits se envía por un enlace que incluye 10 enrutadores que tienen un tiempo de cola de 2 us (microsegundos=10-6 s) y tiempo de procesamiento de 1 us. La longitud del enlace es de 2000 Km. La velocidad de la luz dentro del enlace es 2x108 m/s (metros por segundo) y el ancho de banda es de 5 Mbps .

**Latencia = tiempo de propagación + tiempo de transmisión + tiempo en cola + retardo de procesamiento**

Latencia = (2000x103/2x108)s + (5x106/5x106) s + 10x2 us + 10x1 us

             = 10,000 us + 106 us + 20 us + 10 us = 1010030 us = 1.010030 s

## Tabla de Conversión

A continuación resumimos algunas conversiones entre unidades cuando trabajamos con redes de datos.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Tiempo** | | **Ancho de Banda (Hertz)** | | | **Ancho de Banda (bps)** | | |
| **Unidades** | **Equivalencia** | | **Unidades** | **Equivalencia** | | **Unidades** | **Equivalencia** | |
| Segundos (s) | 1 s | | Hertz (Hz) | 1 Hz | | Bits por segundo (bps) | 1 bps | |
| Milisegundos | 10-3 s | | Kilo Hertz (kHz) | 103 Hz | | Kilobit por segundo (kbps o kbit/s) | 103 bps | |
| Microsegundos | 10-6 s | | Mega Hertz (MHz) | 106 Hz | | Megabit por segundo (Mbps o Mbit/s) | 106 bps | |
| Nanosegundos | 10-9 s | | Giga Hertz (GHz) | 109 Hz | | Gigabit por segundo (Gbps o Gbit/s) | 109 bps | |
| Picosegundos | 10-12 s | | Tera Hertz (THz) | 1012 Hz | | Terabit por segundo (Tbps o Tbit/s) | 1012 bps | |

Tabla 1. Conversiones entre unidades.

A través de este recurso instruccional, hemos visto que el ancho de banda es el rango de frecuencias que un canal puede pasar, medidos en Hertz o el número de bits por segundo que un enlace o red puede transmitir. Es importante conocer que la transmisión a través de un canal está, expuesta a muchos factores como el ruido, la longitud del medio, entre otros, que pueden afectar el envío de los datos. Estos factores deben ser considerados para realizar las estimaciones necesarias sobre la transmisiòn por un determinado canal.

3.4. Lectura: Medios de Transmisión

# Cápsula de conocimiento

# Medios de Transmisión

¡Saludos! En esta oportunidad realizaremos una breve introducción a los medios de transmisión.

Los medios de transmisión se dividen en medios guiados y no guiados. Los primeros proporcionan un conductor para transmitir las señales de la fuente al destino, mientras que los segundos emplean el espacio libre para el envío de las señales. La Figura 1 muestra una clasificación de estos medios de transmisión.

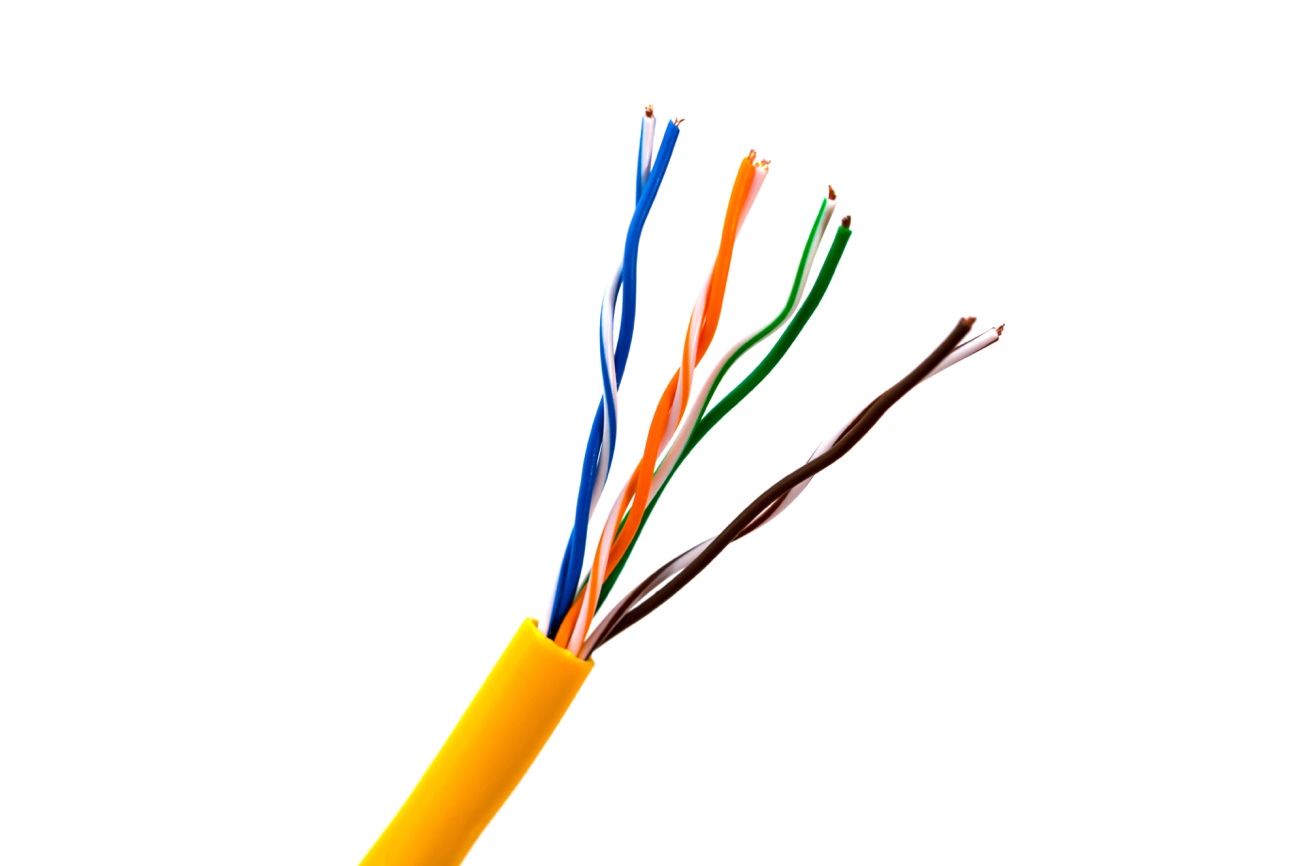
Imagen que contiene texto

Descripción generada automáticamente

Figura 1: Clasificación de los Medios de Transmisión.

## Medio de Transmisión Guiados

### Cable Par Trenzado



##### Cable UTP

#### Estructura

Es un tipo de cable que tiene dos conductores eléctricos aislados y entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes.

#### Funcionamiento

Dos alambres paralelos constituyen una antena simple. Cuando se trenzan los alambres, las ondas de diferentes vueltas se cancelan, por lo que la radiación del cable es menos efectiva. Así la forma trenzada reduce la interferencia eléctrica.

#### Tipos

##### Cable de par trenzado sin blindado (unshielded twisted pair (UTP))

Contiene pares trenzados sin blindar que se utilizan para diferentes tecnologías de redes locales y telefonía.

##### Cable de par trenzado blindado (shielded twisted pair (STP))

Contiene pares trenzados, cada uno de los cuales está rodeado de una cubierta protectora hecha de aluminio. Se utiliza principalmente en redes de computadoras.

#### Categorías

La Asociación de Industrias Electrónicas (Electronic Industries Association (EIA)) ha desarrollado una clasificación del cable UTP basada en el ancho de banda y su uso. Dichas categorías determinan la calidad del cable siendo 1 la más baja. A continuación las categorías comúnmente usadas en la redes de área local:

|  |  |  |
| --- | --- | --- |
| **Categoría** | **Tasa de Datos (aproximada)** | **Ejemplo de Uso** |
| 3 | 10 Mbps | LANs (e.g. Ethernet 10BASE-T) |
| 4 | 16 Mbps | LANs (e.g. Token Ring) |
| 5 | 100 Mbps | LANs (e.g. Ethernet 100BASE-TX) |
| 5e | 1 Gbps | LANs (e.g. Ethernet 1000BASE-T) |
| 6 | 1 Gbps | LANs (e.g. Ethernet 1000BASE-T) |
| 6a | 10 Gbps | LANs (e.g 10GBASE-T) |

##### Ejemplos de Conectores RJ-45

#### Conectores

El conector para el cable UTP más comúnmente empleado en las LANs es el denominado RJ45.

#### Ventajas

Este tipo de cable es caracterizado por ser fácil de manipular y por ser económico en comparación a sus contrapartes.

#### Desventajas

Una de las mayores limitaciones del cable par trenzado y en particular del UTP es que es que las señales transmitidas son propensas a interferencias. Adicionalmente, la distancia máxima que se puede alcanzar con enlaces que empleen este tipo de cable es más corta que las que se pueden alcanzar con otros tipos de medios.

### Cable Coaxial

Imagen que contiene cielo

Descripción generada automáticamente

##### Cable Coaxial

#### Estructura

Un cable coaxial consiste de dos conductores, un conductor cilíndrico con un agujero que rodea al otro, usualmente hecho de una malla de alambre o una lámina metálica.

#### Funcionamiento

El cable coaxial consta de lo siguiente:

* Un **conductor** de cobre utilizado para transmitir las señales electrónicas.
* El conductor de cobre está rodeado por una capa de **aislamiento plástico** flexible.
* Sobre este material aislante, hay una **malla de cobre trenzado** o una hoja metálica que actúa como segundo hilo en el circuito y como blindaje para el conductor interno. La segunda capa o blindaje reduce la cantidad de interferencia electromagnética externa.
* La totalidad del cable está cubierta por un **revestimiento** para protegerlo contra daños físicos menores.



##### Ejemplos de Conectores para Cable Coaxial

#### Conectores

El conector más ampliamente usado con este tipo de cable es el Bayonet Neill-Concelman (BNC).

#### Ventajas

El cable coaxial es menos susceptible a las interferencias y sus características hacen que opere mejor a altas frecuencias y tasas de datos, en comparación con el cable par trenzado.

#### Desventajas

La atenuación, el ruido termal y el ruido de intermodulación son factores que imponen restricciones en el rendimiento de la señal que viaja por este medio.

#### Twinaxial

El twinaxial es similar al cable coaxial, pero posee dos conductores internos que van paralelamente.

Son usados para la transmisión a corta distancia a velocidades superiores que ronda entre los 5 Gbps y 25 Gbps. En particular, se emplea en las implementaciones de Ethernet 10GBASE-CX4 a 10 Gbps.

### Fibra Óptica

Imagen que contiene instrumentos de escritura, papelería

Descripción generada automáticamente

##### Cable de Fibra Óptica

#### Estructura

Un cable de fibra óptica está constituido por un filamento de vidrio ultra puro hecho principalmente de silicio, que permite guiar ondas de luz a través de distancias muy largas. El filamento de fibra óptica está compuesto de:

* Núcleo: es el centro de vidrio por donde viaja la luz.
* Recubrimiento (Cladding): rodea al núcleo y es altamente reflexivo para que la luz pueda rebotar en él.
* Revestimiento (jacket): rodea al cladding y protege la fibra de daños externos.

#### Funcionamiento

Un transmisor óptico envía información codificada en haces de luz. La luz viaja por el núcleo de la fibra óptica rebotando continuamente en el cladding gracias a un principio llamado “Reflexión total Interna”. Los haces de luz llegan a un receptor óptico colocado al otro lado de la instalación de fibra óptica.

En el caso de este medio de transmisor se pueden emplear dos tipos de dispositivos de emisión de luz: el diodo emisor de luz (light-emitting diode (LED)) y el diodo láser de inyección (the injection laser diode (ILD)).

### Tipos de Fibra Óptica

Imagen que contiene cable, conector, interior, mesa

Descripción generada automáticamente

##### Ejemplo de Conector ST (izquierda) y LC (derecha)

#### Multimodo

En esta forma, múltiples rayos de luz se transmiten a través del núcleo pero siguiendo diferentes caminos. Este tipo de fibra presenta limitaciones en la distancia que puede alcanzar.

#### Monomodo

El rayo de luz transmitido sigue una trayectoria recta o casi recta, haciendo este medio eficiente en largas distancias con un mejor rendimiento que la anterior.

#### Conectores

Los tipos de conectores comúnmente usados con fibra óptica son:

* Straight tip (ST)
* Subscriber channel (SC)
* Lucent connector (LC)
* Media termination recommended jack (MTRJ)

#### Ventajas

Las ventajas de la fibra óptica se resumen a continuación:

* Mayores anchos de banda y tasas de transmisión.
* Menor atenuación de la señal.
* No es susceptible a interferencias de las señales electromagnéticas.
* Es ligera.

#### Desventajas

Entre las limitaciones de este tipo de medio de transmisión destacan:

* Requiere de mayor experticia en la instalación y mantenimiento.
* Es más costosa que los otros medios de transmisión guiados.

### Medio de Transmisión No Guiados

Los medios inalámbricos transportan señales electromagnéticas que viajan a través del espacio libre empleando ondas de radio, microondas o infrarrojo. Estas opciones se identifican basado en el rango de frecuencias que ocupan en el espectro electromagnético cuyas frecuencias usadas para la comunicación inalámbrica se encuentran aproximadamente entre los 3 KHz y 900 THz.

Los sistemas inalámbricos no se limitan a conductores o canaletas, como en el caso de los medios de fibra o de cobre, proporcionando mayores opciones de movilidad a los usuarios de dispositivos con interfaces de comunicación inalámbricas. Sin embargo, existen algunas áreas de importancia para la tecnología inalámbrica, que incluyen las siguientes:

* **Área de cobertura:** las tecnologías inalámbricas de comunicación de datos funcionan bien en entornos abiertos. Sin embargo, existen determinados materiales de construcción utilizados en edificios y estructuras, además del terreno local, que limitan la cobertura efectiva.
* **Interferencia:** la tecnología inalámbrica también es vulnerable a la interferencia y puede verse afectada por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos de microondas y otras comunicaciones inalámbricas.
* **Seguridad:** la cobertura de la comunicación inalámbrica no requiere acceso a un hilo físico de un medio. Por lo tanto, dispositivos y usuarios sin autorización para acceder a la red pueden obtener acceso a la transmisión. En consecuencia, la seguridad de la red es un componente importante en la administración de una red inalámbrica.

El tipo de medio es un factor determinante en la calidad de transmisión que se realice. Tanto en los medios guiados como no guiados, tenemos limitaciones relacionadas con la velocidad de transmisión, ancho de banda soportado y espacio entre repetidores. De allí la importancia de una buena selección del medio a la hora de realizar el diseño y configuración de una red de comunicaciones.

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

3.6. Actividad 2

3.7. Taller

# Medidas de Rendimiento: Throughput y Latencia

¡Hola! Con este reto vas a seguir profundizando en los aspectos más importantes de las redes de comunicación. En este sentido, vamos a destacar algunos tópicos relacionados con las medidas de rendimiento.

## Throughput

Es una medida de cuántos bits pueden ser efectivamente enviados por la red. Aunque el throughput puede parecer semejante al ancho de banda en bits por segundo, no lo es. Una determinada red puede tener un máximo ancho de banda de 100 Mbps, mientras que la tasa de datos efectiva sea la mitad, es decir, 50 Mbps. Diferentes factores pueden influir en el throughput de la red incluyendo los mecanismos y procedimientos usados en las capas superiores del modelo OSI, los cuales pueden retardar el envío efectivo de los datos.

Para entender mejor esta medida, vamos a determinar el throughput de la conexión a Internet que tengamos disponible. Para ello vamos a utilizar alguna de las múltiples herramientas que están disponibles en la red y veremos como sus resultados pueden variar, de acuerdo a los métodos que se utilizan para hacer la medición y determinar el throughput.

### Actividades

1. Abre una ventana de tu navegador Web y dirígete a los siguientes sitios web que permiten probar las velocidades de tu conexión activa.
   * <https://www.nperf.com/es/>
   * <https://www.test-velocidad.com/>
   * [https://fast.com/es/#](https://fast.com/es/)
2. **Navega** por Internet utilizando tu buscador de preferencia y selecciona tres sitios más donde medir la velocidad de tu conexión activa a Internet.
3. **Elabora una tabla** donde relaciones las **velocidades de subida** (upload) y **bajada** (download) y latencia. La tabla debe contener una fila por cada sitio web utilizado y una columna para cada uno de los resultados (latencia y throughput (upload y download)) en Mbps.
4. **Elabora tus conclusiones** respecto a los resultados obtenidos.

## Latencia

Es el tiempo que toma un mensaje en llegar completamente a su destino y está constituido por el retardo de transmisión, el retardo de propagación, el retardo en cola y el tiempo de procesamiento. Recordemos que en una transmisión se envía un mensaje; el **tiempo de transmisión** es aquel medido desde que el primer bit del mensaje sale del emisor hasta que el último llega al receptor.

Esta medida de rendimiento la vamos a poder entender mejor usando el comando **ping.**

### Comando Ping

Para obtener estadísticas reales sobre latencia, se debe realizar esta actividad en una red activa. En ella vamos a medir y evaluar la latencia de red en el tiempo y durante diferentes momentos del día para capturar una muestra representativa de la actividad típica de la red. Esto se logrará mediante el análisis del **retardo del retorno** desde un computador remoto con el comando **ping**. El tiempo de retraso del retorno, medido en milisegundos, se resume calculando la latencia promedio (media) y el intervalo (máximo y mínimo) del tiempo de retraso.

### Actividades

Primero se examinará la latencia de red a varios sitios Web en distintas partes del mundo. Este proceso se puede utilizar en una red de producción empresarial para crear una línea de base de rendimiento.

1. **Verificar la conectividad**
   * Haga ping a los siguientes sitios Web de Registros Regionales de Internet (RIR) para verificar la conectividad:
     + ping www.arin.net
     + ping www.lacnic.net
     + ping www.afrinic.net
     + ping www.apnic.net
   * Nota: www.ripe.net no responde a solicitudes de ICMP, por lo que no puede utilizarse para esta práctica de laboratorio.  
     Imagen que contiene texto, captura de pantalla

     Descripción generada automáticamente
2. **Recopilar los datos de red**
   * El objetivo es recopilar una cantidad de datos significativa para calcular estadísticas sobre el resultado del comando **ping** mediante el envío de 25 solicitudes de eco a cada dirección del paso 1. Posteriormente procede a registrar los resultados para cada sitio Web en archivos de texto.
     + En el símbolo del sistema, tipea el comando **ping** para que muestre las opciones disponibles.  
       Imagen que contiene captura de pantalla, texto, negro, sentado

       Descripción generada automáticamente
     + Si utilizamos el comando ping con la opción de cuenta (-n count), se podrá enviar 25 solicitudes de eco al destino, como se muestra a continuación. Además, creará un archivo de texto con el nombre arin.txt en el directorio actual. Este archivo de texto contendrá los resultados de las solicitudes de eco. Para ello, ejecuta el siguiente comando:  
       **ping –n 25 www.arin.net > arin.txt**  
       **Nota:** La línea de comandos permanecerá en blanco hasta que el comando haya finalizado, porque en este ejemplo el resultado se redirigió a un archivo de texto: **arin.txt**. El símbolo > se utiliza para redirigir el resultado que se muestra por pantalla hacia un archivo e incluso sobrescribir en él, si ya existe. Si deseas adicionar más resultados al archivo, reemplaza este símbolo > por este otro >>, en el comando.
     + Repite el comando **ping** para los otros sitios Web.
       - **ping –n 25 www.afrinic.net > afrinic.txt**
       - **ping –n 25 www.apnic.net > apnic.txt**
       - **ping –n 25 www.lacnic.net > lacnic.txt**
3. **Verificar la recopilación de datos**
   * Para ver los resultados de cada uno de los archivos creados, tipea el comando notepad en el símbolo del sistema y seguidamente indica el nombre del archivo.  
     **notepad arin.txt**
   * Para verificar que los archivos se crearon, utiliza el comando dir para listar los archivos en el directorio. También se puede utilizar el carácter comodín \* y especificar la extensión txt, para filtrar sólo los archivos de texto.  
     **dir \*.txt**
   * Registra tus resultados en la siguiente tabla:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Mínimo** | **Máximo** | **Promedio** |
| [www.afrinic.net](http://www.afrinic.net/) |  |  |  |
| [www.apnic.net](http://www.apnic.net/) |  |  |  |
| [www.arin.net](http://www.arin.net/) |  |  |  |
| [www.lacnic.net](http://www.lacnic.net/) |  |  |  |

* + Compara los resultados de retardo. **¿De qué manera afecta el retardo la ubicación geográfica?.**

El comando ping es de gran utilidad ya que puede proporcionar información importante sobre la latencia de red. Un análisis detallado de retardo, a través de días consecutivos, durante distintos momentos del día puede alertarte sobre cambios en el rendimiento de la red. Por ejemplo, los dispositivos de red pueden saturarse durante determinados momentos del día y el retardo de red tendrá un pico. En este caso, las transferencias de datos de rutina deben programarse para las horas no pico, cuando el retardo es menor.

¡Felicitaciones! Has logrado culminar el reto utilizando diferentes herramientas que te ayudarán a  medir la latencia de la red.   ¡Continúa avanzando!

3.8. Ejercicio

4. Lección 3: Control de Acceso al Medio

**Aprende haciendo**

**Chequeando la Tarjeta de Interfaz de Red (Network Interface Card, NIC)**

¡Felicitaciones por llegar hasta aquí! Eso significa que ya revisaste el material correspondiente a las redes Ethernet y los dispositivos de interconexión. Vas avanzando muy bien. Ahora  podrás consolidar y aplicar los conocimientos adquiridos.

A continuación nuestro primer acercamiento a los dispositivos físicos con los que nuestro computador se conecta a la red. La conexión puede hacerse a través de diferentes medios cableados e inalámbricos.

Para acceder al medio de transmisión, nuestro computador utiliza una o más interfaces de red. Por ejemplo, una para acceder a la red cableada usando cable UTP RJ-45 y otra para acceder  vía inalámbrica, a la red WiFi. A continuación veamos cómo sabemos que tarjetas tenemos instaladas en nuestro computador y sus características.

**1. Abre el administrador de dispositivos.**

Para ello puedes hacer clic con el botón derecho en el ícono de Windows en la esquina inferior izquierda de la pantalla.

**2. Expande la pestaña de “Adaptadores de Red”**

Aquí puedes ver las diferentes NICs (físicas y algunas virtuales) que dispone el computador. En este ejemplo tenemos que la conexión a nuestra red cableada es mediante el adaptador llamado “Intel(R) PRO/1000 MT Desktop Adapter. En tu caso, seguramente será diferente, pero siempre tendrás al menos un adaptador para conectarte a la red.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

**3. Explora las propiedades del adaptador para red cableada.**

* Para ello coloca el cursor sobre el adaptador, haz clic en el botón derecho y selecciona del menú contextual que aparece, la opción “Propiedades”.
* Selecciona las propiedades avanzadas y encontrarás una serie de Propiedades y su valor actual.
* Selecciona “Link Speed & Duplex” y en el valor abre la lista desplegable de Valor, para que puedas apreciar las diferentes velocidades a las que puede transmitir tu tarjeta de red.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

Elabora una lista de las diferentes velocidades y modos (Half Duplex o Full Duplex) que están disponibles en la tarjeta de red cableada en tu computador.

**Cómo encontrar la dirección MAC e IP en tu computador**

Ahora que hemos visto las diferentes NICs en tu computador, vamos a explorar un poco más acerca de sus características, averiguando su dirección física (MAC address) y la dirección IP.

**1. Abre una ventana de comandos.**

Para ello puedes hacer clic con el botón derecho en el ícono de Windows, en la esquina inferior izquierda de la pantalla, y seleccionas “Ejecutar”

**2. Ejecuta una ventana de comandos.**

En la ventana Ejecutar, coloca “cmd” para activar la interfaz de línea de comandos (CLI).

**3. Accede a la configuración de todas las interfaces de red.**

En la ventana de comandos, coloca ipconfig/all y se desplegará toda la información relativa a tus interfaces de red.

Imagen que contiene captura de pantalla, texto

Descripción generada automáticamente

Elabora una lista con las direcciones MAC e IP presentes en los diferentes adaptadores de red en tu computador.

**Dispositivos de interconexión en nuestra red.**

Para finalizar vamos a explorar un poco, las funciones del dispositivo con el que te conectas normalmente a Internet, por ejemplo, en tu casa. El Router inalámbrico es el dispositivo más usual, hoy en día, con el cual nos conectamos a Internet. El mismo es un equipo que nos permite tanto conexiones inalámbricas como conexiones cableadas o alámbricas. Es importante señalar que aquí estamos hablando de dos tipos de redes, la inalámbrica (o Wifi) y la alámbrica (Ethernet). Cada una de estas redes utilizan diferentes medios y estándares para establecer la conexión. Así, cuando tenemos dos dispositivos conectados a un mismo medio (por ejemplo WiFi) el router ejecuta funciones de enrutador (valga la redundancia). Sin embargo, cuando tenemos dos dispositivos que se conectan entre sí, pero que uno está conectado al router con un cable y el otro está conectado vía WiFi (están en redes diferentes), el dispositivo de interconexión ejecuta funciones de puente (bridge), ya que debe hacer el proceso de traducción asociado a los diferentes protocolos de comunicación que emplean ambas tecnologías, por ejemplo, se debe tomar en cuenta que los tamaños y estructura de las tramas de la capa de MAC en Ethernet y Wi-Fi difieren.

Si aplicamos esto a nuestro computador, podemos estar conectados a las dos redes usando diferentes interfaces, y si establecemos alguna comunicación entre ellas (por ejemplo haciendo ping a sus direcciones), el router tiene que hacer las funciones de puente para que se logre la comunicación.

**1. Conecta tu computador a dos redes**

Para ello debes conectar un cable de red UTP a la interfaz Ethernet de tu computador, vía el conector RJ45. Al mismo tiempo, mantén la conexión Wifi. Cuando hagas eso, te deben aparecer dos adaptadores con características de conexión diferentes.

**2. Abre  “Conexiones de Red”**

Haciendo clic con el botón derecho en el ícono de Windows.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

**3. Explora las propiedades del adaptador para cada red a la que estás conectado.**

Para ello coloca el cursor sobre la red Wifi y la red Ethernet que aparecen en el panel izquierdo. Cada uno de ellos muestran la propiedades de esa interfaz (adaptador) con esa red, tales como su dirección IP (version IPv4 e IPv6), su dirección MAC, entre otros.

**Ethernet:**

Imagen que contiene captura de pantalla

Descripción generada automáticamente

**Wifi:**

**Imagen que contiene captura de pantalla

Descripción generada automáticamente**

Aplica lo que acabamos de estudiar y explora las propiedades de las conexiones Wifi y de Ethernet que has establecido ahora en tu computador.

# Cápsula de conocimiento

# VLANs

¡Enhorabuena! Te felicitamos por seguir progresando y ampliando los conocimientos con nuevos conceptos y herramientas de gran utilidad. Ahora vamos a considerar los aspectos relacionados con las Redes Virtuales o VLANs.

### **Definición de VLAN**

Una VLAN es un grupo de dispositivos en una o más redes de área local (LAN) que están configurados para comunicarse como si estuvieran unidos al mismo cable, cuando en realidad se encuentran en diversos segmentos de la LAN. Debido a que las VLANs se basan en conexiones lógicas, en lugar de conexiones físicas, son extremadamente flexibles.

Las VLANs definen dominios de difusión en una red de capa 2. Un **dominio de difusión** es el conjunto de todos los dispositivos que recibirán tramas de difusión **(broadcast frames)** procedentes de cualquier dispositivo dentro del conjunto. Dominios de difusión son, por lo general, delimitados por ruteadores, ya que ellos no reenvían tramas de difusión. Los conmutadores de capa 2 crean dominios de difusión basados en la configuración del switch. Los switches a su vez son puentes multipuertos que permiten crear múltiples dominios de difusión. Cada dominio de difusión es como un puente virtual (virtual bridges) distinto dentro de un switch.

Se pueden definir uno o varios puentes virtuales dentro de un switch. El tráfico no puede pasar directamente a otra VLAN (entre dominios de difusión) en el switch o entre dos switches. Para interconectar dos VLAN diferentes, se deben utilizar ruteadores o switches de capa 3. La figura muestra un ejemplo de tres VLANs que crean tres redes definidas lógicamente.

Imagen que contiene captura de pantalla

Descripción generada automáticamente

Figura 1. Tipos de VLANs

Dependiendo de la fuente consultada e incluso del fabricante, se pueden distinguir hasta seis tipos de redes virtuales.  Los enfoques más utilizados para asignar la pertenencia a una VLAN son los siguientes:

* **VLAN basadas en puertos:** (también se denominan **VLAN de nivel 1**): Las asignaciones de VLAN estáticas se crean asignando puertos a una VLAN. Cuando un dispositivo entra en la red, el dispositivo asume automáticamente la VLAN del puerto. Si el usuario cambia los puertos y necesita acceso a la misma VLAN, el administrador de red debe realizar manualmente una asignación de puerto a VLAN para la nueva conexión. En este tipo se especifica qué puertos del switch forman parte de la VLAN y sólo los que puedan conectarse a dichos puertos formarán parte de la VLAN. El traslado físico de un usuario no es admitido, ya que tendría que reconfigurarse el sistema.
* **VLAN basadas en direcciones MAC:** (también se denominan **VLAN de nivel 2**): Los hosts se asignan a la VLAN en función de su dirección MAC, lo que permite al usuario trasladarse a otra ubicación física, sin que se requiera una reconfiguración. Con un servidor de directivas de administración de VLAN (VMPS, VLAN Management Policy Server), el administrador puede asignar dinámicamente puertos de conmutador a una VLAN, basándose en información relacionada con la dirección MAC origen del dispositivo conectado al puerto, el nombre de usuario utilizado para iniciar sesión en ese dispositivo o por el contenido del campo, tipo de protocolo, de la trama MAC. Cuando un dispositivo entra en la red, el conmutador consulta una base de datos para la pertenencia a una VLAN, del puerto al que está conectado el dispositivo. Para la configuración automática de información de VLAN se utiliza el método MVRP (Multiple VLAN Registration Protocol), que reemplazó al método GVRP (Generic Attribute Registration Protocol).
* **VLAN basada en direcciones de subred:**(también se denominan **VLAN de nivel 3**): Se vinculan a la VLAN, paquetes y no estaciones de trabajo. En este tipo de VLAN son los paquetes quienes pertenecen a la VLAN, no las estaciones de trabajo, una misma estación puede estar en varias VLAN de este tipo.
* **VLAN de nivel superior:** La pertenencia a una VLAN puede basarse en una combinación de factores tales como: puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo, aplicación, entre otros.

### **Ventajas de uso de las VLANs**

Las VLAN ofrecen diversas ventajas, entre ellas tenemos: mayor flexibilidad en la administración y en los cambios de la red, aumento de la seguridad y disminución en la transmisión de tráfico en la red. Las redes VLAN permiten a los administradores de red agrupar hosts, incluso si los hosts no están en el mismo conmutador de red. Esto puede simplificar en gran medida el diseño y la implementación de la red, ya que la pertenencia a la VLAN puede configurarse a través de software. Si no disponemos de VLANs, agrupar los hosts de acuerdo a sus necesidades de recursos, requiere el trabajo de reubicar nodos o recablear enlaces de datos.

Las VLANs también presentan ventajas al permitir que las redes y los dispositivos se mantengan separados sin interactuar, aunque compartan el mismo cableado físico, por razones de simplicidad, seguridad, administración del tráfico o economía. Una VLAN puede utilizarse para separar el tráfico entre tipos de usuario o entre tipos de tráfico, por ejemplo el tráfico correspondiente a los usuarios o a los administradores de red, o el tráfico de alta y baja prioridad, de tal modo que no puedan afectar directamente al resto del funcionamiento de la red.

Las VLAN trabajan a través de etiquetas dentro de los paquetes de red, recreando la apariencia y funcionalidad del tráfico de red que está físicamente en una sola red, pero actuando como si estuviera dividida en redes separadas. De esta forma, las VLAN pueden mantener las redes separadas a pesar de estar conectadas a la misma red física, sin necesidad de que se desplieguen múltiples conjuntos de dispositivos de cableado y de red. En este contexto, el término “virtual” se refiere a un objeto físico recreado y alterado por una lógica adicional.

Como hemos podido apreciar a lo largo del contenido de este recurso instruccional, el manejo de redes virtuales o VLANs es muy importante en las redes modernas, ya que contribuyen a potenciar las habilidades necesarias para la administración e implementación de esquemas de seguridad de las mismas.

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