# Repaso Teoría

1. Dentro del contexto de este módulo define los siguientes términos:
   1. Dispositivos de usuarios

Son los dispositivos o sistemas finales que están conectados a una red de comunicación y que se utilizan para transmitir, emitir y recibir datos.

* 1. Red de computadoras

Es el conjunto de dispositivos de usuario que intercambian datos a través de una red de comunicación, cooperando con la misma en la comunicación.

* 1. Entidad

Es cualquier programa de un dispositivo de usuario que puede intercambiar información con otra entidad.

* 1. Protocolo

Es el conjunto de reglas que gobierna el intercambio de datos entre dos entidades.

* 1. Sintaxis y semántica de un paquete de datos

La sintaxis refiere el formato de datos dentro del paquete de datos. Por ejemplo, la cantidad de campos, su ubicación y tamaño.

La semántica se refiere al significado de la información dentro del paquete. Por ejemplo, comprende el manejo de la información de control para el control de la comunicación y manejo de errores.

* 1. Arquitectura de protocolos

Es una estructura que divide la comunicación en capas donde cada una se ocupa de una tarea específica. Cada capa implementa un protocolo específico para llevar a cabo su tarea. El conjunto de los protocolos se conoce como arquitectura de protocolos y permite completar el proceso de comunicación.

* 1. SAP

Sus siglas significan punto de acceso al servicio. Es la dirección única de una aplicación en un dispositivo de usuario. En el caso del protocolo TCP/IP se conoce como puerto.

* 1. PDU

Las siglas significan Unidad de Datos del Protocolo. Son los datos generados por una capa de protocolo, que incluye los datos que se quieren transmitir más la información de control.

* 1. Norma

Es un conjunto de reglas o directrices establecidas por organizaciones de estandarización (como IEEE, ISO, IETF, ITU) para garantizar la compatibilidad e interoperabilidad de sistemas y dispositivos en redes.

1. Sobre el modelo de 3 capas responda
   1. ¿Cuáles son las funciones de cada una de las capas?

El modelo de tres capas está compuesto por:

* Capa de Acceso a la Red: se encarga del intercambio de datos entre el dispositivo de usuario y la red a la que está conectada. Es el encargado de encaminar y entregar los datos mediante la dirección del computador de destino provista. Además, es el encargado de proveer servicios de red como la gestión de prioridades.
* Capa de Transporte: comprende las tareas para asegurar que los datos de una aplicación lleguen al destino de forma segura, sin errores y en orden.
* Capa de Aplicación: especifica la lógica necesaria para cada aplicación. Indica cómo procesar y preparar los datos, y las señales de control.
  1. ¿Cómo está compuesto el Header de Transporte?

El Header de Transporte está compuesto, en primer lugar, por SAP Destino, que le permite identificar la aplicación a la que están destinados los datos. También, contiene un número de secuencia, que numera las fracciones de datos generadas por la capa de transporte para que puedan ser ordenadas en el destino. Por último, contiene un código de detección de error. Se genera un código en función del contenido del resto del PDU. De esta manera, el receptor hará el mismo cálculo y lo compara con el original para detectar un error en el paquete de datos.

* 1. ¿Cómo está compuesto el Header de acceso a la red?

El header de acceso a la red está compuesto por la dirección del computador destino, la dirección del emisor y solicitud de recursos, que permite solicitar recursos cómo gestión de prioridades o fijar velocidades de transmisión.

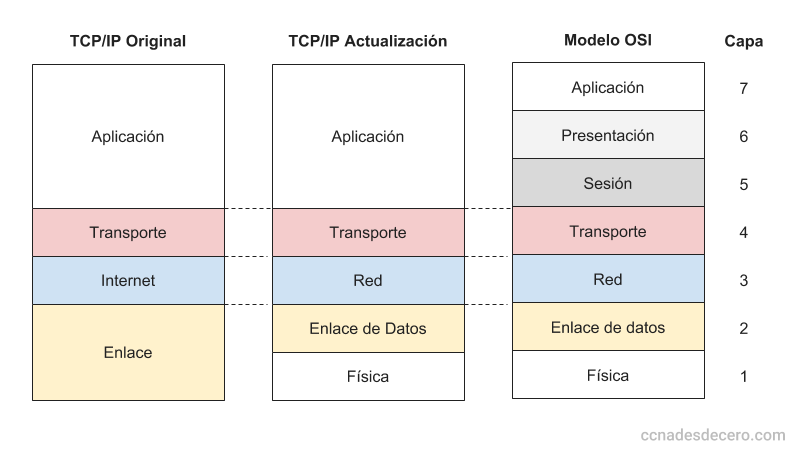
1. Sobre el modelo de referencia OSI responda:
   1. ¿Cuál es el objetivo del modelo de referencia?

Surgió por la necesidad de intercambiar datos entre sistemas heterogéneos en los cuales software, hardware y el formato de los datos tiene características distintas. Con este modelo de referencia se definió un modelo de interfaz común para la comunicación de sistemas heterogéneos. De esta manera, cualquier sistema que siga las normas OSI puede comunicarse con otros sistemas que las implementan.

* 1. ¿Cuántas capas lo componen y cuales son sus principales funciones?

El modelo de referencia OSI está compuesto por 7 capas:

* Capa física: define la interfaz física entre los dispositivos y cómo debe realizarse la transmisión de señales a través del medio de transmisión. Se deben realizar una serie de especificaciones:
* Mecánicas: referidas a los elementos que intervienen en la conexión física de la interfaz. Por ejemplo: especificación de los conectores que vinculan circuitos electrónicos o especificaciones del número, tamaño y distribuciones de los pines del conductor.
* Eléctricas: referidas a las señales que generan los circuitos electrónicos para representar los bits como velocidad de transmisión, niveles de corriente o tensión, etc.
* Funcionales: referidas a las funciones de cada circuito en la interfaz física y el modo de transmisión. Ejemplo: en ambos sentidos, half dúplex o full dúplex.
* De procedimientos: secuencia de eventos que deben llevarse a cabo para la transmisión de señales.
* Capa de enlace de datos: se encarga de lograr que la comunicación mediante un enlace físico se produzca sin error. Implica un conjunto de tareas coordinadas entre dispositivos que comprenden el acceso al medio de transmisión y la iniciación, mantenimiento y terminación del intercambio de datos. Estas tareas son:
* Sincronización de trama: los datos enviados se fraccionan en tramas. Se agregan bits especiales para reconocer el inicio y fin de cada una.
* Control de flujo: la estación emisora no debe enviar los datos más rápido que la capacidad de la estación receptora de almacenarlos.
* Control de error: corrige bits erróneos en cada trama. Se generan en el transmisor bits especiales mediante un código de control que se agregan al final de la trama para que el receptor pueda detectar y corregir errores.
* Capa de red: especifica cómo debe realizarse la transferencia de datos entre dos sistemas finales a través de una red. Debe realizar dos tareas básicas:
* El dispositivo emisor establece diálogo con la red para especificarle la dirección del dispositivo destino y la solicitud de servicios de red.
* La red debe realizar lo necesario para que los paquetes de datos atraviesen la red evitando en lo posible congestiones de tráfico en enlaces y dispositivos internos de la red. Esto implica llevar a cabo la función de ruteo y control de tráfico.
* Capa de Transporte: se encarga de que los datos generados en la aplicación de un computador lleguen a otro. Provee una comunicación extremo a extremo entre dos entidades finales. Se involucra en la solicitud de servicios de red. Se encarga de la segmentación de datos, su secuenciamiento, control de flujo y define el modo de envío de datos, su tamaño, la velocidad de transferencia de paquetes, la cantidad de conexiones lógicas necesarias, etc.
* Capa de Sesión: se encarga de administrar, establecer, mantener y finalizar las sesiones de comunicación entre aplicaciones en dispositivos diferentes. Funciones Principales de la Capa de Sesión
* Establecimiento de sesión: inicia la comunicación entre dos dispositivos o aplicaciones. Asegura que ambas partes estén listas para intercambiar datos.
* Mantenimiento de sesión: gestiona el flujo de datos durante la sesión. Detecta interrupciones y permite la recuperación en caso de fallos. Implementa puntos de sincronización para evitar la pérdida de información.
* Finalización de sesión: termina la comunicación de manera ordenada para evitar pérdida de datos. Libera los recursos utilizados en la comunicación.
* Capa de presentación: se ocupa de los aspectos de sintaxis y semántica de los datos a transmitir. Funciones:
* Codificación: maneja la representación estándar de lo datos y la convierte a la propia de cada computador.
* Seguridad: indica el encriptado de mensajes dotar de privacidad y autentificación la comunicación.
* Compresión: comprime los datos para disminuir la cantidad de bits a transmitir.
* Capa de aplicación: se encarga de la interfaz aplicación-usuario y la interfaz aplicación-servicios de red. Por ejemplo, los servicios de transferencia de archivos (FTP), el correo, servicios de páginas web, etc.
  1. Compare TCP/IP con el modelo OSI

El modelo OSI es un modelo de referencia teórico diseñado para estandarizar la comunicación en redes. El modelo TCP/IP es una implementación real del modelo OSI, a través de 5 capas.

Al igual que en el modelo OSI, el modelo TCP/IP define una capa física que define la interfaz física entre un dispositivo de transmisión de datos y un medio de transmisión de red. Tiene las mismas características que la capa física del modelo OSI (inciso b) y, además, especifica las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos y otros aspectos relacionados.

Luego, se define la capa de acceso a la red o enlace de datos. Es la responsable del intercambio de datos entre el sistema final y la red a la que está conectada. Se preocupa por el acceso y el enrutamiento de datos a través de una red a partir de la dirección de destino proporcionada por el emisor. Además, maneja los requerimientos de servicios de red. Se utiliza algún tipo de protocolo como Ethernet o Wifi para conectar la computadora a una subred. El software que implementa estas funciones depende del tipo de red.

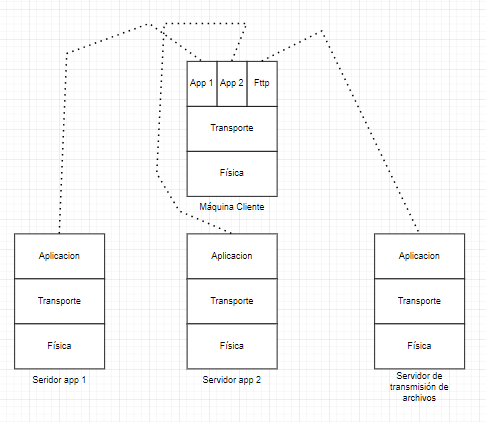
La siguiente capa es la capa de Internet o de red, que al igual que la capa de red del modelo OSI. Se encarga de proporcionar el enrutamiento a través de dispositivos conectados por múltiples redes. Se encarga de las funciones de ruteo y control del tráfico. Estas funciones se realizan utilizando el protocolo IP, aplicado en sistemas finales y enrutadores.

Luego, se encuentra la capa de transporte (o capa host a host), que implementa las funciones de su capa homónima en el modelo OSI. Transporta los datos de una aplicación a otra en forma confiable y los entrega en el mismo orden en que fueron enviados. El protocolo más utilizado es TCP aunque también se utiliza el protocolo UDP cuando no se necesita confiabilidad. Los módulos de estos protocolos se instalan en los sistemas finales que intercambian datos. Se conoce como capa origen-destino.

Por último, la capa de aplicación del modelo TCP/IP implementa las capas de sesión, presentación y aplicación del modelo OSI. Contiene la lógica necesaria para soportar las aplicaciones de usuario. Permite generar y preparar los datos para que sean enviados (en el emisor) y recibir los datos de otra aplicación para poder presentárselos al usuario (en el receptor). Cada aplicación debe implementar una interfaz que le permite comunicarse con la capa de transporte.

# Práctica

1. Ud usa en una pc un navegador web con 2 pestañas abiertas una para revisar el webmail de su empresa y la segunda para leer un diario. Al mismo tiempo está subiendo un sitio a un hosting vía ftp.
   1. Usando la arquitectura de 3 capas de la teoría grafique las conexiones.



* 1. ¿Cuántas entidades participan en este escenario?

Participan 6 entidades: las dos pestañas del navegador, el cliente ftp, el servidor de webmail, el servidor de sitio de noticias y el servidor de hosting.

* 1. ¿Cómo identifica la pc a qué aplicación debe entregar los paquetes que llegan?

La identifica a partir del número de puerto al que está asociado la aplicación, la cual es su dirección única en la computadora. Este puerto es identificado por la capa de transporte en la cabecera de su PDU.

* 1. ¿Como diferencia a que pestaña del navegador enviar la información que llega?

Cada pestaña tiene una conexión TCP única con el servidor del sitio web que está visitando.

La PC identifica los paquetes según la combinación de dirección IP de origen, puerto de origen, dirección IP de destino y puerto de destino.

* 1. ¿Que información de control se utiliza? ¿En qué capa se genera y en cual se utiliza?

La capa de aplicación comparte la SAP de destino y la dirección de la computadora de destino. En la capa de transporte, se dividen los datos enviados en paquetes y se genera un número de secuencia y código de error para cada paquete. Se agregan como cabecera de transporte a cada paquete, éstos últimos datos junto con la SAP de destino formando la PDU de transporte. Ésta PDU de transporte se pasa a la capa de acceso a la red con la dirección del computador de destino. Aquí se agrega la cabecera de red la dirección del dispositivo de destino y el emisor. También, se agrega como información de control la solicitud de recursos de red.

* 1. ¿Cuál es el contenido del campo de datos de la PDU de acceso a la red?

El campo de datos del PDU de acceso a la red contiene el PDU de la capa de transporte.

1. Identifique a qué capa del Modelo OSI le corresponde cada una de las siguientes funciones:
   1. Detección de n bits erróneos en un paquete de datos al ser transmitido entre un nodo y otro de una red. CAPA DE ENLACE DE DATOS
   2. Especificación de las medidas de los conectores para comunicación serie RS232-C. CAPA FÍSICA
   3. Detección de paquetes de datos perdidos. CAPA DE TRANSPORTE
   4. Determinar la ruta que debe seguir un paquete para llegar a destino. CAPA DE RED
   5. Detección de errores en el secuenciado de paquetes. CAPA DE TRANSPORTE
   6. Definir la codificación del mensaje. CAPA DE PRESENTACIÓN
   7. Traducción de la codificación de datos de ASCII a EBCDIC. CAPA DE PRESENTACIÓN
   8. Sincronización entre nodos unidos por un enlace. CAPA DE ENLACE DE DATOS
   9. Conmutar, enrutar y controlar la congestión de paquetes de datos en la red. CAPA DE RED
   10. Encriptado de los datos. CAPA DE PRESENTACION
   11. Agrupar el flujo de bits en tramas.

CAPA DE ENLACE DE DATOS

1. Cuando el módulo del protocolo TCP recibe los datos de la aplicación, puede decidir dos cosas: 1º) Fraccionar el bloque de datos recibido conformando varios segmentos TCP (segmentación) 2º) Agrupar varios bloques de datos recibidos en un único segmento TCP (agrupamiento)

Responda y explique:

* 1. ¿En la segmentación es necesario que cada segmento TCP contenga una copia de la cabecera de la PDU de aplicación?

No es necesario que cada segmento TCP contenga una copia de la cabecera de la PDU de aplicación, ya que estaría enviando datos redundantes: Hay ciertos datos, que se usan en la capa de aplicación, pero ya no se utilizarán en ninguna otra capa. Por lo tanto, si mi capa de transporte tiene una copia de la capa de aplicación, estaría mandando información redundante. La cabecera va en el primer paquete.

* 1. ¿En el agrupamiento es necesario que cada una de las PDU de aplicación conserve su cabecera o se pueden agrupar los datos en una única PDU de aplicación con una única cabecera?

Cada capa, debe tener potestad sobre sobre su cabecera únicamente, por lo tanto, no puede agregar ni quitar cabeceras, por lo cual podríamos decir, que en el agrupamiento, no corresponde agrupar los datos en una única PDU de aplicación con una única cabecera.

1. El siguiente ejercicio puede realizarlo en el simulador GNS3 o directamente sobre su pc si cuenta con un servidor DHCP en su red.

Tomando como base la red básica generada en el práctico anterior siga los siguientes pasos:

* Agregue un nodo de tipo nat y conéctelo al switch
* Encienda una de las vpc y conéctese a su consola.
* Comience a capturar el tráfico sobre la placa de esta vpc
* En la consola de la vpc ejecute el comando **ip dhcp -d**

Opción: si no puede realizar la captura puede descargar una de https://wiki.wireshark.org/uploads/ moin\_import /attachments/SampleCaptures/dhcp.pcap

* 1. En wireshark filtre un paquete dhcp e indique cómo están compuestas las distintas cabeceras

La cabecera FRAME:

* La cantidad de bytes que tiene el paquete entregado
* Los protocolos usados: en este caso eth, ethertype, ip, udp, dhcp.
* Hora de llegada del paquete
* La identificación de la interfaz de red en la que se capturó el paquete

La cabecera Ethernet:

* Dirección MAC computador destino (en este caso el switch)
* Dirección MAC computador origen (en este caso la PC1)
* Tipo de protocolo (en este caso IPV4)

La cabecera IP:

* Version: Tipo de protocolo usado en este caso dice 4, por ser IPV4
* Longitud de la cabecera
* Differentiated Services Field: Servicios utilizados para guiar el transporte del paquete en la red
* Flags:Sirven para activar flags. Este campo consta de 3 números:

 Un 0 inicial (siempre va en 0)

 El segundo bit, irá en 1 si el paquete no debe ser fragmentado en transporte, 0 si si

 El tercer bit, será 1 si hay más bits detrás de este paquete, 0 si no

* Ip origen
* Ip destino

La cabecera de transporte:

* Puerto de origen (o SAP origen, para que luego se pueda mandar a este SAP la respuesta)
* Puerto de destino (o SAP destino).
* Stream Index: Indica el valor que identifica a este flujo.
* stream packet number: Indica el número de secuencia en el paquete de datos

La cabecera de aplicación:

* Tipo de conexión física.
* Ip computador origen
* Ip servidor DHCP
* Tipo de mensaje (Request)
* Dirección Mac computador origen, entre otros

* 1. ¿En qué cabecera encuentra la dirección MAC cuál es su sintaxis?

La dirección MAC, se encuentra en la cabecera de enlace de datos. Su sintaxis es en Hexadecimal, formada por 12 digitos separados. El conjunto de 2 dígitos, representa un byte, por lo tanto, el tamaño que ocupa es de 6 bytes. El formato es el siguiente:

o Los primeros 3 bytes, representan al proveedor o fabricante del hardware. Es el identificador único de la organización que lo fabrica

o Los últimos 3 bytes, son un identificador único de la interfaz de red. Ejemplo, puertos de red o tarjetas de red que se hayan integrados a la computadora y le permiten conectarse a internet.

* 1. ¿En qué cabecera se observa si el paquete es un fragmento de un conjunto de datos de aplicación aún mayor?

En la cabecera de transporte, UDP en este caso. El valor stream index nos indica el flujo al que perteneces y el valor stream packet number nos indica su número de secuencia en el flujo que indica index.

Nota: comandos para renovar ip en otros sistemas operativos:

Linux:

sudo dhclient -r sudo dhclient Windows:

ipconfig /release ipconfig /renew

1. Utilice un escáner de puertos para identificar los puertos abiertos en una pc. ¿Los puertos “ABIERTOS” en una pc dependen solo de cómo esté configurado el firewall del equipo o de algo más? Investigue qué herramientas podría utilizar en windows y en linux.

**Herramientas para escanear puertos:**

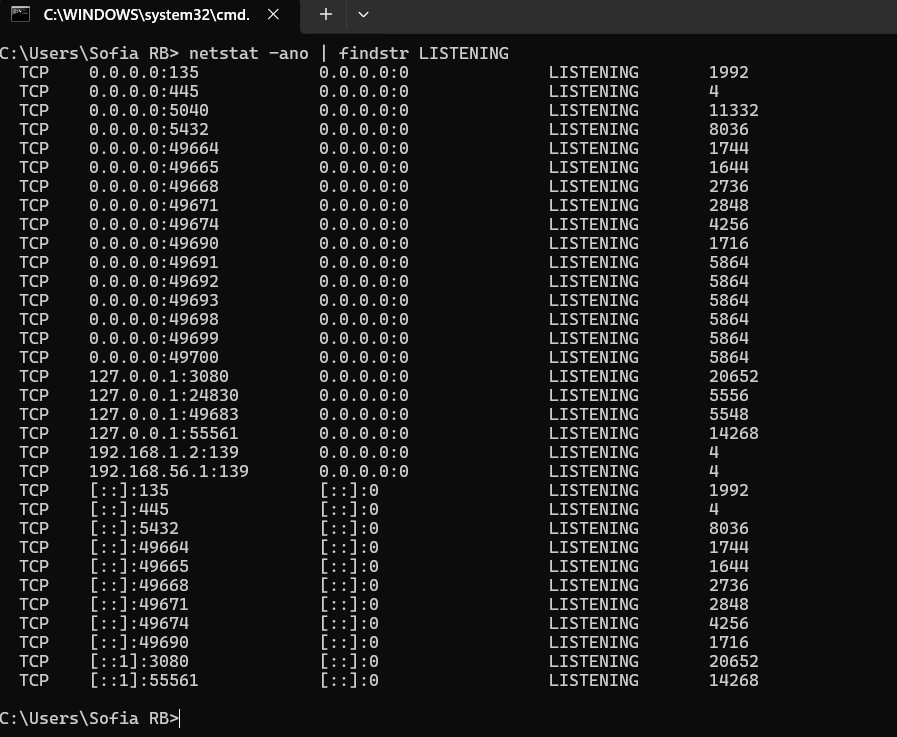
**Windows**

* **Nmap: Un escáner de puertos muy popular y potente. Puedes descargarlo desde nmap.org.**
* **Netstat (comando integrado en Windows): netstat -ano muestra las conexiones activas y los puertos en uso. El** **comando netstat -ano | findstr "LISTENING" permite ver puertos abiertos.**
* **PowerShell (Get-NetTCPConnection): Permite ver puertos abiertos con Get-NetTCPConnection | Where-Object { $\_.State -eq "Listen" }.**
* **Angry IP Scanner: Herramienta gráfica fácil de usar (angryip.org).**

Linux

* Nmap: sudo nmap -p- IP\_DEL\_OBJETIVO escanea todos los puertos de un equipo.
* Netcat: nc -zv IP\_DEL\_OBJETIVO PUERTO verifica si un puerto está abierto.
* ss (reemplazo de netstat): ss -tuln muestra puertos en escucha.
* lsof: sudo lsof -i -P -n lista conexiones y puertos abiertos.

Los puertos abiertos en mi pc:



El firewall, es un dispositivo de software que actúa como una barrera entre una red externa y una red local. Es el que controla el tráfico que entra y sale de la red local, según como esté configurado.

Los puertos abiertos en una PC no dependen únicamente del firewall, sino también de:

* Servicios y aplicaciones en ejecución: una aplicación lo debe estar utilizando.
* Configuración del sistema operativo: Algunas configuraciones del sistema pueden habilitar o deshabilitar puertos específicos.
* Routers y NAT: Si estás detrás de un router, algunos puertos pueden estar bloqueados a nivel de red.

1. ¿Con qué comando podría Identificar las conexiones abiertas en su equipo en este momento y que aplicación las inicio? Indique la sintaxis para windows y linux. ¿Qué significa que un puerto está abierto?

Un puerto está abierto, cuando un programa o servicio está en escucha de este puerto, es decir, espera recibir datos desde otro dispositivo en la red a través de este puerto.

Se puede utilizar el comando netstat en Windows (y en Linux si está instalado) con los siguientes parámetros:

-a Muestra todas las conexiones y puertos de escucha.

-n Muestra direcciones y números de puerto en formato numérico.

-o Muestra el identificador de proceso propietario asociado a cada conexión.

-p Muestra el programa o proceso que está utilizando la conexión.

-t Muestra conexiones TCP.

-u Muestra conexiones UDP.

En Linux, se usa el comando ss como reemplazo de netstat. Los argumentos -tuln y -tun permiten ver los puertos abiertos y los puertos activos respectivamente.