

ITEDES

Educación Digital

Módulo:

Fundamentos de Ingeniería de Software

Segmento:

Elementos Informáticos

Tema:

Introducción a las Comunicaciones

Prof. Germán C. Basisty
german.basisty@itedes.com

Índice de Contenidos

Índice de Contenidos	2
Redes de Datos	3
Qué son las redes de datos	3
Contextualización histórica	3
Modelo OSI	4
Modelo TCP/IP	6
Clasificación de redes según su extensión	7
Clasificación de redes según su topología	8
TCP/IP	10
Definición	10
Dirección IP	10
Máscara de Subred	10
Clases de red TCP/IP	11
Enrutamiento	11
Ejercitación	12

Redes de Datos

Qué son las redes de datos

Una **red de datos**, también llamada **red de telecomunicaciones**, es un conjunto de equipos de informática y software que se encuentran conectados entre ellos de la mano de dispositivos físicos que envían y reciben impulsos eléctricos u ondas electromagnéticas, o en todo caso cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos informáticos y ofrecer servicios para el beneficio del usuario.

Contextualización histórica

La historia se puede remontar a:

1957: Cuando los Estados Unidos crearon la Advanced Research Projects Agency (**ARPA**), como organismo afiliado al departamento de defensa para impulsar el desarrollo tecnológico. Posteriormente a la creación de **ARPA**, **Leonard Kleinrock**, un investigador del **MIT**, escribía el primer libro sobre tecnologías basadas en la transmisión por un mismo cable de más de una comunicación.

1969: es un año clave para las redes de computadoras, ya que se construye la primera red de computadoras de la historia. Denominada **ARPANET**, estaba compuesta por cuatro nodos situados en UCLA (Universidad de California en los Angeles), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, Los Angeles) y la Universidad de UTA. La primera comunicación entre dos computadoras se produce entre UCLA y Stanford el 20 de octubre de 1969. El autor de este envío fue Charles Kline (UCLA). En ese mismo año, La Universidad de Michigan crearía una red basada en conmutación de paquetes, con un protocolo llamado X.25, la misión de esta red era la de servir de guía de comunicación a los profesores y alumnos de dicha universidad. En ese mismo año se empiezan a editar los primeros **RFC** (petición de comentarios). Los **RFC** son los documentos que normalizan el funcionamiento de las redes de computadoras basadas en TCP/IP y sus protocolos asociados.

1970: **ARPANET** comienza a utilizar para sus comunicaciones un protocolo Host-to-host. Este protocolo se denominaba **NCP** y es el predecesor del actual **TCP/IP** que se utiliza en toda la **Internet**. En ese mismo año, *Norman Abramson* desarrolla la **ALOHANET** que era la primera red de conmutación de paquetes vía radio y se uniría a la **ARPANET** en 1972.

1971: **ARPANET** estaba compuesta por 15 nodos y 23 máquinas que se unían mediante conmutación de paquetes. En ese mismo año *Ray Tomlinson* realiza un programa de e-mail para distribuir mensajes a usuarios concretos a través de **ARPANET**.

1972: Se elige el @ como tecla de puntuación para la separación del nombre del usuario y de la máquina donde estaba dicho usuario. Se realiza la primera demostración pública de la **ARPANET** con 40 computadoras. En esa misma demostración se realiza el primer chat.

Este hito es considerado como el inicio de las telecomunicaciones modernas.

Modelo OSI

Durante los años 60 y 70 se crearon muchas tecnologías de redes. Cada una basada en un diseño específico de hardware. Estos sistemas eran construidos de una sola pieza de forma monolítica. Esto significa que los diseñadores debían ocuparse de todos los elementos involucrados en el proceso.

Estos elementos forman una cadena de transmisión que tiene diversas partes:

- Los dispositivos físicos de conexión.
- Los protocolos usados en la comunicación .
- Los programas de aplicación que realizaban la comunicación.
- La interface que permiten al usuario utilizar la red.

Este modelo, que considera la cadena como un todo, es poco práctico pues el más pequeño cambio puede implicar alterar todos sus elementos.

En respuesta a esta problemática, en 1978 la organización **ISO** (International Standards Organization), propuso un modelo de comunicaciones para redes al que titularon "The reference model of Open Systems Interconnection", generalmente conocido como modelo **OSI**, que proponía la metodología de diseñar el hardware por módulos y el software por capas.

Su idea arquitectónica consiste en descomponer la funcionalidad de la cadena de transmisión en diversos módulos, cuya interfaz con los adyacentes esté estandarizada. Esta filosofía de diseño presenta una doble ventaja:

1. el cambio de un módulo no afecta necesariamente a la totalidad de la cadena.
2. Además puede existir una cierta interoperabilidad entre diversos productos y fabricantes hardware/software, dado que los límites y las interfaces están perfectamente definidas.

El modelo **OSI** está compuesto por 7 capas, a saber:

1) **Capa Física** (Physical layer): es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas. Como resumen de los cometidos de esta capa, podemos decir que se encarga de transformar un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión.

2) **Capa de Enlace** (Data Link layer): Puede decirse que esta capa traslada los mensajes hacia/desde la capa física a la capa de red. Especifica como se organizan los datos cuando se transmiten en un medio particular. Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión.

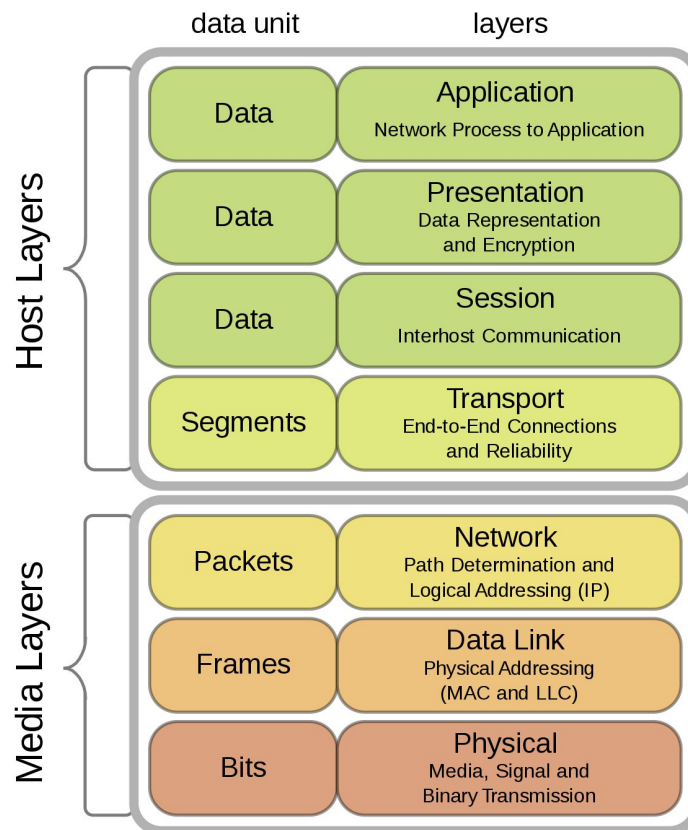
3) **Capa de Red** (Network Layer): Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada, tarea esta que puede ser complicada en redes grandes como **Internet**, pero no se ocupa para nada de los errores o pérdidas de paquetes. Por ejemplo, define la estructura de direcciones y rutas de **Internet**. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta.

4) **Capa de Transporte** (Transport Layer): Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Por ejemplo esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío.

5) **Capa de Sesión** (Session Layer): Es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella. Algunos autores indican que la capa de sesión es meramente una consideración teórica de los autores del modelo sin absolutamente ninguna utilidad práctica conocida.

6) **Capa de Presentación** (Presentation Layer): Esta capa se ocupa de los aspectos semánticos de la comunicación (describe la sintaxis de los datos a transmitir), estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Por ejemplo, describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos.

7) **Capa de Aplicación** (Application Layer): Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia de ficheros etc). Por ejemplo, esta capa implementa la operación con ficheros del sistema. Por un lado interactúan con la capa de presentación; por otro representan la interfaz con el usuario, entregándole la información y recibiendo los comandos que dirigen la comunicación. Ejemplos de protocolos utilizados por los programas de esta capa son **HTTP**, **FTP**, **SMTP**, **POP3**, **IMAP**, etc.



Modelo OSI

Modelo TCP/IP

El **TCP/IP** (que domina las comunicaciones modernas) trabaja mediante un esquema de cuatro capas, similar al diseño original de **DARPA**. Aunque data de los 70 es mas o menos el que se sigue utilizando:

- Capa Física o de Acceso de Red (Network Access Layer): Responsable del envío de la información sobre el sistema hardware utilizado en cada caso. Se utiliza un protocolo distinto según el tipo de red física.
- Capa de Red también llamada capa Internet (Internet Layer): Es la responsable de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión, como el IP, están íntimamente asociados a esta capa.
- Capa de transporte (Host-to-Host Layer): Controla el establecimiento y fin de la conexión, control de flujo de datos, retransmisión de datos perdidos, y otros detalles de la transmisión entre dos sistemas. Los protocolos mas importantes a este nivel son TCP y UDP (mutuamente excluyentes).
- Capa de aplicación (Application layer): Conformada por los protocolos que sirven directamente a los programas de usuario; navegador, e.mail, FTP, TELNET, etc.

Clasificación de redes según su extensión

En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes se encuentran:

Personal Area Network (PAN): Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarse ad hoc a una red. Las redes de área personal se basan principalmente en tecnología **Bluetooth**.

Local Area Network (LAN): Se denominan así a las redes domésticas o empresariales que ocupan una misma infraestructura edilicia. Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa. Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también pueden ser redes LAN. Una tecnología estándar para redes de área local es **Ethernet**.

Metropolitan Area Network (MAN): La red de área metropolitana es una red de telecomunicaciones que comunica varias redes LAN en una zona geográficamente cercana. Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de líneas destinadas a ese propósito.

Wide Area Network (WAN): Mientras que las **Metropolitan Area Networks** comunican puntos que se encuentran cerca unos de los otros, las **Wide Area Networks (WAN)** o redes de área amplia se extienden por zonas geográficas como países o continentes. En la mayoría de los casos, las Wide Area Networks suelen pertenecer a empresas y se gestionan o alquilan de manera privada. Los proveedores de servicios de Internet también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet.

Global Area Network (GAN): Una red global como Internet recibe el nombre de **Global Area Network**, sin embargo no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial.

Clasificación de redes según su topología

La topología de red es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

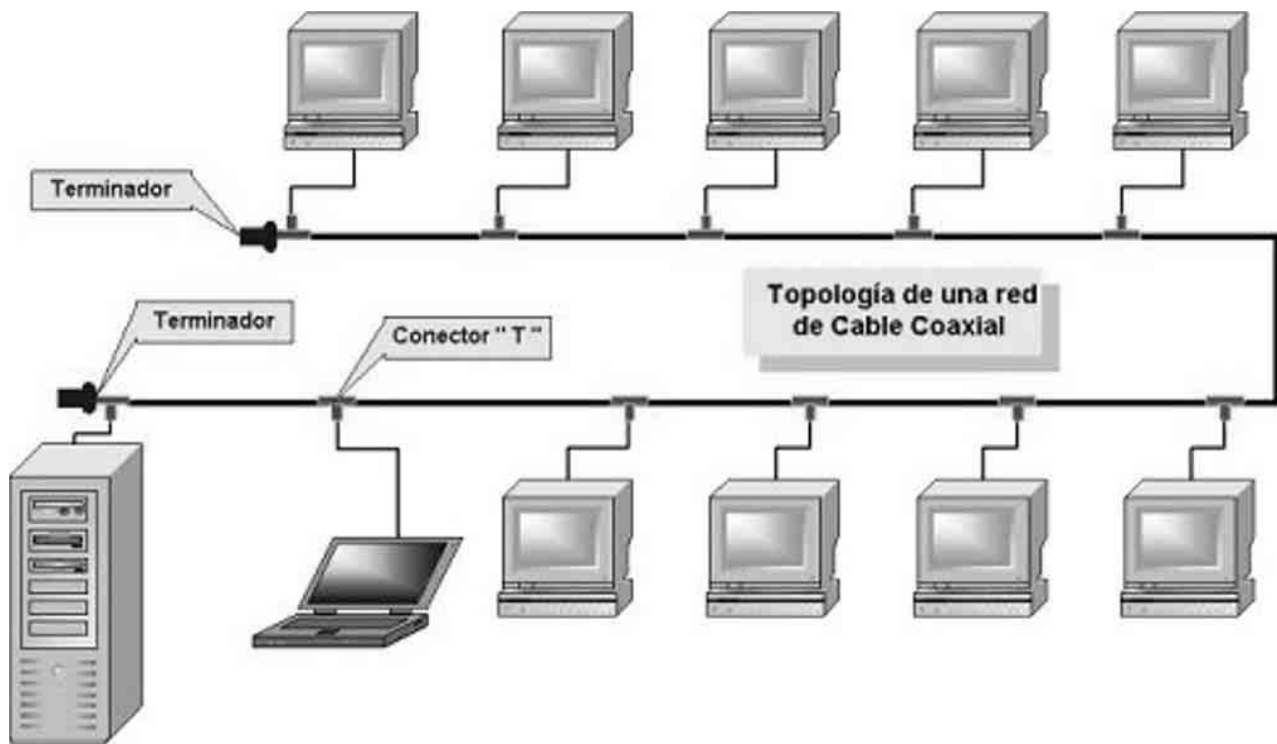
Red en anillo: Topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo.

En este tipo de red la comunicación se da por el paso de un token o testigo, de esta manera se evita pérdida de información debido a colisiones.

Cabe mencionar que si algún nodo de la red se cae (termino informático para decir que esta en mal funcionamiento o no funciona para nada) la comunicación en todo el anillo se pierde.

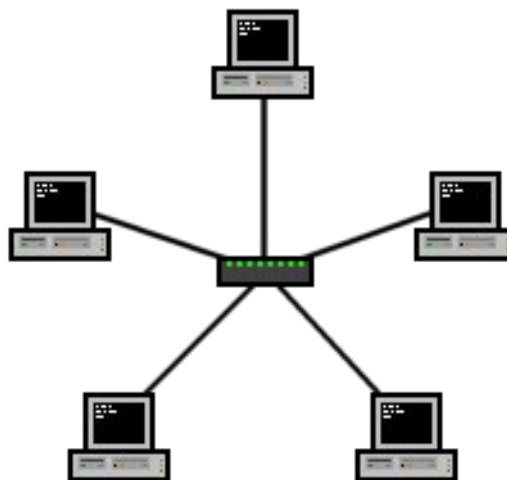


Red en Bus: En la topología de bus todos los nodos están conectados a un circuito común (bus). La información que se envía de una computadora a otra viaja directamente o indirectamente, si existe un controlador que enruta los datos al destino correcto. La información viaja por el medio de transmisión en ambos sentidos y tiene en sus dos extremos una resistencia (terminador). Se pueden conectar una gran cantidad de nodos al bus. Si un nodo falla, la comunicación se mantiene, pero no sucede lo mismo si el bus es el que falla.



Topología en Bus

Red en Estrella: La topología estrella es una de las topologías más populares en las redes LAN. Es implementada conectando cada nodo a un concentrador central. El concentrador puede ser activo, pasivo o inteligente. Un concentrador pasivo es solo un punto de conexión y no requiere energía eléctrica. Un concentrador activo es actualmente un repetidor con múltiples puertos, que amplifica la señal antes de pasarla al siguiente nodo. Un concentrador Inteligente es similar al activo pero con capacidad de diagnóstico; puede detectar errores y corregirlos on the fly.



Topología en Estrella

TCP/IP

Definición

TCP/IP son las siglas de *Protocolo de Control de Transmisión/Protocolo de Internet* (en inglés Transmission Control Protocol/Internet Protocol), un sistema de protocolos que hace posible la interconexión de redes.

Si bien la interconexión de ordenadores existe desde los 60, la posibilidad de interconectar nodos que pertenezcan a distintas redes es un problema que no logró solucionarse satisfactoriamente hasta entrados los años 80, con la aparición de diversas tecnologías, en donde prevaleció el **TCP/IP** por su simpleza, robustez, escalabilidad y flexibilidad.

El **Protocolo de Control de Transmisión** (TCP) permite a dos nodos establecer una conexión e intercambiar datos. El **TCP** garantiza la entrega de datos, es decir, que los datos no se pierdan durante la transmisión y también garantiza que los paquetes sean entregados en el mismo orden en el cual fueron enviados.

El **Protocolo de Internet** (IP) utiliza direcciones que son series de cuatro octetos binarios (expresados en decimal para mayor comodidad) con un formato de punto decimal, por ejemplo: 69.5.163.59

Dirección IP

Una dirección IP es un identificador numérico único dentro de cada red que se utiliza para individualizar al nodo al que está asignada. Está compuesta por 4 números separados por puntos, por ejemplo 192.168.0.1

Cada número es un octeto binario, como con 8 bits se pueden expresar en decimal los valores del 0 al 255, cada octeto expresado en decimal debe estar en el rango del 0 al 255.

Máscara de Subred

La máscara de subred, en conjunto con la dirección IP, sirve para nombrar a un nodo dentro de una red. Puntualmente sirve para definir qué parte de la dirección IP denomina al host y qué parte denomina a la red. Por ejemplo, para la dirección IP 192.168.0.1 / 255.255.255.0, los tres primeros octetos ya están en 255, y esto nos indica que esos octetos no pueden utilizarse para denominar host, puesto que son el "nombre" de la red. El último octeto, cuya porción de la máscara está en 0, sí puede utilizarse para nombrar al host. En este caso, en esta red podrían nominarse 254 nodos.

Clases de red TCP/IP

Según la cantidad de nodos que pueden nominar, existen 3 clases de redes:

- **Clase A:** 1 octeto nomina a la red, 1 octeto nomina al host. Ejemplo: 10.0.0.0 / 255.0.0.0 Puede contener 16777214 nodos.
- **Clase B:** 2 octetos nominan a la red, 1 octeto nomina al host. Ejemplo: 160.216.11.0 / 255.255.0.0 Puede contener 65534 nodos.
- **Clase C:** 3 octetos nominan a la red, 1 octeto nomina al host. Ejemplo: 192.168.0.1 / 255.255.255.0 Puede contener 254 nodos y es la más utilizada en redes LAN.

En todas las redes **TCP/IP** la primera dirección posible se utiliza para nominar a la red (**nombre de la red**), y la última para multidifusión (**broadcast**). Es por eso que estas direcciones no deben utilizarse para denominar a ningún nodo.

Enrutamiento

Es la técnica que permite la comunicación de redes. Se debe recordar que el protocolo TCP/IP fue creado fundamentalmente a estos fines, aunque por su flexibilidad se utiliza también a nivel local para interconectar nodos.

Para interconectar redes existen dispositivos especiales llamados **ROUTERS** (enrutadores), cuya característica distintiva es la de poseer más de un adaptador de red, uno por cada red a la que esté conectado.

Los **routers** poseen una **tabla de ruteo**, en donde se encuentra detallado las diversas redes de las que se tiene conocimiento y cómo llegar hasta ellas. Esto se conoce como **ruta**.

Las **tablas de ruteo** pueden ser estáticas o dinámicas. Las tablas estáticas deben cargarse manualmente, mientras que las dinámicas se populan en función de la información que difunden los diversos routers entre sí, a través de protocolos especiales creados a tales fines, siendo algunos de los más conocidos **RIP** y **ZEBRA**.

Ejercitación

1) Determinar nombre de la red, dirección de broadcast y clase de red para las siguientes direcciones IP:

- a) 192.168.0.25 / 255.255.255.0
- b) 10.10.10.10 / 255.0.0.0
- c) 160.32.22.166 / 255.255.0.0
- d) 192.160.11.78 / 255.255.255.0

2) Realizar una investigación respecto a los siguientes dispositivos físicos:

- a) Router
- b) Switch
- c) Hub
- d) Access Point

3) Investigar la tecnología Ethernet. Considerar:

- a) Que es una dirección MAC (dirección física)
- b) Que es un datagrama

4) Investigar los siguientes conceptos:

- a) Que es un servidor
- b) Que es un servicio
- c) Que es un puerto. Que relación tiene un puerto con un servicio.

5) Investigar los siguientes servicios (que son, para que sirven, en que puerto escuchan):

- | | |
|---------|----------|
| a) FTP | e) HTTP |
| b) SSH | f) POP3 |
| c) SMTP | g) IMAP |
| d) DNS | h) HTTPS |

6) Investigar los siguientes comandos:

- a) ping
- b) traceroute
- c) nslookup