Indice

1 Introducción

Comunicación de Datos se refiere al proceso de intercambio de información entre dos o más equipos electrónicos.
Un ejemplo muy simple de Comunicación de Datos se da en una configuración compuesta por dos PCs conectadas por un cable UTP, lo que constituye una red Ethernet punto a punto (con sólo dos equipos conectados).
La información, que se almacena en los equipos en forma binaria (bits) se envía a través del cable UTP para concretar la comunicación.
Lógicamente, en el proceso de la comunicacion, podemos distinguir un emisor que envía los datos (bits), un receptor que los recibe y el canal, que es el medio que se utiliza para que la información llegue desde el emisor hasta el receptor.
Como consecuencia de que las señales utilizadas por los equipos para representar bits no pueden ser enviadas satisfactoriamente por el canal (si se las enviara sin modificar, no serían reconocidas por el receptor) se las debe transformar: un bit que debe ser enviado, se transforma a una señal que lo represente y que pueda viajar satisfactoriamente por el canal (codificación); cuando la señal llega al receptor, se hace la conversión inversa (decodificación), para que pueda ser interpratada por el equipo receptor.
Como cada equipo debe ser capaz de enviar y recibis bits, el proceso de codificación y decodificación está integrado en un único dispositivo, generalmente denominado MODEM (modulador-demodulador).

Se podría decir que la Comunicación de Datos incluye todos los aspectos relacionados con el intercambio de información, no sólo en configuraciones tan simples como la presentada, sino también en otras mucho más complejas, como pueden ser redes en el hogar, empresas, y la Internet.
A modo de ejemplo, entre los aspectos que se tratan en Comunicación de Datos, podemos mencionar:

- la manera en que deben transformarse los bits que almacenan los equipos en señales electromagnéticas que puedan ser transportadas por el canal para que el receptor pueda reconocerlas.

- el tratamiento de los errores que pueden producirse, por ejemplo que un bit con valor cero, debido a una interferencia llegue con valor 1.

- la coordinación entre emisor y receptor

- en el caso de configuraciones complejas como la Internet, cómo se identifica al otro equipo, y cómo se llega hasta él.

- de qué manera el emisor se da cuenta de que un mensaje (conjunto de bits) enviado no llegó o llegó con error al receptor.

- aspectos de seguridad, por ejemplo asegurarnos de que la información que enviamos no pueda ser cambiada o leída por un tercero.

- etc.

1.1 Redes, inter redes y sistemas distribuidos (Transparencia 1)

Se podría considerar que la comunicación de datos aparece cuando en los sistemas centralizados se separa físicamente la entrada/salida de los datos, de su proceso.
Las terminales, que estaban conectadas directamente al equipo, se van alejando, primero a varios metros, y luego a mayores distancias (dentro de una ciudad, o entre ciudades), utilizando como canal o medio de comunicación, la infraestructura de la red telefónica, que ofrecía una amplia cobertura.
Surgen asılos modems telefónicos, que eran los equipos encargados de adaptar las señales de los equipos (pulsos que representan bits) a las señales que podían viajar por los canales telefónicos (senales analógicas entre 0KHz y 4KHz).
En esta primera etapa, la comunicación de datos posibilita implementar aplicaciones que necesitaban la entrada y salida online con el proceso, por ejemplo, reserva de pasajes aéreos.

Hasta ese momento, había una clara diferenciación entre los equipos conectados: un equipo central, donde residía la capacidad de proceso, y terminales remotas (conocidas como terminales bobas), que sólo se encargaban de la entrada y salida de datos.
La relación del equipo central con las terminales era de maestro/esclavo (master/slave), ya que las terminales sólo podían enviar datos por la línea cuando el equipo central lo solicitaba.
Posteriormente, se producen avances tecnológicos significactivos, tanto en el aspecto del procesamiento (mayor capacidad de memoria, mayor velocidad de proceso), como en el aspecto de la transmisión (canales de mayor capacidad y menor porcentaje de errores - fibra óptica-). Esto acompañado de

una disminución significativa en los costos de equipos y canales de comunicación.
Se produce entonces la integración de las tecnologías de proceso y comunicaciones (las comunicaciones incluyen chips con capacidad de procesar señales, y las computadoras integran la tecnología de comunicación para conectarse entre sí) hace posible que se evolucione del esquema anterior, a otro en que los equipos generalmente son similares en cuanto a capacidad de procesamiento, y pueden transmitir datos de manera independiente, sin ser autorizados por un equipo central. En esta etapa, ya podemos habler de redes de computadoras.

Es difícil caracterizar una red y distinguirla de otros esquemas, tales como multiprocesadores o mainframes con terminales remotas.
Una posible definición de red es: "un conjunto de computadoras autónomas interconectadas por la misma tecnología de comunicación"; es decir que ninguna puede controlar a otra desde el punto de vista de uso del canal y que pueden intercambiar información entre ellas.
Esta definición de red se da en función de la visión habitual que se tenía antes, en la cual existía una relación master/slave entre una computadora central y los demás equipos de menor funcionalidad (terminales, impresoras, etc) pertenecientes a una organización.

De aquí en adelante, para evitar ambiguedades, definimos el significado de los siguientes términos:

- Red (network): conjunto de equipos interconectados entre sí por una misma tecnología de transmisión, por ejemplo un grupo de PCs conectadas a través de tecnología Ethernet, constituye una red Ethernet.
- Interred (internetwork o internet): dos o más redes conectadas de la misma o diferente tecnología entre sí. Por ejemplo, dos redes Ethernet conectadas por un router, o una red Ethernet conectada con una red Wifi.
- intranet: una interred privada, por ejemplo la intranet de una empresa, o la intranet de la Facultad
- Internet (Internet -con mayúscula-): Se refiere a la internet, que es una interred de alcance global)
- Sistema distribuido: Un sistema distribuido, es una red con agregado de software. Este soft hace que se logre una mayor transparencia, es

decir, un usuario no nota la existencia de varios equipos ni que estos están situados en lugares remotos.
Por ejemplo, en una red, un usuario que desea acceder a un archivo y procesar su contenido, debe especificar en qué máquina está el archivo, dónde el programa y en qué máquina realizar el proceso. En un sistema distribuido, directamente solicita el proceso del archivo como si los recursos fueran locales. Un ejemplo de sistema distribuido podria ser la Web.

1.2 Usos y ventajas de las redes (Transparencia 2)

Entre los usos y características más comunes de las redes y sus ventajas sobre los sistemas con un único equipo con mayor capscidad de proceso (mainframe), encontramos:

- Las redes permiten compartir recursos entre diferentes usuarios, sin importar la ubicación geográfica de los mismos.
  Entre los recursos que se pueden compartir se encuentran la capacidad de proceso de los equipos, los datos y el software. En una intranet, por ejemplo, se puede compartir una impresora o el acceso a Internet.

- Es posible duplicar las funciones, es decir, que esten presentes en diferentes equipos y que puedan ser accedidos indistintamente por los usuarios que requieren los servicios ofrecidos.
  La duplicación de recursos permite mejorar la confiabilidad, ya que si uno de los equipos que ofrecen el servicio deja de funcionar, los usuarios pueden acceder a otro de manera transparente.
  Por otro lado, la duplicación permite el balanceo de carga entre los servidores, ya que el usuario puede elegir consultar a cualquiera de ellos.
  Un ejemplo de duplicacion de recursos lo constituyen por ejemplo los servidores de Google: es posible ver que asociadas al nombre de Google (www.google.com, por ejemplo) hay varias direcciones de equipos (direcciones IP); cuando invocamos a Google desde un browser éste trata de obtener la dirección IP de Google, consultando al DNS; puede obtener como respuesta varias direcciones IP, y decide a cuál de ellas consultar, ya que resultan equivalentes. Esto produce un balanceo de carga entre los servidores, y además, en caso de que el seleccionado no responda, el browser purde elegir otro mejorando la confiabilidad. (Es posible consultar al DNS usando el comando nslookup (Linux). Si consultamos por un nombre, devuelve las direcciones IP asociadas).

- Una característica de las redes de computadoras es que gradualmente se ha incrementado su uso para la comunicación entre los usuarios; el primer tipo de comunicación usado fue el email, cuando se estaba desarrollando ARPANET, para comunicación entre los desarrolladores de la red. A medida que fue aumentando la capacidad de los equipos y de los vínculos de comunicación, ha ido reemplazando a otras redes de comunicación, como telefonía, televisión, etc.

- La escalabilidad se refiere a que es posible instalar una configuración mínima de equipos y luego ir aumentándola gradualmente en función de las necesidades de la organización.
  Por ejemplo, al principio, se instalan equipos en determinadas secciones, y posiblemente se los interconecta, pasado un tiempo y como consecuencia del crecimiento de la organización, se instalan nuevos equipos en otras secciones y se integran de manera natural a los anteriores.
  Esto no es posible hacerlo si se tuviera un equipo central, y por lo tanto o bien habría que sobredimensionarlo previendo el futuro crecimiento, o cambiarlo por otro de mayor capacidad cuando ese crecimiento se produce.
  Por otro lado, es posible ir actualizando la red gradualmente, ya que los cmbios tecnológicos son muy rápidos y los equipos se desactualizan fácilmente.

- Otro aspecto importante es la flexibilidad. Las redes permiten integrar equipos configurados para diferentes tareas, por ejemplo diseño gráfico, control de procesos, etc. Para estos casos, es más conveniente utilizar equipos conectados en red que un único equipo que cubra esas características.

1.3 Criterios para clasificar las redes (Transparencia 3)

Consideramos tres criterios para clasificar las redes:

- Alcance o área de cobertura: determina la tecnología que puede utilizarse, y el control que el usuario tiene sobre la red. Si la red está restringida a un área limitada (por ejemplo una Ethernet en una oficina u hogar) por un lado puede configurarse de acuerdo a las necesidades del usuario. En cambio, si el alcance es mayor, generalmente la red es propiedad de una tercera parte que ofrece servicios de comunicación (p.ej. cablemodem para acceso a Internet), y en este caso los usuarios

deben adaptarse a lo ofrecido. Por otro lado, el área parala cual está diseñada la red, determins la tecnología que puede usarse y su costo.

- Difusión de los mensajes emitidos: hace referencia al conjunto de equipos que recibe un mensaje cuando alguno de ellos emite.
  En las redes punto a punto, cuando un equipo emite, solo lo recibe el que esta adyacente a él considerando el link sobre el cual se transmite; en los vínculos de acceso múltiple, cualquier emisión realizada es recibida por todos los equipos conectados a la red.

- Por la naturaleza del medio de comunicación, se pueden clasificar en medios que estan materializados por un conductor, como cable o fibra óptica, o cuando se trata de transmisión por radiofrecuencia (por ejemplo redes Wifi).

1.4 Tipos de redes según su alcance (Transparencias 5 y 6)

Por el alcance o cobertura geográfica podemos distinguir los siguientes tipos de redes:

- PAN (Personal Area Network): las redes de área personal tienen un alcance muy limitado, y están pensadas para conectar los distintos dispositivos (mouse, teclado, etc.) al equipo, evitando de esta manera las conexiones por cable.
  Tienen también otras aplicaciones, por ejemplo los controles remoto de televisores, etc. Son redes inalámbricas de muy baja capacidad.
  La tecnología más difundida para estas redes es Bluetooth. Este tipo de red se basa en un esquema master/slave en el que la PC actúa como master y los dispositivos como esclavos. La PC indicaa a cada dispositivo la dirección a usar, en qué momento y por cuánto tiempo puede transmitir, y en qué frecuancia hacerlo.
  Opera en la banda 2.4 a 2.485 GHz. El esquema básico puede extenderse con el fin de cubrir áreas algo más extensas.

- LAN (Local Area Network): Las redes de área local son aquellas que abarcan áreas que cubren desde un domicilio particular hasta un campus, desde unos metros hasta 1 Km o más.
  Debido al área limitada que cubren, es posible utilizar tecnologías de mayor costo que en redes más extendidas, y principalmente, al ser generalmente propiedad de la misma organización que las utiliza, es posible configurarlas específicamente teniendo en cuenta las necesidades de la organización. // Las dos tecnologías más utilizadas son

Ethernet (red cableada) y Wifi (o IEEE 802.11) (red inalámbrica). Dependiendo de las necesidades, puede usarse una u otra o bien combinar ambas.
Las redes Wifi surgen cuando Ethernet estaba ampliamente difundida en el ámbito de las redes locales, y fueron diseñadas de manera de que fueran compatibles con Ethernet, resultando muy simple su interconexión.

- MAN (Metropolitan Area Network):Las redes de área metropolitana cubren áreas que abarcan una ciudad, (normalmente hasta 10 Kms). En general, estas redes son propiedad de un proveedor de servicios de comunicación, y son compartidas por una cantidad considerable de usuarios. Debido a que pueden conectar equipos dentro del área de una ciudad, pueden ser usadas para comunicar pares de usuarios, por ejemplo dos sitios de la misma organización que se encuentran geográficamente separados.
  Este uso ha cambiado con la aparición de Internet, y en la actualidad se utilizan para conectar a los usuarios con el proveedor de servicios de Internet (ISP) -en la mayoría de los casos el ISP es tamién el propietario de la red-.
  Entre las tecnologías utilizadas encontramos Cablemodem (cableada), MetroEthernet (estensión de Ethernet al área metropolitana) y Wimax -IEEE 802.16- (inalámbrica).
  A diferencia de las redes locales, estas redes no se configuran en función de las necesidades de cada usuario, sino que se ofrecen diferentes tipos de servicio a los que los usuarios deben adaptarse.

- WAN (Wide Area Network): Las redes de área extendida son aquellas que cubren extensiones mayores, por ejemplo una región o un país. El servicio para el cual estan pensadas, es mucho más general, debido a la cantidad de usuarios. A veces una WAN utiliza varias tecnologias de red diferentes, y por lo tanto sería una interred.
  Ejemplos de WAN son las redes satelitales o las que utilizan cable submarino. La tecnología es más sofisticada, teniendo mayor alcance y prestaciones que las anteriores.

- Internet: En todos los casos anteriores, nos referimos a una red, es decir, un conjunto de equipos conectados por la misma tecnología de comunicaciones (Ethernet, WiMax, Wifi, etc).
  En el caso de Internet, si bien la incluímos en esta clasificación por área de cobertura, debemos tener en cuenta que no se trata de una red

(como definimos antes el término) sino que se trata de una internet o inter red (interconexión de redes de diferente tecnología)

1.5 Tipos de redes según la tecnología de transmisión (Transparencia 6)

Otro criterio de clasificación de las redes es de acuerdo a la manera en que se difunde la información que transmiten los equipos.

- En las redes punto a punto, cada equipo está conectado a otro a través de un canal dedicado a la comunicación entre esos equipos; es decir si A esta conectado con B, existirá un canal (por ejemplo un cable UTP) destinado a enviar a B toda la información que transmita A y a A toda la transmitida por B. Ningún otro equipo de la red puede acceder directamente al vínculo que une A y B.
  Cualquier equipo puede tener un número arbitrario de canales que lo conecten con otros.
  En el canal que une por ejemplo A con B, puede circular información originada por un equipo C, pero ésta debe ser retransmitida ya sea por A o por B.

- En las redes de acceso múltiple, hay un único medio de comunicación que es compartido por todos los equipos. Cuando un equipo envÃa, lo reciben todos los demás. El equipo al que está destinada la información, reconoce los datos porque llevan su identificación, y entonces lo entrega al sistema operativo para que lo procese; los demás equipos lo reciben y lo descartan.

Comparación de ambos tipos de red

- Ruteo: ruteo es la función que permite que un paquete (conjunto de bits enviados por un equipo) llegue a destino.
  En las redes de acceso múltiple, no es necesaria esta función, ya que si un equipo emite información para un destino B, por ejemplo, todos los equipos de la red lo reciben, procesándolo B y descartándolo los demás.
  En cambio, en una red punto a punto, el paquete debe pasar por ciertos nodos intermedios para llegar a destino, y cada nodo intermedio debe decidir por cuál de las líneas que lo conectan con otros nodos (interfaces) enviarlo para que llegue a destino. En este tipo de redes,

el ruteo adquiere una importancia fundamental, como veremos más adelante para Internet.

- Seguridad: el concepto de seguridad abarca muchos aspectos, por ejemplo que la información no sea leída o alterada por un tercero, etc.
  En las redes punto a punto la seguridad está garantizada en la medida que los nodos que componen la red (que son los encargados de reenviar la información para que llegue a destino) sean confiables; en cambio, en las redes de acceso múltiple todos los usuarios escuchan lo que un equipo enviía, y por lo tanto se deben tomar medidas de acuerdo al tipo de protección que requieran los usuarios (por ejemplo cifrar la información, o autenticar las partes que se comunican).

- Comunicación grupal: la comunicación grupal se refiere a la capacidad de enviar información desde un equipo a varios receptores a la vez (no a uno solo).
  Este tipo de comunicación se conoce como transmisión multicast (a diferencia de la transmisión de un equipo a sólo un receptor, que se denomina unicast).
  El emisor debe especificar a qué conjunto de emisores (grupo) desea enviar, y la red es responsable de distribuir esta información.
  Esta función es muy simple de implementar en las redes de acceso múltiple, ya que como fue explicado en ruteo, la información la reciben todos los equipos, y en este caso, la procesan sólo aquellos que estén interesados en recibir la información para ese grupo multicast.
  En cambio, en las redes punto a punto, debe existir una función tal que dado un emisor y un grupo de receptores, se encarge de difundir el paquete de manera que llegue a todos ellos.
  Aclaracion: la comunicación o transmisión unicast se refiere a enviar a un solo receptor; la transmisión multicast se refiere a enviar a un grupo de receptores; la transmisión broadcast se refiere a enviar a todos los receptores (que estén conectados a la red) y es un caso particular de la transmisión multicast (cuando el grupo está constituido por todos los equipos).

- Escalabilidad: nos referimos a los límites de la red en cuanto a su crecimiento, ya sea en cantidad de equipos como en extensión geográfica.
  Las redes punto a punto son escalables, tanto respecto a la cantidad de usuarios como a la cobertura geográfica, ya que basta con agregar mayor cantidad de nodos intermedios (y eventualmente aumentar la

capzcidad en los nodos ubicados en el centro de la red).
En el caso de redes de acceso múltiple, no es posible incrementar arbitrariamente la cantidad de equipos, ya que la capacidad del canal se agotaría y los equipos se verían saturados al recibir todos los paquetes que se envían; por otra parte, tampoco pueden extenderse geográficamente, ya que la señal se va degradando a medida que se propaga por el medio de comunicación.

- Demora: Cuando se envía un paquete, se demora un cierto tiempo que entre otras cosas depende de la cantidad de bits que tenga el paquete (ya que enviar cada bit requiere un tiempo). Le llamaremos T al tiempo de envío de un paquete.
  Si consideramos un emisor en una red de acceso múltiple, vemos que el tiempo que insume la transmisión de un paquete, cualquiera sea el receptor, es T (sólo es necesaria una transmisión).
  En las redes punto a punto, el paquete se va pasando de nodo en nodo, hasta que llega a destino. Cada nodo, para retransmitir el paquete, necesita (en general) recibirlo de manera completa.
  Entonces, si el emisor por ejemplo está separado del receptor por tres nodos intermedios, el tiempo para que el paquete sea recibido será 4*T.

1.6 Tipos de redes según el medio de transmisión (Agregado - incompleto)

La información está representada por bits. Estos bits deben ser transmitidos por el canal de comunicación, para lo cual se transforman (codifican) en señales electromagnéticas.
Estas señales pueden viajar ya sea por un conductor (cable o fibra) -por ejemplo la placa Ethernet convierte bits en señales a ciertas frecuencias para que sean enviadas por el UTP-) o ser irradiadas por una antena en una cierta banda de frecuencias (por ejemplo los eqipos Wifi irradian a frecuencias de las bandas 2.4 GHz o 5GHz).
Podemos distinguir entonces dos maneras de enviar la información: a través de conductores o a través de ondas de radio. En general, estos dos tipos de medios de transmisión se complementan, y tienen cada uno sus ventajas y desventajas.

- Facilidad de instalación: La transmisión por radio sólo requiere equipos emisores y receptores, no es necesario el tendido de cables. En algunos casos, esto posibilita o simplifica la instalación de la red, por ejemplo

las redes Wifi son una alternativa a Ethernet cuando es imposible o muy costoso el tendido de cables en un edificioo o campus.
En el ámbito de las MAN, la aparición de las redes WiMax dio lugar a que pequeñas empresas pudieran convertirse en ISPs, ya que para hacerlo no necesitaban tender cables para llegar a los usuarios (las redes ya tendidas erann propiedad de los grandes proveedores).
Para la cobertura de grandes áreas, sobre todo en regiones donde no se cuenta con una infraestructura adecuada de comunicaciones, se utiliza la transmisión satelital; ésta consiste básicamente de satélites geoestacionarios que retransmiten las señales (microondas) emitidas por las antenas terrestres; este tipo de transmisión se caracteriza por presentar una considerable demora de propagación debido a la altura a la que deben orbitar los satélites para aparecer fijos respecto de puntos en la superficie terrestre).

- Respecto de la seguridad, las redes inalámbricas deben ser protegidas a través de cifrado y autenticación ya que con el equipamiento adecuado es posible acceder a las señales (por ejemplo se utiliza WPA en las redes Wifi para evitar que terceras partes accedan a la i nformación). Por otra parte, la señal está sujeta a interferencias de distintos tipos, que pueden provocar una disminución en la calidad de servicio ofrecida, por ejemplo factores climáticos en las redes WiMax o satelitales, objetos fijos o móviles, aparatos electróncos y hasta otras redes cercanas en el caso de Wifi.

- Capacidad y posibilidad de uso: las redes inalámbricas utilizan bandas de frecuencia determinadas. Esto por un lado significa que en un cierto entorno, la capacidad de la red es limitada. Por otro lado, los diferentes paises regulan el uso de las diferentes bandas de frecuencias, y por lo tanto en muchos casos se debe pedir autorización para su uso.

.....

1.7 Packet switching, circuirt switching (Transparencias 7,8, 9 y 10)

En las redes punto a punto, los recursos empleados para la comunicación (capacidad de los medios de transmisión y buffers en los nodos) deben compartirse entre los usuarios de la red.
Existen dos técnicas de adminstrar esos recursos: circuit switching (conmutación de circuitos) y packet switching (conmutación de paquetes).

Circuit switching fue muy utilizado en las redes telefónicas, mientras que packet switching es más adecuado (y el que se utiliza) en las redes de datos. (Aclaración: en la actualidad, las redes transmiten datos, y en ellos se codifica la señal telefonica).
Para diferenciar ambas técnicas, supongamos que dos usuarios A y B desean intercambiar información. Los usuarios A y B están representados en la red por sus respectivos equipos, capaces de conectarse a la red (en una compañía telefónica, estos equipos serían los teléfonos, mientras que en una red de datos, serían las PCs).

- Circuit switching: Cuando el usuario A desea comunicarse con B, debe reservar recursos en la red para realizar esa comunicación: hay un período previo al intercambio de datos en sí, en el cual A indica a la red que desea comunicarse con B, y posiblemente especifica las necesidades de recursos (por ejemplo tasa de transmisión).
  Los nodos de la red que se ven involucrados en la comunicación (cualquier subconjunto que forme un camino entre A y B), intercambian información de control, y como resultado, van reservando recursos (buffers y capacidad en las líneas) que se asignan de manera fija a la comunicación entre A y B.
  Esta asociación se denomina conexión (entre A y B), y los nodos de la red deben guardar estado para esta conexión.
  En la etapa de intercambio de datos, cada paquete emitido tiene asegurado el tiempo que se dede dedicar en cada línea para transmitirlo, y buffers en cada nodo para que pueda ser almacenado antes de que se reenvíe al siguiente.

- Packet switching: Cuando A desea enviar datos, ya sea a B o a cualquier otro usuario, simplemente envía el paquete. No es necesario establecer una conexión.
  Los nodos de la red encaminan cada paquete hacia el destino; los paquetes no tienen asegurados los recursos para llegar a destino y puede ocurrir que deban esperar demasiado tiempo porque alguna línea esta ocupada, o que sean descartados por un nodo que los recibe y no tiene buffer disponible para almacenarlos.
  Cada paquete que A envía a B, es manejado de manera independiente por la red.

Packet switching se adapta mejor a la transmisión de datos debido a su flexibilidad: en caso de que un nodo o línea falle la red se encarga de encontrar un camino alternativo, perdiendo sólo algunos paquetes; en cambio, en cir-

cuit switching, es necesario que los usuarios reestablezcan la conexión.
Por otra parte, circuit switching reserva una cantidad fija de recursos para la conexión; los que no se utilizan para esa conexión en particular, durante el tiempo que permanezca establecida,se desperdician. Esto no se adapta a la transmisión de datos que por naturaleza produce ráfagas de datos en ciertos momentos, mientras que en otros no se envía información.

1.8 Arquitecturas de niveles (Transparencia 11)

Si consideramos una aplicación cualquiera, por ejemplo una que permita acceder y modificar datos almacenados en un archivo, y comparamos la complejidad y volumen de su implementación para que funcione dentro de un único equipo o en red, veremos que en este último caso dicha complejidad y volumen se incrementan, ya que a los propios de la aplicación, se le suman los derivados de los mecanismos de comunicación. De esto resulta un software de mayor volumen y complejidad.
La complejidad que agrega la comunicación de datos se debe a las siguientes causas:

- Sincronización: Los procesos que se comunican y residen en los diferentes equipos, corren cada uno con su propio reloj, y por lo tanto deben proveerse mecanismos para sincronizarlos.

- Errores, duplicaciones y demoras: Deben preverse y corregir las alteraciones sufridas por los paquetes al transitar por la red: posibles pérdidas de paquetes, errores en los mismos y demoras variables en llegar a destino.

- Interoperabilidad: Si se desarrolla una aplicación para que funcione en un equipo, no es necesario que esté sujeta a ningún tipo de convención, funciona independientemente de cualquier otro equipo.
  En cambio, la funcionalidad de las aplicaciones en red se implementa en diferentes equipos; es estrictamente necesario que los procesos respeten normas que les permitan entenderse de manera no ambigua: por ejemplo, si queremos escribir un browser, debemos conocer y respetar la manera de interactuar con un web server; si decidimos producir placas Ethernet, debemos ajustarnos a las señales y formato de los datos de la norma que describe las redes Ethernet.

- Cambios tecnológicos: En las redes, sobre todo en el nivel de transmisión, el cambio tecnológico es constante; como ejemplo se puede ver los cambios producidos en poco tiempo en la norma IEEE 802.11, que

dieron lugar a las variantes b, g y n.
Esto debe ser tenido en cuenta, ya que estos cambios no deben afectar a otros aspectos del software de red (no debe ser necesario, por ejemplo, modificar o cambiar el software que interactúa con el usuario cuando cambiamos el tipo de placa de red).

Para tratar estos problemas de una manera eficiente, se desarrollan las llamadas arquitecturas de niveles.
Consisten en dividir la funcionalidad de un sistema de comunicación de datos en diferentes niveles, agrupando en cada uno de ellos las funciones con el mismo grado de abstracción.
Cada uno de estos niveles cumple con una función que le ofrece en forma de servicio al nivel superior.
Por ejemplo, en el nivel más bajo se agrupan aquellas funciones relativas a la transmisión de bits a a través del medio de transmisión; en el nivel inmediato superior, se pueden agrupar las funciones que permiten que un programa simple, que sólo se dedica a enviar y recibir datos entre dos equipos separados por el canal de comunicación, funcione correctamente (por ejemplo, cuando se pierde un paquete, que sean capaces de detectarlo y volverlo a enviar).
En esta arquitectura simple, tenemos dos niveles: el 1, que se encarga de transmitir cada uno de los bits por el canal, y el 2, que se encarga de transmitir paquetes de bits de un equipo a otro.
Podemos ver que el nivel inferior ofrece una función (servicio) al nivel superior, y éste, por su parte, cumple otra función que ofrece como servicio al nivel superior a él, basándose en el servicio que le provee el nivel inferior.
En este caso, si cambiamos el nivel de transmision de bits, el programa del nivel superior (2) no necesitará ser modificado.

1.9 Modelo OSI/ISO (Transparencia 12)

La ISO International Standards Organization) es una organización internacional que tiene por objetivo producir normas de diferentes tipos.
Una norma es un documento que especifica las características que debe tener un producto; se emite para que todos los fabricantes de ese tipo de producto lo hagan como especifica la norma, y de esa forma todos los productos sean compatibles entre sí.
El proyecto OSI (Open Systems Interconnection), es un proyecto de la ISO cuyo objetivo es estandarizar las funciones de los sistemas de comunicación de datos.

Para ello define un modelo conocido como modelo de referencia OSI/ISO. A través de él se intenta proveer un framework que permita comprender el funcionamiento de los sistemas de comunicación de datos de una manera abstracta, en el sentido de ser independiente de los equipos y medios de comunicación que lo componen. Además se propone una división concreta de las funciones de un sistema de comunicacion de datos en 7 niveles bien definidos.

En el modelo se define el concepto de "Sistema Abierto". Un Sistema Abierto representa un equipo (PC, mainframe, etc.) de manera abstracta, es decir, no se hace referencia a su hardware ni a su software ni a su capacidad, sólo se considera como un sistema de procesamiento genérico, que es capaz de comunicarse con otros (por eso el término Abierto). Entonces, en este contexto, nos referiremos a cualquier equipo con el término "Sistema abierto".
El modelo de referencia define además otros conceptos que son de suma importancia para comprender los sistemas de comunicación de datos, por ejemplo el término "nivel" en el sentido que se vio antes -agrupación de funciones con el mismo grado de abstracción-; "protocolo", como el conjunto de reglas que deben seguir dos procesos residentes en diferentes equipos (Sistemas Abieros) para poder comunicarse, etc.
Estos conceptos y algunas herramientas definidas, asociadas con ellos, son importantes para comprender y desarrollar sistemas de comunicación de datos concretos -es decir producir el código escrito en algún lenguaje de programación-.

La funcionalidad definida consiste en una arquitectura que divide la funcionalidad de las aplicaciones de comunicación de datos, agrupándolas en 7 niveles; el nivel inferior (1) es el que se encarga de convertir los bits en señales que viajan por el canal, y el más alto (7) trata de las funciones referidas a la aplicación, que se ofrecen al programador por ejemplo como una librería y que permiten que el código sea más sencillo.
Por ejemplo, se define una función "conexión", que permite conectarse con un proceso remoto sólo con invocarla, evitando así escribir el código, que puede llegar a resultar extenso y complicado, y que además es utilizado en muchas aplicaciones y por lo tanto no tiene sentido reescribilo en cada caso.

Podemos decir que el objetivo del modelo, es estandarizar las interacciones entre sistemas abiertos, a través de la elaboración de conceptos y creación de herramientas adecuadas que faciliten el desarrollo de aplica-

ciones distribuidas.

Este "Modelo OSIISO' se especifica a través de documentos denominados "normas" o "recomendaciones" que se conocen como "normas de la serie X" (por ejemplo X.21, etc.).

1.10 Conceptos definidos en el modelo OSI/ISO (Transparencias 13, 14, 15, 16, 17, 18, 19)

Se definen a continuación los conceptos de mayor relevancia para la materia:

- Nivel: es la agrupación de funciones y recursos que colaboran entre sí para proveer cierta funcionalidad bien definida dentro de la arquitectura de niveles.
  Por ejemplo, en una arquitectura se define al nivel m as bajo como el que provee la función de transportar los bits de un equipo a otro, unidos por un medio simple de comunicación -un cable, no una red-.
  De manera simple, podemos enumerar los elementos que componen el nivel: en el lado emisor, una función tal que recibe un bit y lo transforma en una señal que viaja por el cable; en el lado receptor, una función que está continuamente monitoreando las señales que se reciben por el cable, es capaz de detectar la generada por el otro lado, y de convertirla ya sea a cero o uno.
  Podemos decir que el nivel está compuesto por estas dos funciones y el cable que materializa el canal de comunicación.

- Servicio ofrecido por un nivel: es la funcionalidad que ofrece; en este caso "transportar los bits que le entreguen, de un equipo a otro (unidos por un canal).
  La importancia de la separación en niveles radica por un lado en que los programas del nivel inmediato superior, se abstraen de la funcionalidad provista por el nivel, es decir, para el programador que escribe una aplicación que manda información al otro equipo, no es necesario ocuparse de hacerlo, sólo debe invocar al servicio (por ejemplo a través de una llamada a una rutina en el lenguaje que se esté utilizando).
  Por otra parte, en el caso de que se decida cambiar la tecnología de transmisión (no es este el caso, pero para dar un ejemplo), si tenemos dos equipos conectados a través de Ethernet, y decidimos cambiar a una conexión Wifi), no será necesario cambiar el programa; sólo seguimos invocando a las funciones anteriores para emitir y recibir bits, aunque las funciones internas del nivel hayan cambiado.

- Usuario del servicio ofrecido por un nivel: es el programa que invoca al nivel a través del llamado a la rutina para enviar o recibir bits. El usuario del nivel se puede identificar concretamente (por ejemplo, es el programa que envía bits ubicado en la PC 1 (sistema abierto en el contexto del modelo OSIISO).

- Proveedor del servicio ofrecido por el nivel: en este caso, no podemos identificar ningún proceso o recurso; la transmisión de un bit (con su correspondiente recepción) no es llevada a cabo por un único proceso, sino por (en este caso) dos procesos que ubicados en lugares físicos diferentes colaboran entre sí.
  Por lo tanto, desde el punto de vista del nivel inmediato superior, no podemos identificar una entidad en particular como proveedor. No se debe confundir el proveedor del nivel con el proceso local al cual invocamos (a través del llamado a una rutina) para solicitar la función; este proceso (local al usuario del servicio) es con el que interactuamos (sería el representante local del proveedor del servicio).

Resumiendo, en una arquitectura de niveles, cada uno de los niveles definidos se caracteriza por proveer un servicio bien definido al nivel superior (es decir, a las entidades de nivel superior).
Puede decirse entonces que los usuarios del servicio provisto por el nivel N, son elementos concretos que pueden individualizarse en el nivel N+1: entidades (procesos) de nivel N+1. Cada una de estas entidades está situada en un determinado equipo, y es parte del subsistema de nivel N+1 en dicho equipo.
En cambio, el proveedor del servicio de nivel N es un concepto más abstracto, porque involucra a la totalidad de las entidades (locales y remotas) que cooperan en el nivel N para ofrecer dicho servicio, y también a las entidades que componen los niveles inferiores al N.
Un nivel está compuesto de procesos que colaboran entre sí para llevar a cabo una cierta función. Estos procesos residen por lo general en equipos diferentes y deben comunicarse para proveer lo solicitado. Por ejemplo, un browser debe poder comunicarse con un Web server remoto para ofrecer al usuario el servicio de navegar por la web.
Los programas que implementan estas funciones están escritos en lenguajes de programación diferentes y por distintos programadores; por otra parte, como veremos más adelante, comunicar procesos residentes en equipos remotos presenta cierta complejidad. Para posibilitar que esta comunicación sea exitosa es necesario que los programas puedan entenderse entre sí, para inetrcambiar la información, recuperar posibles errores, etc.

Las reglas de comunicación entre ellos deben estar especificadas de manera no ambigua y ser conocidas por todos aquellos que decidan realizar una implementación (ya sea de un browser o de un server). Estas reglas se denominan protocolos.
Un protocolo es la especificación de reglas sintácticas (formato de mensajes), semánticas (significado de cada mensaje) y gramáticas (reglas procedurales que debe seguir cada parte) que determinan la comunicación entre procesos (entidades) del mismo nivel (en distintos lugares fÃsicos).
Los protocolos son puntos de visibilidad de la arquitectura; es decir, deben ser conocidos para que las implementaciones se realicen de acuerdo a estas especificaciones y sean compatibles entre sí. Por ejemplo, si queremos escribir un browser, debemos consultar la norma que define el protocolo HTTP para poder entendernos con los servidores.

Cuando definimos la función de un nivel, normalmente lo hacemos en lenguaje natural, pero debe utilizarse una manera menos ambigua de hacerlo para evitar malas interpretaciones, por ejemplo que un programador de nivel N solicite una función que el nivel N-1 no provee, o la solicite de manera errónea, como resultado de una mala interpretación.
Una manera precisa de definir la función de un nivel, es especificando las funciones que podemos invocar, con el tipo de resultado y el tipo de parámetros. Se podría utilizar para eso, por ejemplo, lenguaje C.
El problema es que el Modelo OSIISO es genérico, independiente de las implementaciones.
Es por eso que se decide especificar el servicio provisto por un nivel a través de interacciones genéricas y abstractas entre el usuario del servicio y el proveedor del servicio (su representante local).
Por ejemplo: enviar(bit) y recibir(bit). Estas funciones, se implementan en cada equipo en función del lenguaje usado y del sistema operativo. En un equipo se implementan en C usando llamadas al SO y en otro en Java usando una librería. Estas interacciones abstractas se denominan primitivas.

Las primitivas son maneras de representar las interacciones entre dos entidades locales entre sí y de niveles contiguos.
Definen lo que se denomina interfaz entre los niveles. El objetivo de las primitivas es poder especificar el servicio a través de interacciones abstractas, que sean independientes de las diferentes implementaciones.
Estas interacciones permiten definir de manera genérica y abstracta, el servicio provisto por un nivel.

Hay primitivas que tienen significado remoto, es decir, que cuando se invoca una en un equipo (por ejemplo enviar-bit) produce una primitiva del lado remoto (el proveedor del servicio activa la primitiva recibir-bit); otras primitivas, sólo tienen significado local, y no interesan al Modelo OSI/ISO (por ejemplo, cuando se cae la línea el proveedor del servicio invocará linea-interrumpida).

Las primitivas indican el tipo de interacción y la función de la siguiente manera: "funcion.tipo", donde los tipos son los que se mencionan abajo, y la función es variable y depende del servicio prestado por el nivel. Por ejemplo la función "data" se refiere a transferencia de datos.

Los tipos de primitivas indican el tipo de interacción entre las entidades de niveles contiguos a través de la interfaz. No indican nada acerca del objeto de la primitiva (datos, conexión, etc).

Los tipos de interacción son:

- request: invocada por el usuario del servicio para solicitar el servicio. Por ejemplo "data.request" es invocada por el usuario para enviar datos. En general estas primitivas llevan parámetros, por ejemplo "data.request(destino, datos)".
- confirm: el proveedor del servicio indica al usuario que lo solicitado en un request fue cumplido (de manera exitosa o fallida). Por ejemplo "data.confirm" y se agregaría un parámetro que indique si la transferencia fue exitosa o no.
- indication: el proveedor del servicio notifica al usuario que ha ocurrido un evento. Por ejemplo "data.indication", con posibles parámetros equipo emisor y datos.
- response: es la respuesta del usuario a un indication. Un "data.indication" daría lugar a un "data.response" (puede ser positivo o negativo, por ejemplo si el usuario que recibe el "data.indication" no tiene buffer disponible y debe descartar la información recibida.

Un ejemplo de primitiva local sería un "fail.indication", a través de la cual el proveedor del servicio comunica al usuario que se produjo una falla por ejemplo en la línea.

Los servicios ofrecidos por por un nivel pueden clasificarse en base a diferentes criterios.

- Orientados a conexión y no orientados a conexión: Una conexión es la asociación entre dos procesos; si el servicio es orientado a conexión, el proveedor genera estado y conoce que existe la relación entre los dos usuarios, esto le permite por ejemplo corregir errores, recuperar datos que se pierden etc. Es decir, mejorar el servicio provisto.
  Por ejemplo, podemos tener un servicio de transferencia de datos ("data") orientado a conexión. En un servicio orientado a conexión, antes de iniciar el servicio en sí, se debe establecer la conexión, para esto el proveedor del servicio define un servicio de establecimiento de conexión, que debe ejecutarse previamente de manera exitisa para comenzar por ejemplo la transferencia de datos.

- Servicio confirmado y no confirmado: un servicio confirmado es aquel en el cual está previsto que el proveedor informe al usuario del éxito o fracaso de lo solicitado. En uno no confirmado, el usuario no recibe esta información, y tiene que asegurarse por otro método del éxito o no (por ejemplo a través de una respuesta por parte del proceso que recibe).
  En un servicio confirmado, se utilizan los 4 tipos de proimitivas menccionados arriba; en uno no confirmado, ólo se utiliza "request" e "indication".

- Servicio confiable y no confiable: Un servicio es confiable cuando el proveedor "asegura" al usuario que cumplira con lo solicitado.
  En realidad, el proveedor asegura que hará todo lo posible por cumplir con lo solicitado, pero en algunos casos puede fallar. Para "asegurar" el servicio, debe agregarse capacidad de proceso en el nivel del proveedor, por ejemplo para realizar retransmisiones de datos en los casos en que estos sean transmitidos con error.
  En general, un servicio confiable es orientado a conexión.
  Un servicio no confiable es aquel en el cual el proveedor no asegura al usuario que el servicio será cumplido (envío "best effort" de IP).

Es importante resaltar la diferencia entre un servicio confiable y uno confirmado. Un servicio es confirmado cuando el proveedor contesta al usuario si pudo o no llevar a cabo lo que se le pidio. Puede ser confirmado, pero no confiable, es decir, puede responder con un confirm negativo.

1.11 Descripción de las funciones en una arquitectura híbrida OSI/ISO - TCP/IP (Transparencias 21, 22, 23, 24, 25 y 26)

A continuación se describe la función y características de una arquitectura genérica, que engloba los modelos TCPIP e ISOOSI.

- Nivel 1: Nivel físico en el modelo OSI/ISO, incluido dentro del nivel "link layer" de TCP/IP.
  El nivel 1 del modelo trata con las características del nivel físico, es decir, transmisión de señales a través del canal y conexión del equipo al canal de transmisiń. Provee un servicio de transmisión de bits, cada uno independiente de los demás.
  Las características con las que trata son por ejemplo qué tipo de conector usar para conectarse al medio de transmisión, cómo codificar en seńales cada bit que se le solicita enviar (para esto debe tener en cuenta la forma de la seńal a enviar, el voltaje, la duracion de cada bit, etc). Otros aspectos son los mecanismos para establecer efectivamente el vínculo físico, en el sentido de que sea operativo. Por ejemplo, en una conexión Ethernet, cuando ambos equipos se detectan uno al otro -cuando prendemos las PCs- existe un mecanismo -autonegociación- a través del cual ambos extremos se ponen de acuerdo en la manera de utilizar el UTP (velocidad, etc). Un procedimiento similar -ahora obsoleto- era el que se producía en los modems para línea telefónica -línea dial up-: había que marcar el número del destino (esto lo hacía el operador o el modem), y de esta forma se establecía un vínculo físico entre ambas partes, luego, entre los modems se intercambiaban una serie de seńales específicas, para que el vínculo lógico (canal) quedara listo para transmitir datos. Luego de esto, comenzaba a operar el nivel 2 (por ejemplo PPP -Point to point protocol-). En particular en estos casos debía especificarse de qué manera terminar este nexo entre ambas partes, a nivel lógico y a nivel físico (terminar la conexión telefónica).
  Otro aspecto que se trarta es la coordinación para el envío de seńales, por ejemplo si se puede enviar en un único sentido a la vez, o si es posible enviar simultáneamente en ambos sentidos.

- Nivel 2: Nivel "data link" en el modelo OSI/ISO, incluido dentro del nivel "link layer" de TCP/IP.
  El nivel 2 también opera entre dos equipos conectados por un vínculo de transmisión. Utiliza los servicios del nivel 1, es decir, dispone de un canal virtual entre el emisor y el receptor, capaz de transportar bits.

Una de las funciones básicas del N2 es delimitar los conjuntos de bits, para conformar lo que se denomina bloques o frames. Es fundamental tratar a nivel 2 los bits en conjunto, ya que de otra manera los procesos de control de errores, etc, se harían imposibles de llevar a cabo. En resumen, es esencial proveer mecanismos que permitan saber dónde comienza y termina un bloque. Para esto hay varias alternativas a ver más adelante. Se puede decir que la unidad de transmision con la cual opera el nivel 2, es el bloque, mientras que la del nivel 1 es el bit.
En el caso en que el nivel 2 provea un vínculo libre de error, se debe encargar de detectar y recuperar todo tipo de errores que puedan producirse en la transmisión. Podemos distinguir dos tipos de errores que ponen en juego diferentes mecanismos. Los más simples de corregir son los errores que se producen en los bits del bloque. Otro tipo de errores que requiere mecanismos más complejos (o adicionales a los anteriores) es la pérdida total de uno o más bloques, o la duplicación de un bloque como consecuencia de una desincronización entre emisor y receptor (la duplicación en el nivel 2 sólo puede producirse debido a que el emisor transmita dos veces el mismo bloque).
Otro aspecto a tratar (que se da en cualquiera de los niveles), es lo que se denomina control de flujo. Consiste en la implementación de mecanismos que eviten que un emisor muy rápido sature a un receptor más lento (y que a su vez tiene menos capacidad de recibir información que lo que la línea es capaz de enviar).
Con la aparición de vínculos de acceso múltiple (donde cualquier equipo puede enviar y todos los demás reciben), surge otro tipo de problema, que consiste en que los equipos se pongan de acuerdo respecto de quién va a transmitir por el canal en un momento determinado, y por cuánto tiempo.
Esto introduce una complejidad significativa en el nivel 2, a tal punto que se lo considera un subnivel dentro del mismo. Se lo denomina control de acceso al medio. Esto ocasionó que el modelo OSI/ISO debiera ser modificado, introduciendo el concepto de subnivel, ya que para incorporar esta funcion, se creó el subnivel MAC (Medium Access Control).

- Nivel 3: Este nivel abarca la funcionalidad de la red. Como vimos, hay una diferencia entre una red y una interred, pero la funcionalidad es similar.
  En el modelo OSIISO se dio importancia a los aspectos tecnológicos y no al internetworking, ya que en ese momento las redes eran ho-

mogéneas (X.25) y el internetworking era muy simple (solo contemplaba conectar redes de la misma tecnología).
Esto dio lugar a que el nivel de red del modelo OSI/ISO tuviera que ser ampliado luego de la aparición de las distintas tecnologías de red.
En cambio, el modelo TCP/IP se basa directamemte en el internetworking (nivel IP), dejando de lado los aspectos tecnológicos de cada posible tipo de red, que se incluyen en el nivel link layer (no tratado en TCPIP).
El nivel de red difiere de los dos anteriores en el sentido que involucra a equipos que no están directamente conectados por un vínculo de transmisión. El nivel 3 trata aspectos de la transmisión de paquetes entre cualquier par de usuarios de la red (o interred).
El servicio consiste en proveer transmisión de paquetes de un punto a otro de la interred, de manera que el usuario del nivel 3 pueda independizarse de las caracteristicas tecnológicas y topológicas de las subredes que componen la interred.
Una de las funciones del N3 es proveer un sistema de identificacion, que permita que cualquier usuario del nivel pueda conocer y comunicarse con otro. Este mecanismo se denomina direccionamiento y consiste en que a cada usuario se le provee una direccion de red. Esta direccion de red depende de la tecnología (por ejemplo direcciones MAC en Ethernet), y en el caso de interred, es una dirección abstracta y homogénea para todas las redes: la dirección IP.
Otra función importante es el ruteo, que consiste en que los nodos colaboren entre sí para poder ir pasando un paquete que reciben, al siguiente nodo camino al destino. Esta función se implementa mediante algoritos distribuidos en los nodos de la red. La funcion de ruteo no solo trata de encaminar el paquete en direccion al nodo destino, sino que debe hacerlo tratando de mejorar ciertos aspectos de este recorrido, por ejemplo, tratar de que el camino seguido por el paquete sea el más corto en número de nodos, o que la demora sea la menor posible, etc.
El nivel 3 puede proveer o no conexiones a los usuarios (entidades o procesos del nivel 4 o transporte). En el primer caso, debe incluir mecanismos para el manejo de conexiones.
Otro aspecto importante es evitar que la red se cargue con demasiados paquetes, es decir, que la totalidad de paquetes que los usuarios entregan a la red supera la capacidad de la misma. Si esto ocurre, la red se congestiona y finalmente colapsa. Este aspecto es complejo, ya que de alguna manera debe controlarse globalmente la cantidad de

información recibida por la red.
Un problema que surge de la interconexión de redes de diferente tecnología (internetworking) es cómo compatibilizar las características particulares de cada red (por ejemplo, la longitud máxima de bits que puede tener cada paquete). Este aspecto está muy bien resuelto por IP.
Otros problemas a resolver en internetworking son calidad de servicio (QoS) de las diferentes redes, aspectos de seguridad, etc.

- El nivel 4 o nivel de transporte coincide en ambas arquitecturas, OSI/ISO y TCP/IP. Es un nivel "punta a punta", lo que significa que conecta dos procesos en los extremos de la red, separados por una red o interred. Los niveles 1 y 2, se denominan "punto a punto", porque conectan dos procesos en equipos residentes en equipos adyacentes, separados por un canal simple de comunicación.
  Se distingue también del nivel de red, al cual se dice que es "chained", porque colaboran varios nodos a lo largo del camino emisor-receptor.
  Una caracteristica fundamental para los usuarios (aplicaciones) es el tipo de servicio de transmisión que se les provee. El nivel 4 es el responsable de ofrecer a los usuarios el tipo de servicio que requieren.
  El nivel de red provee un servicio homogéneo, igual para todos los usuarios; el nivel 4 se encarga, a través de software ubicado en los equipos de los usuarios, de mejorar y adaptar el servicio provisto por el nivel de red.
  Tenemos por ejemplo el caso de IP, que provee un servicio no orientado a la conexión, no confiable y no confirmado. En el nivel 4, los protocolos más comunes que encontramos son UDP, que prácticamente provee el mismo servicio que IP, y TCP, que provee un servicio confiable orientado a la conexión.
  El nivel de transporte lleva a cabo otras funciones a ver más adelante.

- Nivel de aplicación: Este nivel en la arquitectura que estamos utilizando, coincide con el nivel de aplicacón del modelo TCP/IP, mientras que en el modelo OSI/ISO abarca tres niveles -esta división, al igual que la poca importancia dada al internetworking y la ausencia de la funcionalidad de acceso al medio, fueron errores en el modelo de la ISO, posiblemente debido a que cuando se concibió, no se tenía demasiada experiencia en redes. Podemos considerar que el nivel de aplicación, como su nombre lo indica, contiene la funcionalidad que necesitan las aplicaciones, cuando las diseńamos basándonos en el nivel

de transporte (TCP on UDP).
El nivel de sesión tiene muy poca funcionalidad. Su objetivo es proveer un transporte de datos mejorado (respecto del de N4) a las aplicaciones. Los servicios del nivel de sesión deben ser invocados explícitamente por las aplicaciones que los requieran. De esta manera, es posible simplificar esas aplicaciones. Por ejemplo, la función de sincronización se refiere a establecer puntos de referencia durante la interacción de dos procesos de nivel aplicación, de manera tal que si esta interacción es interrumpida, por ejemplo debido a fallas en la red, pueda reanudarse desde el último punto de sincronización establecido. Esto puede verse en casos de transferencia de archivos, donde ante una caída de la red y pérdida de conexión TCP, cierto software es capaz de reanudar la transferencia desde donde se habia dejado, en lugar de realizarla desde el principio.
El nivel 6 de la ISO (presentación) se ocupa de la manera en que se representan los datos en los distintos equipos, y de qué se debe hacer para que programas que fueron escritos en diferentes lenguajes que por ejemplo trabajan con enteros de diferentes longitudes o en distintos sistemas (cero desplazado, complemento a la base, etc.), puedan entenderse sin errores.
En TCP/IP, tenemos (no como nivel, sino como una función que puede incorporarse a la aplicación), XDR (External data representatoion -RFC 4506-)que es un lenguaje para la descripción y codificación de datos.
El nivel 7 de la ISO (nivel de aplicación) provee módulos con funciones comunes a las aplicaciones; de esta forma, alguien que escribe una aplicación, puede usar una librería con funciones comunes, sin necesidad de reescribirlas.

1.12 Internet (Transparencias 27, 28, 29, 30, 31, 32, 33

La percepción que tenemos de la Internet desde el punto de vista de un usuario, es la de una red global que interconecta equipos para ofrecer una gran cantidad de servicios y que es administrada y/o propiedad de algunas compañías proveedoras de servicios de comunicaciones.
Es interesante conocer con más detalle aspectos tales como de qué manera surgió Internet, cómo está materializada, es decir, cuales son los componentes físicos que permiten que la información sea transportada a diferentes lugares, dónde se almacenan los grandes volúmenes de información (por ejemplo las bases de datos de Google), de quién(es) es propiedad, cómo y

quien la administra, quienes toman decisiones, etc.
A fines de la década del sesenta, el Departamento de defensa de los EEUU, a través de su agencia ARPA (Agencia de Proyectos Avanzados de Investigación -Advanced Research Projects Agency-).establece un convenio con algunas universidades para el denominado proyecto ARPANET. El objetivo era interconectar varias computadoras en red. En ese momento, tanto la tecnología de comunicaciones como de procesamiento estaban en sus comienzos, por ejemplo, los primeros equipos que se intentaría conectar, llamados IMP (Interface Message Processor) eran "minicomputadoras", primera de ellas instalada en la UCLA, con un peso de 400 Kg y un costo de 80000 dólares en esa época. En octubre de 1969 se produjo la primer comunicación entre el IMP1 y el IMP2, situado en la Universidad de Standford. (A completar)
La estructura de la Internet cambió a partir de que se desmanteló la NSFNET: de estar centralizada alrededor de un backbone como lo era la NSFNET, pasó a ser en la actualidad, una interconexión de redes de diferentes proveedores, que son compañías que venden servicios de Internet. Cada una de estas redes pertenece a un ISP (Internet Service Provider). (A COMPLETAR)

La Internet es una inter red; puede ser considerada como un conjunto de redes interconectada por dispositivos llamados routers. Cada una de estas redes tiene su propia tecnología, y uno de los problemas es hacer que todo esto sea compatible, de manera de lograr una conectividad global y transparente. Este es el rol del protocolo IP.
Es una red de packet switching, los paquetes son reenviados por los routers teniendo en cuenta la red de destino del equipo a quien van dirigidos; el camino que deben seguir está determinado por una función distribuida entre los routers: la función de ruteo.
Desde el punto de vista del control de la Internet, en cuanto a protocolos en uso y otros aspectos relacionados, puede decirse que esta supervisado por the Internet Advisory Board (IAB). Este organismo coordina otros, entre ellos la IETF (Internet Engeneering Task Force), que se encarga de trabajar sobre las normas.

En cuanto a la estructura de la Internet, podemos distinguir varios componentes: ISP (Internet Service Provider): Es una compañía que ofrece servicio de acceso a Internet. Existe una cantidad de ISPs, de diferente importancia: algunos ofrecen servicios a los usuarios, mientras que otros (por ejemplo los que tienen redes que cubren una región, país o continente) ofrecen servicios a los ISPs de menor tamaño. NAP (Network Access Point): son facilidades públicas de acceso a la Internet. A ellos se conectan los ISPs para lograr conectividad entre sí. Actualmente se denominan Internet Ex-

change Points (IXPs).
POP (Point of prescence): son puntos de acceso que provee el ISP. A ellos se conectan los usuarios. Un ISP puede tener varios POPs en diferentes lugares, dependiendo del área que cubre o de la cantidad de usuarios.

Un ISP (proveedor de servicios de Internet), es una organización o empresa, con o sin fines de lucro, que ofrece como servicio la transmisión de paquetes IP y forma parte de la internet pública. Los ISP son muchos y de muy variados tamaños. Como la Internet esta constituida por la interconexión de las redes de los ISPs, éstos deben colaborar entre sí prestándose servicios de conectividad para poder cumplir con sus objetivos. Esta colaboración se realiza a través de acuerdos entre los ISPs. Hay dos tipos de acuerdos entre los ISPs, peering y tránsito. Peering es un acuerdo privado entre dos ISP, y consiste en que cada uno de ellos acepte transportar la información recibida o generada por el otro. Normalmente, el tráfico entre ellos es del mismo volumen, y por lo tanto, no se paga por el peering. Un acuerdo de tránsito consiste en que un ISP (generalmente con mayor área de cobertura e importancia) presta servicios de transmisión a otro a otro, aceptando la información que este último le entrega, ya sea generada por él o de terceras partes, cobrando por este servicio. Generalmente, la relación de tránsito se da entre ISPs de diferentes tamaños, con diferentes áreas de cobertura.

La estructura actual de Internet es jerárquica, pudiendo reconocerse en ella tres tipos de operadores a los que se puede clasificar según su área de cobertura. Estos niveles (de mayor a menor importancia o cobertyura) se denominan "tiers" (Tier 1, Tier 2 y Tier 3).
Las principales características de cada nivel son: Las redes Tier 1 pertenecen a los grandes operadores globales (Global Carriers) que tienen tendidos de fibra óptica que cubren al menos dos continentes (estos tendidos pueden involucrar cable submarino). Desde una red Tier 1 se puede acceder a cualquier punto de Internet gracias a que es una condición necesaria que todas las redes Tier 1 tengan que estar conectadas entre sí. Se puede decir que las redes Tier 1 forman el actual backbone de Internet. Algunos ejemplos de operadores a nivel Tier 1 son AOL a través de ATDN (AOL Transit Data Network), Verizon, Inteliquent, NTT Communications, Telefónica International Wholesale Services (TIWS).
Las redes Tier 2 son operadores que cubren una región, pudiendo abarcar parte de un pais, un país o varios. Estos operadores necesitan conectarse a una red Tier 1 para tener conectividad con toda la Internet. Su principal función es ofrecer servicios de conectividad a los operadores Tier 3. Ejemplos de operadores Tier 2: British Telecom, SingTel (Singapore Telecommunica-

tions Limited), etc.
Las redes Tier 3 pertenecen a los operadores que dan servicio de conexión a Internet a los usuarios finales, ya sean empresas, instituciones o usuarios residenciales. Son los que conocemos como ISP (Internet Service Provider). Algunos ejemplos son: Fibertel, Movistar, Claro, etc.

Puntos de intercambio de trÃ¡fico de Internet (IXP) Un IXP (Internet eXchange Point o Punto de intercambio de trÃ¡fico de Internet), antes conocido como NAP (Network Access Point) es una infraestructura física que permite a varios ISP intercambiar tráfico de Internet. Las conexiones entre los ISPs a travás de los IXP, son de peering. Los IXP permiten a los ISPs de menor nivel (también pueden ser instituciones o empresas) que se conectan a ellos, intercambiar información sin necesidad de utilizar los servicios de los ISPs de mayor nivel. Por ejemplo, un IXP que interconecta a varios ISPs de nivel Tier 1 y algunas instituciones y empresas, mejorara la eficiencia de la comunicación y los costos, ya que para el intercambio de la información entre ellos, no necesitan llegar hasta la red del Tier 2. Un ejemplo de IXP en el país es CABASE.

Puntos de Presencia (POPs): Los PoPs son lugares físicos que el provedor de nivel inferior (Tier 3) distribuye en una ciudad o zona, con el objeto de que los usuarios finales puedan acceder físicamente a su equipamiento, que a su vez, los conecta con el resto de la Internet. El acceso de los usuarios al PoP se da a través de diferentes medios de transmisiín, como ADSL, CableModem, TE, WiMax, etc. En muchos casos, cuando se accede a través de conductores, la compańía propietaria del medio de comunicación es también el ISP.

La Internet es un fenómeno que surgió paulatinamente, no fue planificada ni imaginada su magnitud cuando se fueron diseńando algunos de sus componentes; esto dió lugar a que se tuvieran que hacer cambios y modificaciones a través del tiempo, y tal vez el más significativo fue el cambio del protocolo IP (en el nivel de interred -red- del modelo), de su versión 4 a la versión 6.