

Preparador Informática

www.preparadorinformatica.com

TEMA 65 INFORMÁTICA

**FUNCIONES Y SERVICIOS DEL NIVEL
DE RED Y DEL NIVEL DE TRANSPORTE.
TÉCNICAS. PROTOCOLOS**

TEMA 65 INF: FUNCIONES Y SERVICIOS DEL NIVEL DE RED Y DEL NIVEL DE TRANSPORTE. TÉCNICAS. PROTOCOLOS

1. INTRODUCCIÓN

2. NIVEL DE RED

2.1. FUNCIONES Y SERVICIOS DEL NIVEL DE RED

2.2. TÉCNICAS

2.2.1. DIRECCIONAMIENTO

2.2.2. TÉCNICAS DE ENCAMINAMIENTO

2.2.3. MECANISMOS DE CONTROL DE LA CONGESTIÓN

2.3. PROTOCOLOS DEL NIVEL DE RED

3. NIVEL DE TRANSPORTE

3.1. FUNCIONES Y SERVICIOS DEL NIVEL DE TRANSPORTE

3.2. TÉCNICAS

3.2.1. ESTABLECIMIENTO Y LIBERACIÓN DE LA CONEXIÓN

3.2.2. CONTROL DE FLUJO

3.2.3. CONTROL DE LA CONGESTIÓN

3.3. PROTOCOLOS DE NIVEL DE TRANSPORTE

3.3.1. UDP

3.3.2. TCP

4. CONCLUSIÓN

5. BIBLIOGRAFÍA



1. INTRODUCCIÓN

En los inicios de la informática y de las telecomunicaciones el diseño de un ordenador o de una red era tan complejo que no se tomaba en consideración la compatibilidad con otros modelos de ordenadores o de redes. Las redes y los protocolos se diseñaban pensando únicamente en el hardware a utilizar en cada momento, sin tener en cuenta la evolución previsible, ni por supuesto la interconexión y compatibilidad con equipos de otros fabricantes. A medida que la tecnología avanzaba y se mejoraba la red, los programas de comunicaciones tenían que ser reescritos para utilizarlos con el nuevo hardware.

Cada fabricante elaboraba su propia arquitectura de red, que permitía independizar las funciones y el software del hardware concreto utilizado. De esta forma cuando se quería cambiar algún componente la función o el módulo afectado tenía que ser sustituido.

Como consecuencia de esto en la década de los 70, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes. El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El modelo OSI tiene siete capas o niveles.

7	APLICACIÓN
6	PRESENTACIÓN
5	SESIÓN
4	TRANSPORTE
3	RED
2	ENLACE DE DATOS
1	FÍSICO

En el modelo de referencia OSI se fijan los protocolos que normalizan la comunicación entre niveles de máquinas diferentes y entre los propios niveles.

El presente tema está dedicado a conocer las funciones y servicios que se prestan en los niveles de red y transporte, así como las técnicas utilizadas y los principales protocolos de cada uno de estos niveles.

2. NIVEL DE RED

El nivel de red es la capa que ofrece sus servicios al nivel de transporte. Es la responsable de la conmutación y enrutamiento de la información.

Este nivel sólo es necesario en las redes de conmutación o redes interconectadas. En redes punto a punto o de difusión existe un canal directo entre los dos equipos, por lo que el nivel 2 proporciona directamente conexión fiable entre los dos equipos.

2.1. FUNCIONES Y SERVICIOS DEL NIVEL DE RED

Las funciones principales del nivel de red son:

- Conocimiento de la topología de la red, es decir, de la forma en que están interconectados los nodos, con objeto de determinar la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.
- División de los mensajes de la capa de transporte en unidades más complejas, llamadas paquetes (NPDUs), y asignación de direcciones lógicas a los mismos.
- Ensamblado de paquetes en el host destino.
- Establecimiento, mantenimiento y liberación de las conexiones de red entre sistemas.
- Determinación del encaminamiento de los paquetes de la fuente al destino a través de dispositivos intermedios (routers).
- Las rutas se pueden basar en tablas estáticas.
- Las rutas se pueden determinar al inicio de cada conversación.
- Las rutas pueden ser dinámicas, determinándose con cada paquete en función de la carga de la red.
- Envío de paquetes de nodo a nodo usando un circuito virtual (orientado a la conexión) o datagramas (no orientado a la conexión).
- Control de la congestión.
- Control de flujo.
- Control de errores.

- Reencaminamiento de paquetes en caso de caída de un enlace.
- Con frecuencia, funciones de contabilidad, para determinar cuántos paquetes, caracteres o bits envía cada cliente y producir información de facturación.

2.2. TÉCNICAS

2.2.1. DIRECCIONAMIENTO

El protocolo utilizado para direccionar los equipos de una red es IP (Internet Protocol). Este protocolo se basa en la asignación de una dirección lógica a cada interfaz de red de un equipo (dirección IP).

Los paquetes del nivel IP se denominan datagramas, y son de longitud variable. Constan de dos partes:

- Campo de datos, donde se encapsulan las PDUs (Protocol Data Unit) del nivel superior. Es decir, donde se encapsulan los datos de los niveles superiores.
- Cabecera denominada PCI (Protocol Control Information) en el modelo OSI (Open System Interconnection). Contiene información necesaria para el encaminamiento de los paquetes. Su longitud puede variar entre 20 y 60 octetos.

Versión	IHL	Tipo de servicio	Longitud total datagrama	Cabecera	
Identificación					
TTL (Tiempo de vida)	Protocolo		Suma de comprobación de la cabecera		
Dirección de origen					
Dirección de destino					
Opciones			Relleno		
Datos					Datos

El significado de algunos de los campos más relevantes de la cabecera son:

- Versión (4 bits): versión del protocolo IP utilizada (actualmente, IPv4 o IPv6).



- Longitud total (16 bits). Longitud total en octetos del datagrama, incluyendo cabecera y datos
- Protocolo (8 bits). Indica la entidad de la capa de transporte a la que debe entregarse el datagrama una vez que la capa de red del host destino lo ensambla por completo.
- Dirección de origen y dirección de destino (32 bits, cada una). Indican la dirección IP origen y la dirección IP destino.

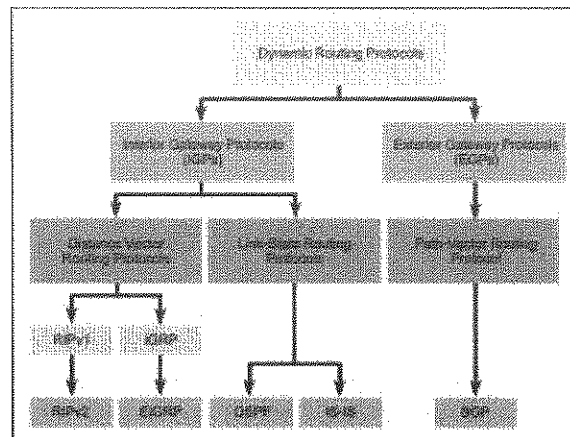
2.2.2. TÉCNICAS DE ENCAMINAMIENTO

El encaminamiento consiste en encontrar un camino, desde el origen al destino, a través de nodos de conmutación o **encaminadores** (routers) intermedios.

Entre las técnicas de encaminamiento se encuentran:

- **Encaminamiento estático:** donde las decisiones de encaminamiento consideran la topología de la red. Las tablas de encaminamiento se construyen manualmente y no se adaptan a los cambios de la red.
- **Encaminamiento dinámico:** las tablas de encaminamiento se construyen de forma automática, mediante el intercambio periódico de información entre los routers. Permite adaptar automáticamente el encaminamiento a los cambios en la topología de la red. Dentro de estos, se pueden clasificar los protocolos en: de puerta de enlace internos (IGP) y externos (EGP).
 - IGP (Interior Gateway Protocols): intercambian información de encaminamiento dentro de un único AS (sistema autónomo).
 - EGP (Exterior Gateway Protocols): intercambian rutas entre diferentes AS.

Nota: AS (Autonomous System) o también denominado sistema autónomo es un conjunto de redes y routers de la misma entidad.



2.2.3. MECANISMOS DE CONTROL DE LA CONGESTIÓN

Las técnicas de control de la congestión pueden ser:

- **Activas** (o de bucle cerrado): actúan cuando se detectan problemas en la red.
- **Pasivas** (o de bucle abierto): se centran en el correcto diseño de la red para evitar la congestión (control preventivo).

Entre las técnicas más utilizadas para el control de la congestión en redes podemos destacar:

- **Algoritmo de descarte de paquetes:** algoritmo de bucle cerrado basado en el descarte de paquetes por parte de los nodos cuando su ocupación es alta. Para ello monitorizan tanto sus recursos como las necesidades de cada línea, de forma que si llegan datos a una línea (que no sean de control u otra información relevante) y el buffer de salida de la línea está lleno, se descarta el paquete.
- **Algoritmo de paquetes reguladores:** algoritmo activo de control de la congestión que asocia un peso variable a cada línea, que se calculará en base a una serie de paquetes reguladores de tráfico. Si el peso supera un umbral, se pone la línea en estado de alerta y se considera que puede haber congestión, por lo que se decrementa su flujo. Si pasa un determinado tiempo sin recibir notificaciones de congestión, se vuelve a subir el flujo que puede cursar. Si por el contrario se supera un umbral mayor, se pasa directamente a hacer descarte de paquetes.

- **Mecanismo de Traffic Shaping:** es un mecanismo en bucle abierto que establece el tráfico que una fuente puede inyectar a la red antes de que esta lo envíe. Se usa en redes ATM, donde el proveedor únicamente garantiza la transmisión a una tasa determinada, que si sobrepasa provocará la pérdida de paquetes, de modo que antes de cada transmisión el cliente debe acordar con el proveedor la tasa de transferencia que puede utilizar

2.3. PROTOCOLOS DEL NIVEL DE RED

Podemos clasificar los protocolos más importantes del nivel de red en base a su funcionalidad en tres grupos.

- **De direccionamiento:** encapsulan información de direccionamiento en los paquetes que permitirá seleccionar su destino. Ejemplo: IP
- **De enrutamiento:** se emplean para establecer las rutas a través de las que se enviarán los paquetes. Ejemplo: RIP, OSPF, BGP
- **Auxiliares:** aportan funcionalidades adicionales a los protocolos de direccionamiento o enrutamiento, como la resolución de direcciones (ARP), envío de información de control (ICMP), asignación dinámica de direcciones IP (DHCP), resolución de nombres (DNS), traducción de direcciones (NAT), etc.

A continuación, se describen brevemente algunos de los protocolos más importantes de cada tipo:

A) IP

El protocolo IP es el protocolo de nivel de red utilizado para la transmisión de datos a través de Internet. Se caracteriza por:

- Transmisión de datos en datagramas (paquetes IP).
- No es orientado a la conexión, por lo que los paquetes son tratados de forma independiente y cada uno puede seguir una trayectoria diferente en su viaje hacia el host destino.

- No es fiable, por lo que no garantiza la entrega de los paquetes, ni la entrega en secuencia, ni la entrega única. Esto es responsabilidad del protocolo TCP de la capa superior.
- No implementa control de errores ni control de congestión.
- Puede fragmentar los paquetes si es necesario.
- Direcciona los paquetes empleando direcciones lógicas IP de 32 bits. (IPv4)
- Verifica la integridad del paquete en sí, no de los datos que contiene.

El protocolo IP se encuentra definido en la RFC 791

B) RIP

El Protocolo RIP (Routing Information Protocol) o protocolo de Información de Encaminamiento es un protocolo de puerta de enlace interna utilizado por los routers para intercambiar información acerca de redes a las que se encuentran conectados. Los protocolos de puerta de enlace interna son utilizados por los routers internos, para el encaminamiento dentro de un AS (Autonomous System). RIP mantiene dinámicamente tabla de rutas utilizando **vector distancia**. La primera versión (RIPv1) del protocolo no enviaba información de máscaras de subred, por lo que no permitía mascarar de subred variables (VLSM). La segunda versión (RIPv2) del protocolo si implementa esta funcionalidad.

C) OSPF

El protocolo OSPF (Open Shortest Path First) es un protocolo interno de puerta de enlace para el encaminamiento dentro de un AS. Se diseñó como el sucesor del RIP y puede manejar AS más grandes. Los intercambios de los mensajes con información acerca del encaminamiento son autenticados. Los routers utilizan el algoritmo de encaminamiento de **estado de enlace** para calcular los caminos de coste mínimo. Los costes de los enlaces no tienen que ser siempre 1 como en el RIP. La especificación vigente de OSPF está en el RFC 2328.



D) BGP

El protocolo BGP (Border Gateway Protocol) es un protocolo de puerta de enlace exterior (EGP, External Gateway Protocol). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Sirve principalmente para el intercambio de rutas entre sistemas autónomos (como ISPs).

Entre los sistemas autónomos se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

E) ARP

El protocolo ARP (Address Resolution Protocol) o protocolo de resolución de direcciones actúa del siguiente modo: cuando un host quiere enviar un paquete a otro, del cual conoce su dirección IP pero no su dirección física, envía un paquete ARP a la red con la dirección IP que se quiere resolver. La difusión llegará a cada host de la red, que revisará su propia dirección IP, y sólo aquel que coincida responderá con su dirección física. El host origen pone en su caché el resultado de esta operación por si necesita establecer contacto con el mismo host posteriormente. Se encuentra definido en el RFC 826

F) ICMP

El protocolo ICMP (Internet Control Message Protocol) se utiliza para informar a la máquina origen de un datagrama IP de que ha ocurrido un fallo en el envío de ese paquete. Los mensajes de este protocolo se utilizan con fines de diagnósticos de la red. Los mensajes ICMP se encapsulan dentro de datagramas IP.

G) DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol), es un protocolo de red mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

3. NIVEL DE TRANSPORTE

El nivel de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos transparente entre dos entidades de sesión. Se encarga de la transferencia libre de errores de los datos entre el emisor y el receptor, proporcionando un transporte de datos confiable entre la máquina origen y la máquina destino, independientemente de las redes físicas y tipos de encaminamiento subyacentes.

3.1. FUNCIONES Y SERVICIOS DEL NIVEL DE TRANSPORTE

Su función más importante es la aceptación de datos de la capa de sesión, división en unidades más pequeñas, si es preciso, denominadas segmentos, y envío de esta información a la capa de red, asegurando que todos los pedazos lleguen correctamente al otro extremo de forma eficiente, donde son reensamblados.

Otras funcionalidades son:

- Establecimiento, mantenimiento y terminación adecuados de los circuitos virtuales (conexiones que se establecen dentro de una red). Cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.
- Determinación, en el momento del establecimiento de la sesión, del tipo de clase de servicio de transporte que se proporcionará a la capa de sesión:
 - Canal punto a punto libre de errores, que entrega los mensajes o bytes en el orden en que se envían.

- Mensajes aislados sin garantía respecto al orden de entrega.
- Difusión de mensajes a múltiples destinos.
- Control de flujo, que desempeña un papel clave en esta capa. El control de flujo entre nodos es distinto del control de flujo entre enrutadores, que tiene lugar en la capa de red. Los datos pueden ser normales o urgentes. Estos últimos se saltan los mecanismos de control de flujo.
- Detección y recuperación de errores de transporte.
- Control de la congestión.
- Numeración de los segmentos para prevenir pérdidas y doble procesamiento de transmisiones.
- Garantía de recepción de todos los datos y en el orden adecuado, sin pérdidas ni duplicados.
- Asignación de una dirección única de transporte a cada usuario.
- Aislamiento a las capas superiores de los cambios inevitables de la tecnología del hardware.
- Contabilidad a través de la red.

3.2. TÉCNICAS

A continuación, se describen algunas de las principales técnicas de este nivel:

3.2.1. ESTABLECIMIENTO Y LIBERACIÓN DE LA CONEXIÓN

Método TOMLINSON:

- Utiliza tiempos de vida acotados para abrir conexiones de forma segura. Cada host tiene un reloj (no importan las caídas pues sigue funcionando). No se necesita sincronización entre los hosts. Un reloj es un contador binario actualizado a intervalos regulares. El número de bits debe igualar o superar al tamaño de un número de secuencia.
- Nunca existen dos TPDU's con el mismo número de secuencia a la vez. Al abrir una conexión se usan los k bits menos significativos del reloj como número inicial de secuencia. El periodo de repetición debe ser largo (32 bits) para que las TPDU's viejas desaparezcan antes de reutilizar el mismo número.

- Las T-entidades pueden después acordar el número inicial de secuencia para sus TPDU y controlar el flujo por ventana. Debe evitarse usar el mismo número de secuencia antes del tiempo de vida desde la última vez que usó.

Protocolo THREE WAY HANDSHAKE (TWH)

- Es un protocolo a dos bandas (de ida y vuelta) que utiliza el método Tomlinson.
- Si una TPDU de control que lleva el número inicial de secuencia a usar en la conexión se retrasa y se envía una copia podría provocarse una apertura errónea de conexión con la entidad destino. TWH evita esos problemas.
- No se necesita que ambos extremos empiecen a enviar con el mismo número de secuencia, y por tanto puede usarse con mecanismos de sincronización no basados en un reloj global.

3.2.2 CONTROL DE FLUJO

El control de flujo más simple es el que se lleva a cabo mediante el sistema de **parada y espera**. El transmisor guarda un registro de cada segmento que envía, esperando un **ACK** antes de enviar el siguiente. También arranca un temporizador cuando envía el segmento. Si el temporizador expira antes de recibir el acuse de recibo, retransmite el segmento y reinicia el temporizador. Este mecanismo es el más barato y el más usado cuando se transmiten tramas muy grandes pero es ineficiente ya que está el canal de transmisión desaprovechado la mayor parte del tiempo.

El control de flujo mediante **ventana deslizante** permite que el transmisor envíe varios segmentos sin esperar los ACK correspondientes. En este sistema el emisor y el receptor se ponen de acuerdo en el número de segmentos sin procesar que puede guardar éste último, dependiendo del tamaño de sus buffers. También se ponen de acuerdo en el número de bits a utilizar para numerar cada segmento. Cuando la ventana tiene un tamaño cero el emisor no puede enviar más segmentos, salvo en dos casos excepcionales: cuando se trata de datos urgentes y cuando el emisor envía un segmento de 1 byte para provocar que el

receptor genere un nuevo acuse de recibo con un nuevo tamaño de ventana, evitando así un bloqueo indefinido de la conexión. Este sistema es mucho más eficiente que el de parada y espera ya que puede haber más de un segmento a la vez en las líneas de transmisión.

Una variedad mejorada del sistema de ventana deslizante es el sistema de control de flujo con **adelante-atrás-N**, en el que cuando la estación destino encuentra un segmento erróneo devuelve un ACK negativo, rechazando todos los que le lleguen hasta que no reciba otra vez el segmento incorrecto en buenas condiciones. El emisor, al recibir el ACK negativo, sabe que tiene que volver a transmitir ese segmento y todos los siguientes.

Por último, existe otro sistema denominado sistema de control con **rechazo selectivo**, que se basa en que los únicos segmentos que se vuelven a retransmitir son aquellos rechazados por el receptor o aquellos cuyo temporizador expira sin confirmación. Este método es más eficiente que los anteriores pero precisa que el receptor disponga de un buffer intermedio de gran capacidad (y por lo tanto caro) en el que guardar todos los segmentos recibidos tras el rechazo de uno dado hasta recibir de nuevo el segmento rechazado de forma correcta. Además, debe ser capaz de colocarlo en su lugar de secuencia correcto. Por su parte, el emisor debe tener la capacidad de reenviar segmentos fuera de orden. Estos motivos hacen que este método, a pesar de ser el más efectivo, sea el menos utilizado.

3.2.3. CONTROL DE LA CONGESTIÓN

Cuando la carga ofrecida a la red es mayor que la que puede gestionar se produce congestión. Todos los algoritmos TCP suponen que las terminaciones de temporización son causadas por congestiones y las revisan en busca de problemas.

Cada transmisor mantiene dos ventanas diferentes:

- Ventana negociada con el receptor al establecerse la conexión, cuyo tamaño está basado en el tamaño del buffer de memoria del destino. Esto

permite que el transmisor no envíe más datos de los que el receptor puede almacenar evitando así que le sature.

- Ventana de congestión, determinada por el tamaño de los datos que se pueden enviar sin que se produzca timeout.

El transmisor sólo puede mandar un número de segmentos limitado por el tamaño de la ventana más pequeña. Al establecerse una conexión, el transmisor asigna a la ventana de congestión el tamaño de segmento máximo usado por la conexión. Cada envío reconocido con éxito duplica la ventana de congestión. Este algoritmo se llama arranque lento y permite que el tamaño de la ventana de congestión crezca exponencialmente hasta que se produzca una terminación de temporización (timeout) o se alcance el tamaño de la ventana receptora.

Este crecimiento exponencial puede producir saturación. Para evitarlo, se introduce otro parámetro, denominado umbral, que toma un determinado valor inicial. Cuando se produce el timeout se cambia el valor del umbral a la mitad del tamaño de la ventana de congestión, se establece el valor de la ventana al del tamaño de un segmento máximo y se inicializa otra vez el proceso de arranque lento. Ahora, cuando el tamaño de la ventana llega al del umbral ésta crece solamente en saltos de un segmento máximo, es decir, con un progreso lineal hasta que se produzca una nueva terminación de temporización.

3.3. PROTOCOLOS DE NIVEL DE TRANSPORTE

Los protocolos de transporte que van a ser objeto de estudio en este tema son el TCP (protocolo de control de transporte) y UDP (protocolo de datagramas de usuario).

Por tanto, se ofrecen dos opciones de protocolo de transporte al nivel de aplicación cada uno de ellos con unas características determinadas. La aplicación de un protocolo u otro va a depender directamente del uso al que esté orientado, de forma que es posible encontrar aplicaciones que utilizan TCP y otras que usan UDP

3.3.1. UDP

UDP (User Datagram Protocol) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de dichos datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP (Dynamic Host Configuration Protocol), BOOTP (BOOTstrap Protocol), DNS (Domain Name Server) y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

3.3.2. TCP

Transmission Control Protocol (TCP) es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn.

TCP (Transmission Control Protocol - protocolo de control de transmisión) permite que grandes volúmenes de información lleguen a su destino correctamente, pudiendo recuperar la pérdida esporádica de paquetes.

Se trata un protocolo de transferencia fiable que asocia un contador cada vez que un paquete es enviado, de forma que al expirar un tiempo máximo establecido sin haber recibido la confirmación el paquete se reenvía. TCP emplea un protocolo de ventana deslizante en el que se define un tamaño de ventana que indicará el número de paquetes a enviar sin necesidad de recibir su confirmación. Según se va recibiendo a confirmación de los primeros paquetes enviados, la ventana avanza posibilitando el envío de los siguientes paquetes.

5. CONCLUSIÓN

Los siete niveles que configuran el modelo OSI suelen agruparse en dos bloques. Los tres niveles inferiores (físico, enlace y red) constituyen el bloque de transmisión. Son niveles dependientes de la red de conmutación utilizada para la comunicación entre los dos sistemas. Por el contrario, los tres niveles superiores (sesión, presentación y aplicación) son niveles orientados a la aplicación y realizan funciones directamente vinculadas con los procesos de comunicación. El nivel intermedio (de transporte) enmascara a los niveles orientados a la aplicación el funcionamiento detallado de los niveles dependientes de la red.

En este tema se ha presentado una visión global del nivel de red y del nivel de transporte. Para cada uno de estos niveles se han detallado sus funciones y servicios más importantes, así como los protocolos más representativos de cada nivel.

6. BIBLIOGRAFÍA

- Stallings, W. **Comunicaciones y redes de computadores**. Ed. Prentice-Hall.
- Tanenbaum, A. **Redes de computadores**. Editorial Prentice-Hall
- Prieto, A., Lloris, A. y Torres, J.C. **Introducción a la informática**. Editorial McGraw-Hill.
- www.itu.int (International Telecommunication Union)
- www.ieee802.org