

## Unidad 6.

### La familia de protocolos TCP/IP

#### 1.-Introducción

La estructura de capas de Arpanet:

ARPANET		
Aplicación	FTP, Telnet, SMTP...	RPC, NFS, SNMP...
Transporte	TCP (conexión)	UPD (sin conexión)
Nivel de Internet	IP, ICMP, ARP, ...	
Interface de red	IEEE 802.2, X.25	
Nivel físico	Nivel físico	

(SMTP: Simple mail Transfer Protocol// SNMP Simple Network Manager Protocol. Protocolo para la gestión de redes)

Arquitectura de los protocolos de red de Microsoft.

	Aplicaciones API* de Windows		Aplicaciones TCP/IP telnet, ftp, etc.
Aplicación y Presentación	NetBios		Sockets Windows
Sesión		NetBios sobre TCP/IP	
	Interfaz TDI		
Transporte			
Red	NWLink	NetBeui	TCP/IP
Enlace de Datos	Interfaz NDIS		
	Controladores de adaptadores de Red		
Física	Adaptadores de Red		

\*(API: Application Program Interface: Software construido de modo estándar cuyas rutinas pueden ser invocadas por las aplicaciones)

Principalmente TCP/IP engloba las capas OSI de red y transporte cuyas funciones principales según la arquitectura OSI son:

Transporte	Control de errores Segmentación Gestión de conexiones Calidad del servicio
Red	Encaminamiento Control del Tráfico

Observando la arquitectura de Arpanet y la de OSI podemos ver que no hay una equivalencia exacta, así que estudiaremos esta familia de protocolos por separado y centrándonos en la arquitectura de Arpanet.

## **2.- La capa de Internet o Interred.**

La capa de interred se encarga de la distribución de los datos a través de una interred. IP(protocol Internet) es el protocolo principal de esta capa y asume la mayor cuota de responsabilidad. El RFC 791 contiene las especificaciones actuales de IP que han sido ampliadas en los RFC 919, 922 y 950.

(RFS – Request For Comments) Petición de opiniones. <http://isi.edu/rfc.editor/>

IP utiliza otros protocolos para llevar a cabo tareas específicas. El protocolo de mensajes de control de Internet (ICMP – Internet Cotnrol Messaging Protocol) se utiliza para entregar los mensajes a la capa host a host. Además deben implementarse protocolos de encaminamiento para mejorar la eficacia de IP:

IP es un protocolo que ofrece las siguientes funciones:

- Direccionamiento
- Fragmentación y reensamblaje de datagramas.
- Entrega de datagramas a través de la interred. / Encaminamiento IP

### **2.1 Direccionamiento de IP:**

La identificación de un nodo en una interred requiere el uso de dos porciones de información: la red específica a la que está conectado el nodo y la identificación del nodo en esa red.

Los protocolos de las capas superiores de TCP/IP no utilizan directamente las direcciones del hardware de la red. Estos protocolos utilizan un sistema de direcciones lógicas para identificar los hosts (host es el nombre oficial de una estación terminal en una red TCP/IP).

Las direcciones lógicas, denominadas direcciones IP, ofrecen varias ventajas:

- El encaminamiento se simplifica gracias a que la información de una dirección de red se codifica en la dirección.
- Las direcciones lógicas permiten que TCP/IP sea resistente a los cambios en el hardware de la red. Por otro lado, el servicio de nombres de dominio (DNS – Domain Name Service) nos permitirá identificar a los host por un nombre en vez de por su número.(IP).

#### **2..1.1 Formato de una dirección IP**

Las direcciones IP tienen una longitud de 32 bits y constan de dos campos:

- Un campo identificador de red (netid) identifica la red a la que está conectado el host
- Un campo identificador de host (hostid) asigna un identificador único a cada host de una red específica.

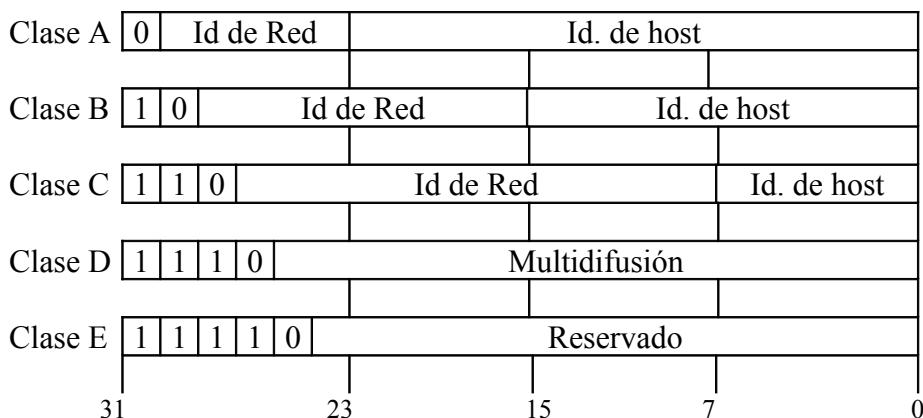
En terminología TCP/IP, una red consiste en un grupo de hosts que pueden comunicarse directamente sin utilizar un encaminador (gateway). Todos los hosts TCP/IP que componen una misma red deben tener asignado el mismo identificador de red. Los hosts con distintos identificadores de red comunicarse a través de un encaminador.

Una interred TCP/IP (intranet) es una red de redes interconectadas a través de encaminadores. Cada una de las redes de una interred debe disponer de un identificador de red único.

### 2.1.2 Clases de direcciones

Existen cinco clases de direcciones IP. Los bits de las direcciones se organizan en cuatro octetos.

- **Direcciones de clase A:** Comienzan por un 0. El primer octeto de la dirección IP comprende el identificador de red y los tres octetos restantes son el identificador del host.
- **Direcciones de clase B:** Comienzan por los bits 10. Los dos primeros octetos componen el identificador de red, los dos restantes son el identificador de host.
- **Direcciones de clase C:** Comienzan por los bits 110. Los tres primeros octetos se dedican al identificador de red y sólo se dispone de un octeto para el identificar del host.
- **Direcciones de clase D:** Comienzan por los bits 1110. Estas direcciones se utilizan para las multidifusiones.
- **Direcciones de clase E:** Comienzan por los bits 11110. Su uso es experimental.



Las direcciones de clase A se agotaron hace mucho tiempo. Las pocas direcciones de clase B que quedan disponibles están reservadas para las grandes industrias. Las direcciones de clase C están disminuyendo muy rápidamente y se espera que con la última versión de IP (versión 6 – IPNG – IP Next Generation) se alivie la crisis actual de direcciones.

Para registrar una dirección IP hay que hacerlo a través de InterNic. La organización Network Solution es la encargada de gestionar el servicio de registro. Se puede hacer a través de <http://ds.internic.net>

Recordar una dirección en binario, sería casi imposible por lo que frecuentemente se utiliza una notación decimal (193.10.30.2 – dirección de clase C). Por convenio, cuando los campos identificadores de red tienen el valor 0 la dirección hace referencia a una red.(135.8.0.0 – Dirección de clase B. Hace referencia a la red 135.8)

### 2.1.3 Restricciones de las direcciones IP.

- (Netid = 0, hostid = 0) Esta dirección sólo permite identificar la red y el host que originan un mensaje. Equivale a “este host de esta red”. Sólo puede corresponder al host de origen de un mensaje.
- (Netid = 0, hostid) Esta dirección identifica un host específico de “esta red” y sólo puede corresponder al host de origen de un mensaje.
- (Netid, hostid = 0). Esta dirección identifica un host que origina un mensaje y el número de red del host. Sólo puede corresponder al host de origen de un mensaje.
- (Netid = 1s, hostid = 1s) Corresponde a una dirección de difusión local. Los mensajes con esta dirección llegan a todos los hosts de la red local y no se encaminan hacia otras redes. (255.255.255.255)
- (Netid, hostid = 1s). Corresponde a una dirección de difusión para una red específica. Los mensajes que tienen esta dirección se encaminan hacia la red de destino adecuada.  
( por lo tanto el último octeto de una dirección IP no puede ser ni 0 ni 255)
- (Netid = 127 – 01111111) tiene un uso especial. Es una dirección de retorno utilizada para verificar la configuración de la red. Los mensajes dirigidos al identificador de red 127 se reflejan en lugar de enviarse a la red.

Considerando estas restricciones y utilizando la numeración decimal tenemos el siguiente conjunto de direcciones posibles:

Clase	Desde	Hasta	Identificadores de red	Identificadores de host
A	1	126	126	16.777.214
B	128	191	16.384	65.534
C	192	223	2.097.152	254

Existen también unos rangos que no se pueden utilizar en Internet para cada una de las clases de redes. (propuestos por InterNic)

Clase A: 10.0.0.0 a 10.255.255.255

Clase B: 172.16.0.0 a 172.16.255.255

Clase C: 192.168.0.0 a 192.168.255.255

Se pueden utilizar estas direcciones en su red sin temor de entrar en conflicto con otros host de internet, lo que las hace idóneas para el envío de mensajes internos y para realizar pruebas.

### 2.1.4 Modos de transmisión y direcciones IP

Existen tres modos para realizar una transmisión IP, cada uno de ellos asociado a un tipo distinto de dirección IP.

#### **2.1.4.1 Mensajes de difusión única o dirigidos**

La mayoría de los mensajes IP se envían en modo de difusión única: procedentes de un host y dirigidos a otro. Estos mensajes pueden encaminarse, es decir, pueden salir de la red y dirigirse a través de un encaminador a otra red distinta. El mensaje lleva una dirección IP completa (Netid, Nethost)

#### 2.1.4.2 Mensaje de difusión

Los mensajes de difusión son recibidos por todos los hosts activos de un segmento de red. Su dirección IP es de la forma ( Netid, Nethost = 1s) o (Netid = 1s , Nethost = 1s) Dado que los mensajes de difusión pueden afectar al rendimiento de la red, los encaminadores IP no los tienen en cuenta.

Los mensajes de difusión se utilizan en dos circunstancias:

- Cuando un host necesita enviar un mensaje a todo el mundo
- Cuando un host debe acceder a otro sin conocer su identidad.

La dirección utiliza para estos mensajes es la 255.255.255.255, ya que los mensajes de difusión no atraviesan los encaminadores. También es posible encontrar mensajes de difusión que especifican una red explícitamente.

#### 2.1.4.3 Mensaje de Multidifusión

Los mensajes de multidifusión van dirigidos a grupos de hosts pertenecientes a un segmento de red local o remoto. Estos mensajes de utilizan un rango especial de direcciones IP, las direcciones de clase D, cuyo rango decimal abarca desde 224.0.0.0 hasta 239.255.255.255

Los mensajes de multidifusión pueden atravesar los encaminadores especialmente configurados para ello.

#### 2.1.5 Direccionamiento de subredes

Si una red no va a estar conectada a Internet, los administradores pueden utilizar cualquiera de las clases de direcciones IP existentes. Es difícil imaginar una organización que llegue a saturar el número de direcciones IP disponibles.

Sin embargo, al conectar una red a Internet, deben utilizarse las direcciones asignadas. Desgraciadamente, la disponibilidad de direcciones Internet está disminuyendo incluso puede resultar difícil conseguir una dirección de clase C. Como resultado muchas organizaciones operan con un número excesivamente reducido de direcciones IP y no pueden asignar un identificador distinto a cada red.

Para solucionar este problema se ha desarrollado un procedimiento de subred (RFC 950) que permite que los administradores *distribuyen los identificadores de host de una red en varias subredes*. El mecanismo de subredes utiliza algunos bits de los octetos del identificador de host para identificar la subred.

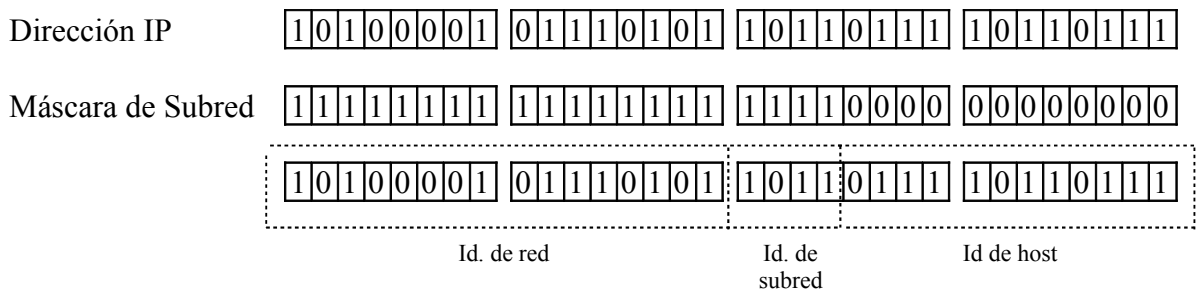
Una dirección IP siempre consta de 32 bits y si no utiliza subredes se divide en dos campo:

Identificador de red + identificador de host

Y si utiliza subredes, la dirección IP se interpreta en tres campos:

:Identificador de red + identificador de subred + identificador de host.

La máscara de subred es un número de 32 bits. Un 1 indica que el bit correspondiente de la dirección IP forma parte del identificador de subred. Un 0 indica que el bit pertenece al identificador de host.



La máscara de subred casi siempre consiste en bits adyacentes de máximo orden. Por consiguiente, sólo es necesario recordar ocho números decimales para poder reconocer la mayoría de máscaras de subred. Las nueve máscaras de subred más frecuentes son las siguientes:

Binario	Decimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

El número de bits en la máscara de subred se ajusta en función del número de subredes necesarias. Al igual que los identificadores de red, los de subred no pueden constar por completo de ceros o unos.

Ejemplo: (dirección de clase B)

La máscara de subred 255.255.255.0 reserva el tercer octeto para el direccionamiento de subredes y permite 254 identificadores de subred.

Al configurar una red que admita direccionamiento de subredes, es necesario designar una máscara de subred aunque no se utilicen subredes. Las máscaras de subredes son las siguientes:

Clase A: 255.0.0.0.  
 Clase B: 255.255.0.0  
 Clase C: 255.255.255.0

Es necesario configurar la máscara de subred utilizando unos en los bits que corresponden al campo identificador de red de la clase de dirección.

Ejemplo:

Red : 195.100.205.0 (Clase C)

Máscara: 255.255.255.224

En binario el último octeto: 11100000

Es decir tenemos 3 bits del identificador del host para identificar subredes.

Con tres bits podemos tener 8 combinaciones pero como no se puede utilizar todo 0 ni todos 1s tenemos 6 subredes posibles.

Con esta máscara de subred podemos identificar 30 hosts. ( con 5 bits = 32 posibilidades pero todo 0 ni 1s se puede)

La dirección IP 195.100.205.175 , con la máscara de subred 255.255.255.224 identifica al nodo 15 de la subred 160.

175 = 101 01111

101 00000 = 160

01111 = 15

El empleo de subredes facilita la organización de una red pero a su vez desperdicia un número considerable de direcciones IP para host. Por un lado los bits que reservamos para la identificación de la subred y por otro lado hay que tener en cuenta que para cada subred no se puede emplear ni la dirección 0 ni la 255 para cada nodo.

Ejemplo

Subred 001    identificador de host 00001-11110                    00100001-00111110 (33-62)

Subred 010    identificador de host 00001-11110                    01000001-01011110 (65-94)

Etc...

Cuando utilizemos subredes hay que tener presente:

-1º- Las subredes deben organizarse para tener la apariencia de una sola red de cara a los encaminadores. Un encaminador muestra una red con subredes al exterior como una única red.

-2º- Los encaminadores deben utilizar protocolos que comprendan el uso de las máscaras de subred.

Nota:

Los sistemas de direccionamiento IP y de subredes se crearon mucho antes del crecimiento explosivo de Internet de los años noventa. En los últimos tiempos, dos tendencias han complicado la asignación de direcciones en Internet

- La direcciones de clase B están agotadas y muchas organizaciones han tenido que hacer trampas en las direcciones para operar con direcciones de clase C.
- Las direcciones de clase C están en vías de extinción y las pequeñas organizaciones deberían aprovechar lo estrictamente necesario.

El encaminamiento interdominio sin clase (CIDR-Classless Inter-Domain Routing) definido en el RFC 1519 es una técnica que permite asignar bloques de direcciones de clase C para adaptarlos a organizaciones con más o menos de 254. Esta técnica utiliza la máscara de subred, pero sin poner 1s en la parte del identificador de red. Esto se denomina *direccionamiento de superred*. De esta forma se permite que las grandes organizaciones agreguen múltiples direcciones de clase C y administren así un mayor nº de hosts.

## 2.2 Fragmentación y reensamblaje de datagramas

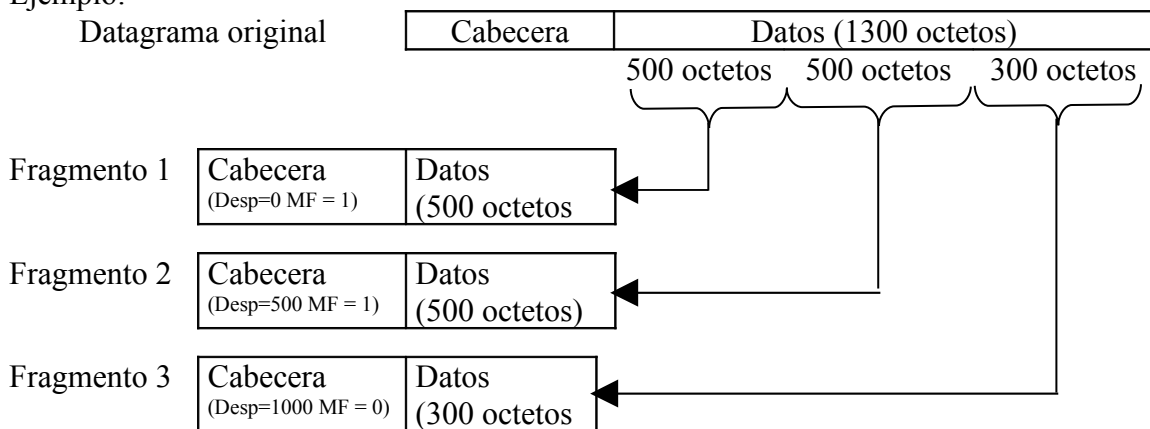
IP se encarga de la distribución de los datagramas a través de la interred. El tamaño de un datagrama IP puede alcanzar un máximo de 65.535 octetos, sin embargo, muchas redes no admiten unidades de datos de tal tamaño. (Ethernet 1500 octetos). La unidad máxima de transferencia (MTU – Maximum Transfer Unit) describe el número de octetos del tamaño máximo de trama que una red puede transmitir sin recurrir a la fragmentación

La especificación del protocolo IP establece que todo host debe ser capaz de aceptar y reensamblar datagramas de al menos 576 octetos. Todos los encaminadores deben tener capacidad para gestionar datagramas de longitud igual a la MTU máxima de las redes a las que están conectados. Además, todo encaminador debe poder gestionar datagramas de hasta 576 octetos.

Ip se encarga de fragmentar los datagramas largos en datagramas compatibles con la capa física utilizada. La cabecera de cada fragmento incluye información que permite al protocolo IP del host receptor identificar la posición del fragmento y reensamblar el datagrama original.

Cuando un datagrama excede el tamaño máximo y se fragmenta, la cabecera de cada fragmento incluye un parámetro de desplazamiento que especifica la posición del primer octeto del fragmento en el datagrama global.

Ejemplo:



Cada uno de los fragmentos constituyen un datagrama estándar IP. Las cabeceras de los fragmentos son prácticamente idénticas a la cabecera del datagrama original con la diferencia de que el bit MF se utiliza para indicar si se trata de un fragmento intermedio o del fragmento final.

El protocolo IP no implementa ningún mecanismo para la detección y recuperación de errores. Si un fragmento de un datagrama se pierde o contiene un error, IP no puede solicitar su retransmisión. IP se ve obligado a informar del error al protocolo de la capa superior que se encarga de retransmitir el datagrama.

Cuando se utiliza TCP como protocolo de la capa superior es preferible evitar que IP realice la fragmentación. TCP incorpora un mecanismo para identificar la MTU mínima entre los hosts de origen y destino y así construir los datagramas de tamaño óptimo evitando la fragmentación.

### 2.3 Entrega de datagramas a través de la interred / Encaminamiento IP

IP se encarga de la distribución de datagramas en la interred. Cuando los datagramas IP viajan a una red distinta a la local, IP lleva a cabo el encaminamiento asegurando que el datagrama llegue a la red de destino.

IP es un protocolo que utiliza su propio esquema de direcciones lógicas, por lo que la entrega de un datagrama en la red implica que IP debe proporcionar a la capa MAC la dirección física del host de destino. (IP tiene funciones en la capa de enlace)

El protocolo de resolución de direcciones (ARP – Address Resolution Protocol) proporciona esta información. IP llama a ARP utilizando la dirección IP del host de destino y ARP devuelve la dirección física correspondiente. Para conseguir esto ARP opera siguiendo estos pasos:

- 1.- El protocolo ARP del host que desea enviar, emite una trama de solicitud ARP difundiendo a la red.(255.255.255.255). La trama de solicitud ARP incluye las direcciones IP y MAC del emisor y la dirección IP del destinatario.
- 2.- Todos los host de la red reciben la trama de solicitud ARP y comparan la dirección IP de destino con la suya propia.
- 3.- Si un host determina que la direcciones coinciden, crea una trama de respuesta ARP que contiene su dirección IP y lo devuelve al host que ha emitido la solicitud.(junto con la dirección hardware).
- 4.- Cuando el protocolo ARP original recibe la trama de respuesta ARP pasa la información a IP:

ARP mantiene una tabla con las direcciones recibidas recientemente para reducir el número de solicitudes de direcciones. Esta tabla se consulta antes de difundir solicitudes ARP.

Microsoft y otros clientes TCP/IP utilizan ARP para evitar que se dupliquen las direcciones IP en la red. Cuando un host entra por primera vez en la red, difunde una trama de solicitud ARP con su propia dirección ARP para anunciar su presencia. Si otro host responde a la trama de solicitud ARP, el nuevo host sabe que su dirección IP ya está siendo utilizada y se impide su entrada en la red.

#### 2.3.1 Entrega local de datagramas IP

Si el datagrama hay que entregarlo en la misma red local, no existirá encaminamiento.

Se realiza siguiendo los siguientes pasos:

- 1.- IP recibe una trama de un protocolo de nivel superior.
- 2.- IP compara el identificador de red de destino incluido en la trama con el de la red local. Si coinciden la trama puede enviarse directamente a la dirección hardware del host de destino.
- 3.- IP llama a ARP y obtiene la dirección hardware de destino.
- 4.- IP construye un datagrama que contiene, entre otros datos las direcciones IP de origen y de destino.
- 5.- IP pasa el datagrama al protocolo de la capa de acceso a la red, junto con las direcciones hardware de origen y destino.

- 6.- La capa de acceso a la red construye una trama que incorpora las direcciones hardware de origen y destino. El datagrama IP se guarda en el campo de datos de la trama.
- 7.- El host de destino examina la trama, reconoce su dirección hardware y recibe la trama

### 2.3.2 Entrega de datos en redes remotas.

#### *2.3.2.1 Encaminamiento Simple*

Cuando un datagrama debe encaminarse a una red adyacente el procedimiento resulta sencillo. Cada host de la red está configurado con la dirección de la gateway (encaminador) predeterminada, la cual especifica el host al que deben enviarse las tramas que van dirigidas a un host situado en una red remota.

Un encaminador IP (gateway o router IP) es básicamente un host TCP/IP equipado con dos o más conexiones de red. Un encaminador puede ser una computadora o una estación de trabajo configurada para llevar a cabo esta tarea.

El proceso de encaminamiento simple sigue los siguientes pasos:

- 1.- El host que desea enviar determina que el datagrama no es para un host de la misma red comparando el identificador de red de destino con el suyo propio. La trama debe de ser encaminada.
- 2.- Obtenemos la dirección de su gateway predeterminado difundiendo una solicitud ARP. IP dirige la trama a su encaminador predeterminado. Sin embargo la dirección IP de destino no corresponde al destinatario final de la trama.
- 3.- El protocolo IP del encaminador recibe la trama, examina la dirección IP de destino y determina que debe encaminar la trama a su otra red.
- 4.- El protocolo IP del encaminador llama a ARP para obtener la dirección hardware del host de destino.
- 5.- El encaminador envía el paquete a la red destinataria con la dirección IP de origen, dirección hardware de origen (la del encaminador), la dirección IP de destino y la dirección hardware de destino.
- 6.- El host destino reconoce su dirección hardware y recibe el paquete.

Nota:

- Las direcciones IP de origen y de destino no cambian a medida que el datagrama recorre la red.
- Las direcciones hardware de origen y de destino cambian cada vez que se envía la trama

#### *2.3.2.1 Encaminamiento Complejo*

Cuando la red destino no está conectada directamente a un encaminador de la ruta de entrega. Para averiguar la dirección de destino lo hacemos a través de las tablas de encaminamiento que residen en los encaminadores IP. En una interred compleja, las tablas deben contener todas las rutas disponibles, así como una estimación de su eficacia.

Existen dos tipos de tablas de encaminamiento:

- Tablas estáticas: Mantenedas por el administrador de la red.
- Tablas dinámicas: Mantenedas automáticamente por un protocolo de encaminamiento.

Tablas de encaminamiento estáticas

Son las únicas admitidas por Windows NT. Su mantenimiento es manual y se realiza con la utilidad "route"

La tabla contiene una entrada (fila) por cada una de las redes conocidas junto con las direcciones IP que deben utilizarse para llegar a ellas. Cada entrada contiene la siguiente información:

<u>Dirección de red</u>	<u>Masacara</u>	<u>Gageway</u>	<u>Métrica</u>
Dirección de redes Conocidas	Máscara de subred	IP que debe recibir los datagramas de cada red	Coste de la ruta en saltos

Tabla de encaminamiento dinámicas:

El mantenimiento de las tablas resulta tedioso y por este motivo, la mayoría de las redes emplea encaminadores con protocolos para el mantenimiento de las tablas.

Uno de estos protocolos es el RIP \_- Routing Information Protocol o protocolo de información de rutas). RIP representa la información de las rutas en términos de coste para alcanzar las redes de destino.(nº comprendido entre 1 y 15). Normalmente cada red que debe ser atravesada supone un coste de 1. RIP se utiliza para descubrir el coste de las rutas disponibles hasta la red de destino y para guardar la información en una tabla de encaminamiento que permita a IP seleccionar la ruta menos costosa.

La entrada de una tabla de encaminamiento RIP contiene al menos la siguiente información:

- La dirección IP de destino
- Una medida que representa la suma de los costes que permiten alcanzar el destino
- La dirección IP del siguiente encaminador en la ruta hacia el destino
- Un indicador que señala un cambio en la ruta.
- Temporizadores.

RIP construye y mantiene las tablas difundiendo periódicamente la tabla de un encaminador a los demás.

La versión 1 de RIP (RIP-1) según especifica el RFC 1058 tiene limitaciones significativas. La peor de ellas es su imposibilidad para trabajar con subredes y máscaras de red. La versión 2 de RIP (RIP-2) está descrita en el RFC 1723. RIP-2 incorpora varias mejoras con respecto a su predecesor.

RIP funciona de manera fiable y es razonablemente rápido. Si embargo hay diferentes problemas con RIP que hacen buscar nuevas soluciones como es el protocolo OSPF (Open Shortest path first – abrir la ruta más corta en primer lugar).

OSPF es un protocolo incluido en las normas de Internet cada vez más utilizado Este protocolo está basado en el estado de los enlaces, ya que cada encaminador mantiene una base de datos con la descripción de la topología del sistema local. La estructura de datos topológica es arborescente y cada encaminador está situado en la raíz de su propio árbol. Los encaminadores del sistema autónomo anuncian el estado de sus enlaces y esta información permite construir las bases de datos (encaminamiento jerarquizado)

Existen otros protocolos relacionados con IP para el encaminamiento como es el EGP – Exterior Gateway Protocol y el BGP - Border Gateway Protocol empleados para el encaminamiento entre sistemas autónomos y el exterior.

Por último existe el protocolo ICMP que dota a IP de la capacidad de mensajería para poder solucionar problemas. ICMP cuenta con un mecanismo para informar de los errores al host de origen de un datagrama, pero no tiene la capacidad de corregirlos.

### **3.- La capa de host a host o Transporte**

La capa de host a host cumple dos funciones principales:

- Proporcionar una interfaz adecuada para que los procesos de la capa superior y las aplicaciones accedan a la red.
- Entrega los mensajes de la capa superior entre hosts.

Dado que las necesidades de los procesos de la capa superior son distintas, se han implementado dos protocolos host a host.

#### **3.1 Protocolo de control de transmisión (TCP – Transmission Control Protocol)**

TCP (RFC 793) proporciona una comunicación fiable entre los procesos que se ejecutan en los hosts interconectados. La comunicación host a host funciona con independencia de la estructura de red. TCP utiliza direcciones IP para identificar a los hosts sin considerar las direcciones físicas.

Las características y funciones más importantes de TCP son:

##### 3.1.1 Mantenimiento de las corrientes de datos

El interface entre TCP y los procesos o aplicaciones (capa superior) se denomina *puerto*. Es un mecanismo que permite que el proceso llame a TCP y que TCP, a su vez, entregue las corrientes de datos a los procesos adecuados.

Los puertos se identifican mediante un n° de puerto. Estos n°. están ya estandarizados por IANA ( Internet Assigned Numbers Authority) que ha dedicado números de puertos específicos a una serie de procesos comunes.

Para especificar plenamente una conexión, a la dirección IP del host se añade el n° de puerto. Esta combinación se denomina *socket* (enchufe). Una conexión entre dos hosts queda totalmente descrita por los sockets asignados a cada terminal de la conexión.

TCP/IP utiliza dos tipos de sockets:

- Sockets de corriente: Se utilizan con TCP para lograr un intercambio de datos fiable, secuencial y bidireccional

- Sockets de datagramas: Se utilizan con UDP para lograr transferencias de datos no fiables y bidireccionales.

### 3.2.2 Administración y Mantenimiento de las conexiones garantizando la fiabilidad

Para la capa de nivel superior, la comunicación con la red implica un envío y recepción de corrientes de datos continuas. Esta labor se realiza según descenden los datos por los distintos protocolos de TCP/IP y siguen los siguientes pasos:

1. TCP recibe una corriente de datos desde el proceso de la capa superior.
2. TCP puede fragmentar la corriente de datos en segmentos (función del nivel de transporte de la arquitectura OSI) que se adapten al tamaño máximo del datagrama IP:
3. IP puede fragmentar los segmentos a medida que prepara los datagramas para adaptarlos a las restricciones de la red.
4. Los protocolos de red transmiten el datagrama en forma de bits.

En recepción se realiza estos mismos pasos en forma inversa.

TCP se encarga de controlar el flujo entre los hosts (Función nivel de sesión (sincronismo) según OSI). El objetivo principal del control de flujo consiste en garantizar que el host emisor no transmite a mayor velocidad de la que admite el host receptor. Esta labor se realiza por el método de ventana deslizante (visto para el control del flujo del nivel de enlace de la arquitectura OSI)

La eficacia de la transmisión de mensajes aumenta cuando éstos se fragmentan según la unidad máxima de transferencia (MTU). Cuando se establece una conexión TCP utiliza la MTU de la red para adaptarse al tamaño máximo de segmento (MSS – Maximum Segment Size). Normalmente el MSS equivale a la MTU menos 40 bytes deducidas a las cabeceras TCP e IP.

	Unidad de datos	Protocolos
Aplicación	Corriente de datos	
Transporte	Segmentos (Mss)	TCP/UDP
Internet	Datagrama	IP
Red	Trama (MTU)	IEEE 802.x
Físico	Bit	

### 3.3.3 Medidas para mantener la precedencia y la seguridad

La cabecera IP proporciona los campos tipo de servicio y opción de seguridad. TCP puede utilizar estos campos para implementar la precedencia y la seguridad. Los módulos TCP que funcionan en un entorno de seguridad deben identificar los segmentos mediante la información necesaria. TCP también permite que los procesos de la capa superior especifiquen la seguridad requerida.

### 3.2 Protocolo de datagrama de usuario (UDP – User Datagram Protocol)

UDP ofrece un transporte alternativo a aquellos procesos que no requieren una entrega fiable. UDP es un protocolo de datagramas que no garantiza la entrega de los datos ni protege frente a su duplicación. (TCP protocolo de circuito virtual) por consiguiente UDP es un protocolo muy sencillo y mucho más ligero que TCP.

Se recomienda el uso de UDP en las siguientes situaciones:

- Mensajes que no requieren acuse de recibo. – Como son los avisos del protocolo de administración de red (SNMP – Simple Network Management Protocol)
- Mensajes entre hosts esporádicos. Mucha perdida de tiempo en abrir y cerrar la conexión.
- Cuando la fiabilidad se implementa a nivel de proceso.

Diferencias clave entre TCP/UDP.

<b>TCP</b>	<b>UDP</b>
Fiable	No fiable
Orientado a conexiones	No orientado a conexiones
Circuito virtual	Datagramas
Elevado tráfico de control	Tráfico de control reducido
Segmentación de mensajes	Sin segmentación ni reensamblaje de mensajes
Segmentos de mensajes secuenciales	No secuenciales

#### **4.- La capa de proceso/aplicación**

Esta capa contiene programas que proporcionan servicios de red como servidores de correo, servidores de transferencia de archivos, terminales remotos y servidores de administración de sistemas. Además, existen programas que actúan a modo de interfaces con el usuario final como FTP y Telnet.

Hay que tener en cuenta que pueden existir otras capas sobre la de proceso/aplicación, es decir, aplicaciones que utilizan servicios proporcionados por ciertos procesos. Un ejemplo de esto es el protocolo SMTP (Simple Mail Transfer Protocol) para enviar y recibir correo. El usuario no emplea directamente el protocolo SMTP sino que acceden al protocolo mediante un programa de correo electrónico que genere mensajes utilizando dicho protocolo.

**Servicio de nombres de dominio.**

El uso de nombres de hosts requiere un sistema que permita asociarlos a sus direcciones IP. A tal efecto, se han empleado dos tecnologías en Internet:

- Uso de archivos hosts para asignar nombres estáticos
- Sistema de nombres de dominio (DNS – Domain Name System)

Inicialmente (en Arpanet) se utilizaba unos ficheros de texto donde se almacenaba el nombre del host junto con su dirección IP. Estos ficheros denominados HOST.TXT.

fueron útiles en internet mientras su crecimiento no fue exagerado. El mantenimiento de estos archivos era manual y muy pronto fue imposible seguir utilizando este sistema para una red como Internet.

DNS fue diseñado pensando en las dimensiones de Internet, que imposibilitaban la administración central de un solo *espacio de nombres*. (nombre que recibe la base de datos jerárquica por la que cada host recibe un único nombre – *juan.sw.eng.*).

Los *servidores de nombres* son programas que almacenan datos sobre el espacio de nombres y proporcionan información en respuesta a consultas DNS.

### FTP: Protocolo de transferencia de archivos

FTP es a la vez un protocolo y un programa que puede utilizarse para realizar operaciones básicas sobre los archivos de un host remoto y para transferir archivos entre hosts. FTP es una aplicación segura y fiable, ya que opera sobre TCP. Los usuarios que acceden a un host utilizando FTP deben autenticar su conexión, proporcionando su nombre y contraseña.

FTP incluye componentes cliente y servidor. Un host que ofrece su sistema de archivos a los usuarios debe ejecutar una aplicación de tipo *servidor FTP*. Los usuarios que acceden al servidor FTP deben ejecutar un software de tipo *cliente FTP* en sus computadoras.

FTP no permite ejecutar archivos remotos a modo de programas pero puede listar directorios, ver el contenido de los archivos, manipular los directorios locales y copiar los archivos de un host a otro.

FTP es una aplicación basada en texto (como el MS-Dos) que se utiliza desde la línea de ordenes. Hoy día existen una amplia gama de aplicaciones gráficas FTP basadas en Windows. La utilidad FTP se sigue encontrando tanto en Windows NT como en windows 98. (*ftp.exe*)

### TFTP: Protocolo trivial de transferencia de archivos

FTP fue diseñado para garantizar la seguridad de las operaciones con archivos en redes poco fiables. Utiliza TCP como protocolo de transporte para conseguir entregas fiables. TFP opera sobre circuitos virtuales TCP y requiere que los hosts establezcan una conexión antes de iniciar las operaciones con archivos. Una conexión FTP lleva implícito un proceso de autenticación.

Cuando una red es fiable, por ejemplo, una red de área local, la carga de trabajo adicional de FTP puede no ser deseable. Esta razón ha impulsado el desarrollo de un protocolo más sencillo, el protocolo trivial de transferencia de archivos (TFTP; RFC 1350). TFTP utiliza el protocolo no fiable UDP como transporte. No obliga a establecer una conexión ni implica un proceso de autenticación antes de permitir la transferencia de archivos.

La falta de seguridad de TFTP hace que su uso resulte arriesgado en una red pública. TFTP es un protocolo de pequeño tamaño y de gran eficacia que puede incluirse fácilmente en la ROM de arranque de una computadora. Por ejemplo, las estaciones de

trabajo UNIX se Sun utilizan TFTP para descargar una imagen del sistema operativo central cuando se inician en una red.

### Telnet

El acceso en modo terminal remoto es una característica crítica de muchas computadoras. Puede lograrse mediante una conexión telefónica, o mediante Internet. Telenet es un programa que posibilita el acceso en modo terminal remoto a través de una red.

Al igual que TFP, se basa en procesos cliente-servidor. Un servidor Telnet ejecutándose en un host remoto mantiene un terminal virtual: una imagen software de un terminal que puede interactuar con el host. Un usuario inicia una sesión Telnet ejecutando un programa cliente Telnet y conectándose al servidor Telnet. El servidor recibe las pulsaciones de teclas del cliente y las aplica al terminal virtual que interactúa con otros procesos del host. El servidor Telnet también recibe los datos destinados a la pantalla del terminal y los envía al cliente Telnet. La sensación que percibe el usuario es que la sesión de terminal tiene lugar en la computadora local mientras que el host remoto “piensa” que está interactuando con un terminal local.

Telnet se basa en la emulación de un terminal de texto, normalmente Digital VT220, VT100/VT102 o VT52. Estos terminales pueden llevar a cabo operaciones sofisticadas basadas en texto, por ejemplo, mostrar menús que permitan seleccionar una opción utilizando las teclas del cursor. No obstante, sólo pueden trabajar en modo texto.

Otra limitación de Telnet consiste en que la computadora local no tiene capacidad para procesar información. Todos los procesos tienen lugar en el servidor Telnet remoto, el cual convierte el host local en un terminal “tonto”. Por consiguiente, Telnet no puede utilizarse como base para realizar operaciones sofisticadas en la red, como por ejemplo la transferencia de archivos, que es labor de FTP.

Es posible utilizar Telnet para acceder a servicios como archie, gopher y veronica, aunque todos ellos van perdiendo importancia debido a la popularidad de la World Wide Web. Se utiliza Telnet muchas veces, en entornos LAN para la configuración de dispositivos a distancia como encaminadores o concentradores.

### SMTP: Protocolo simple de transferencia de correo.

Probablemente, el correo electrónico es la aplicación más importante de Internet. Se basa en el protocolo SMTP descrito en el RFC 821/822). SMTP transporta mensajes de correo electrónico entre distintos hosts TCP/IP.

Los hosts que admiten correo electrónico utilizan un agente de transferencia de correo (MTA –Mail Transfer Agent) para gestionar el proceso. El MTA tiene dos grandes responsabilidades:

- Enviar y recibir mensajes desde/hasta otros servidores de correo.
- Proporcionar una interfaz que permita que las aplicaciones accedan al sistema de correo.

El MTA se encarga de proporcionar a los usuarios buzones de correo dotados de una dirección. La dirección de correo electrónico consta de dos partes separadas por el

carácter “@”. La primera parte es el nombre del usuario y la segunda es el nombre del dominio del host que ejecuta el MTA.

Los usuarios finales se comunican con el MTA utilizando uno de los muchos agentes de usuario (UA – User Agent) disponibles. El UA es un sistema de correo que evita al usuario todas las complicaciones del proceso. Los UA utilizan un protocolo de correo para comunicarse con el MTA, como por ejemplo el POP3 (Post Office Protocol Version 3 ; RFC 1460).

Existen multitud de programas que utilizan el protocolo POP3 para enviar y recibir correo como es el Outlook Express, Eudora, etc...El elevado uso del correo electrónico de Internet ha provocado que un importante número de aplicaciones (navegadores Web, examinadores de grupos de noticias , IRQ, etc...) incorporen un sistema de gestión de correo.

Los sistemas de correo electrónico no están diseñados para realizar intercambios de mensajes en tiempo real(para ello existen los programas de conversación en tiempo chat). Los servidores de correo electrónico utilizan un método de almacenamiento temporal y envío de mensajes. Supongamos que tenemos 3 servidores de correo (A, B y C). El servidor B se encuentra como servidor intermedio entre A y C. Cuando B recibe un mensaje de A, lo almacena en su disco duro local. Si B tiene otras prioridades, por ejemplo, la recepción de otros mensajes, espera hasta que la actividad descienda antes de enviar el mensaje a C. Es posible configurar B para que envíe los mensajes a C cuando existan varios mensajes pendientes o cuando transcurra un periodo de tiempo dado. La eficacia de B aumenta al transferir varios mensajes con una sola conexión en lugar de abrir una conexión distinta para cada mensaje.

El envío de datos binarios a través de los sistemas de correo SMTP requiere su codificación en un formato compatible con la transmisión de caracteres de 7 bits. El host receptor descodifica el mensaje para recuperar los datos binarios. Muchos de los agentes de usuario realizan estas conversiones de forma automática en los archivos adjuntos. El método más utilizado en máquinas UNIX es el uuencode. Existen muchos programas que permiten realizar esta codificación-descodificación en computadoras DOS, Windows y Macintosh.

Las extensiones de propósito general para correo Internet (MIME- Multipurpose Internet Mail extenions; RFC 1512) constituyen un protocolo opcional que admite transferencia de mensajes binarios a través de SMTP.

#### SNMP: Protocolo simple de administración de red.

La administración de una red engloba una amplia gama de actividades. Para SNMP, consiste en recopilar , analizar y ofrecer datos sobre el rendimiento de los componentes de la red. Los datos recopilados por SNMP incluyen estadísticas de rendimiento, informes rutinarios y avisos de problemas potenciales o existen en la red.

SNMP pertenece a la familia de protocolos Internet para la administración de la red:

- SNMP- El protocolo que permite la comunicación entre las estaciones de administración de la red y los dispositivos administrados.
- MIB La base de información administrativa (Management Information Base) es la base de datos que almacena la información administrativa del sistema.
- SMI: La estructura e identificación de la información administrativa (Struture and Identification of Management Information) describe los objetos de la MIB.

Aunque SNMP fue diseñado para Internet, no depende de los protocolos TCP/IP y puede funcionar sobre varios protocolos de nivel inferior (por ejemplo IPX/SPX de Novell). Si se utiliza TCP/IP , SNMP se basa en el protocolo de datagramas UDP para reducir el tráfico en la red.

#### NFS: Sistema de archivos de red.

Desde el punto de vista de la informática distribuida, las limitaciones de FTP y Telnet dejan mucho que desear. Es posible utilizar FTP para transferir archivos y Telnet para ejecutar sesiones de terminal en una computadora remota, pero no para ejecutar una aplicación cuyos archivos de datos se encuentran en una computadora remota.

El sistema de arvhivos de red (NFS) es el equivalente TCP/IP de la capacidad para compartir archivos de los productos Microsoft. NFS fue desarrollado por Sun Microsystems, y muchos fabricantes disponen de licencias y lo han implementado en varias plataformas.

Un servidor NFS puede exportar parte de su árbol de directorios para uso de clientes NFS. Los clientes pueden montar los directorios exportados como si formaran parte del

su sistema de archivos nativo. Por ejemplo, los usuarios de DOS acceden al directorio exportado como si se tratara de una letra de unidad incluida en la estructura de archivos local de DOS.

NFS es un protocolo sofisticado y fiable que no utiliza el transporte TCP. Por razones de eficacia, NFS funciona sobre UDP. NFS implementa la seguridad, la fragmentación de mensajes y la recuperación de errores.

## **5.- Comandos de TCP/IP**

### **5.1 Utilidad Ping**

Sirve para enviar mensajes a una dirección de red concreta que se especifica como argumento, con el fin de realizar un test a la red. El nodo destinatario nos reenviará el paquete recibido para confirmarnos que se realiza el transporte entre los dos nodos correctamente. Además proporciona información sobre la red.

Ejemplos:

Ping	Muestra todas las posibles opciones de la instrucción
Ping 192.168.0.205	Envía y recibe las tramas enviadas a este host.
Ping 127.0.0.1	Envía y recibe tramas a sí mismo. Comprobación del funcionamiento de la tarjeta de red.
Ping -n 192.168.0.205	Envía y recibe tramas al host especificado durante n veces.

### **5.2 Utilidad Arp**

Se emplea para asignar direcciones IP a direcciones físicas, es decir, para gestionar el protocolo ARP.

Ejemplos:

Arp -a	muestra la tabla arp.
Arp -s 192.168.0.205	00-aa-00-62-c6-09 Añade una entrada estática

### **5.3 Utilidad hostname**

Devuelve el nombre del nodo en el que se ejecuta.

#### 5.4 Utilidad ipconfig

Configura la dirección del host, o bien proporciona información sobre la configuración actual.

Ejemplo:

Ipconfig /? -	Muestra las posibilidades de Ipconfig
Ipconfig	Muestra la dirección IP, mascara y puerta predeterminada
Ipconfig /all	muestra toda la información del host.

#### 5.5 Utilidad lpq

Se utiliza para preguntar por el estado de impresoras remotas que utilicen protocolo TCP/IP en sus comunicaciones.

#### 5.6 Utilidad nbtstat

Sirve para gestionar los nombres NetBios de nodos concretos.

Ejemplo:

Nbtstat	Lista de posibilidades de la instrucción
Nbtstat -n nombre de host	Lista de los nombres Netbios en un determinado host.

#### 5.7 Utilidad Netstat

Proporciona información sobre el estado de la red.

Ejemplo:

Netstat	Conexiones activas
Netstat -e	Información estadística de los sobre los paquetes de red enviados y recibidos
Netstat /?	Lista de comandos de la instrucción.

#### 5.8 Utilidad route

Sirve para determinar las rutas que deben seguir los paquetes de red.

Ejemplo:

Route	Lista de posibles opciones de la instrucción.
Route print	lista de los rutas disponibles en el host.

#### 5.9 Utilidad tracert

Se emplea para controlar los saltos de red que deben seguir los paquetes hasta alcanzar su destino. Además, proporciona información sobre los otros parámetros de la internet.

Ejemplo:

Tracert	Lista de posibles opciones de la instrucción
Tracert ds.internic.net.	Información para alcanzar la ruta de destino ds.internic.net.

### 5.10 Utilidad finger

Sirve para determinar si un usuario está presentando o no en un nodo TCP/IP.

Ejemplo:

Finger alfredo @128.100.10.2      Nos informa si el usuario “alfredo” se encuentra en el nodo 128.100.10.2

### 5.11 Utilidad FTP y Tftp

La utilidad ftp sirve para intercambiar ficheros entre dos nodos de red utilizando el protocolo FTP. Cuando se ejecuta ftp, aparece la marca “FTP>” sobre la que se ejecutan los comandos ftp: listar, traer, o dejar ficheros, etc. Previamente a la utilización del TFP es necesario hacer una conexión segura a través del protocolo TCP. Esto se realiza con el comando open, seguido de la dirección IP o el nombre DNS del host remoto.

El comando tftp es similar a ftp, pero más fácil de configurar.

### 5.12 Utilidad lpr

Se utiliza para enviar trabajos a las impresoras remotas que se especifican como argumentos.

### 5.13 Utilidad telnet

Sirve para realizar conexiones remotas interactivas en forma de terminal virtual a través del protocolo TELNET. El comando va acompañado de la dirección IP del nodo o de su dirección DNS.

### 5.14 ficheros HOSTS y LMHOSTS

En estos ficheros podemos configurar el nombre que queremos dar a cada uno de los hosts con dirección IP dentro de nuestra red.

Son ficheros de texto que se encuentran dentro del directorio de Windows en Windows 95 o Windows 98 y en c:\winnt\system32\drivers\etc. en Windows NT.

Simplemente hay que configurar el nombre deseado junto a su dirección IP correspondiente. Desde el momento que tengo este fichero configurado, puedo referirme a un nodo por su nombre en vez de hacerlo por su dirección IP.

Para que en todos los equipos de la red se empleen los mismos nombres, al arrancar cada equipo deberá copiar el fichero HOST de la máquina servidora a su directorio correspondiente.

(El otro sistema para dar nombre a los Host es DNS).