

Conociendo al Enemigo

# EL ATACANTE INFORMÁTICO

Protocolos de Comunicación  
Ambientes Operativos

DoS

Buffer Overflow

Exploits

Enumeración

## CAPÍTULO 2

PROTOCOLOS DE COMUNICACIÓN

Rookits

Virus

Criptografía

Metodologías y Estándares



Jhon Cesar Arango Serna

www.itforensic-la.com

# CAPITULO 2

---

## INTRODUCCIÓN

---

Una vez conocida los pasos utilizados por los atacantes informáticos, es necesario conocer en profundidad como funciona los diferentes protocolos de comunicación que intervienen en una conexión de red, este capítulo nos ayudara a entender los diferentes mecanismos que intervienen en una comunicación, la estructura de IPv4 e IPv6.

Sin duda al finalizar este tema, estará preparado para emprender el fascinante mundo de la Enumeración, tema que será tratado en el capítulo 4. No solo entenderá lo que es una dirección IP si no que también entenderá su estructura y sus diferentes cálculos que ayudan de forma ágil a dimensionar el tamaño de una red basada en TCP/IP.

### ***Modelo de Referencia OSI***

En 1980 Organización Internacional para la Estandarización (ISO), con sede en ginebra desarrollo un Modelo de Referencia para la Interconexión de los Sistemas Abiertos el cual le dio el nombre del modelo OSI. Este modelo separa las comunicaciones de red en siete niveles los cuales explican lo que sucede cuando un computador se desea comunicar con otro, cada computador utiliza una serie de protocolos para realizar las funciones asignadas a cada nivel. El conjunto de niveles forma lo que se conoce con el nombre de “pila de protocolos”.

En otras palabras, cuando dos computadores desean comunicarse entre si, una serie de modulo de software operan sobre cada sistema para garantizar la comunicación. Un modulo se asegura de formatear apropiadamente los datos para la transmisión, otro se encarga de la retransmisión de los paquetes perdidos y así sucesivamente. Cada uno de estos módulos es lo que llamamos Capa o Nivel.

Las capas del modelo OSI se muestran a continuación:

CAPA	NOMBRE	DESCRIPCION
7	Aplicación	Servicios de Red a Aplicaciones
6	Presentación	Representación de los Datos (ASCII)
5	Sesión	Comunicación de Dispositivos de Red
4	Transporte	Conexión Extremo a Extremo y Fiabilidad de los Datos
3	Red	Determinación de ruta IP
2	Enlace a Datos	Dirección Física (Mac y LLC)
1	Física	Señal y Transmisión Binaria

### ***Modelo de Referencia TCP/IP***

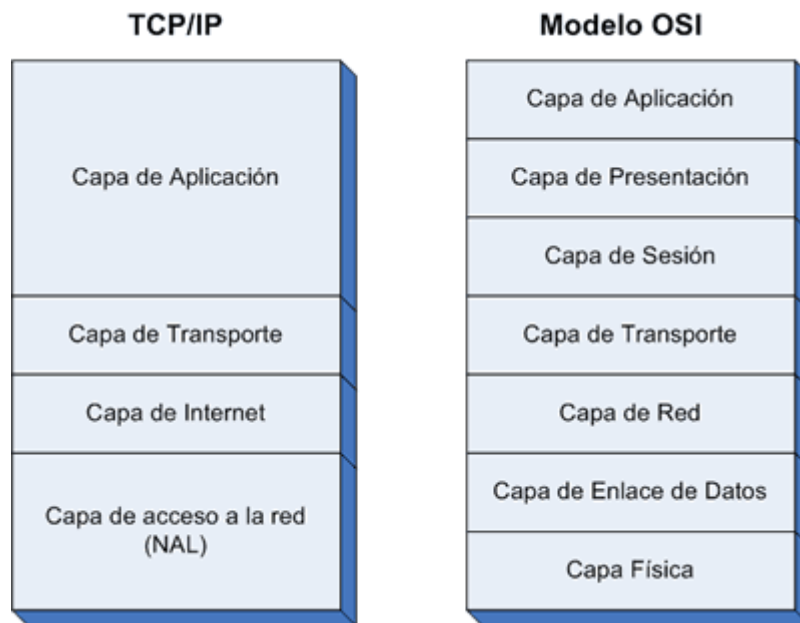
A mediados de los años sesenta el Departamento de Proyecto e Investigaciones Avanzadas para la Defensa de los EE.UU (ARPA o DARPA como se llamo más tarde) empezaron la investigación de para crear una red que enlazara los contratantes de ARPA. Los resultados no se hicieron esperar y a finales de los años 70 empezó a ver a luz lo que hoy conocemos con el nombre de TCP/IP. La RFC<sup>1</sup> 760, que describe el protocolo de Internet que se entrego al publico el 1 de enero de 1980, sufro luego

---

<sup>1</sup> [http://es.wikipedia.org/wiki/Request\\_For\\_Comments](http://es.wikipedia.org/wiki/Request_For_Comments)

modificaciones en los RFC 791, 793 y 768 los cuales integran el Protocolo de Control de Flujo (TCP) y el Protocolo de Datagramas de Usuario (UDP).

Los diseñadores de la familia de protocolos de TCP/IP eligieron un modelo más simple con menos niveles para mejorar el rendimiento y facilitar la implementación. Este modelo consta de 4 capas, a continuación se muestra el modelo TCP/IP comparado con el modelo OSI.



Para entender como atacan un sistema de cómputo a través de una red, necesitamos conocimientos del más popular de los protocolos, el TCP/IP ampliamente usado hoy en Internet. Este protocolo incluye varios componentes: el Protocolo de Control de Flujo (TCP), el Protocolo de Datagramas de Usuario (UDP), el Protocolo de Internet (IP) y Protocolo de Control de Mensajes de Internet (ICMP). Exploraremos ahora cada uno de estos protocolos.

### *Protocolo de Internet (IP)*

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser

distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos computadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos computadores con la misma dirección IP (privadas) siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

### Direcciones IP públicas.

Son visibles en todo Internet. Un computador con una IP pública es accesible (visible) desde cualquier otro computador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

### Direcciones IP privadas (reservadas).

Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por enrutadores (routers). Se utilizan en las empresas para los puestos de trabajo. Los computadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a computadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

### Direcciones IP estáticas (fijas).

Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas a través de un proveedor de servicios (ISP) o registrándolas directamente a través de <http://lacnic.net/sp/index.html>

### Direcciones IP dinámicas.

Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un Módem, Router Adsl, Router inalámbrico, Etc. Los proveedores de

Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

## Clases de Direcciones

Las direcciones IP versión 4 están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP 201.228.3.147.

Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en forma binaria, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Utilizando la calculadora científica de un computador podemos realizar las siguientes conversiones:

Decimal	201.228.3.147
Hexadecimal	C9.E4.3.93
Binario	11001001.11100100.00000011.10010011

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 (232) obtenemos 4,294,967,296 direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: la porción de red y la porción de host.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

### CLASE A

0	1	8	16	24	31
0	Red (7 bits)		Dirección local (24 bits)		

Su primer octeto en su forma binaria empieza por 0, por lo que una IP como: 00101001.11100010.01010101.10101010 se considera como una dirección de clase A.

En su forma decimal son todas aquellas que en su primer octeto están entre 0-127, si convertimos el ejemplo anterior tenemos: 41.226.85.170 lo que lo hace una IP de clase A.

#### CLASE B

0	1	2		15	16		31
10	Red (14 bits)				Dirección local (16 bits)		

Su primer octeto en su forma binaria empieza por 10, por lo que una IP como: 10101001.11100010.01010101.10101010 se considera como una dirección de clase B.

En su forma decimal son todas aquellas que en su primer octeto están entre 128-191, si convertimos el ejemplo anterior tenemos: 169.226.85.170 lo que lo hace una IP de clase B.

#### CLASE C

0	1	2	3		24	25		31
110	Red (21 bits)				Dirección local (8 bits)			

Su primer octeto en su forma binaria empieza por 110, por lo que una IP como: 11001001.11100010.01010101.10101010 se considera como una dirección de clase C.

En su forma decimal son todas aquellas que en su primer octeto están entre 192-223, si convertimos el ejemplo anterior tenemos: 201.226.85.170 lo que lo hace una IP de clase C.

#### CLASE D

Las direcciones de clase D son direcciones de IP de multidifusión los cuales se usan para enviar un único paquete de uno a muchos. Los 4 primeros bits se establecen al valor de 1110. los 28 restantes se usan para direcciones IP de multidifusión.

#### CLASE E

Las direcciones de clase E son direcciones experimentales, reservadas para usos futuros. Los primeros 5 bits se establecen al valor 11110.

Clase	Bits Red (m)	Número de redes (2 <sup>m</sup> )	Bits de Hosts (n)	Número de Host por red (2 <sup>n</sup> - 2)	Rango de direcciones de redes	Máscara de Subred
<b>A</b>	7	128	24	16.777.214	0.0.0.0 – 127.0.0.0	255.0.0.0
<b>B</b>	14	16.384	16	65.534	128.0.0.0 – 191.255.0.0	255.255.0.0
<b>C</b>	21	2.097.152	8	254	192.0.0.0 – 223.255.255.0	255.255.255.0
<b>D</b>		-		-	224.0.0.0 - 239.255.255.255	-
<b>E</b>		-		-	240.0.0.0 - 255.255.255.255	-

### Difusión (broadcast) y multidifusión (multicast).

El término difusión (broadcast) se refiere a todos los hosts de una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión (unicast) para referirse a un único host.

### Direcciones IP especiales y reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales.

Difusión o broadcasting es el envío de un mensaje a todos los computadores que se encuentran en una red. La dirección de loopback (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio computador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
<b>A</b>	10.0.0.0
<b>B</b>	172.16.0.0 - 172.31.0.0
<b>C</b>	192.168.0.0 - 192.168.255.0

Por ejemplo, si estamos construyendo una red privada con un número de computadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer computador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas,



tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros computadores podremos acceder a la totalidad de los servidores de Internet (si utilizásemos en un computador de nuestra red una dirección de un servidor de Internet, nunca podríamos acceder a ese servidor).

### Intranet.

Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

### Extranet.

Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, ADSL, punto a punto, etc.) o a través de Internet.

### Internet.

La mayor red pública de redes TCP/IP.

### Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred	Bits de Red
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

Si expresamos la máscara de subred de clase A en notación binaria, tenemos: 11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer

byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un computador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

$$\begin{array}{rcl}
 148.120.33.110 & = & 10010100.01111000.00100001.01101110 \\
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 \hline
 148.120.0.0 & = & 10010100.01111000.00000000.00000000 \\
 & & <-----\text{RED}-----><-----\text{HOST}----->
 \end{array}$$

Al hacer la operación AND entre la dirección IP y la Mascara (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera que se considera la dirección de RED.

Si hacemos lo mismo con otro computador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

$$\begin{array}{rcl}
 148.115.89.3 & = & 10010100.01110011.01011001.00000011 \\
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 \hline
 148.115.0.0 & = & 10010100.01110011.00000000.00000000
 \end{array}$$

Para calcular la dirección de Broadcast o Difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara, en otras palabras tomamos como una plantilla el numero de ceros que existe en la máscara, en nuestro ejemplo anterior son los 16 últimos bits.

$$\begin{array}{rcl}
 255.255.0.0 & = & 11111111.11111111.00000000.00000000 \\
 & & <-16 \text{ bits (16 Ceros)}->
 \end{array}$$

Con este valor de 16 bits, lo que hacemos en la dirección de red en su forma binaria es cambiar los últimos 16 dígitos a su base contraria, es decir lo que este en 0 sea 1 y viceversa.

$$\begin{array}{rcl}
 \text{Dr. de Red} & 148.115.0.0 & = 10010100.01110011.00000000.00000000 \\
 \text{Dr de Difus.} & 148.115.0.0 & = 10010100.01110011.11111111.11111111
 \end{array}$$

Para este caso podemos decir que la dirección de broadcast es forma decimal es: 148.115.255.255

En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un computador sabe si otro computador se

encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

Para cada clase de dirección IP corresponde mínimo una máscara obligatoria según los visto anteriormente, sin embargo es posible aumentar el número de bits en unos (1) de la máscara para realizar algo que se conoce con el termino de sub enmascaramiento. Esta técnica nació debido a que el direccionamiento IP versión 4 se está agotando, por tanto los proveedores de servicios de internet solo entregan un pequeño rango de IP publicas con las cuales la empresa debe sacar todas sus maquinas a internet utilizando técnicas de NAT.

Si retomamos el ejemplo anterior tenemos:

IP	148.115.89.3	=	10010100.01110011.01011001.00000011
Mas	255.255.0.0	=	11111111.11111111.00000000.00000000

Note que por su primer octeto (148) la dirección se considera de clase B y a su vez esta le corresponde una máscara obligatoria, la cual es 255.255.0.0.

El sub enmascaramiento consiste en cambiar a uno (1) los primeros bits de la porción de host (los ceros) de la máscara de subred. El numero de ceros que desee cambiar depende de el numero de subredes que quiera construir, si escoge 1 seria  $2^1$  lo que representaría 2 subredes, si escoge 2 seria  $2^2$  lo que representaría 4 subredes, si escoge 3 seria  $2^3$  lo que representaría 8 subredes y así sucesivamente. Sin importar la clase de dirección mínimo tiene que dejar dos ceros en la máscara cuando está haciendo sub enmascaramiento.

Supongamos que vamos a convertir 5 bits de la porción de host de la máscara del ejercicio anterior, lo cual nos daría una nueva mascara, una nueva dirección de red y una nueva dirección de broadcast:

Ip	148.115.89.3	=	10010100.01110011.01011001.00000011
Mas	255.255. <b>248</b> .0	=	11111111.11111111. <b>11111</b> 000.00000000
D.red	148.115. <b>88</b> .0	=	10010100.01110011.01011000.00000000
D.bro	148.115. <b>95.255</b>	=	10010100.01110011.01011 <b>111.11111111</b>

Con esta nueva mascara podemos deducir:

Se pueden tener  $2^{16}$  posibles redes, por cada una se puede construir  $2^5$  subredes y cada una puede albergar  $2^{11}$  posibles host.

---

## PRACTICA DE LABORATORIO

- Dada la dirección y la máscara de red hallar:
- Dirección de la Red
- Primera dirección de la Red
- Dirección de Broadcast
- Última dirección de Red

Dirección IP : 129.5.208.17  
Máscara de Red : 255.255.252.0

Para hallar la dirección de Red desarrollamos un AND entre la Dirección IP y la Máscara de Red en binario

IP : 10000001.00000101.11010000.00010001  
Máscara : 11111111.11111111.11111100.00000000  

---

10000001.00000101.11010000.00000000 \*

Al convertir a Decimal: Dirección de Red: 129. 5. 208. 0  
La primera dirección de red es la siguiente a la dirección de red:  
Primera Dirección de Red: 129. 5. 208. 1

Para averiguar la dirección de Broadcast, pasamos la máscara a binario:  
Máscara : 11111111.11111111.11111100.00000000

El posible número de Hosts es igual a  $2^n - 2$ , donde n es igual al número de ceros a la derecha de la máscara, en este caso  $n=10$ , luego el número posible de Hosts =  $2^{10} - 2 = 1022$ .

El número de posibles subredes es igual a  $2^{16-n} = 2^{16-10} = 2^6 = 64$   
Se pueden crear 64 subredes de 1022 Hosts cada una, para un total de Hosts de  $1022 \times 64 = 65408$

Luego convertimos el número de ceros en unos y unos en ceros, hasta n dígitos, tomando la AND de los últimos 16 dígitos de la dirección IP y los 16 dígitos de la máscara.

11010000.00010001 \*  
11010011.11111111, tenemos entonces así:  
211 . 255

Luego: La dirección de Broadcast es 129. 5. 211. 255

La última dirección de red es una menos que la de Broadcast  
La última dirección de Red es: 129. 5. 211 .254

---

## Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la trama Ethernet) de las distintas redes que va atravesando.

Cada vez que un datagrama tiene que atravesar un router, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ADSL, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.

0										10										20										30	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	3	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VERS				Long En		Tipo de servicio										Longitud total															
Identificación										Bandrs		Desplazamiento de fragmento																			
TTL						Protocolo						CRC cabecera																			
Dirección IP origen																															
Dirección IP destino																															
Opciones IP (si las hay)																								Relleno							
Datos																															
...																															

*VERS (Versión, 4 bits)* Indica la versión del protocolo IP que se utilizó para crear el paquete. Actualmente se utiliza la versión 4 (IPv4) aunque ya está implementándose la versión, la 6 (IPv6).

*Long En (Longitud del Encabezado, 4 bits)* Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.

*Tipo de servicio.* Los 8 bits de este campo se dividen a su vez en:

Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima. Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los enrutadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no. Bit D (Delay). Solicita retardos cortos (enviar rápido). Bit T (Throughput). Solicita un alto rendimiento (enviar mucho en el menor tiempo posible). Bit R (Reliability). Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien). Los siguiente dos bits no tienen uso.

*Longitud total (16 bits).* Indica la longitud total del paquete expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un paquete será de 65, 535 bytes.

*Identificación (16 bits).* Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un paquete en toda la red. Si se trata de un paquete fragmentado, llevará la misma identificación que el resto de fragmentos.

*Banderas o indicadores (3 bits).* Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más fragmentos (MF) indica que no es el último paquete. Y el bit de No fragmentar (NF) prohíbe la fragmentación del paquete. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.

*Desplazamiento de fragmentación (13 bits).* Indica el lugar en el cual se insertará el fragmento actual dentro del paquete completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.

*Tiempo de vida o TTL (8 bits).* Número máximo de saltos que puede estar un paquete en la red de redes. Cada vez que el paquete atraviesa un router se resta 1 a este número. Cuando llegue a cero, el paquete se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.

*Protocolo (8 bits).* Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.

*CRC cabecera (16 bits).* Contiene la suma de comprobación de errores sólo para la cabecera del paquete. La verificación de errores de los datos corresponde a las capas superiores.

*Dirección origen (32 bits).* Contiene la dirección IP del origen.

*Dirección destino (32 bits).* Contiene la dirección IP del destino.

*Opciones IP.* Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

*Relleno.* Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

*Datos.* Son los datos que se están transmitiendo

## Protocolo ICMP

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema:

		Tipo	Datos ICMP	
		↓	↓	
	Encabezado del datagrama	Área de datos del datagrama IP		
	↓		↓	
Encabezado de la trama	Área de datos de la trama			Final de la trama

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP<sup>2</sup>.

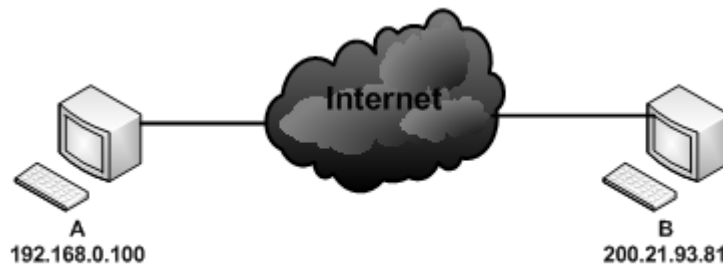
Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (Echo Reply)
3	Destino inaccesible (Destination Unreachable)
4	Disminución del tráfico desde el origen (Source Quench)
5	Redireccionar (cambio de ruta) (Redirect)
8	Solicitud de eco (Echo)
11	Tiempo excedido para un datagrama (Time Exceeded)
12	Problema de Parámetros (Parameter Problem)
13	Solicitud de marca de tiempo (Timestamp)
14	Respuesta de marca de tiempo (Timestamp Reply)
15	Solicitud de información (obsoleto) (Information Request)
16	Respuesta de información (obsoleto) (Information Reply)
17	Solicitud de máscara (Addressmask)
18	Respuesta de máscara (Addressmask Reply)

<sup>2</sup> El formato y significado de cada mensaje ICMP está documentado en la RFC 792 (en inglés, en español).

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden PING envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

A envía un mensaje ICMP de tipo 8 (Echo) a B  
B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (Echo Reply) a A  
A recibe el mensaje ICMP de B y muestra el resultado en pantalla



```
C:\Users\usuario>ping 200.21.94.81 -n 1

Haciendo ping a 200.21.94.81 con 32 bytes de datos:
Respuesta desde 200.21.94.81: bytes=32 tiempo=52ms TTL=244

Estadísticas de ping para 200.21.94.81:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 52ms, Máximo = 52ms, Media = 52ms
```

En la orden anterior hemos utilizado el parámetro "-n 1" para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (Time Exceeded).

```
C:\Users\usuario>ping 200.21.94.85 -n 1

Haciendo ping a 200.21.94.85 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 200.21.94.85:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```



Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los enrutadores no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (Destination Unreachable).

Pero también puede suceder que el equipo al que se le está haciendo Ping tenga deshabilitado las respuestas eco por cuestiones de seguridad:

```
C:\Users\usuario>ping www.unicauca.edu.co -n 1  
Haciendo ping a acuario.unicauca.edu.co [190.5.195.137] con 32 bytes de datos:  
Tiempo de espera agotado para esta solicitud.  
Estadísticas de ping para 190.5.195.137:  
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1  
    (100% perdidos),
```

En este ejemplo vemos como el DNS resuelve la IP sin problemas, pero el Ping no responde. Para estos casos hay que utilizar otros mecanismos como por ejemplo la apertura de conexión a un puerto, como veremos más adelante.

El comando Ping es ampliamente utilizado para diagnosticar errores en la red, que van desde la interfaz local de red a condiciones de red o equipos de comunicación de datos.

*Mensajes ICMP de tiempo excedido.* Los datagramas IP tienen un campo TTL (tiempo de vida - TDV) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (Time Exceeded) para informar al origen. Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario). El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.

## Puertos

Un computador puede estar conectado con distintos servidores a la vez; por ejemplo, con un servidor de noticias y un servidor de correo. Para distinguir las distintas conexiones dentro de un mismo computador se utilizan los puertos. Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada computador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known (bien conocidos). Estos puertos están definidos en la RFC 1700 y se pueden consultar en <http://www.ietf.org/rfc/rfc1700.txt>. A continuación se enumeran los puertos well-known más usuales:

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
<b>7</b>	TCP/UDP	echo	792
<b>20</b>	TCP	Protocolo de transferencia de archivos (FTP)	959
<b>21</b>	TCP	Control de FTP	959
<b>22</b>	TCP	Shell segura (SSH)	-
<b>23</b>	TCP	Telnet	854
<b>25</b>	TCP	Protocolo simple de transferencia de correo (SMTP)	5321
<b>53</b>	TCP/UDP	Sistema de nombres de dominio (DNS)	1034
<b>67</b>	UDP	Servidor de protocolo de inicio (BootP, bootps)	951
<b>68</b>	UDP	Cliente de protocolo de inicio (bootpc)	951
<b>69</b>	UDP	Protocolo trivial de transferencia de archivos (TFTP)	1350
<b>79</b>	TCP	Finger	1288
<b>80</b>	TCP	Protocolo de transferencia de hipertexto (HTTP)	2616
<b>88</b>	TCP	Kerberos	4120
<b>106</b>	TCP	Servidor de contraseñas (Uso no registrado)	-
<b>110</b>	TCP	Protocolo de oficina de correos (POP3) Protocolo de oficina de correos de autenticación (APOP)	1939
<b>111</b>	TCP/UDP	Llamada a procedimiento remoto (RPC)	1057, 1831
<b>113</b>	TCP	Protocolo de identificación	1413
<b>115</b>	TCP	Programa seguro de transferencia de archivos (SFTP)	913
<b>119</b>	TCP	Protocolo de transferencia de noticias de red (NNTP)	3977
<b>123</b>	TCP/UDP	Network Time Protocol (NTP)	1305
<b>137</b>	UDP	Windows Internet Naming Service (WINS)	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
<b>138</b>	UDP	Servicio de datagramas de NETBIOS	-
<b>139</b>	TCP	Bloque de mensaje de servidor (SMB)	-
<b>143</b>	TCP	Protocolo de acceso a mensajes de Internet (IMAP)	3501
<b>161</b>	UDP	Protocolo simple de administración de red (SNMP)	1157
<b>192</b>	UDP	-	-
<b>311</b>	TCP	Server Admin, Workgroup Manager, Server Monitor, Xsan Admin	-
<b>389</b>	TCP	Protocolo ligero de acceso a directorios (LDAP)	4511
<b>427</b>	TCP/UDP	Protocolo de ubicación de servicios (SLP)	2608
<b>443</b>	TCP	Capa de sockets seguros (SSL o "HTTPS")	-
<b>445</b>	TCP	Servidor de dominio SMB de Microsoft	-
<b>497</b>	TCP/UDP	Dantz Retrospect	-
<b>500</b>	UDP	ISAKMP/IKE	-
<b>514</b>	TCP	shell	-
<b>514</b>	UDP	Syslog	-
<b>515</b>	TCP	Impresora de línea (LPR), Protocolo LPD (Line Printer Daemon)	-
<b>532</b>	TCP	netnews	-
<b>548</b>	TCP	Protocolo de archivos de Apple (AFP) a través de TCP	-
<b>554</b>	TCP/UDP	Protocolo de secuencias en tiempo real (RTSP)	2326
<b>587</b>	TCP	Envío de mensajes para Mail (SMTP autenticado)	4409
<b>600-1023</b>	TCP/UDP	Servicios basados en RPC de Mac OS X	-
<b>623</b>	UDP	Lights-Out-Monitoring (LOM)	-
<b>625</b>	TCP	Directory Service Proxy (DSProxy) (Uso no registrado)	-
<b>626</b>	TCP	AppleShare Imap Admin (ASIA)	-
<b>626</b>	UDP	serialnumberd (Uso no registrado)	-
<b>631</b>	TCP	Protocolo de impresión de Internet (IPP)	2910
<b>636</b>	TCP	LDAP seguro	-
<b>660</b>	TCP	MacOS Server Admin	-
<b>687</b>	TCP	Agregar Server Admin a usos	-
<b>749</b>	TCP/UDP	Kerberos 5 admin/changepw	-
<b>985</b>	TCP	Puerto estático NetInfo	-
<b>993</b>	TCP	Mail IMAP SSL	-
<b>995</b>	TCP/UDP	Mail POP SSL	-
<b>1085</b>	TCP/UDP	WebObjects	-
<b>1099 &amp; 8043</b>	TCP	RMI remoto y Acceso IIOP a JBOSS	-
<b>1220</b>	TCP	QT Server Admin	-
<b>1649</b>	TCP	IP Failover	-
<b>1701</b>	UDP	L2TP	-
<b>1723</b>	TCP	PPTP	-
<b>2049</b>	TCP/UDP	Sistema de archivos de red (NFS) (versión 3)	1094
<b>2236</b>	TCP	Macintosh Manager (Uso no registrado)	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
<b>2336</b>	TCP	Directorios de inicio portátiles	
<b>3004</b>	TCP	iSync	-
<b>3031</b>	TCP/UDP	Eventos de Apple Remote	-
<b>3283</b>	TCP/UDP	Asistente de red	-
<b>3306</b>	TCP	MySQL	-
<b>3632</b>	TCP	Compilador distribuido	-
<b>3659</b>	TCP/UDP	Autenticación simple y capa de seguridad (SASL)	-
<b>3689</b>	TCP	Protocolo de acceso de audio digital (DAAP)	-
<b>4111</b>	TCP	XGrid	-
<b>4500</b>	UDP	IKE NAT Traversal	-
<b>49152-65535</b>	TCP	Xsan	-
<b>5003</b>	TCP	FileMaker: transporte y enlace de nombres	-
<b>5009</b>	TCP	(Uso no registrado)	-
<b>5060</b>	UDP	Protocolo de iniciación de sesión (SIP)	3261
<b>5100</b>	TCP	-	-
<b>5190</b>	TCP/UDP	America Online (AOL)	-
<b>5222</b>	TCP	Jabber  (Uso no registrado)	-
<b>5223</b>	TCP	Servidor iChat SSL/XMPP	-
<b>5269</b>	TCP	Comunicación servidor a servidor de iChat	-
<b>5297</b>	TCP	-	-
<b>5298</b>	TCP/UDP	-	-
<b>5353</b>	UDP	DNS de difusión múltiple (MDNS)	-
<b>5354</b>	TCP	Respondedor DNS de difusión múltiple	-
<b>5432</b>	TCP	Base de datos de ARD 2.0	-
<b>5678</b>	UDP	Servidor SNATMAP	-
<b>5897-5898</b>	UDP	(Uso no registrado)	-
<b>5900</b>	TCP	Computación en red virtual (VNC)  (Uso no registrado)	-
<b>5988</b>	TCP	WBEM HTTP	-
<b>6970-9999</b>	UDP	-	-
<b>7070</b>	TCP	RTSP (Uso no registrado)  Protocolo de configuración de router automático (ARCP - Uso registrado)	-
<b>7070</b>	UDP	RTSP alternativo	-
<b>7777</b>	TCP	Proxy de transferencia de archivos del servidor iChat	-
<b>8005</b>	TCP	Apagado remoto Tomcat	-
<b>8080</b>	TCP	Puerto alternativo para Apache	-
<b>8170</b>	TCP	HTTPS (servicio o sitio web)	-
<b>8175</b>	TCP	Pcast Tunnel	-

Puerto	TCP o UDP	Nombre de protocolo o servicio	RFC
<b>8000-8999</b>	TCP	-	-
<b>8821</b>	TCP	Almacenado (almacena servidor para comunicarse con el servidor)	-
<b>8891</b>	TCP	Idsd (transferencias de datos)	-
<b>9006 &amp; 8080 &amp; 8443</b>	-	Puertos HTTP y HTTPS para Tomcat Standalone y JBOSS (J2EE)	-
<b>16080</b>	TCP	-	-
<b>16384-16403</b>	UDP	Protocolo de transferencia en tiempo real (RTP), Protocolo de control en tiempo real (RTCP)	-
<b>24000-24999</b>	TCP	-	-
<b>42000-42999</b>	TCP	-	-
<b>50003</b>	-	Servicio de servidor de FileMaker	-
<b>50006</b>	-	Servicio de aplicación auxiliar de FileMaker	-

Los puertos tienen una memoria intermedia (buffer) situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

Los dos protocolos principales de la capa de transporte son UDP y TCP. El primero ofrece una transferencia de mensajes no fiable y no orientada a conexión y el segundo, una transferencia fiable y orientada a conexión.

Para conocer los puertos que puede utilizar su equipo puede editar los archivos “services”, estos se encuentra en el caso de Linux en el directorio /etc, para el caso de Windows los encuentra en el directorio c:\windows\system32\drivers.

## Protocolo UDP

El protocolo UDP (User Datagram Protocol, protocolo de datagrama de usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos computadores. Al igual que el protocolo IP, UDP es: No orientado a conexión. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino. También involucra que puedan perderse o que lleguen dañados por los que se considera un protocolo No fiable

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

		Encabezado UDP	Área de datos UDP	
		↓	↓	
	Encabezado del datagrama	Área de datos del datagrama IP		
	↓		↓	
Encabezado de la trama	Área de datos de la trama			Final de la trama

### *Formato del mensaje UDP*

0										10										20										30									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Puerto UDP origen															Puerto UDP destino																								
Longitud mensaje UDP															Suma verificación UDP																								
Datos																																							
...																																							

Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.

Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.

Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.

Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.

Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la Red de redes.

## Protocolo TCP

El protocolo TCP (Transmission Control Protocol, protocolo de control de transmisión) está basado en IP, es Orientado a conexión. Por lo que es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir algún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

Se considera Fiable ya que la información que envía el emisor llega de forma correcta al destino. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viajan por un circuito virtual. Sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los enrutadores intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logró la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que los todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el byte, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes. Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un segmento y se envía el segmento completo. Para ello son necesarias unas memorias intermedias o buffers. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

El protocolo TCP envía un flujo de información no estructurado. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

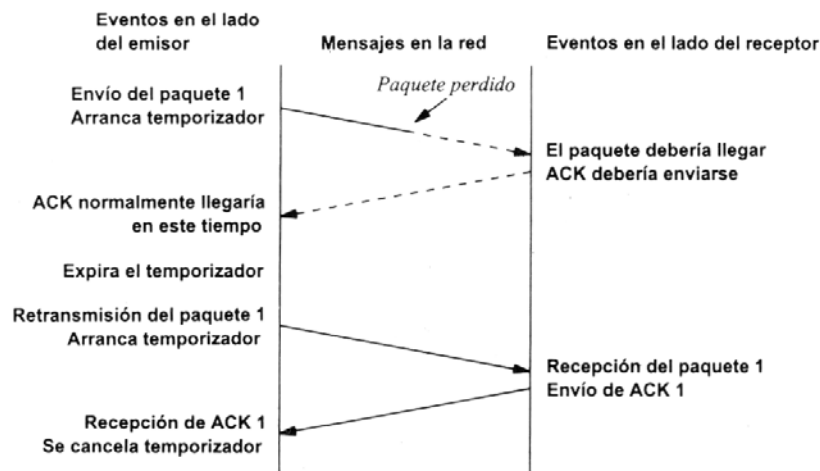
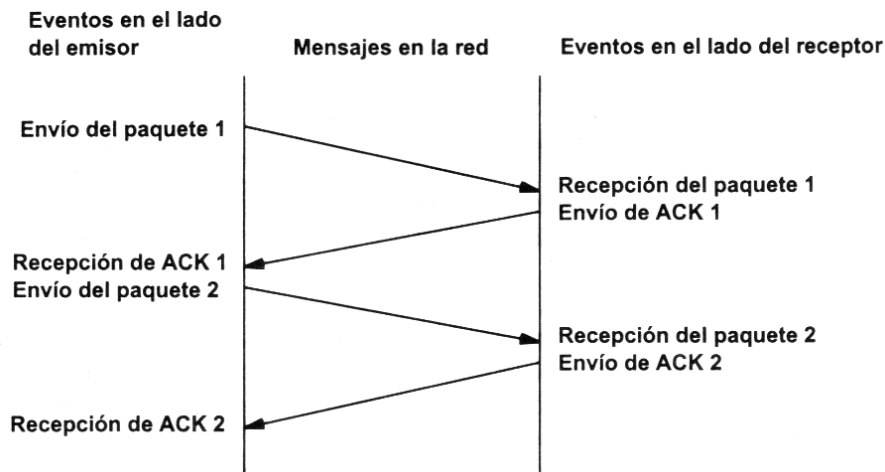
Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es full-dúplex.

## Fiabilidad

¿Cómo es posible enviar información fiable basándose en un protocolo no fiable? Es decir, si los datagramas que transportan los segmentos TCP se pueden perder, ¿cómo pueden llegar los datos de las aplicaciones de forma correcta al destino?

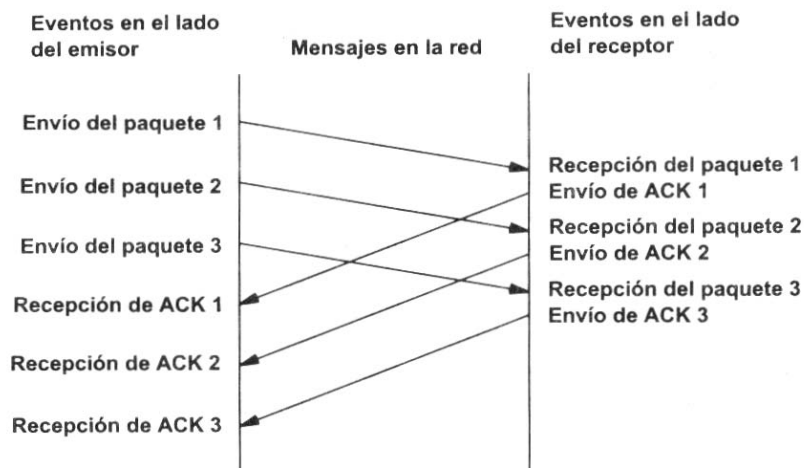
La respuesta a esta pregunta es sencilla: cada vez que llega un mensaje se devuelve una confirmación (acknowledgement) para que el emisor sepa que ha llegado correctamente. Si no le llega esta confirmación pasado un cierto tiempo, el emisor reenvía el mensaje.

Veamos a continuación la manera más sencilla (aunque ineficiente) de proporcionar una comunicación fiable. El emisor envía un dato, arranca su temporizador y espera su confirmación (ACK). Si recibe su ACK antes de agotar el temporizador, envía el siguiente dato. Si se agota el temporizador antes de recibir el ACK, reenvía el mensaje. Los siguientes esquemas representan este comportamiento:





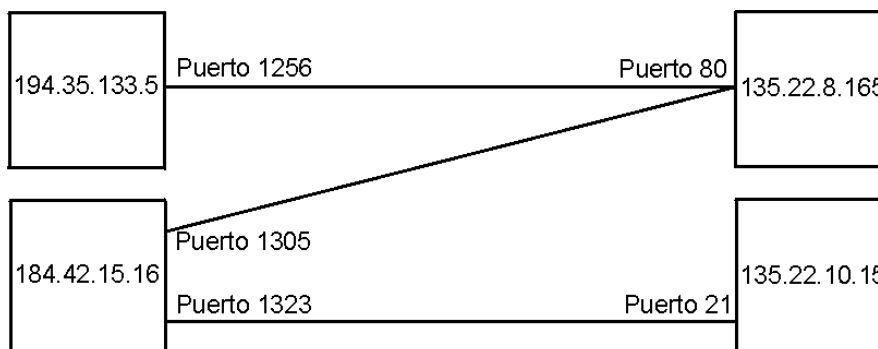
Este esquema es perfectamente válido aunque muy ineficiente debido a que sólo se utiliza un sentido de la comunicación a la vez y el canal está desaprovechado la mayor parte del tiempo. Para solucionar este problema se utiliza un protocolo de ventana deslizante, que se resume en el siguiente esquema. Los mensajes y las confirmaciones van numerados y el emisor puede enviar más de un mensaje antes de haber recibido todas las confirmaciones anteriores.



## Conexiones

Una conexión son dos pares dirección IP y Puerto. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que un mismo computador tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones. En el siguiente ejemplo se han creado tres conexiones. Las dos primeras son al mismo servidor Web (puerto 80) y la tercera a un servidor de FTP (puerto 21).

PC 1	PC 2
194.35.133.5:1256	135.22.8.165:80
184.42.15.16:1305	135.22.8.165:80
184.42.15.16:1323	135.22.10.15:21



Para que se pueda crear una conexión, el extremo del servidor debe hacer una apertura pasiva del puerto (escuchar su puerto y quedar a la espera de conexiones) y el cliente, una apertura activa en el puerto del servidor (conectarse con el puerto de un determinado servidor).<sup>3</sup>

### Formato del segmento TCP

Ya hemos comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión.

Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta. Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe).

0										10										20										30									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Puerto TCP origen															Puerto TCP destino																								
Número de secuencia																																							
Número de acuse de recibo																																							
HLEN				Reservado				Bits código								Ventana																							
Suma de verificación															Puntero de urgencia																								
Opciones (si las hay)																								Relleno															
Datos																																							
...																																							

*Puerto TCP origen (16 bits).* Puerto de la máquina origen. Al igual que el puerto destino es necesario para identificar la conexión actual.

*Puerto TCP destino (16 bits).* Puerto de la máquina destino.

*Número de secuencia (32 bits).* Indica el número de secuencia del primer byte que transporta el segmento.

*Número de acuse de recibo (32 bits).* Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente.

*HLEN (4 bits).* Longitud de la cabecera medida en múltiplos de 32 bits (4 bytes). El valor mínimo de este campo es 5, que corresponde a un segmento sin datos (20 bytes).

<sup>3</sup> El comando NetStat muestra las conexiones abiertas en un computador, así como estadísticas de los distintos protocolos de Internet.

*Reservado (6 bits).* Bits reservados para un posible uso futuro.

*Bits de código o indicadores (6 bits).* Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.

- URG. El campo Puntero de urgencia contiene información válida.
- ACK. El campo Número de acuse de recibo contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.
- PSH. La aplicación ha solicitado una operación push (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).
- RST. Interrupción de la conexión actual.
- SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (veremos que no tiene porqué ser el cero).
- FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.

*Ventana (16 bits).* Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino.

*Suma de verificación (24 bits).* Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino.

*Puntero de urgencia (8 bits).* Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo Datos que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).

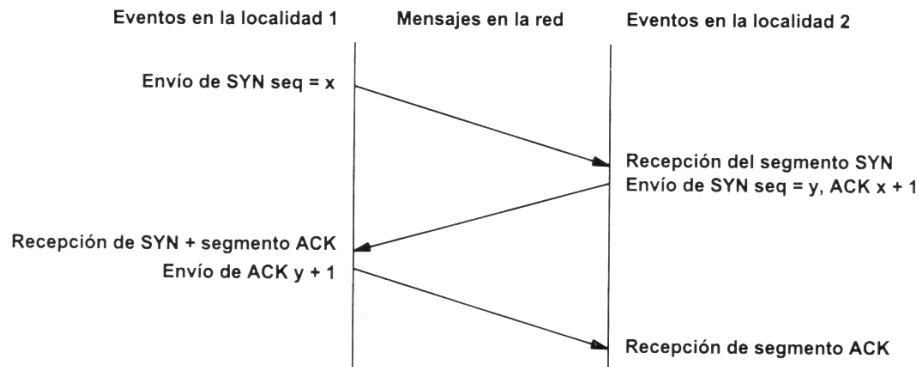
*Opciones (variable).* Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.

*Relleno.* Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.

*Datos.* Información que envía la aplicación.

## Establecimiento de una conexión

Antes de transmitir cualquier información utilizando el protocolo TCP es necesario abrir una conexión. Un extremo hace una apertura pasiva y el otro, una apertura activa. El mecanismo utilizado para establecer una conexión consta de tres vías.



La máquina que quiere iniciar la conexión hace una apertura activa enviando al otro extremo un mensaje que tenga el bit SYN activado. Le informa además del primer número de secuencia que utilizará para enviar sus mensajes.

La máquina receptora (un servidor generalmente) recibe el segmento con el bit SYN activado y devuelve la correspondiente confirmación. Si desea abrir la conexión, activa el bit SYN del segmento e informa de su primer número de secuencia. Deja abierta la conexión por su extremo.

La primera máquina recibe el segmento y envía su confirmación. A partir de este momento puede enviar datos al otro extremo. Abre la conexión por su extremo.

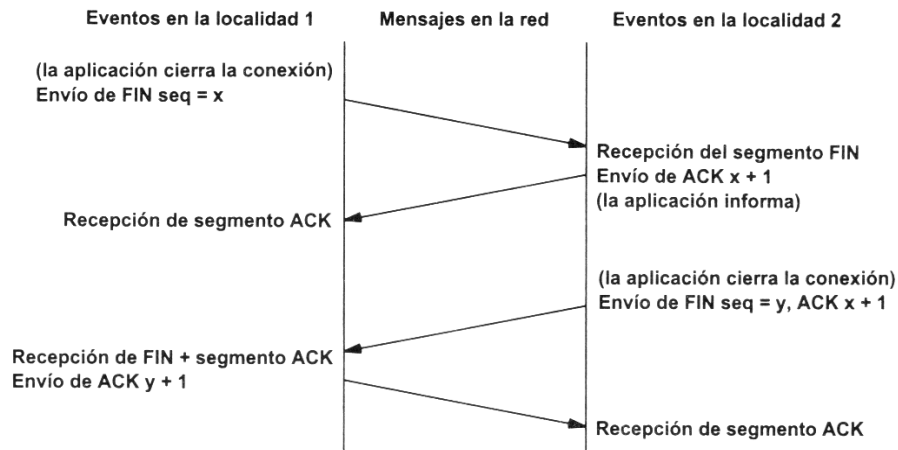
La máquina receptora recibe la confirmación y entiende que el otro extremo ha abierto ya su conexión. A partir de este momento puede enviar ella también datos. La conexión ha quedado abierta en los dos sentidos.

Observamos que son necesarios 3 segmentos para que ambas máquinas abran sus conexiones y sepan que la otra también está preparada.

*Números de secuencia* - Se utilizan números de secuencia distintos para cada sentido de la comunicación. Como hemos visto el primer número para cada sentido se acuerda al establecer la comunicación. Cada extremo se inventa un número aleatorio y envía éste como inicio de secuencia. Observamos que los números de secuencia no comienzan entonces en el cero. ¿Por qué se procede así? Uno de los motivos es para evitar conflictos: supongamos que la conexión en un computador se interrumpe nada más empezar y se crea una nueva. Si ambas han empezado en el cero es posible que el receptor entienda que la segunda conexión es una continuación de la primera (si utilizan los mismos puertos).

## Cierre de una conexión

Cuando una aplicación ya no tiene más datos que transferir, el procedimiento normal es cerrar la conexión utilizando una variación del mecanismo de 3 vías explicado anteriormente.



El mecanismo de cierre es algo más complicado que el de establecimiento de conexión debido a que las conexiones son full-duplex y es necesario cerrar cada uno de los dos sentidos de forma independiente.

La máquina que ya no tiene más datos que transferir, envía un segmento con el bit FIN activado y cierra el sentido de envío. Sin embargo, el sentido de recepción de la conexión sigue todavía abierto.

La máquina receptora recibe el segmento con el bit FIN activado y devuelve la correspondiente confirmación. Pero no cierra inmediatamente el otro sentido de la conexión sino que informa a la aplicación de la petición de cierre. Aquí se produce un lapso de tiempo hasta que la aplicación decide cerrar el otro sentido de la conexión.

La primera máquina recibe el segmento ACK.

Cuando la máquina receptora toma la decisión de cerrar el otro sentido de la comunicación, envía un segmento con el bit FIN activado y cierra la conexión.

La primera máquina recibe el segmento FIN y envía el correspondiente ACK. Observemos que aunque haya cerrado su sentido de la conexión sigue devolviendo las confirmaciones.

La máquina receptora recibe el segmento ACK.

## *IPv6 (Protocolo de Internet versión 6)*

Surge ante la necesidad de crear un protocolo para la nueva generación de Internet que brinde solución o mejora a los problemas que IPv4 (Protocolo utilizado actualmente) posee y que no fueron tomados en cuenta en el momento de su creación a principios de los años 70. (Escasez de direcciones, ineficiente ruteo y falta de seguridad).

Uno de los grandes inconvenientes de la implementación de IPv6, consiste en la transición de redes soportadas en IPv4 a redes que soporten IPv6. Tunneling o túneles surge como mecanismo básico de transición al IPv6 con la menor interrupción posible. La idea básica de tunneling consiste en encapsular paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4. Una vez implementadas redes IPv6 se debe instalar y configurar servicios de red como DHCPv6, DNSv6 y HTTPv6.

### Motivos de Ipv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), es la necesidad de crear un nuevo protocolo, ante la falta de direcciones. Ipv4 tiene un espacio de direcciones de 32 bits, es decir, 2<sup>32</sup> (4.294.967.296); en cambio, Ipv6 nos ofrece un espacio de 2<sup>128</sup>:

(340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo Ipv4 tiene otros problemas o dificultades que Ipv6 solucione o mejore. Los creadores de Ipv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no solo científicos y de educación, sino también en innumerables facetas de la vida cotidiana. Ipv4 presenta varios problemas:

- Escaso direccionamiento, junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos.
- Gran dimensión de las tablas de enrutamiento en el troncal de Internet, que la hace ineficiente, y perjudica enormemente los tiempos de respuesta.
- Imposibilidad práctica de muchas aplicaciones que quedan relegadas a su uso en intranet ya que muchos protocolos no soportan atravesar dispositivos NAT
- (solución temporal a la escasez de direcciones IP).
- No es escalable.

El crecimiento de Internet esperado en los próximos años es enorme, aparte del aumento de internautas a nivel mundial, tenemos el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto Enrutadores, Videoconferencia, Voz sobre IP, seguridad, e incluso juegos. También dispositivos de la red y los innumerables dispositivos que se van creando, o los ya existentes que se le dan nuevas o mejoradas aplicaciones, mediante su conexión a la red.

Algunos ejemplos:

- Teléfonos IP
- Radio y Televisión basados en tecnologías IP.
- Sistemas de seguridad, tele vigilancia y control.
- Refrigeradores que evalúan nuestros hábitos de consumo y nos permiten incluso navegar por un supermercado virtual y llenar nuestro carro según nuestras necesidades.
- Despertadores que conocen nuestros tiempos de desplazamiento habituales y nos pueden informar del estado del tiempo, tráfico etc... mediante servicios de la red.
- Nuevas tecnologías emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc... hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere.
- En general, casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también dispositivos de control médico, marcapasos, etc.

### Características principales de IPv6:

- Mayor espacio de direcciones.
- “Plug and Play”: autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los Router alineados a 64 bits.
- Posibilidad de paquetes con carga útil de más de 65.535 bytes.
- Enrutado más eficiente en el troncal de la red debido a una jerarquía de direccionamiento basada en la agregación.
- Características de movilidad.
- Escalabilidad.

## Especificaciones básicas de Ipv6

### *Datagrama*



La longitud de esta cabecera es de 32 bytes, el doble que en el caso de Ipv4, pero con muchas ventajas, al haberse eliminado campos redundantes. Además, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones. Los campos estas alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera Ipv6.

La MTU (Unidad Máxima de Transmisión), debe ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños mayores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

Dado que Ipv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo de su propio mecanismo de checksum<sup>4</sup>.

---

4 RFC 2460, Internet Protocol Version 6(IPv6) Specification (Disponible en Internet [www.ietf.org/rfc/rfc2460.txt](http://www.ietf.org/rfc/rfc2460.txt))

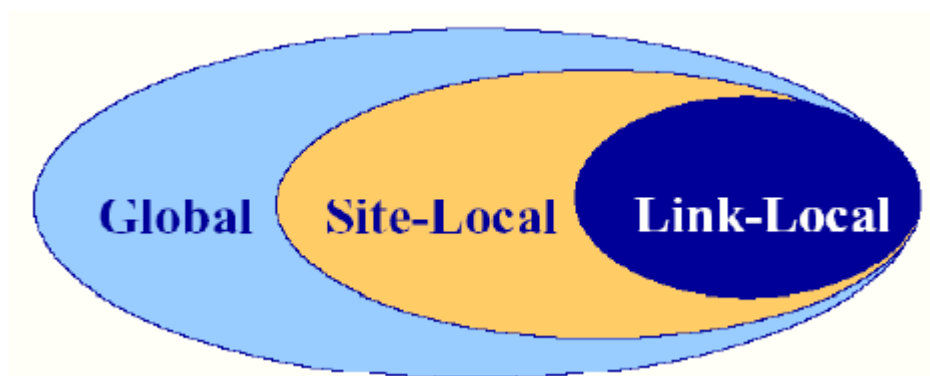


## Direcciones IPv6

Las direcciones IPv6 son identificadores de 128 bits que se asignan a interfaces lógicas, una interfaz puede tener muchas direcciones. Las direcciones tienen ámbitos de acción local link, site local y global.

La representación de las direcciones Ipv6 se realiza mediante 8 grupos de 16 bits en valor hexadecimal separados por ":" ejemplo:

FEDC:BA98:76FA:3210:BA14:417A:FECB



Estas direcciones se clasifican en 3 tipos<sup>5</sup>:

*Unicast*: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con dicha dirección. (es el equivalente a las actuales direcciones Ipv4). Puede ser usada en un ámbito global como dirección pública de Internet y también como dirección local en una red local, para esto se han definido dos tipos de direcciones unicast de uso local: local de enlace (Link Local) y local de sitio (Site Local).

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers. Por tanto, los enrutadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Sus primeros 10 bits [1111111010], seguido de 54 bits [0000...] y por último 64 bits del identificador de interfaz. Por tanto se trata de direcciones:

**FE80::<ID de interfaz>/10.**

---

<sup>5</sup> The TCP/IP Guide A comprehensive, Illustrated Internet Protocols Reference, Capítulo 25 IPv6 addressing, Charles M. Kozierok, Octubre del 2005. (disponible en [internetnostarch.com/download/tcpip\\_ch25.pdf](http://internetnostarch.com/download/tcpip_ch25.pdf))

Las direcciones locales de sitio permiten direccional dentro de un “sitio” local u organización, sin necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los enrutadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea “local de sitio” (su ámbito esta limitado a la red local o de la organización). Sus primeros 10 bits [1111111011] seguidos de 38 bits[000...] seguidos de 16 bits [ID de subred] y por ultimo 64 bits del identificador de interfaz. Por tanto se trata de direcciones:  
FEC0::<ID subred>:<ID de interfaz>/10.

*Anycast:* Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la mas próxima, de acuerdo a las medidas de distancia del protocolo de enrutamiento).

*Multicast:* Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es hacer broadcast. Los primeros 8 bits [11111111], los siguientes 4 bits [000T], los siguientes 4 bits [ámbito] y por ultimo 112 bits [identificador de grupo]. El bit T significa, si su valor es 0, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es 1, significa que se trata de una dirección multicast temporal.

El “identificador de grupo” identifica el grupo concreto al que nos referimos dentro de un determinado ámbito. Los bits “ámbito” tienen los siguientes significados:

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

Direcciones especiales.

Ipv6 maneja ciertas direcciones especiales como:

- Dirección de loopback (::1).
- Dirección no especificada (::)
- Dirección túneles dinámicos/automáticos de Ipv6 sobre Ipv4 (::<dirección Ipv4>).

La representación de los prefijos Ipv6 se realiza así: dirección Ipv6/longitud del prefijo(valor decimal que indica cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo). Ejemplo: 12ab::cd30:0:0:0/60

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Direcciones locales de enlace para cada interfaz.
- Direcciones unicast asignadas.
- Dirección de loopback.
- Direcciones multicast de todos los nodos.
- Direcciones multicast solicitadas para cada dirección unicast o anycast asignadas.
- Direcciones multicast de todos los grupos a los que dicho host pertenece.
- En el caso de los routers también se tienen que reconocer:
- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router.
- Todas las direcciones anycast con las que el router ha sido configurado.
- Las direcciones multicast de todos los routers.
- Las direcciones multicast de todos los grupos a los que el router pertenece.

## Mecanismos de Transición<sup>6</sup>

Para coexistir con una infraestructura Ipv4 y proveer una eventual transición a una infraestructura Ipv6, son usados los siguientes mecanismos: Ipv4 e Ipv6 al tiempo y túneles Ipv6 sobre Ipv4.

### IPv4 e IPv6 al tiempo

Durante el tiempo que una infraestructura de red hace su transición de IPv4, a IPv4/IPv6, y finalmente a una red IPv6 pura, los host deben tener la posibilidad de alcanzar sus destinos ya sea utilizando IPv4 o IPv6. Esto es gracias a que los host puedan soportar ambos protocolos IPv4 e IPv6.

---

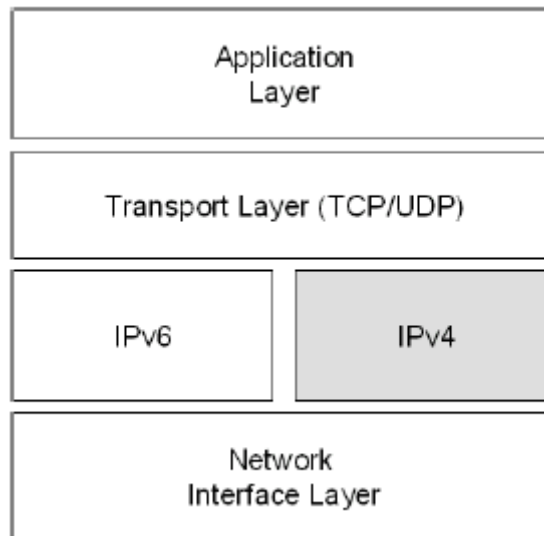
<sup>6</sup> IPv6 Transition Technologies, Microsoft Corporation, enero del 2007 (disponible en internet [www.microsoft.com/downloads](http://www.microsoft.com/downloads))

Para que esto sea posible los host deben tener las siguientes arquitecturas:

- Arquitectura de doble capa IP
- Arquitectura de doble pila.

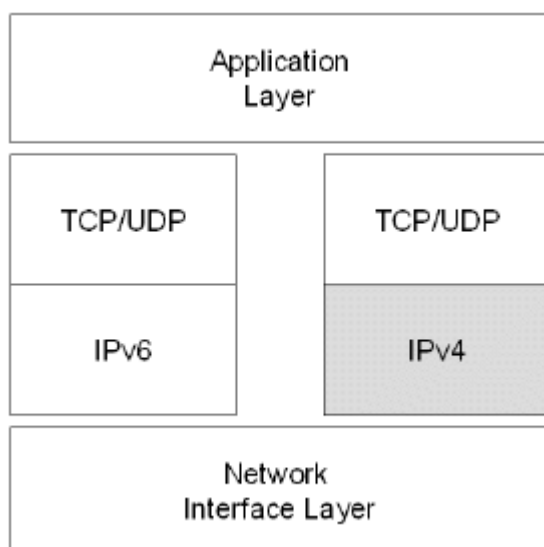
#### *Arquitectura de doble capa IP*

Una arquitectura de doble capa IP contiene ambos protocolos IPv4 e IPv6 con una única implementación de protocolos de la capa de transporte como TCP y UDP.



#### *Arquitectura de doble pila.*

Una arquitectura de doble pila contiene ambos protocolos IPv4 e IPv6 en pilas de protocolos separados que contienen implementaciones separadas de la capa de transporte como TCP y UDP.



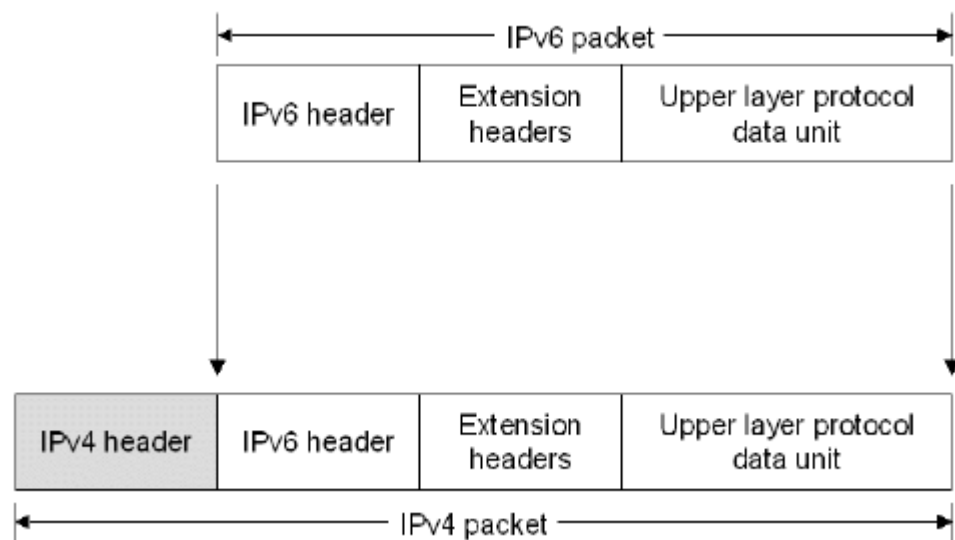
## IPv6 sobre IPv4 Tunneling

IPv6 sobre IPv4 tunneling es la encapsulación de paquetes IPv6 en un encabezado IPv4, para permitir que los paquetes IPv6 puedan ser enviados a través de un paquete IPv4.

Características del paquete IPv4:

El campo del protocolo IPv4 se identificara con 41 para indicar que es encapsulado con un paquete IPv6.

Los campos fuente y destino contiene las direcciones IPv4 de los puntos finales del túnel. Los puntos finales del túnel pueden ser configurados como parte de la interface del túnel o se generan automáticamente de la dirección de siguiente salto que coincida con la ruta de destino y la interface del túnel.

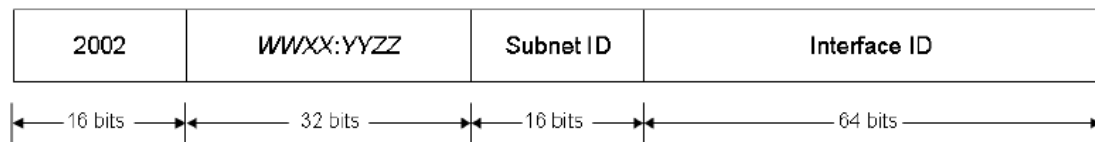


### *6to4 (RFC 3056)*

6to4 es un asignador de direcciones y una tecnología automática de túneles (router-a-router, host-a-router, y router-a-host). Provee conectividad unicast entre sitios y hosts IPv6 a través de una red IPv4.

6to4 toma toda la red IPv4 como un solo enlace.

6to4 utiliza un prefijo global 2002:WWXX:YYZZ::/48, en el cual WWXX:YYZZ es la representación hexadecimal de la dirección IPv4 (w.x.y.z) asignada a el sitio o a el host.



*Host 6to4:* no requiere ninguna configuración manual, crea direcciones 6to4 usando un estándar de auto configuración de direcciones. Los hosts 6to4 no ejecutan túneles IPv6 sobre IPv4. Usa las siguientes rutas:

1. una ruta de enlace para el prefijo de la subred de la interfaz LAN. En nuestro ejemplo será 2002:9D3C:1:1::/64 .
2. una ruta por defecto que usa la interfaz LAN y tiene la dirección del siguiente salto de un router 6to4, esta ruta permite que los host 6to4 puedan ver otros host 6to4 u otros sitios en la red IPv6. en nuestro ejemplo sera ::/0.

*Router 6to4:* son enrutadores IPv6/IPv4 que usan una interface de túnel 6to4 para reenviar trafico de direcciones 6to4 entre hosts 6to4 dentro de un sitio y a otros enrutadores 6to4, estos enrutadores requieren una configuración adicional. Usa las siguientes rutas:

1. una ruta de enlace para el prefijo de la subred de la interfaz LAN. Esta ruta permite que el router 6to4 pueda enviar tráfico desde y hacia hosts 6to4 en la subred. En nuestro ejemplo será 2002:9D3C:1:1::/64 .
2. una ruta de enlace para el prefijo de la dirección 6to4 (2002::/16) que use la interface de túnel 6to4. esta ruta permite que el router 6to4 pueda crear un túnel router-a-router para alcanzar otros 6to4 routers.
3. una ruta que use la interfaz de túnel 6to4 y tenga el siguiente salto de dirección 6to4. esta ruta permite que el enrutador 6to4 envíe tráfico IPv6 a destinos IPv6 en la red IPv6. ::/0.<sup>7</sup>

<sup>7</sup> RFC 3056, Connection of IPv6 Domains via IPv4 Clouds (disponible en Internet [www.ietf.org/html/rfc2460](http://www.ietf.org/html/rfc2460))

## ARP

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo. El protocolo de resolución de direcciones es responsable de convertir las direcciones de protocolo de alto nivel(direcciones IP) a direcciones de red físicas. Consideremos algunos aspectos generales acerca de Ethernet.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.

Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

### ARP y subredes

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

- Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
- Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Cuando un router necesita enviar un paquete a un host a través de otro router.
- Cuando un router necesita enviar un paquete a un host de la misma red.

## Tablas ARP

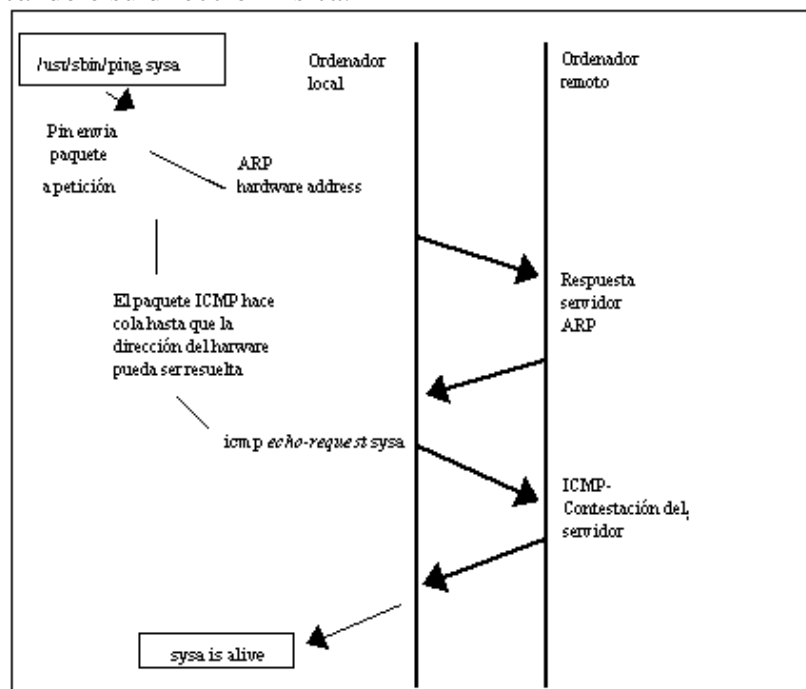
La filosofía es la misma que tendríamos para localizar al señor X entre 150 personas: preguntar por su nombre a todo el mundo, y el señor X nos responderá. Así, cuando a A le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su frame ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física. En este momento A ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla)

### Funcionamiento I

Si A quiere enviar un frame a la dirección IP de B (misma red), mirará su tabla ARP para poner en la frame la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos el frame, no tendrán que deshacer el frame para comprobar si el mensaje es para ellos, sino que se hace con la dirección física.

### Funcionamiento II

Si A quiere enviar un mensaje a C (un nodo que no este en la misma red), el mensaje deberá salir de la red. Así, A envía el frame a la dirección física del router de salida. Esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP. Si esta entrada no esta en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.





Una vez en el router, éste consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por el interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Aquí el proceso cambia: el interfaz del router tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP o preguntando a todos.

### Comprobación de las tablas ARP

En ciertas ocasiones, es útil poder ver o alterar el contenido de las tablas ARP del núcleo, por ejemplo, cuando se sospecha que una dirección IP duplicada es la causa de algún problema intermitente en la red. La herramienta arp se hizo para situaciones como ésta. Sus opciones son:

- Arp [-v] [-t tipohw] -a [hostname]
- Arp [-v] [-t tipohw] -s [hostname] dirección hardware
- Arp [-v] -d máquina [hostname]

Todos los argumentos hostname pueden ser nombres simbólicos, o direcciones IP en notación de cuaterna.

El primer comando muestra el registro de la tabla correspondiente a la dirección IP o máquina especificada, o si no se pasa ninguna, se mostrarán todos los registros. Por ejemplo, al invocar arp en vlager obtendríamos:

```
C:\Users\usuario>arp -a

Interfaz: 192.168.1.135 --- 0xb
Dirección de Internet      Dirección física      Tipo
192.168.1.126              00-1b-77-9d-47-96     dinámico
192.168.1.254              00-1e-58-19-02-72     dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff     estático
224.0.0.22                  01-00-5e-00-00-16     estático
224.0.0.251                 01-00-5e-00-00-fb     estático
224.0.0.252                 01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.117.1 --- 0x16
Dirección de Internet      Dirección física      Tipo
192.168.117.255            ff-ff-ff-ff-ff-ff     estático
224.0.0.22                  01-00-5e-00-00-16     estático
224.0.0.251                 01-00-5e-00-00-fb     estático
224.0.0.252                 01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.92.1 --- 0x18
Dirección de Internet      Dirección física      Tipo
192.168.92.255             ff-ff-ff-ff-ff-ff     estático
224.0.0.22                  01-00-5e-00-00-16     estático
224.0.0.251                 01-00-5e-00-00-fb     estático
224.0.0.252                 01-00-5e-00-00-fc     estático
239.255.255.250            01-00-5e-7f-ff-fa     estático
```

Se puede limitar el listado a un tipo de hardware especificado usando la opción: -t. La opción -s se usa para añadir permanentemente la dirección

Ethernet de la máquina especificada a las tablas ARP. La dirección de hardware son seis bytes en hexadecimal separados por dos puntos o por guiones dependiendo del sistema operativo. Se puede incluso definir las direcciones de hardware para otros tipos de hardware, usando la opción: -t.

Por alguna razón, las peticiones ARP para máquinas remotas fallan algunas veces, por ejemplo cuando el controlador ARP no funciona, o cuando alguna otra máquina se identifica erróneamente como si ella misma tuviera esa dirección IP. Este problema requiere que se añada manualmente una dirección IP en la tabla ARP. También es una forma (muy drástica) de protegerse a sí mismo de otras máquinas de su Ethernet que tratan de hacerse pasar por otras.

El uso de arp con el modificador -d borra todas las entradas ARP referentes a la máquina dada. Este modificador puede ser usado para forzar a la interfaz a intentar obtener la dirección Ethernet correspondiente a la dirección IP en cuestión. Esto es útil cuando un sistema mal configurado ha emitido una información ARP errónea (por supuesto, se debe reconfigurar la máquina estropeada primero).

La opción -s también puede usarse para implementar un proxy ARP. Esta es una técnica especial, en la que una máquina, llamémosla gate, actúa como una pasarela a otra máquina llamada fnord simulando que las dos direcciones hacen referencia a la misma máquina, en este caso gate. Esto se consigue incluyendo una entrada ARP para fnord que apunte a su propia interfaz Ethernet. Cuando una máquina envíe una petición ARP para fnord, gate devolverá una respuesta con su propia dirección Ethernet. La máquina que hizo la petición enviará entonces todos los datagramas a gate, que se los pasará a fnord.

Estos tips pueden ser necesarios cuando usted quiera acceder a fnord desde una máquina DOS con una implementación errónea de TCP, que no entienda el enrutado demasiado bien. Cuando use proxy ARP, éste le aparecerá a la máquina DOS como si fnord estuviera en la subred local, así que no tiene que saber cómo enrutar a través de una pasarela.

Otra aplicación útil del proxy ARP es cuando una de las máquinas actúe como una pasarela para otra máquina sólo temporalmente, por ejemplo a través de un enlace telefónico.

## *Laboratorio Práctico*

Recomiendo seguir este tutorial paso a paso para entender los términos aquí explicados

<http://seguridadyredes.nireblog.com/post/2009/11/05/wireshark-windump-analisis-capturas-trafico-red-interpretacion-datagrama-ip-actualizacion>

## **BIBLIOGRAFÍA**

---

- TANENBAUM, Andrew S. Redes de Computadores: Prentice-Hall.
- STALLING, William. Comunicaciones y Redes de Computadores: Prentice-Hall.
- UYLESS, Black. Tecnologías Emergentes para Redes de Computadores. : Prentice Hall
- DERFLER. Frank, Descubre Redes LAN y WAN. Prentice Hall.
- HALSELL. Fred, Comunicaciones de Datos, Redes de Computadores y Sistemas Abiertos.: Adisson Wesley
- GIBBS, Mark. Redes para Todos. : Prentice-Hall.
- SHELDON. Tom, Enciclopedia de Redes Serie LAN Times.: McGraw-Hill.
- LEE, Davies. Windows 2000 TCP/IP Protocolos y servicios. : McGraw-Hill.
- RODRÍGUEZ, Jorge E. Introducción a las redes de área local. : McGraw-Hill.
- TIM, Parker. Aprendiendo TCP/IP en 14 días. : Prentice Hall.

### **Internet:**

[www.cisco.com](http://www.cisco.com)  
[www.3com.com](http://www.3com.com)  
[www.nortell.com](http://www.nortell.com)  
[www.lucent.com](http://www.lucent.com)  
[www.hispasec.com](http://www.hispasec.com)  
[www.cibercursos.net](http://www.cibercursos.net)  
[www.red.com.mx](http://www.red.com.mx)  
[www.noticias.com](http://www.noticias.com)  
[www.eltiempo.com](http://www.eltiempo.com)  
[www.dragonjar.org](http://www.dragonjar.org)

---

## TABLA DE CONTENIDO

---

<b>INTRODUCCIÓN.....</b>	<b>1</b>
<b>PROTOCOLOS TCP/IP.....</b>	<b>2</b>
MODELO DE REFERENCIA OSI.....	2
MODELO DE REFERENCIA TCP/IP .....	2
<i>Protocolo de Internet (IP)</i> .....	3
Direcciones IP públicas. ....	4
Direcciones IP privadas (reservadas). ....	4
Direcciones IP estáticas (fijas). ....	4
Direcciones IP dinámicas. ....	4
Clases de Direcciones.....	5
Difusión (broadcast) y multidifusión (multicast). ....	7
Direcciones IP especiales y reservadas .....	7
Intranet.....	8
Extranet.....	8
Internet.....	8
Máscara de subred .....	8
Formato del datagrama IP .....	12
Protocolo ICMP.....	14
Puertos .....	17
Protocolo UDP.....	20
Protocolo TCP .....	22
<i>IPv6 (Protocolo de Internet versión 6)</i> .....	29
Motivos de Ipv6.....	29
Características principales de Ipv6: .....	30
Especificaciones básicas de Ipv6.....	31
Direcciones IPv6 .....	32
Mecanismos de Transición .....	34
<i>ARP</i> .....	38
ARP y subredes .....	38
Tablas ARP.....	39
<i>Laboratorio Práctico</i> .....	41
<b>BIBLIOGRAFÍA .....</b>	<b>42</b>