UNIDAD TEMÁTICA 3

DIRECCIONAMIENTO TCP/IP

CONTENIDO

Direccionamiento a nivel de enlace.....4

Protocolo ARP y RARP.....4

Direccionamiento a nivel de red: ipv4.....4

Introducción IPv4.....4

Características básicas de IPv4:.....5

Dirección IP.....5

Partes de una IPv4.....7

División por clases de direcciones IPv4 y máscaras por defecto.....8

Tipos de direcciones en una red IPv4.....10

Máscara de red.....10

Direcciones IPv4 privadas y públicas.....12

Direcciones estáticas y dinámicas.....13

Direcciones especiales.....14

Formato de trama IPv4.....16

Direcciones Unicast, broadcast y multicast. 19

Organismos gestores de IP.....21

División de redes o subredes.....22

Fórmula para calcular subredes.....23

Fórmula para calcular la cantidad de hosts.....24

División en subredes de igual tamaño.....24

División en subredes de diferente tamaño.....25

Agregación de redes.....27

ICMPv4.....29

Direccionamiento a nivel de red: IPv6.....35

Introducción IPv6.....35

Características de IPv6 ... 36
Direccionamiento IP mejorado ... 37
Encabezado simple ... 38
Intensidad de transición ... 39
Direccionamiento IPv6 ... 41
Dirección unicast global de documentación ... 45
Dirección unicast global de IPv6 ... 45
Direcciones unicast local (de enlace, de sitio y local exclusiva) ... 47
Direcciones multicast ... 48
Dirección de loopback ... 49
Dirección no especificada ... 50
Direcciones reservadas ... 50
Direcciones especiales de transición ... 50
Formato URL ... 51
Asignación de ipv6 ... 51
ICMPv6 ... 53
Transición de ipv4 a ipv6 ... 55
Stack doble ó Doble capa IP ó Dual Stack ... 56
Tunneling ... 56
NAT-PT (Network Address Translation – Protocol Translation) ... 57
Direccionamiento a nivel de Transporte ... 57
Introducción ... 57
Diferentes protocolos de Transporte ... 58
TCP ... 59
UDP ... 59
Comparativa entre UDP y TCP ... 60
Direccionamiento del puerto ... 61
Números de puertos ... 62
Establecimiento de la conexión TCP ... 62
Anexo: Algunos números de puertos conocidos ... 64

DIRECCIONAMIENTO A NIVEL DE ENLACE

Cuando un ordenador envía un mensaje a través de una red de difusión, éste permanece en el medio compartido en espera de ser recogida por el destinatario. Puesto que todas las estaciones están conectadas al mismo medio, todas pueden "ver" ese mensaje enviado (a nivel físico). Sin embargo, solamente el nivel de enlace del destinatario lo podrá tomar para sí. Por eso es necesario un mecanismo que identifique los hosts.

Las direcciones a nivel de enlace, (direcciones de la subcapa MAC) están formadas por números binarios (aunque se expresan en formato hexadecimal) que identifican unas estaciones del resto (son únicas).

Por ejemplo: 18:3E:A0:64:F2:01 (6 bytes)

Las direcciones MAC suelen ir grabadas de fábrica en el adaptador de red. La primera mitad (3 bytes) de la dirección identifica al fabricante y el resto a la tarjeta de red.

Las redes construidas sobre conmutadores o switch, necesitan un mecanismo para identificar las estaciones conectadas a cada puerto. Para ello utilizan el protocolo ARP.

PROTOCOLO ARP Y RARP

ARP son las siglas en inglés de **A**ddress **R**esolution **P**rotocol (Protocolo de resolución de direcciones).

Es un **protocolo** de nivel de red (mismo nivel que IPV4 e IPV6) responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = FF:FF:FF:FF:FF:FF)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.

El **protocolo RARP** realiza la operación inversa: Dada una dirección MAC, obtiene la dirección IP. RARP ya no es usado, fue reemplazado por BOOTP (protocolo de red que es usado para obtener una dirección IP de un servidor), el cual fue tiempo más tarde sustituido por el **Protocolo de Configuración Dinámica de *Host*** (DHCP).

DIRECCIONAMIENTO A NIVEL DE RED: IPV4

INTRODUCCIÓN IPV4

Para participar en Internet, un host necesita una dirección IP. **La dirección IP es una dirección de red lógica que identifica un host en particular**. Para poder comunicarse con otros dispositivos en Internet, dicha dirección debe estar adecuadamente configurada y debe ser única.

La dirección IP es asignada a la conexión de la interfaz de red para un host (también a la interfaz de un router). Esta conexión generalmente es una tarjeta de interfaz de red (NIC) instalada en el dispositivo. Algunos ejemplos de dispositivos de usuario final con interfaces de red incluyen las estaciones de trabajo, los servidores, las impresoras de red y los teléfonos IP. Algunos servidores pueden tener más de una NIC, y cada uno de ellas tiene su propia dirección IP. Las interfaces de routers que proporcionan conexiones a una red IP también tendrán una dirección IP.

Cada paquete enviado por Internet tendrá una dirección IP de origen y de destino(no tienen mascara, concepto que ahora veremos). Los dispositivos de red requieren esta información para asegurarse de que la información llegue a destino y de que toda respuesta sea devuelta al origen.

El crecimiento explosivo de Internet ha amenazado con agotar el suministro de direcciones IP. La división en subredes, la Traducción de direcciones en red (NAT) y el direccionamiento privado se utilizan para extender el direccionamiento IP sin agotar el suministro.

Otra versión de IP conocida como IPv6 mejora la versión actual proporcionando un espacio de direccionamiento mucho mayor, integrando o eliminando los métodos utilizados para trabajar con los puntos débiles del IPv4.

CARACTERÍSTICAS BÁSICAS DE IPV4:

- Sin conexión: No establece conexión antes de enviar los paquetes de datos. De este problema se preocuparán los protocolos de nivel superior.
- No confiable (en bibliografía se denomina a veces máximo esfuerzo): No se usan encabezados para garantizar la entrega de paquetes. Esto permite que los paquetes sean más pequeños y sobrecarguen menos la red. De la recuperación de paquetes perdidos o corruptos se encargarán los niveles superiores.
- Medios independientes: Operan independientemente del medio que lleva los datos. Es responsabilidad de los niveles inferiores esta tarea. Existe, no obstante, una característica principal de los medios que la capa de Red considera: el tamaño máximo de la PDU que cada medio puede transportar. A esta característica se la denomina Unidad máxima de transmisión (MTU). Parte de la comunicación de control entre la capa de Enlace de datos y la capa de Red es establecer un tamaño máximo para el paquete. La capa de Enlace de datos pasa la MTU hacia arriba hasta la capa de Red. La capa de Red entonces determina de qué tamaño crear sus paquetes.

DIRECCIÓN IP

La dirección IP es el identificador de cada host (ordenador) dentro de su red.

Las direcciones IP están formadas por 4 bytes (32 bits). Para una persona sería muy difícil leer una dirección IP binaria. Por este motivo, los 32 bits están agrupados en cuatro bytes de 8 bits llamados octetos. Para hacer que las direcciones IP sean más fáciles de entender, cada octeto se presenta como su valor decimal, separado por un punto decimal. Esto se conoce como notación decimal punteada. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

Las direcciones IP también se pueden representar en:

- hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF
- binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111
- decimal 0.0.0.0 a 255.255.255.255

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar la calculadora científica de Windows para realizar las conversiones).

Decimal: 172.16.122.204 Hexadecimal: AC.10.7A.CC Binario: 10101100.00010000.01111010.11001100

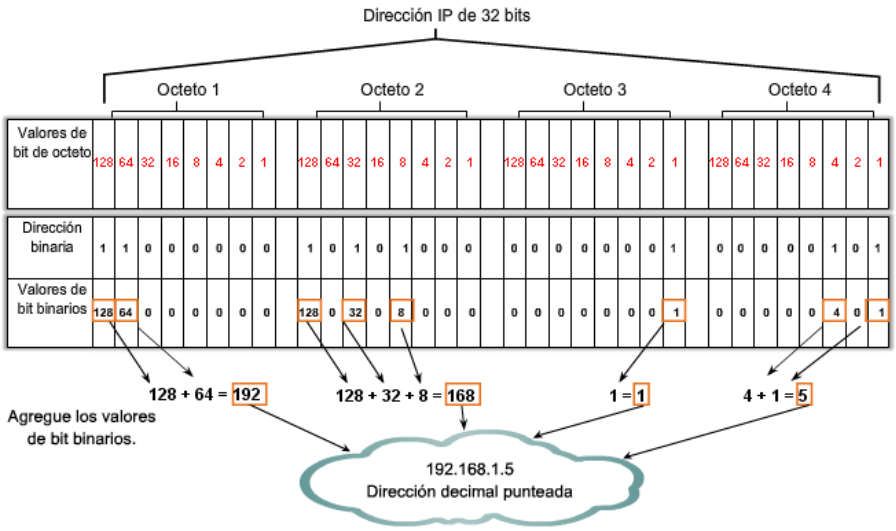
¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts.
La dirección IP de 32 bits está definida con IP versión 4 (IPv4) y actualmente es la forma más común de direcciones IP en Internet.

Cuando un host recibe una dirección IP, lee los 32 bits a medida que son recibidos por la NIC. Una persona, en cambio, debería convertir esos 32 bits en su equivalente decimal de cuatro octetos. Cada octeto está compuesto por 8 bits, y cada bit tiene un valor. Los cuatro grupos de 8 bits tienen el mismo conjunto de valores. En un octeto, el bit del extremo derecho tiene un valor de 1, y los valores de los bits restantes, de derecha a izquierda son 2, 4, 8, 16, 32, 64 y 128.

Determine el valor del octeto sumando los valores de las posiciones cada vez que haya un 1 binario presente.

- Si en esa posición hay un 0, no sume el valor.
- Si los 8 bits son 0, 00000000, el valor del octeto es 0.
- Si los 8 bits son 1, 11111111, el valor del octeto es 255 (128+64+32+16+8+4+2+1).
- Si los 8 bits están combinados, como en el ejemplo 00100111, el valor del octeto es 39 (32+4+2+1).

Por lo tanto, el valor de cada uno de los cuatro octetos puede ir de 0 a un máximo de 255.

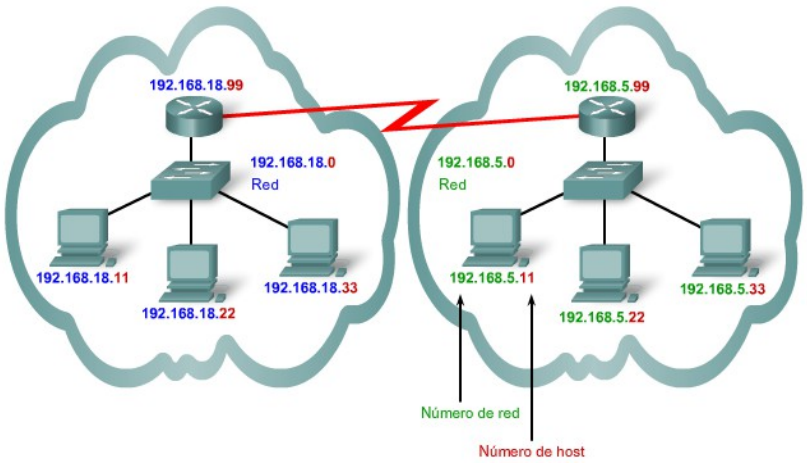


PARTES DE UNA IPV4

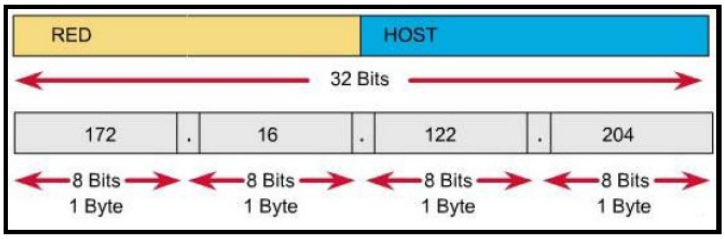
La dirección IP lógica de 32 bits tiene una composición jerárquica y consta de dos partes. La primera parte identifica la red, y la segunda parte identifica un host en esa red. En una dirección IP (de una interfaz, no de un paquete IP), ambas partes son necesarias.

Por ejemplo: si un host tiene la dirección IP 192.168.18.57, los primeros tres octetos (192.168.18) identifican la porción de red de la dirección, y el último octeto (57) identifica el host. Esto se conoce como **direccionamiento jerárquico**, debido a que la porción de red indica la red en la que cada dirección host única está ubicada. Los routers sólo necesitan saber cómo llegar a cada red, sin tener que saber la ubicación de cada host individual.

Otro ejemplo de una red jerárquica es el sistema telefónico. Con un número telefónico, el código de país, el código de área y el intercambio representan la dirección de red; y los dígitos restantes representan un número telefónico local.



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: el identificador de red y el identificador de host.



DIVISIÓN POR CLASES DE DIRECCIONES IPV4 Y MÁSCARAS POR DEFECTO

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema **classless**, se asignan los bloques de direcciones adecuados para la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase de unicast.

Pero originalmente se utilizó el direccionamiento con clases.

A pesar de que este sistema con clase no fue abandonado hasta finales de la década del 90, es posible ver restos de estas redes en la actualidad.

Por ejemplo: al asignar una dirección IPv4 a una computadora, el sistema operativo examina la dirección que se está asignando para determinar si es de clase A, clase B o clase C. Luego, el sistema operativo adopta el prefijo utilizado por esa clase y realiza la asignación de la máscara de subred adecuada.

Otro ejemplo es la adopción de la máscara por parte de algunos protocolos de enrutamiento. Cuando algunos protocolos de enrutamiento reciben una ruta publicada, se puede adoptar la longitud del prefijo de acuerdo con la clase de dirección.

Clases de dirección IP

Clase de dirección	Rango del primer octeto (decimal)	Bits del primer octeto (los bits verdes no se modifican)	Partes de una dirección correspondientes a la red (R) y al host (H)	Máscara de subred por defecto (decimal y binaria)	Cantidad posible de redes y hosts por red
A	De 1 a 127	00000000 - 01111111	R.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 redes (2^7-2) 16 777 214 hosts por red (2^24-2)
B	De 128 a 191	10000000 - 10111111	R.R.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16 382 redes (2^14-2) 65 534 hosts por red (2^16-2)
C	De 192 a 223	11000000 - 11011111	R.R.R.H	255.255.255.0 11111111.11111111.11111111.00000000	2097,150 redes (2^21-2) 254 hosts por red (2^8-2)
D	De 224 a 239	11100000 - 11101111	No es para uso comercial como host	Usada para multicast	
E	De 240 a 255	11110000 - 11111111	No es para uso comercial como host	Usos experimentales	

La dirección IP y la máscara de subred trabajan juntas para determinar qué porción de la dirección IP representa la dirección de red y qué porción representa la dirección del host.

Las direcciones IP se agrupaban en 5 clases. Las clases A, B y C son direcciones comerciales que se asignan a hosts. La Clase D está reservada para uso de multicast, y la Clase E es para uso experimental.

Las direcciones de Clase C tienen tres octetos para la porción de red y uno para los hosts. La máscara de subred por defecto tiene 24 bits (255.255.255.0). Las direcciones Clase C generalmente se asignaban a redes pequeñas.

Las direcciones de Clase B tienen dos octetos para representar la porción de red y dos para los hosts. La máscara de subred por defecto tiene 16 bits (255.255.0.0). Estas direcciones generalmente se utilizaban para redes medianas.

Las direcciones de Clase A sólo tienen un octeto para representar la porción de red y tres para representar los hosts. La máscara de subred por defecto tiene 8 bits (255.0.0.0). Estas direcciones generalmente se asignaban a grandes organizaciones.

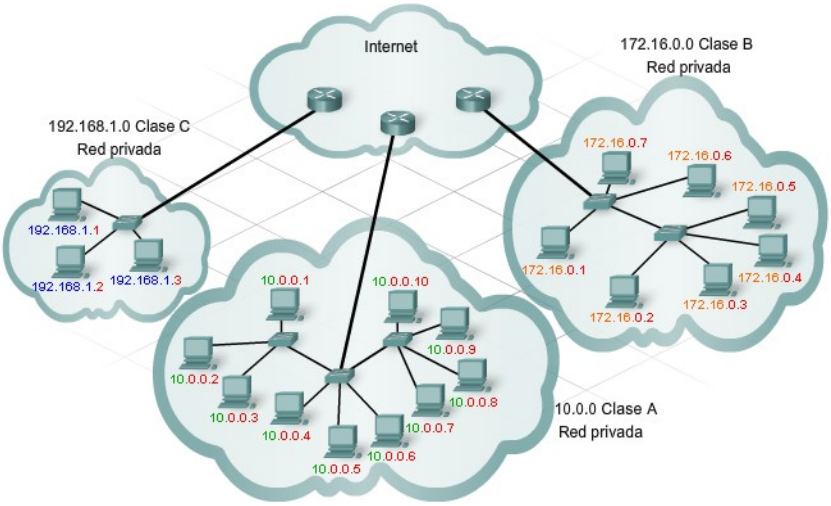
Direcciones experimentales: Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 experimentales de 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones se mencionan como reservadas para uso futuro (RFC 3330). Esto sugiere que podrían convertirse en direcciones utilizables. En la actualidad, no es posible utilizarlas en redes IPv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones reservadas de alcance local. Estas direcciones se utilizarán con grupos multicast en una red local. Los paquetes enviados a estos destinos siempre se transmiten con un valor de período de vida (TTL) de 1. Por lo tanto, un router conectado a la red local nunca debería enviarlos. Un uso común de direcciones de enlace local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones de alcance global son de 224.0.1.0 a 238.255.255.255. Se las puede usar para transmitir datos en Internet mediante multicast. Por ejemplo: 224.0.1.1 ha sido reservada para el Protocolo de hora de red (NTP) para sincronizar los relojes con la hora del día de los dispositivos de la red.

Se puede determinar la clase de una dirección por el valor del primer octeto.

Por ejemplo: si el primer octeto de una dirección IP tiene un valor entre 192 y 223, se clasifica como Clase C. Por ejemplo: 200.14.193.67 es una dirección Clase C.



TIPOS DE DIRECCIONES EN UNA RED IPV4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- Dirección de red: la dirección en la que se hace referencia a la red. Es la primera IP disponible dentro de la red y se usa para representar a todos los equipos de la red. En el gráfico anterior las direcciones de red son 192.168.1.0 172.16.0.0 10.0.0.0. Los routers utilizan estas IPs especiales para sus tablas de enrutamiento.

  Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

- Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red. La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. En la figura anterior serían 192.168.1.255 172.16.255.255 10.255.255.255

- Direcciones host: las direcciones asignadas a los dispositivos finales de la red. Como se describe anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

MÁSCARA DE RED

La máscara de red es un número de 32 bits que nos indica que parte de una dirección ip corresponde a la red y que parte corresponde al host dentro de esta red.

Por ejemplo si tenemos la red: 172.16.16.0 a 172.16.16.255 quiere decir que nuestros equipos tienen fijos los tres primeros números 172.16.16 y variable el cuarto. Dicho en bits indicando los fijos con 1 y los variables con 0: 11111111-11111111-11111111-00000000 que dicho en decimal es 255.255.255.0 También se puede expresar en la notación 172.16.16.0/24, es decir, los primeros 24 bits a uno en la máscara.

Una máscara siempre comenzará por unos y terminará con ceros y no se mezclarán porque los unos indicarán la parte de red de una dirección ip y los ceros la parte de hosts de una dirección ip

Dirección	172.	16	16	0-255
	10101100	00010000	00010000	x
Máscara	11111111	11111111	11111111	00000000
	255	255	255	0

CIDR

(CIDR Encaminamiento Inter-Dominios sin Clases) se introdujo en 1993 y representa la última mejora en el modo como se interpretan las direcciones IP.

CIDR reemplaza la sintaxis previa para nombrar direcciones IP, las clases de redes.

En vez de asignar bloques de direcciones en los límites de los octetos, que implicaban prefijos *naturales* de 8, 16 y 24 bits, CIDR usa la técnica VLSM (Variable-Length Subnet Masking - Máscara de Subred de Longitud Variable), para hacer posible la asignación de prefijos de longitud arbitraria.

Veamos un ejemplo: la red 172.23.0.0/17

1ª IP	172.23.0.1	10101100	00010111	00000000	00000001
Última IP	172.23.127.254	10101100	00010111	01111111	11111110
Máscara	255.255.128.0	11111111	11111111	10000000	00000000
Dirección de red	172.23.0.0	10101100	00010111	00000000	00000000
Dirección de broadcast	172.23.127.255	10101100	00010111	01111111	11111111

Máscara Binario	Mas. Decimal	CIDR	Nº HOSTs	Clase
11111111.11111111.11111111.11111111	255.255.255.255	/32	1	
11111111.11111111.11111111.11111110	255.255.255.254	/31	2	
11111111.11111111.11111111.11111100	255.255.255.252	/30	4	
11111111.11111111.11111111.11111000	255.255.255.248	/29	8	
11111111.11111111.11111111.11110000	255.255.255.240	/28	16	
11111111.11111111.11111111.11100000	255.255.255.224	/27	32	
11111111.11111111.11111111.11000000	255.255.255.192	/26	64	
11111111.11111111.11111111.10000000	255.255.255.128	/25	128	
11111111.11111111.11111111.00000000	255.255.255.0	/24	256	C
11111111.11111111.11111110.00000000	255.255.254.0	/23	512	
11111111.11111111.11111100.00000000	255.255.252.0	/22	1024	
11111111.11111111.11111000.00000000	255.255.248.0	/21	2048	
11111111.11111111.11110000.00000000	255.255.240.0	/20	4096	
11111111.11111111.11100000.00000000	255.255.224.0	/19	8192	
11111111.11111111.11000000.00000000	255.255.192.0	/18	16384	
11111111.11111111.10000000.00000000	255.255.128.0	/17	32768	
11111111.11111111.00000000.00000000	255.255.0.0	/16	65536	B
11111111.11111110.00000000.00000000	255.254.0.0	/15	131072	
11111111.11111100.00000000.00000000	255.252.0.0	/14	262144	
11111111.11111000.00000000.00000000	255.248.0.0	/13	524288	
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048576	
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097152	
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194304	
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388608	

11111111.00000000.00000000.00000000	255.0.0.0	/8	16777216	A
11111110.00000000.00000000.00000000	254.0.0.0	/7	33554432	
11111100.00000000.00000000.00000000	252.0.0.0	/6	67108864	
11111000.00000000.00000000.00000000	248.0.0.0	/5	134217728	
11110000.00000000.00000000.00000000	240.0.0.0	/4	268435456	
11100000.00000000.00000000.00000000	224.0.0.0	/3	536870912	
11000000.00000000.00000000.00000000	192.0.0.0	/2	1073741824	
10000000.00000000.00000000.00000000	128.0.0.0	/1	2147483648	
00000000.00000000.00000000.00000000	0.0.0.0	/0	4294967296	

Utilidad de las mascaras.

Se aplica la lógica AND a la dirección host IPv4 y a su máscara de subred para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND a la dirección y a la máscara de subred, el resultado que se produce es la dirección de red.

Los routers usan AND para determinar una ruta aceptable para un paquete entrante. El router verifica la dirección de destino e intenta asociarla con un salto siguiente. Cuando llega un paquete a un router, éste realiza el procedimiento de aplicación de AND en la dirección IP de destino en el paquete entrante y con la máscara de subred de las rutas posibles. De esta forma, se obtiene una dirección de red que se compara con la ruta de la tabla de enrutamiento de la cual se usó la máscara de subred.

Un host de origen debe determinar si un paquete debe ser directamente enviado a un host en la red local o si debe ser dirigido al gateway. Para tomar esta determinación, un host primero debe conocer su propia dirección de red.

Un host obtiene su dirección de red al aplicar la lógica AND a la dirección con la máscara de subred. La lógica AND también es llevada a cabo por un host de origen entre la dirección de destino del paquete y la máscara de subred de este host. Esto produce la dirección de red de destino. Si esta dirección de red coincide con la dirección de red del host local, el paquete es directamente enviado al host de destino. Si las dos direcciones de red no coinciden, el paquete es enviado al gateway.

DIRECCIONES IPV4 PRIVADAS Y PÚBLICAS

Todos los hosts que se conectan directamente a Internet requieren una dirección IP pública exclusiva. Debido a la cantidad finita de direcciones de 32 bits disponibles, existe la posibilidad de que se acaben las direcciones IP. Una solución para este problema fue reservar algunas direcciones privadas para utilizarlas exclusivamente dentro de una organización. Esto permite que los hosts dentro de una organización se comuniquen entre sí sin necesidad de contar con una dirección IP pública única (que hay que pagar).

RFC 1918 es un estándar que reserva varios rangos de direcciones dentro de cada una de las clases, A, B y C. Como se muestra en la tabla, estos rangos de direcciones privadas constan de una única red Clase A, 16 redes Clase B y 256 redes Clase C. Esto proporciona al administrador de red una flexibilidad considerable para la asignación de direcciones internas. Una red muy grande puede utilizar la red privada Clase A, que permite más de 16 millones de direcciones privadas.

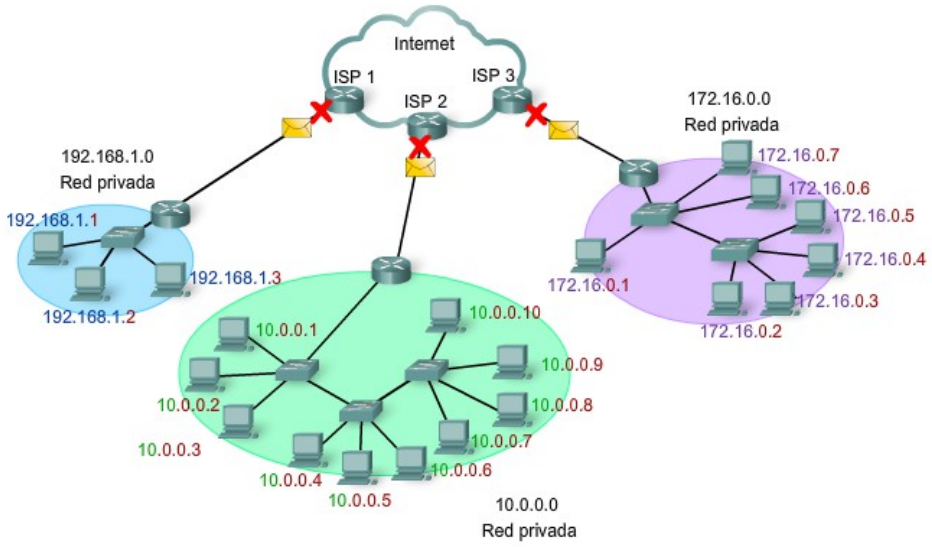
En las redes medianas se puede utilizar una red privada Clase B, que proporciona más de 65.000 direcciones.

Las redes domésticas y de empresas pequeñas generalmente utilizan una única dirección privada Clase C, que permite hasta 254 hosts.

La red Clase A, las 16 redes Clase B o las 256 redes Clase C pueden ser utilizadas dentro de organizaciones de cualquier tamaño. Generalmente, muchas organizaciones utilizan la red privada Clase A.

Clase	Número de redes	Rango de direcciones reservadas de redes
A	**1**	**10.0.0.0**
B	**16**	**172.16.0.0 - 172.31.0.0**
C	256	192.168.0.0 - 192.168.255.0

Las direcciones privadas pueden ser utilizadas internamente por los hosts de una organización, siempre y cuando los hosts no se conecten directamente a Internet. Por lo tanto, múltiples organizaciones pueden utilizar el mismo conjunto de direcciones privadas. Las direcciones privadas no se envían a Internet y son bloqueadas rápidamente por un router de ISP.



DIRECCIONES ESTÁTICAS Y DINÁMICAS

Las direcciones IP se pueden asignar de forma estática o de forma dinámica.

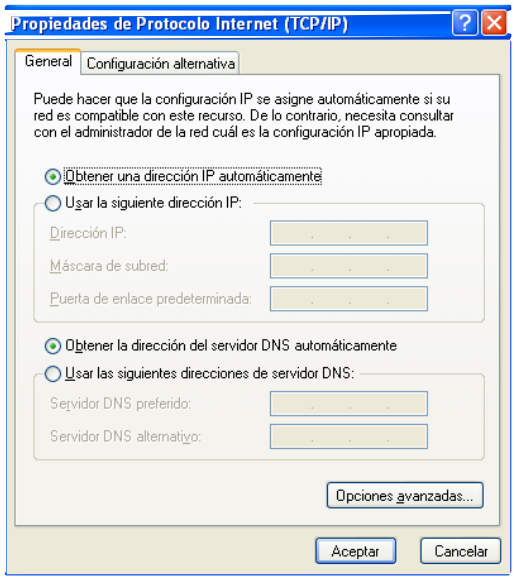
Estática: Con una asignación estática, el administrador de la red debe configurar manualmente la información de la red para un host. Como mínimo, esto incluye la dirección IP del host, la máscara de subred y la gateway por defecto.

Las direcciones estáticas tienen algunas ventajas. Por ejemplo, son útiles para impresoras, servidores y otros dispositivos de red que deben estar accesibles para los clientes de la red. Si el host normalmente accede al servidor en una dirección IP particular, no es adecuado que esta dirección cambie.

La asignación estática de la información de direccionamiento puede proporcionar un mayor control de los recursos de red; pero introducir la información en cada host puede

ser muy lento. Cuando se introducen direcciones IP estáticamente, el host sólo realiza análisis de errores básicos en la dirección IP; por lo tanto, es más probable que haya errores.

Cuando se utiliza el direccionamiento IP estático, es importante mantener una lista precisa de qué direcciones IP se asignan a qué dispositivos. Además, estas direcciones son permanentes y generalmente no se reutilizan.



Dinámica: En las redes locales, es habitual que la población de usuarios cambie frecuentemente. Se agregan nuevos usuarios con computadoras portátiles, y esos usuarios requieren una conexión. Otros tienen nuevas estaciones de trabajo que deben conectarse. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más simple que las direcciones IP se asignen automáticamente. Esto se logra a través de un protocolo denominado protocolo de configuración dinámica de host (DHCP).

El protocolo DHCP proporciona un mecanismo para la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, una gateway por defecto y otra información de configuración.

El protocolo DHCP generalmente es el método preferido para la asignación de direcciones IP a hosts en grandes redes, ya que reduce la carga del personal de soporte de la red y prácticamente elimina los errores de introducción de datos.

Otro de los beneficios del DHCP es que las direcciones no se asignan permanentemente a un host, sino que son arrendadas durante un período. Si el host se apaga o sale de la red, la dirección es devuelta al pool de direcciones para ser reutilizada. Esto es especialmente útil en el caso de los usuarios móviles que entran en una red y salen de ella.

DIRECCIONES ESPECIALES

Direcciones IP especiales

Red o rango	Uso
0.0.0.0 – 0.255.255.255	Reservado (ppio. Clase A)
127.0.0.0 – 127.255.255.255	Reservado (fin clase A)
128.0.0.0 – 128.0.255.255	Reservado (ppio. Clase B)
191.255.0.0 -191.255.255.255	Reservado (fin clase B)
192.0.0.0 – 192.0.0.255	Reservado (ppio. Clase C)
224.0.0.0	Reservado (ppio. Clase D)
240.0.0.0 – 255.255.255.254	Reservado (toda la clase E)
10.0.0.0 – 10.255.255.255	Direccionamiento Privado (NAT)
172.16.0.0 – 172.31.255.255	Direccionamiento Privado (NAT)
192.168.0.0 – 192.168.255.255	Direccionamiento Privado (NAT)
169.254.0.0 – 169.254.255.255	Direcciones de enlace local

Hay determinadas direcciones que no pueden ser asignadas a los hosts por varios motivos. También hay direcciones especiales que pueden ser asignadas a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

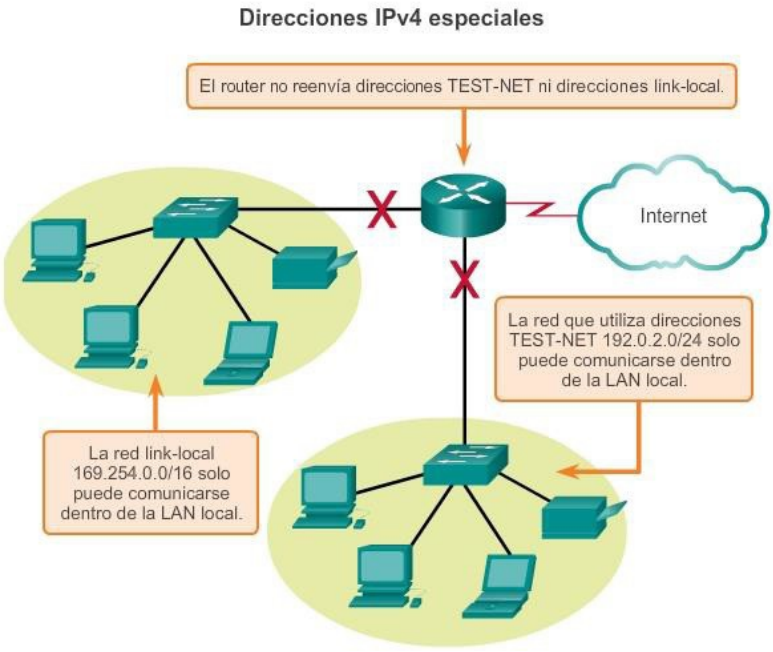
Direcciones de red y de broadcast: Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son la dirección de red y la dirección de broadcast, respectivamente.

Ruta predeterminada, gateway o puerta de enlace: Es la ip correspondiente al dispositivo configurado para dotar a las máquinas de una red local conectadas a él de un acceso hacia una red exterior. Se representa la ruta predeterminada IPv4 como 0.0.0.0. La ruta predeterminada se usa como ruta "comodín" cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

Loopback: Una de estas direcciones reservadas es la dirección IPv4 de loopback 127.0.0.1. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores de la pila TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única **127.0.0.1**, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un **loop-back** dentro del host local. Ni siquiera debe aparecer ninguna dirección en ninguna red dentro de este bloque.

Direcciones de enlace local: Las direcciones IPv4 del bloque de direcciones de 169.254.0.0 a 169.254.255.255 (169.254.0.0 /16) son designadas como direcciones de enlace local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Éstas pueden usarse en una pequeña red punto a punto o con un host que no podría obtener automáticamente una dirección de un servidor de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host, DHCP).



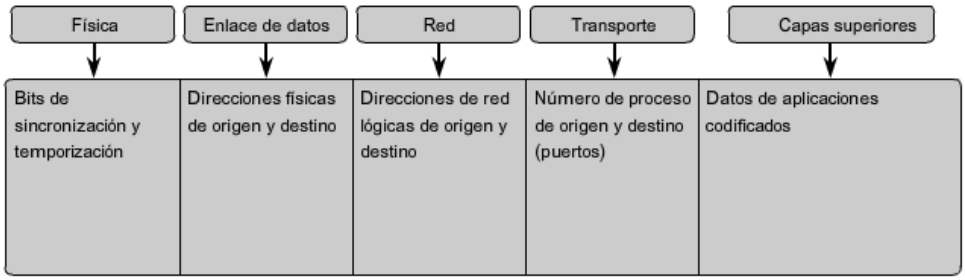
La comunicación mediante direcciones de enlace local IPv4 sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red, como se muestra en la figura. Un host no debe enviar un paquete con una dirección de destino de enlace local IPv4 a ningún router para ser enviado, y debería establecer el TTL de IPv4 para estos paquetes en 1.

Las direcciones de enlace local no ofrecen servicios fuera de la red local. Sin embargo, muchas aplicaciones de cliente/servidor y punto a punto funcionarán correctamente con direcciones de enlace local IPv4.

Direcciones TEST-NET: Se establece el bloque de direcciones de 192.0.2.0 a 192.0.2.255 (192.0.2.0 /24) para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración. A menudo puede encontrar que estas direcciones se usan con los nombres de dominio example.com o example.net en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

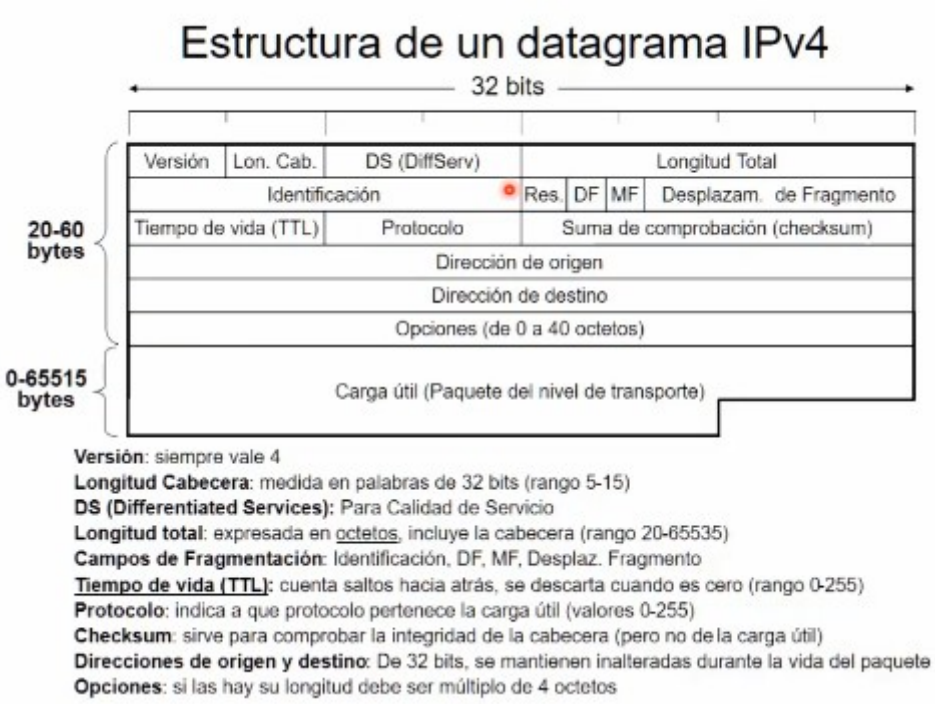
FORMATO DE TRAMA IPV4

El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.



Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizan el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.

El Internet Protocol especificado en RFC 791 define el formato de datagrama IP. El datagrama IP tiene campos específicos que contienen información sobre el paquete y sobre los host emisores y receptores. Campos del datagrama:



Versión: 4 bits: Siempre vale lo mismo (0100). Este campo lleva el registro de la versión del protocolo a la que pertenece el datagrama.

Tamaño Cabecera (IHL): 4 bits: Longitud de la cabecera, en palabras de 32 bits. Su valor mínimo es de 5 para una cabecera sin opciones(20 bytes), y el máximo de 15. Por lo tanto limita la cabecera a 60 bytes y el campo opciones a 40 bytes

Tipo de servicio: permite al host indicar a la subred el tipo de servicio que quiere, antiguamente los routers encaminaban (si era posible) considerando los valores especificados en este campo, en la actualidad los routers ignoran este campo. Especificaba: seguridad, prioridad, retardo y rendimiento.

Longitud Total: 16 bits: Es el tamaño total, en octetos, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. Tamaño máximo 65535 bytes

Identificador: 16 bits: Identificador único del datagrama. Se utilizará, en caso de que el datagrama deba ser fragmentado. Todos los fragmentos del mismo datagrama, tienen el mismo valor de identificación. Esta relacionado con la MTU de las redes por las que deba enrutarse. Se fragmentará si es preciso en el host o en el router(que atraviese).

MTU (Maximum Transfer Unit)

- Cada tecnología del nivel de enlace tiene un tamaño máximo de trama que puede transmitir. Eso es su MTU
- Cualquier interfaz en un host, router, conmutador, etc. tiene una MTU característica que depende de su tipo

Nivel de enlace	MTU (bytes)
PPP normal	1500
PPP bajo retardo	296
Frame Relay	1600 (por defecto)
Ethernet (DIX)	1500
Ethernet con 'jumbo' frames	9018-9216
WiFi (802.11)	2272
Token Ring 4 Mb/s	4440 (por defecto)
FDDI	4500

Indicadores: 3 bits: Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:

- bit 0: Reservado; debe ser 0
- bit 1: 0 = Divisible, 1 = No Divisible (DF) (Información para los enrutadores)
- bit 2: 0 = Último Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos)

Posición de Fragmento: 13 bits: En paquetes fragmentados indica la posición, en unidades de 64 bits(8 bytes), que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0. Como tenemos 13 bits tenemos un valor entre 0 y 8192 fragmentos por datagrama, dando una longitud máxima de 65536 bytes (8192 x 8 bytes), uno más que el campo longitud total.

Tiempo de Vida (TTL): 8 bits: Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado. Así se evita que un paquete vaguen eternamente por la subred.

Protocolo: 8 bits: Indica el protocolo de siguiente nivel utilizado en la parte de datos del datagrama. (TCP o UDP)

Suma de Comprobación: verificación de integridad del encabezado (16 bits)

Dirección IP de origen: 32 bits

Dirección IP de destino: 32 bits

Opciones: En la actualidad hay 5 opciones definidas: pruebas de red, depuración, seguridad (ejemplo, en usos militares, que los paquetes no pasen por los enrutadores de ciertos paises) y otras (0 ó 32 bits, si corresponde). Su longitud es variable

Relleno: Variable: Utilizado para asegurar que el tamaño, en bits, de la cabecera es un múltiplo de 32. El valor usado es el 0.

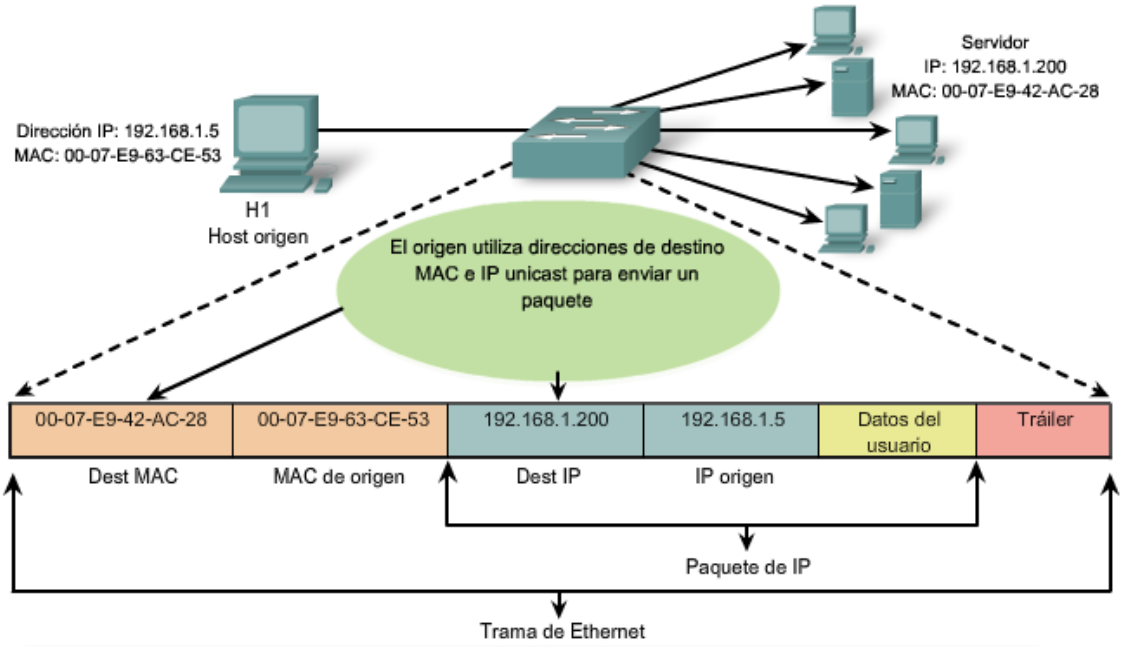
Carga útil: información recibida del nivel superior y que hay que transportar.

DIRECCIONES UNICAST, BROADCAST Y MULTICAST.

Además de las clases de direcciones, las direcciones IP también se categorizan en unicast, broadcast o multicast. Los hosts pueden utilizar las direcciones IP para comunicaciones de uno a uno (unicast), de uno a varios (multicast) o de uno a todos (broadcast).

Unicast: La dirección unicast es el tipo más común en una red IP. Un paquete con una dirección de destino unicast está dirigido a un host específico. Un ejemplo es un host con la dirección IP 192.168.1.5 (origen) que solicita una página Web a un servidor con la dirección IP 192.168.1.200 (destino).

Para que un paquete unicast sea enviado y recibido, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. En el encabezado de la trama de Ethernet también debe estar presente la dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la entrega de datos a un host de destino específico.



Broadcast: Para broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esto significa que todos los hosts de esa red local (dominio de broadcast) recibirán y verán el paquete. Muchos protocolos de red, como ARP y DHCP utilizan broadcasts.

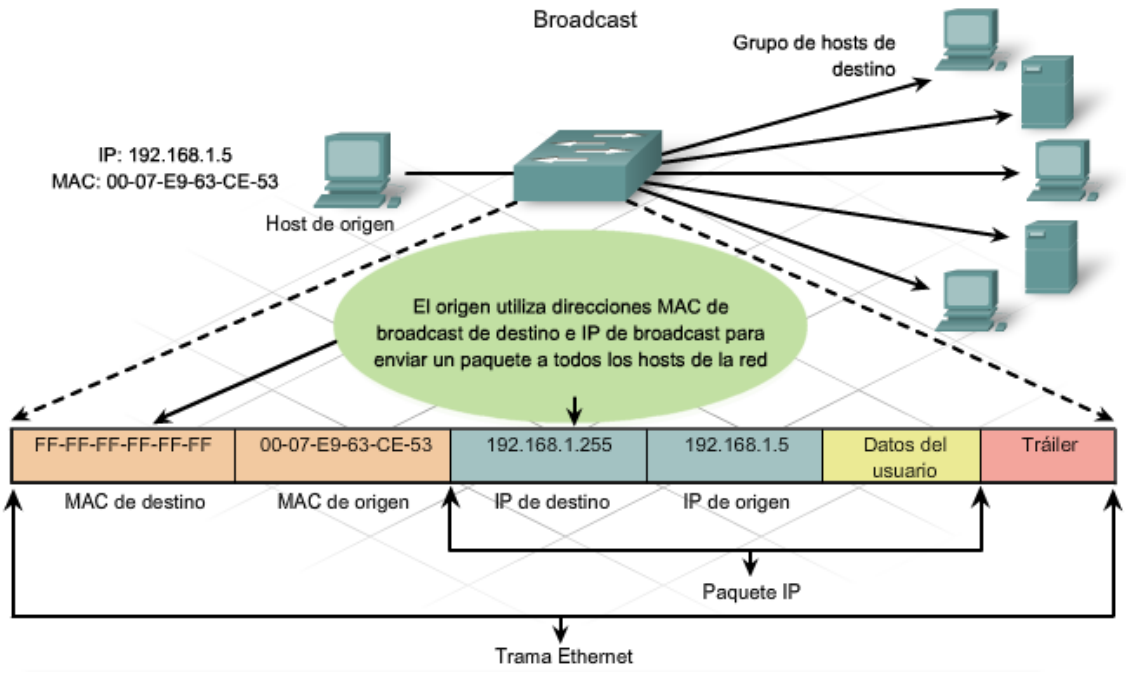
Una red Clase C con la dirección 192.168.1.0 con una máscara de subred por defecto de 255.255.255.0 tiene la dirección de broadcast 192.168.1.255. La porción de host es 255, en formato decimal, o 11111111 (todos unos), en formato binario.

Una red Clase B con la dirección 172.16.0.0 y la máscara por defecto 255.255.0.0, tiene la dirección de broadcast 172.16.255.255.

Una red Clase A con la dirección 10.0.0.0 y la máscara por defecto 255.0.0.0 tiene la dirección de broadcast 10.255.255.255.

Una dirección IP de broadcast para una red requiere una dirección MAC de broadcast correspondiente en la trama de Ethernet. En las redes Ethernet, la dirección MAC de broadcast está formada por 48 unos, que se muestran como un número hexadecimal FF-FF-FF-FF-FF-FF.

Algunos ejemplos para utilizar una transmisión de broadcast son: Asignar direcciones de capa superior a direcciones de capa inferior, Solicitar una dirección y Intercambiar información de enrutamiento por medio de protocolos de enrutamiento



Multicast: Las direcciones multicast permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos.

A los dispositivos que participan de un grupo multicast se les asigna una dirección IP de grupo multicast. El rango de direcciones multicast va de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a menudo denominado grupo de hosts), sólo pueden ser utilizadas como destino de un paquete. El origen siempre será una dirección unicast.

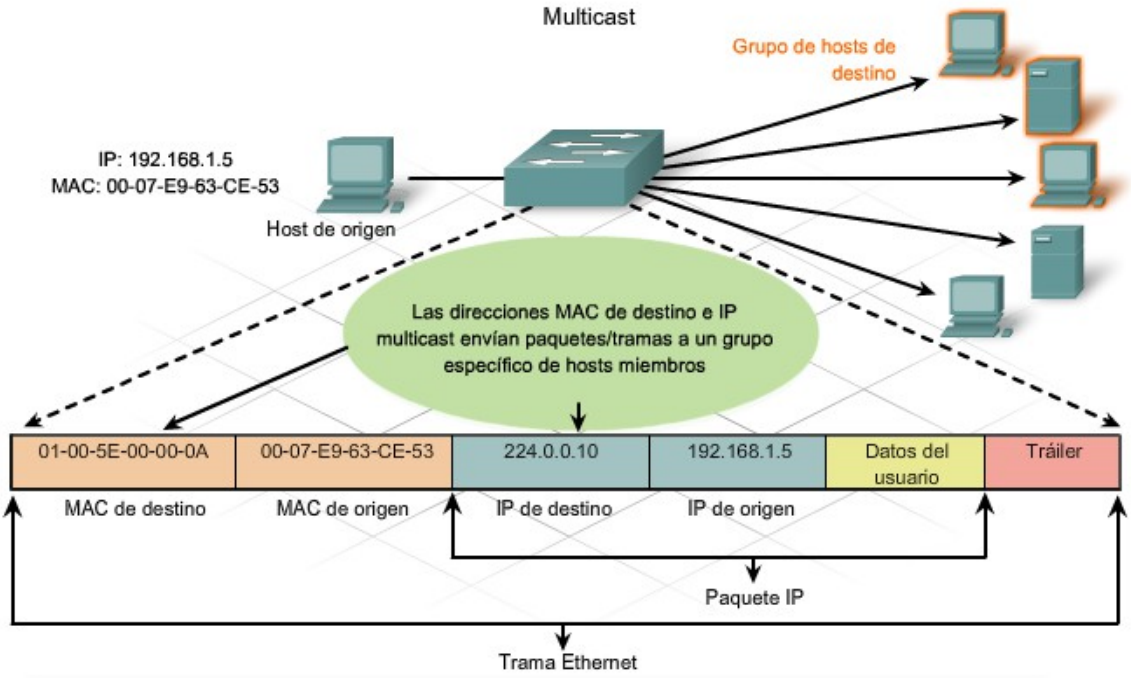
Un ejemplo donde las direcciones multicast pueden ser útiles es en los juegos remotos, donde muchos jugadores se conectan remotamente pero juegan al mismo juego. Otro ejemplo puede ser la educación a distancia a través de videoconferencias, donde muchos estudiantes se conectan a la misma clase.

Como sucede con las direcciones unicast y broadcast, las direcciones IP multicast requieren una dirección MAC multicast correspondiente para poder entregar las tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor finaliza al convertir los 23 bits más bajos de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección Ethernet. Un

ejemplo, como se muestra en el gráfico, es el hexadecimal 01-00-5E-0F-64-C5. Cada carácter hexadecimal representa 4 bits binarios.

Algunos ejemplos de transmisión de multicast son:

Distribución de audio y video, Intercambio de información de enrutamiento por medio de protocolos de enrutamiento, Distribución de software y Suministro de noticias



ORGANISMOS GESTORES DE IP

Una compañía u organización que desea acceder a la red mediante hosts desde Internet debe tener un bloque de direcciones públicas asignado. El uso de estas direcciones públicas es regulado y la compañía u organización debe tener un bloque de direcciones asignado. Esto es lo que sucede con las direcciones IPv4, IPv6 y multicast.

Autoridad de números asignados a Internet (IANA) (http://www.iana.net) es un soporte maestro de direcciones IP. Las direcciones IP multicast y las direcciones IPv6 se obtienen directamente de la IANA. Hasta mediados de los años noventa, todo el espacio de direcciones IPv4 era directamente administrado por la IANA. En ese entonces, se asignó el resto del espacio de direcciones IPv4 a otros diversos registros para que realicen la administración de áreas regionales o con propósitos particulares. Estas compañías de registro se llaman Registros regionales de Internet (RIR)

Los principales registros son:

- AfriNIC (African Network Information Centre) - Región de África
  http://www.afrinic.net

- APNIC (Asia Pacific Network Information Centre) - Región de Asia/Pacífico
  http://www.apnic.net

- ARIN (American Registry for Internet Numbers) - Región de Norte América
  http://www.arin.net
- LACNIC (Registro de dirección IP de la Regional Latinoamericana y del Caribe) - América Latina y algunas islas del Caribe
  http://www.lacnic.net
- RIPE NCC (Reseaux IP Europeans) - Europa, Medio Oriente y Asia Central
  http://www.ripe.net

DIVISIÓN DE REDES O SUBREDES

En lugar de tener todos los hosts conectados en cualquier parte a una vasta red global, es más práctico y manejable agrupar los hosts en redes específicas. Históricamente, las redes basadas en IP tienen su raíz como una red grande. Como esta red creció, también lo hicieron los temas relacionados con su crecimiento. Para aliviar estos problemas, la red grande fue separada en redes más pequeñas que fueron interconectadas. Estas redes más pequeñas generalmente se llaman subredes.

Red y subred son términos utilizados indistintamente, en este apartado, para referirse a cualquier sistema de red hecho posible por los protocolos de comunicación comunes compartidos del modelo TCP/IP. También en otro contexto se conoce la subred como el conjunto de enrutadores y lineas de comunicación de una red.

De manera similar, a medida que nuestras redes crecen, pueden volverse demasiado grandes para manejarlas como una única red. En ese punto, necesitamos dividir nuestra red. Cuando planeamos la división de la red, necesitamos agrupar aquellos hosts con factores comunes en la misma red, por ejemplo por su situación, por su propiedad, etc.

Internet está compuesta por millones de hosts y cada uno está identificado por su dirección única de capa de red. Esperar que cada host conozca la dirección de cada uno de los otros hosts sería imponer una carga excesiva.

Dividir grandes redes para que estén agrupados los hosts que necesitan comunicarse, reduce la carga innecesaria de todos los hosts para conocer todas las direcciones.

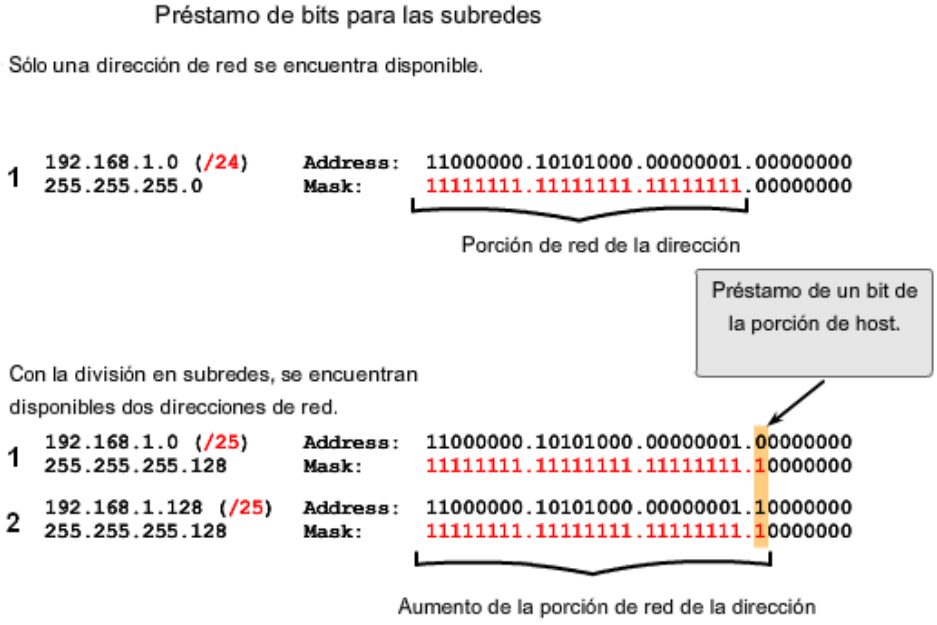
Para todos los otros destinos, los hosts sólo necesitan conocer la dirección de un dispositivo intermediario al que envían paquetes para todas las otras direcciones de destino. Este dispositivo intermediario se denomina gateway o puerta de enlace predeterminada (Aunque un nombre mejor sería enrutador por defecto)

La división en subredes permite crear múltiples redes lógicas dentro de un solo bloque de direcciones de red (asignado por la IANA o RIR). Fuera de la red, la subred no es visible, por lo que no requiere autorización externa(IANA) para crear en nuestra organización subredes.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se usen,

mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es "1".



Direcciones de broadcast:

192.168.1.0/24	11000000.10101000.00000001.00000000
192.168.1.255	11000000.10101000.00000001.11111111
192.168.1.0/25	11000000.10101000.00000001.00000000
192.168.1.127	11000000.10101000.00000001.01111111
192.168.1.128/25	11000000.10101000.00000001.10000000
192.168.1.255	11000000.10101000.00000001.11111111

FÓRMULA PARA CALCULAR SUBREDES

Use esta fórmula para calcular la cantidad de subredes: $\mathbf{2^n}$ donde n es igual a la cantidad de bits que se tomaron prestados.

En este ejemplo, el cálculo es así:

2^1 = 2 subredes

FÓRMULA PARA CALCULAR LA CANTIDAD DE HOSTS

Para calcular la cantidad de hosts por red, se usa la fórmula $\mathbf{2^n - 2}$ donde n es igual a la cantidad de bits para hosts.

La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts.

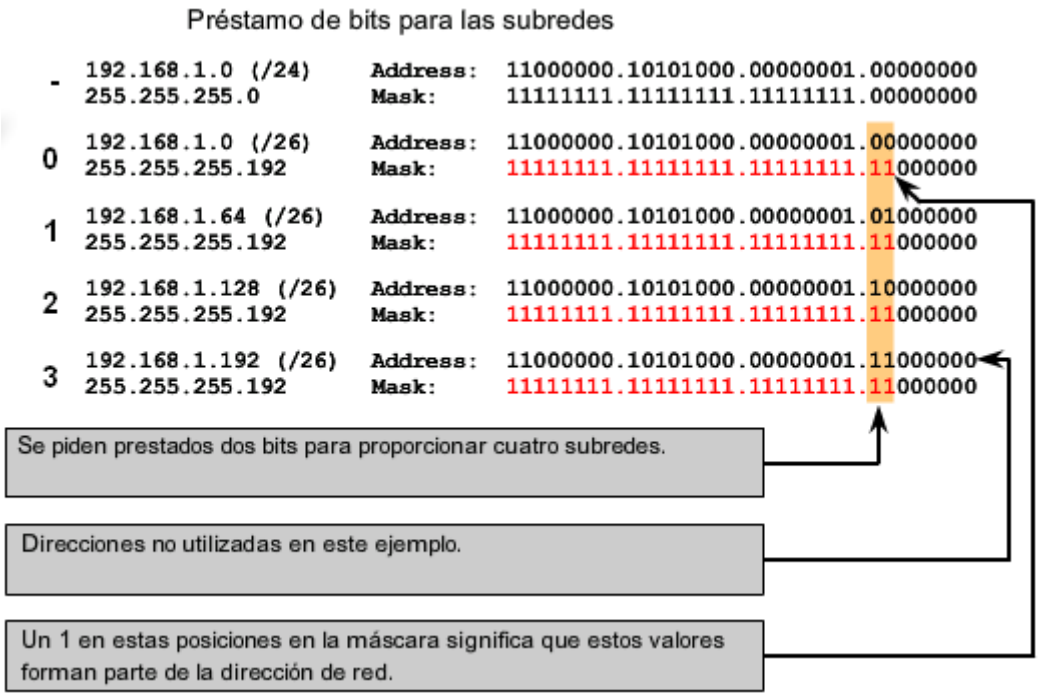
En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: 00000000 = 0

Subred 2: 10000000 = 128

DIVISIÓN EN SUBREDES DE IGUAL TAMAÑO

Por ejemplo, si disponemos de una determinada red con máscara /24 (clase C) que nos permite 2^8 – 2 = 254 equipos y por cuestiones de eficiencia necesitamos 4 grupos de 50 equipos, podemos dividir esta red en 4 subredes de tamaño (/26) 2^6 – 2 = 62 equipos cada una, que nos proporcionarían el tamaño suficiente para albergar a estos 50 equipos. Es decir, hemos tomado para la porción de red de la ip 2 bits que antes se usaban para la porción del host.



Por tanto, para saber la división que necesitamos solo debemos jugar con la ecuación 2^x – 2 que nos determina la capacidad de las subredes resultantes.

Préstamo de bits para las subredes

-	192.168.1.0 (/24)	Address:	11000000.10101000.00000001.00000000
	255.255.255.0	Mask:	11111111.11111111.11111111.00000000
0	192.168.1.0 (/27)	Address:	11000000.10101000.00000001.00000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
1	192.168.1.32 (/27)	Address:	11000000.10101000.00000001.00100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
2	192.168.1.64 (/27)	Address:	11000000.10101000.00000001.01000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
3	192.168.1.96 (/27)	Address:	11000000.10101000.00000001.01100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
4	192.168.1.128 (/27)	Address:	11000000.10101000.00000001.10000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
5	192.168.1.160 (/27)	Address:	11000000.10101000.00000001.10100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
6	192.168.1.192 (/27)	Address:	11000000.10101000.00000001.11000000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000
7	192.168.1.224 (/27)	Address:	11000000.10101000.00000001.11100000
	255.255.255.224	Mask:	11111111.11111111.11111111.11100000

DIVISIÓN EN SUBREDES DE DIFERENTE TAMAÑO

Supongamos que disponemos de la red 192.168.0.0/24 y necesitamos las siguientes subredes: Una subred de 20 hosts, otra subred de 80 hosts, otra de 20 hosts y 3 subredes de 2 hosts.

Ordenamos las subredes en orden decreciente: 80, 20, 20, 2, 2, 2.

Para 80 hosts necesito 7 bits (2^7=128, menos red y broadcast 126 hosts máx.), por lo tanto el prefijo de subred del primer bloque sería /25 (8-7=1; 24+1=25) Tomando la subred cero, la primera dirección de subred sería 192.168.0.0/25, broadcast 192.168.0.127, por lo tanto el rango asignable sería .1 hasta .126.

11000000.10101000.00000000.00000000	red	192.168.0.0
11111111.11111111.11111111.10000000	mascara	255.255.255.128
11000000.10101000.00000000.01111111	broadcast	192.168.0.127

Para 20 hosts necesito 5 bits (2^5=32, es decir 30 hosts máx.). Prefijo: /27 (8-5=3, 24+3=27); Dir. de red: 192.168.0.128/27, broadcast 192.168.0.159. Rango asignable . 129-.158.

11000000.10101000.00000000.10000000	red	192.168.0.128
11111111.11111111.11111111.11100000	mascara	255.255.255.224
11000000.10101000.00000000.10011111	broadcast	192.168.0.159

La siguiente subred es del mismo tamaño y el prefijo es el mismo. Dir. de red: 192.168.0.160/27 , broadcast 192.168.0.191, rango .161-.190.

11000000.10101000.00000000.10100000	red	192.168.0.160

11111111.11111111.11111111.11100000	mascara	255.255.255.224
11000000.10101000.00000000.10111111	broadcast	192.168.0.191

Las redes pequeñas sólo necesitan 2 bits (2^2=4, es decir 2 hosts máx) por lo tanto el prefijo debe ser /30 (8-2=6, 24+6=30). Dir. de enlace 1: 192.168.0.192, dir. de broadcast en enlace 1: 192.168.0.195, rango .193-.194. Dir. enlace 2: 192.168.0.196/30, broadcast en enlace 2: 192.168.0.199, rango .197-.198. Dir. enlace 3: 192.168.0.200/30, broadcast enlace 3: 192.168.0.203, rango: .201-.202.

11000000.10101000.00000000.11000000	red	192.168.0.192
11111111.11111111.11111111.11111100	mascara	255.255.255.252
11000000.10101000.00000000.11000011	broadcast	192.168.0.195

11000000.10101000.00000000.11000100	red	192.168.0.196
11111111.11111111.11111111.11111100	mascara	255.255.255.252
11000000.10101000.00000000.11000111	broadcast	192.168.0.199

11000000.10101000.00000000.11001000	red	192.168.0.200
11111111.11111111.11111111.11111100	mascara	255.255.255.252
11000000.10101000.00000000.11001011	broadcast	192.168.0.203

El esquema resultado es:

Red	Dirección de red	Broadcast	Rango	Máscara
Subred 80	192.168.0.0/25	192.168.0.127	.1-.126	255.255.255.128
Subred 20	192.168.0.128/27	192.168.0.159	.129-158	255.255.255.224
Subred 20	192.168.0.160/27	192.168.0.191	.161-190	255.255.255.224
Subred 2	192.168.0.192/30	192.168.0.195	.193-194	255.255.255.252
Subred 2	192.168.0.196/30	192.168.0.199	.197-198	255.255.255.252
Subred 2	192.168.0.200/30	192.168.0.203	.201-202	255.255.255.252

Se puede observar que los rangos de direcciones asignados son continuos y que queda disponible para crecimiento futuro un rango de direcciones desde 204 en adelante.

En resumen, si la división es subredes de tamaño diferente: primero ordenamos estos tamaños de mayor a menor y empezamos asignando el mayor, el resto de ips no asignadas las utilizamos para asignar el resto de subredes y así sucesivamente.

AGREGACIÓN DE REDES

El resumen de redes, también conocido como agregación o sumarización de redes, es el proceso de publicar un conjunto de direcciones contiguas como una única dirección con una máscara de subred más corta y menos específica. CIDR es una forma de resumen de ruta y es sinónimo del término creación de superredes. se basa en una técnica que permite resumir un conjunto variable de direcciones IP contiguas de red de una clase en una misma dirección de IP de red para, por un lado, disponer de un espacio de direccionamiento superior sin necesidad de solicitar una dirección de clase superior; y, por otro lado, evitar que las tablas de encaminamiento, y los mensajes para una actualización dinámica de éstas entre routers contiguos, crezcan demasiado.

El resumen de redes en una sola dirección y máscara puede realizarse en tres pasos:

Observemos las siguientes cuatro redes de ejemplo:

172.20.0.0/16

172.21.0.0/16

172.22.0.0/16

172.23.0.0/16

El primer paso es enumerar las redes en formato binario.

10101100.00010100.00000000.00000000

10101100.00010101.00000000.00000000

10101100.00010110.00000000.00000000

10101100.00010111.00000000.00000000

El segundo paso es contar la cantidad de bits coincidentes que se encuentran más a la izquierda para determinar la máscara para la ruta resumida. Se puede ver que coinciden los primeros 14 bits coincidentes que se encuentran más a la izquierda. Éste es el prefijo o máscara de subred para la ruta resumida: /14 ó 255.252.0.0.

10101100.000101**00**.00000000.00000000

10101100.000101**01**.00000000.00000000

10101100.000101**10**.00000000.00000000

10101100.000101**11**.00000000.00000000

Mascara:

11111111.111111**00**.00000000.00000000

255.252.0.0

El tercer paso es copiar los bits coincidentes y luego agregar bits cero al resto de la dirección para determinar la dirección de red resumida. Como se puede apreciar los bits coincidentes con ceros al final producen la dirección de red 172.20.0.0.

Dirección de red:

10101100.00010100.00000000.00000000

172.20.0.0

Conclusión:

Las cuatro redes (172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16 y 172.23.0.0/16) pueden resumirse en una única dirección de red y prefijo 172.20.0.0/14.

Otro ejemplo:

192.1.1.0/27 192.1.1.32/27 192.1.1.64/28 192.1.1.80/28 192.1.1.96/29 192.1.1.104/29 192.1.1.112/29 192.1.1.120/29

Resultado: 192.1.1.0/25

Otro ejemplo, se ha utilizado para identificar las VLANs de una sucursal de una empresa las subredes: 10.1.0.0/24 10.1.1.0/24 10.1.2.0/24 10.1.3.0/24 10.1.4.0/24 10.1.5.0/24 10.1.6.0/24 10.1.7.0/24
Por supuesto, en los dispositivos de la sucursal están presentes estas 8 rutas. Pero se desea que la sucursal publique la menor cantidad de rutas posibles hacia la sucursal central. Nos imaginamos que tenemos un router que comunica la sucursal donde están estas redes con la sucursal central.
Para esto debemos sumarizar estas rutas, para que las tablas de encaminamiento del router sea más sencilla. Estas 8 subredes pueden sumarizarse del modo más eficiente en una única ruta /21 : 10.1.0.0/21

00001010.00000001.00000000.00000000

00001010.00000001.00000001.00000000

00001010.00000001.00000010.00000000

00001010.00000001.00000011.00000000

00001010.00000001.00000100.00000000

00001010.00000001.00000101.00000000

00001010.00000001.00000110.00000000

00001010.00000001.00000111.00000000

Mascara:

11111111.11111111.11111000.00000000 255.255.248.0

¿Se podría sumarizar en la 10.1.0.0/16?

Si, ciertamente es posible, el problema de esta última opción es que el rango de rutas sumarizado es mucho más amplio que el las subredes existentes; si se tratara de subredes /16, esta ruta abarca cualquier subred /16 del rango 10.1.x.x. Pudiera ser que otra sucursal tuviera asignada redes, de ese rango, el router no encaminaria correctamente

Esta es una opción posible cuando se ha reservado ese rango de subredes para uso futuro en esa misma sucursal.

Otro ejemplo:

En otras situaciones el conjunto de rutas a sumarizar no se puede encajar en una única ruta sumarizada, y requiere de una arquitectura diferente.

Por ejemplo, el conjunto de subredes de nuestra sucursal es esta vez el siguiente: 10.2.4.0/24 10.2.5.0/24 10.2.6.0/24 10.2.7.0/24 10.2.8.0/24 10.2.9.0/24 10.2.10.0/24 10.2.11.0/24 10.2.12.0/24 10.2.13.0/24 10.2.14.0/24 10.2.15.0/24 10.2.16.0/24

En principio, esto no es prudente sumarizarlo en la ruta 10.2.0.0/16 pues es posible que otras subredes 10.2.x.x/24 se encuentren ya asignadas en otras sucursales. En consecuencia será preciso aplicarse a realizar una sumarización lo más ajustada posible.

En nuestro caso podemos reducir las 13 rutas actuales a sólo 3:

La ruta 10.2.4.0/22 que sumariza 4 rutas:10.2.4.0/24 10.2.5.0/24 10.2.6.0/24 10.2.7.0/24

La ruta 10.2.8.0/21 que sumariza 8 rutas:10.2.8.0/24 10.2.9.0/24 10.2.10.0/24 10.2.11.0/24 10.2.12.0/24 10.2.13.0/24 10.2.14.0/24 10.2.15.0/24

Y la ruta 10.2.16.0/24, que no puede asociarse con ninguna de las demás.

ICMPV4

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de *Internet Control Message Protocol*) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

Los mensejes ICMP, se encapsulan en datagramas IP con el valor 1 en el campo protocolo, suelen contener en el campo datos, la cabecera y los primeros bytes de datos del datagrama IP que ha provocado el mensaje, ademas del mensaje propiamente dicho. Esto ayuda a identificar el causante del mensaje ICMP.

Los mensajes ICMP que se pueden enviar incluyen:

Confirmación de host: Se puede utilizar un Mensaje de eco del ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. El host que recibe el mensaje de eco responde mediante la respuesta de eco de ICMP. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

Destino o servicio inalcanzable: Se puede usar el destino inalcanzable de ICMP para notificar a un host que el destino o servicio es inalcanzable. Cuando un host o gateway

recibe un paquete que no puede enviar, puede enviar un paquete de destino inalcanzable de ICMP al host que origina el paquete. El paquete de destino inalcanzable tendrá códigos que indican el motivo por el cual el paquete no pudo ser enviado. Entre los códigos de destino inalcanzable se encuentran:

- 0 = red inalcanzable
- 1 = host inalcanzable
- 2 = protocolo inalcanzable
- 3 = puerto inalcanzable

Los códigos para las respuestas red inalcanzable y host inalcanzable son respuestas de un router que no puede enviar un paquete. Si un router recibe un paquete para el cual no posee una ruta, puede responder con un código de destino inalcanzable de ICMP = 0, que indica que la red es inalcanzable. Si un router recibe un paquete para el cual posee una ruta conectada pero no puede enviar el paquete al host en la red conectada, el router puede responder con un código de destino inalcanzable de ICMP = 1, que indica que se conoce la red pero que el host es inalcanzable.

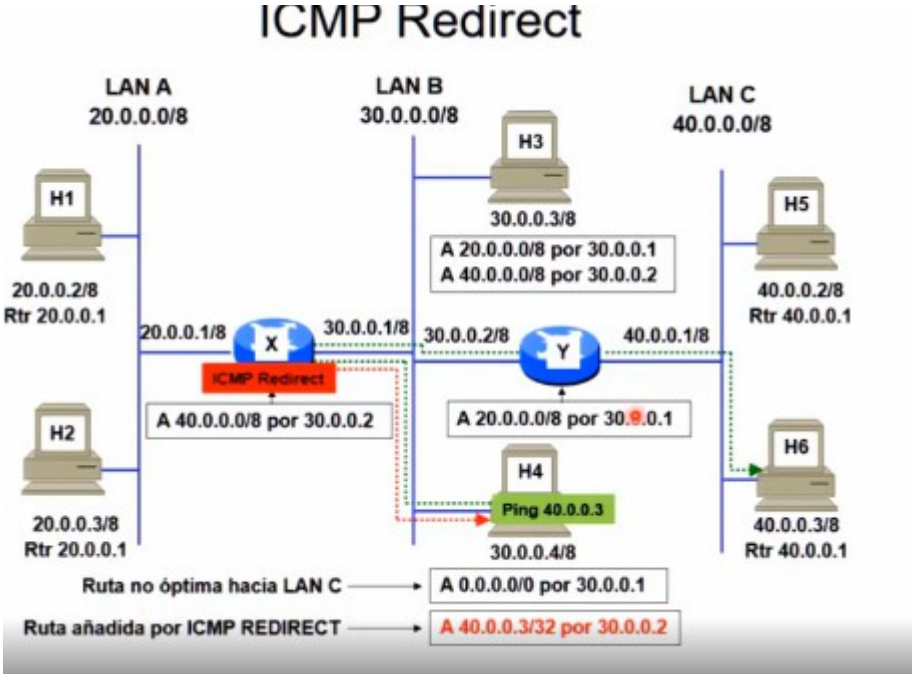
Los códigos 2 y 3 (protocolo inalcanzable y puerto inalcanzable) son utilizados por un host final para indicar que el segmento TCP o el datagrama UDP en un paquete no pudo ser enviado al servicio de capa superior.

Cuando el host final recibe un paquete con una PDU de capa 4 que se enviará a un servicio no disponible, el host puede responder al host de origen con un código de destino inalcanzable de ICMP = 2 o con un código = 3, que indica que el servicio no está disponible. Es posible que el servicio no esté disponible debido a que no hay un daemon en funcionamiento que proporcione el servicio o porque la seguridad del host no permite el acceso al servicio.

Tiempo superado: Un router utiliza un mensaje de tiempo superado de ICMP para indicar que no se puede enviar un paquete debido a que el campo TTL del paquete ha expirado. Sin un router recibe un paquete y disminuye el campo TTL del paquete a cero, éste descarta el paquete. El router también puede enviar un mensaje de tiempo superado de ICMP al host de origen para informar al host el motivo por el que se descartó el paquete.

Su interés es ser la base del programa traceroute o en Windows tracert(creado por Jacobson, uno de los padres de TCP/IP). El programa va enviado mensajes con TTL 1, TTL 2,.... al llegar a los router y hacerse TTL 0, estos generan el mensaje de tiempo superado y con las respuestas (el host, que ejecuta traceroute)obtiene la ip del router, el tiempo, ... así va registrando la ruta

Redireccionamiento de ruta: Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways. SI un router recibe un paquete para el cual tiene una ruta y para el próximo salto se conecta con la misma interfaz del paquete recibido, el router puede enviar un mensaje de redireccionamiento de ICMP al host de origen. Este mensaje informará al host de origen acerca del próximo salto en una ruta de la tabla de enrutamiento.



Disminución de velocidad en origen: El mensaje de disminución de velocidad en origen de ICMP puede usarse para informar al origen que deje de enviar paquetes por un tiempo.

Si un router no posee suficiente espacio en búfer para recibir paquetes entrantes, un router descartará los paquetes. SI debe hacerlo, también puede enviar un mensaje de disminución de velocidad en origen de ICMP a los hosts de origen por cada mensaje que descarta.

Un host de destino también puede enviar un mensaje de disminución de velocidad en origen si los datagramas llegan demasiado rápido para ser procesados.

Cuando un host recibe un mensaje de disminución de velocidad en origen de ICMP, lo informa a la capa de transporte. El host de origen puede utilizar el mecanismo de control de flujo de TCP para adaptar la transmisión.

Aplicaciones del protocolo ICMP.

Las herramientas ping y traceroute(tracert en Windows) envían mensajes de petición Echo ICMP y reciben mensajes de respuesta Echo, para determinar:

- si un host está o no disponible.
- el tiempo que tardan los paquetes en ir y regresar a ese host .
- la cantidad de router por los que pasa.
- ….

En función de estos datos, infieren otros que nos son de utilidad para administrar la red.

Ping.

Ping envía solicitudes de respuestas desde una dirección host específica. Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

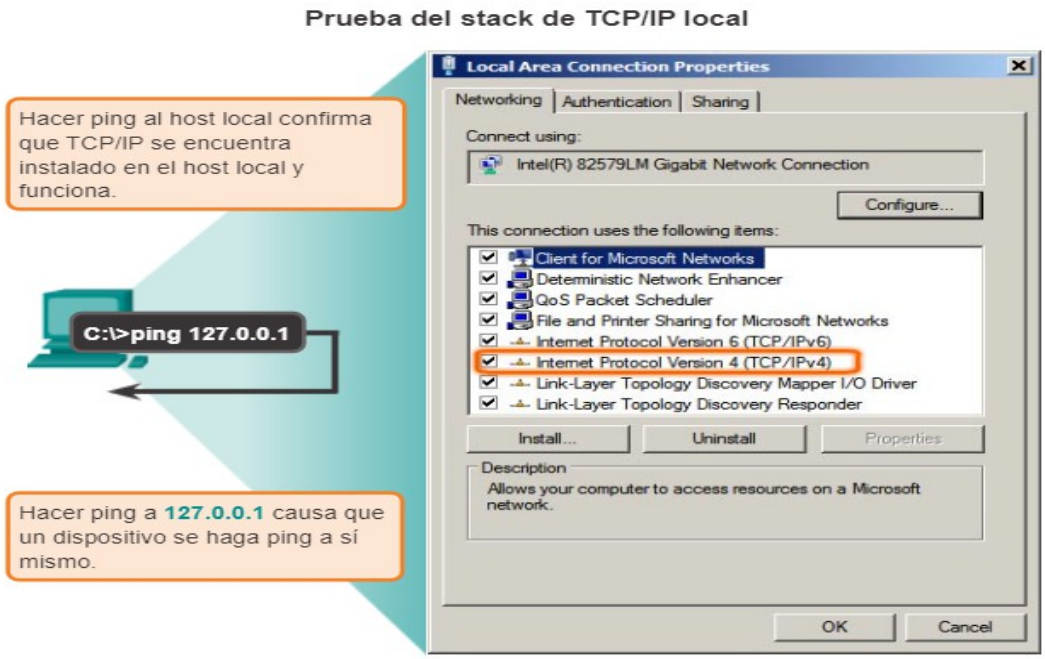
A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. Ping posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

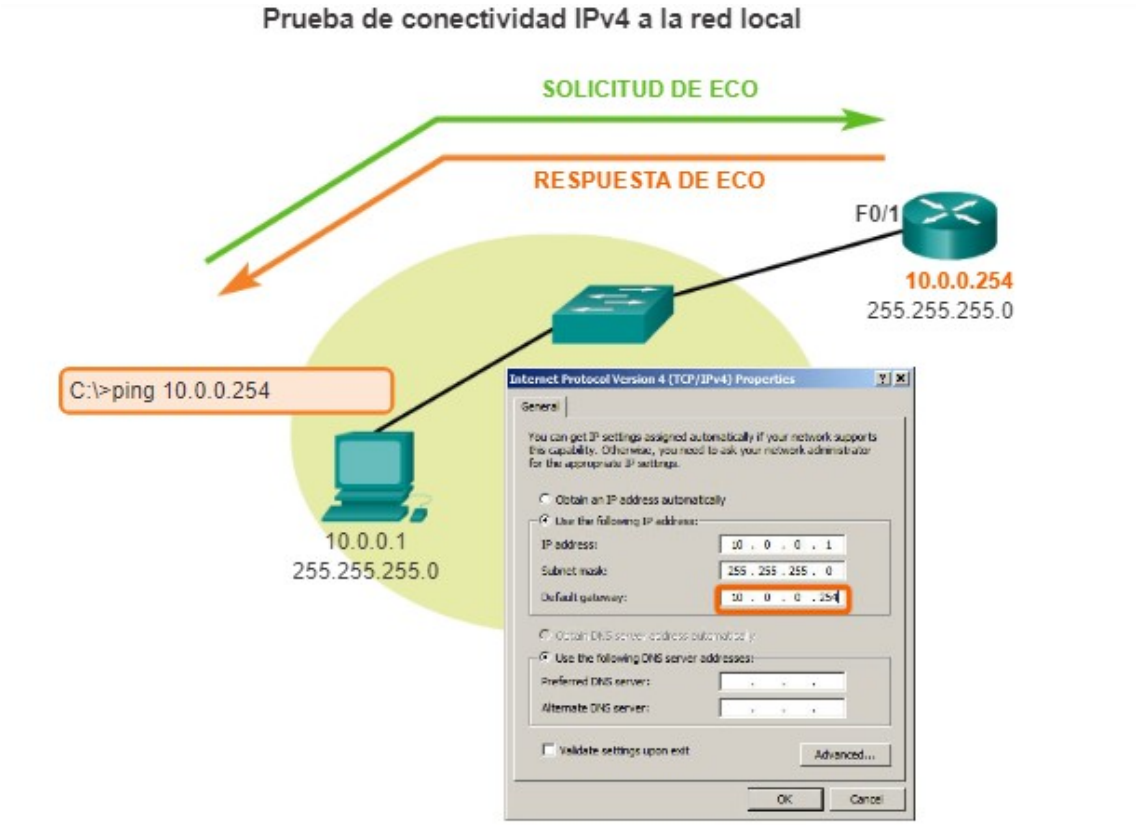
```
C:\Users\RMI>ping www.goole.es

Haciendo ping a www.goole.es [185.53.178.70] con 32 bytes de datos:
Respuesta desde 185.53.178.70: bytes=32 tiempo=48ms TTL=49
Respuesta desde 185.53.178.70: bytes=32 tiempo=48ms TTL=49
Respuesta desde 185.53.178.70: bytes=32 tiempo=49ms TTL=49
Respuesta desde 185.53.178.70: bytes=32 tiempo=49ms TTL=49

Estadísticas de ping para 185.53.178.70:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 48ms, Máximo = 49ms, Media = 48ms

C:\Users\RMI>
```

Son especialmente útiles los siguientes Ping

Ping del loopback local: Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna del IP en el host local. Para hacer esta prueba, se realiza el ping de la dirección reservada especial del loopback local (127.0.0.1), como se muestra en la figura. Una respuesta de 127.0.0.1 indica que el protocolo IP está correctamente instalado en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior del stack de red. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el protocolo TCP/IP no funciona en el host.

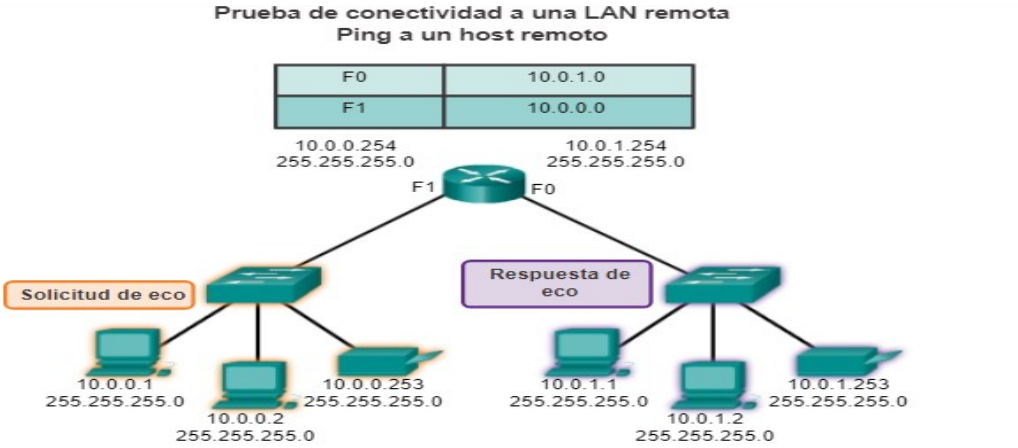


Ping a la dirección IP del gateway: también es posible utilizar el ping para probar la capacidad de comunicación del host en la red local. Generalmente, esto se hace haciendo ping a la dirección IP del gateway del host, como se muestra en la figura. Un ping en el gateway indica que la interfaz del host y del router que funcionan como gateway funcionan en la red local.



Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de gateway no responde, se puede intentar con la dirección IP de otro host que sepa que funciona en la red local.

Ping a host remoto: también se puede utilizar el ping para probar la capacidad de comunicación del host IP local en una internetwork. El host local puede hacer ping a un host que funciona en una red remota, como se muestra en la figura.



Si el ping se realiza con éxito, se habrá verificado la operación de una porción amplia de la internetwork. Esto significa que se ha verificado la comunicación del host en la red local, el funcionamiento del router que se usa como gateway y los demás routers que puedan encontrarse en la ruta entre la red y la red del host remoto.

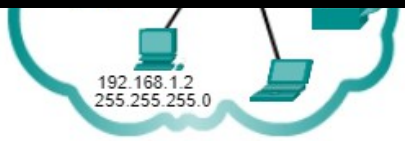
Traceroute.

Si ping se usa para indicar la conectividad entre dos hosts, traceroute (tracert en windows) es una utilidad que permite observar la ruta entre estos hosts. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallos. Si los datos llegan a destino, entonces el rastreador menciona la interfaz de cada router que aparece en el camino.

Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo. Esto indica el lugar donde se encuentra el problema o las restricciones de seguridad.

```
C:\Users\RMI>tracert www.google.es

Traza a la dirección www.google.es [172.217.168.163]
sobre un máximo de 30 saltos:

  1     6 ms     3 ms     1 ms  192.168.0.1
  2    16 ms    12 ms    14 ms  10.194.219.1
  3    11 ms    11 ms    10 ms  10.80.9.201
  4    10 ms    12 ms    11 ms  172.29.192.101
  5     *        *        *     Tiempo de espera agotado para esta solicitud.
  6    17 ms    19 ms    20 ms  212.166.147.222
  7    16 ms    17 ms    16 ms  172.253.50.45
  8    19 ms    18 ms    18 ms  74.125.253.201
  9    21 ms    21 ms    21 ms  mad07s10-in-f3.1e100.net [172.217.168.163]

Traza completa.
```



Tiempo de ida y vuelta (RTT): El uso de traceroute proporciona el tiempo de ida y vuelta (RTT) para cada salto a lo largo del camino e indica si se produce una fallo en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Para que tenga una significación estadistica, lo hace tres veces (para cada router, cada fila). Otra consideración es que se usa un asterisco (*) para indicar que no puede hallar la dirección, esto suele ser por que el router tiene una ip privada en su interfaz(por lo que no pasa el paquete de vuelta por los router del ISP) o un cortafuegos.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si tenemos altos tiempos de respuesta o pérdidas de datos de un salto particular, ésta es una indicación de que los recursos del router o sus conexiones pueden estar estresados.

DIRECCIONAMIENTO A NIVEL DE RED: IPV6

INTRODUCCIÓN IPV6

En nuestros equipos ya aparece configurado el protocolo IPv6. Vemos direcciones semejantes a la figura, sin tener que configurar nada.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Dirección física. . . . . . . . . . . . . : A8-1E-84-19-92-7C
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::a875:f35a:f249:6643%18(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.35(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
```

Para comprender los problemas de direccionamiento IP que enfrentan los administradores de red en la actualidad, hay que tener en cuenta que el espacio de direcciones de IPv4 proporciona aproximadamente 4 294 967 296 direcciones únicas. De éstas, sólo es posible asignar 3700 millones de direcciones porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

A partir de cifras muy recientes aproximadamente 3000 millones de las direcciones IPv4 disponibles ya están asignadas a usuarios finales o ISP. Esto deja unas 700 millones de direcciones disponibles del espacio de direcciones IPv4. Si bien parece ser una cifra importante, el espacio de direcciones IPv4 se está agotando.

En la última década, la comunidad de Internet ha analizado el problema del agotamiento de las direcciones IPv4 y se han publicado enormes cantidades de informes.

El conjunto de números se está reduciendo por los siguientes motivos:

- Crecimiento de la población: la población de Internet está creciendo. En noviembre de 2005, se estimó que había aproximadamente 973 millones de usuarios. Desde entonces, esta cifra se ha duplicado. Además, los usuarios permanecen conectados durante más tiempo, lo que hace que reserven direcciones IP durante períodos más prolongados y se comuniquen con una cantidad creciente de peers cada día.

- Usuarios móviles: la industria ha colocado más de mil millones de teléfonos móviles. Se han vendido más de 20 millones de dispositivos móviles habilitados para IP, incluidos los asistentes digitales personales (PDA, Personal Digital Assistants), pen tablets, blocs de notas y lectores de código de barras. Cada día se conectan más dispositivos habilitados para IP. Los teléfonos antiguos no necesitaban direcciones IP, pero los nuevos sí las necesitan.

- Transporte: los modelos más recientes están habilitados para IP, para permitir el monitoreo remoto y proporcionar mantenimiento y asistencia con rapidez. Lufthansa ya brinda conectividad a Internet en sus vuelos. Más empresas de transporte, incluido el transporte marítimo, proporcionarán servicios similares.

- Productos electrónicos para los consumidores: los dispositivos para el hogar permiten la supervisión remota mediante la tecnología IP. Las grabadoras de video digital (DVR, Digital Video Recorders) que descargan y actualizan guías de programas de Internet son un ejemplo. Las redes domésticas pueden conectar estos dispositivos.

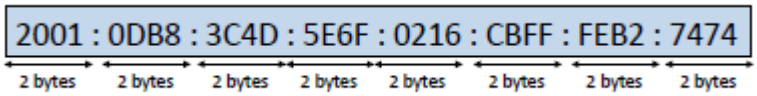
La posibilidad de expandir las redes para exigencias futuras **requiere un suministro ilimitado de direcciones IP** y una mayor movilidad que no se pueden satisfacer sólo con DHCP y NAT. IPv6 satisface los requisitos cada vez más complejos del direccionamiento jerárquico que IPv4 no proporciona.

Dada la enorme base instalada de IPv4 en todo el mundo, no es difícil apreciar que la transición de IPv4 a IPv6 es un desafío. Sin embargo, hay una variedad de técnicas, entre ellas una opción de **configuración automática,** para facilitar la transición. El mecanismo de transición que debe utilizar depende de las necesidades de su red.

CARACTERÍSTICAS DE IPV6

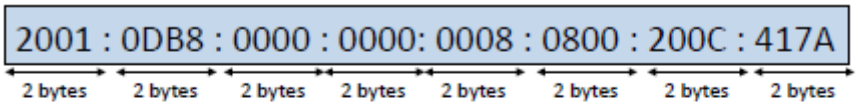
Una dirección IPv6 es un valor binario de 128 bits, que se puede mostrar como 32 dígitos hexadecimales. IPv6 debería proporcionar una cantidad de direcciones suficiente para las necesidades de crecimiento futuras de Internet durante muchos años más. La cantidad de direcciones IPv6 disponibles permiten asignar a cada metro cuadrado del planeta (incluyendo océanos) un espacio de direcciones de Internet de 7 x 10 elevado a 23, mas o menos equivalente al espacio de Ipv4.

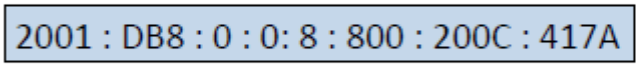
Vemos un ejemplo de dirección Ipv6:

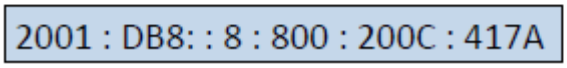


Se suele llamar **hexteto** a cada una de esas partes de 16 bits.

Podemos encontrarlas más cortas, debido a que se simplifican, como por ejemplo:







¿Y qué ocurrió con IPv5? IPv5 se utilizó para definir un protocolo de transmisión en tiempo real experimental. Para evitar confusiones, se decidió no utilizar IPv5 y llamar IPv6 al nuevo protocolo IP.

DIRECCIONAMIENTO IP MEJORADO

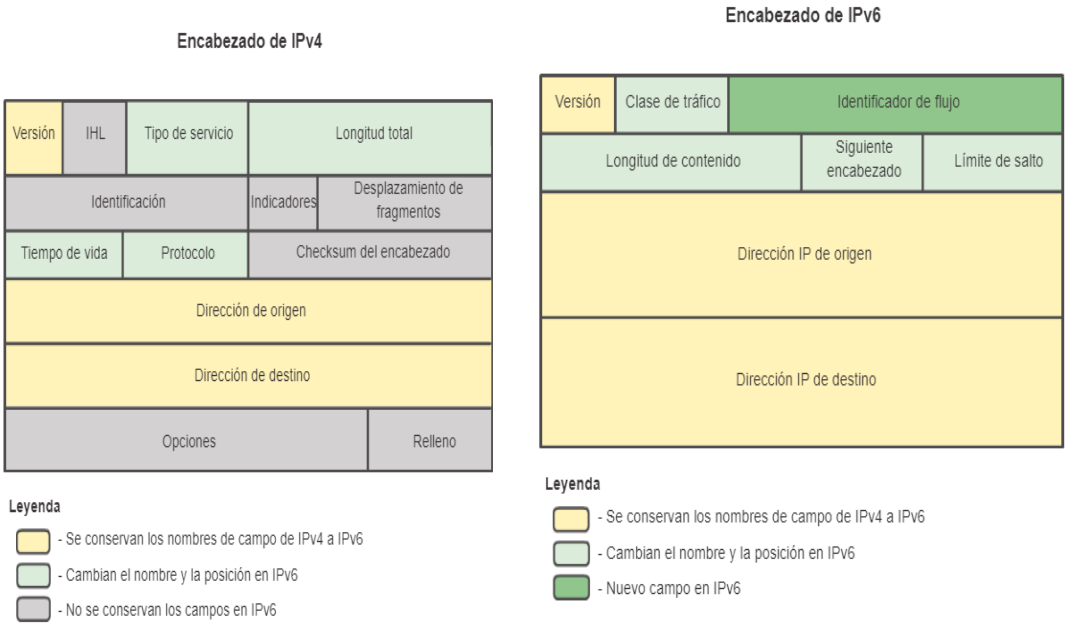
Un espacio de direcciones más grande ofrece varias mejoras, entre ellas:

- Más posibilidad de conexión y flexibilidad global.
- Mejor agrupación de los prefijos IP anunciados en las tablas de enrutamiento.
- Hosts con múltiples conexiones. La multiconexión es una técnica para aumentar la confiabilidad de la conexión a Internet de una red IP. Con IPv6, un host puede tener varias direcciones IP a través de un enlace ascendente físico. Por ejemplo, un host puede conectarse a varios ISP.
- Configuración automática que puede incluir direcciones de capa de enlace de datos en el espacio de la dirección.

- Más opciones plug-and-play para más dispositivos.
- Redireccionamiento de extremo a extremo de público a privado sin traducción de direcciones. Esto hace que las redes entre peers (P2P) sea más funcional y fácil de implementar.

ENCABEZADO SIMPLE

Comparativa de las cabeceras o encabezados de los datagramas de Ipv4 y Ipv6:



(A estos encabezados seguirían el campo de carga útil: paquete del nivel de trasporte u otro protocolo que encapsulara: ICMP, ...)

Estudio de los campos IPv6:

Versión: define la versión del protocolo IP su valor es 6.

Clase de tráfico(prioridad): sirve para distinguir los paquetes que, en origen se puede controlar el flujo (0-7), de los que no (8-15), porque son tráfico en tiempo real (como audio, vídeo,....). Dentro de estos valores los menores son menos importantes; el router prioriza tráfico en función del contenido del campo.

Identificador de flujo: (experimental) si es distinto de 0 requiere tratamiento especial (requisitos como:retardo estricto,...) es un intento de tener lo mejor de una subred de datagramas y de una red de circuitos virtuales. Su valor identificaría un circuito "virtual" de flujo entre el origen y el destino.

Longitud de contenido: indica cuantos bytes siguen a la cabecera de 40 bytes.

Siguiente encabezado: como puede haber cabeceras de extensión, este campo indica cual de las 6 posibles cabeceras de extensión sigue a esta, en caso de ser la ultima indica el manejador de la capa de trasporte(TCP o UDP) al que se entregara el paquete.

Limite de saltos: para evitar que el paquete vague eternamente

Dirección ip origen:

Dirección ip destino:

La figura compara la estructura de encabezado simplificada de IPv6 con la del encabezado de IPv4. El encabezado de IPv4 tiene 20 octetos y 12 campos de encabezado básicos, seguidos por un campo de opciones y una sección de datos (normalmente el segmento de la capa de transporte). El encabezado de IPv6 tiene 40 octetos, tres campos de encabezado de IPv4 básicos y cinco campos de encabezado adicionales.

El encabezado simplificado de IPv6 ofrece varias ventajas con respecto a IPv4:

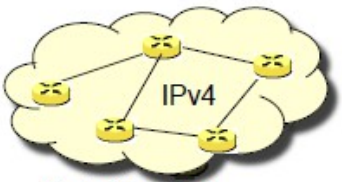
- Mayor eficacia de enrutamiento para obtener mejor rendimiento y más escalabilidad de velocidad de reenvío.
- Ausencia de broadcasts, de manera que no existe peligro potencial de tormentas de broadcasts.
- No hay necesidad de procesar checksums.
- Mecanismos de encabezado de extensión más simples y eficaces.
- Rótulos de flujo, en función del procesamiento de flujo, sin necesidad de abrir el paquete interno de transporte, para identificar los diferentes flujos de tráfico.

INTENSIDAD DE TRANSICIÓN

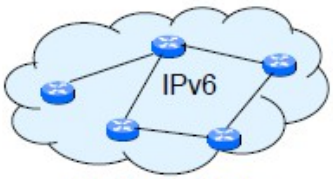
IPv4 no desaparecerá de la noche a la mañana. En realidad, coexistirá durante un tiempo con IPv6 y será reemplazado gradualmente por éste. Por este motivo, IPv6 incluye técnicas de migración que abarcan cada caso de actualización de IPv4 concebible. Sin embargo, muchas de estas técnicas fueron en última instancia rechazadas por la comunidad tecnológica.

En la actualidad hay tres enfoques principales:

- Stack doble.
- Tunneling: encapsulación de paquetes ipv6 en paquetes ipv4.
    - Automáticos: 6to4, ISATAP y Teredo (métodos de último recurso)
    - Manuales.
- Traducción: conversión de paquete ipv4 a ipv6 y viceversa NAT64

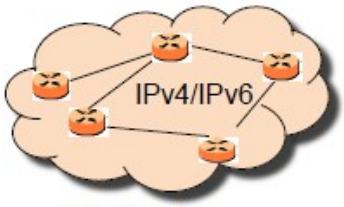


Red sólo IPv4

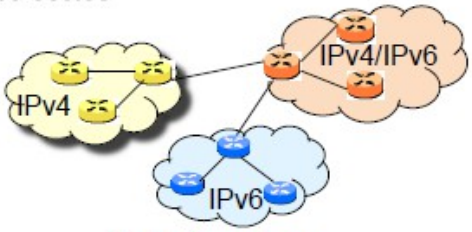


Red sólo IPv6

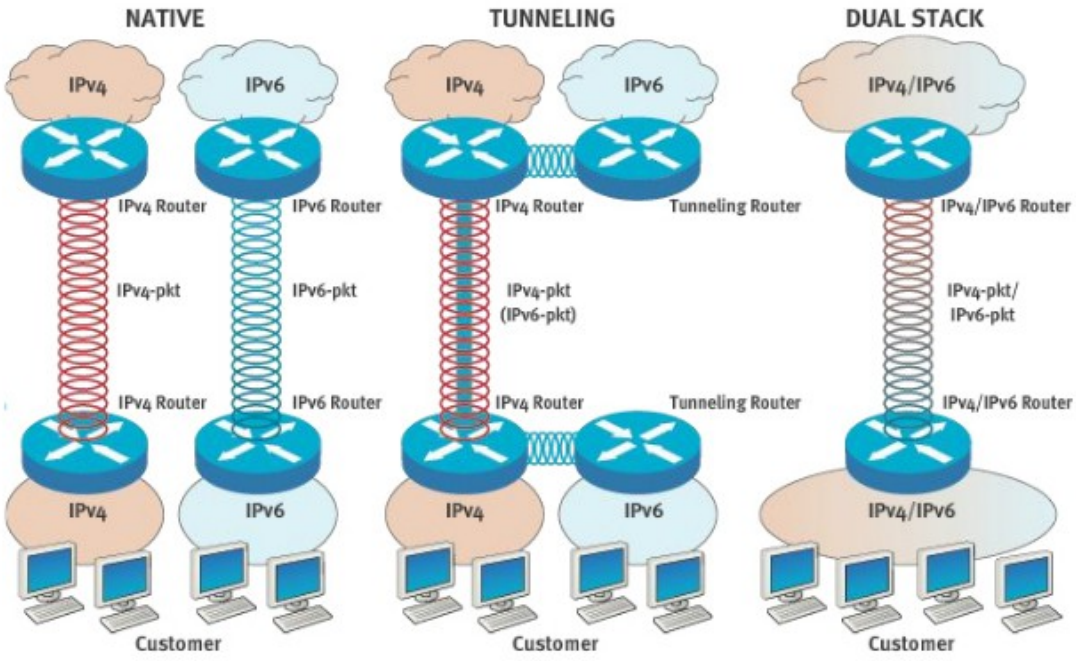
Mecanismos de transición:
Túneles
Traducción de protocolos

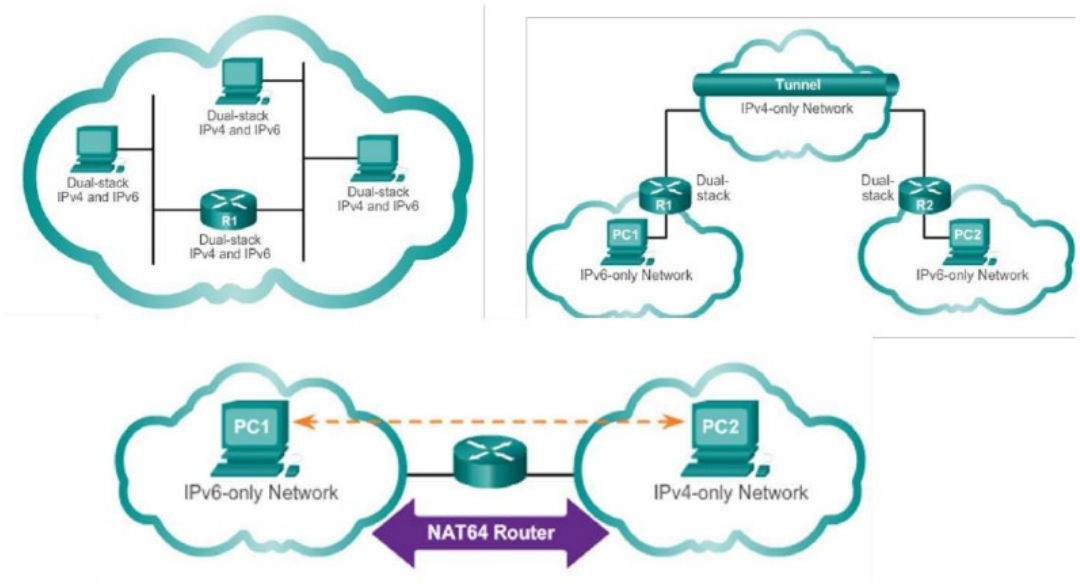


Red dual



Red heterogénea





El consejo actual para hacer la transición a IPv6 se trata de usar “stack doble” cuando pueda y tunneling cuando no tenga otra opción".

DIRECCIONAMIENTO IPV6

Las direcciones IPv4 conocidas tienen 32 bits representados como una serie de cuatro campos de 8 bits separados por puntos. Sin embargo, las direcciones IPv6 de 128 bits son más largas y necesitan una representación diferente a causa de su tamaño. Las direcciones IPv6 utilizan dos puntos (:) para separar entradas en una serie hexadecimal de 16 bits, que se suele conocer con el nombre de **hexteto**.

Sigamos el ejemplo:

2031:0000:130F:0000:0000:09C0:876A:130B

Se pueden acortar la dirección mediante la aplicación de las siguientes pautas:

- Los ceros iniciales de los campos son opcionales. Por ejemplo, el campo 09C0 es igual a 9C0 y el campo 0000 es igual a 0. De manera que

  2031:**0000**:130F:**0000:0000**:**09C0**:876A:130B

  puede escribirse como

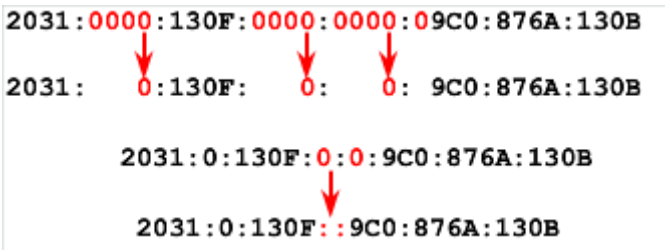
  2031:**0**:130F:**0:0**:**9C0**:876A:130B.

- Los campos sucesivos de ceros pueden representarse con doble dos puntos "::". Sin embargo, este método de abreviación sólo puede utilizarse una vez en una dirección. Por ejemplo 2031:0:130F**:0:0:**9C0:876A:130B puede escribirse como:

  2031:0:130F**::**9C0:876A:130B

- Una dirección no especificada se escribe "::" porque sólo contiene ceros.

El uso de la notación "::" reduce en gran medida el tamaño de la mayoría de las direcciones que se muestran. Un analizador de direcciones identifica la cantidad de ceros faltantes mediante la separación de dos partes de una dirección y la adición de ceros hasta completar los 128 bits.



EJEMPLOS:

- FF01:0:0:0:0:0:0:1 se convierte en FF01::1
- 0:0:0:0:0:0:0:1 se convierte en ::1
- 0:0:0:0:0:0:0:0 se convierte en ::
- FF01:0000:0000:0000:0000:0000:0000:1 se convierte en

  FF01:0:0:0:0:0:0:1 se convierte en FF01::1
- E3D7:0000:0000:0000:51F4:00C8:C0A8:6420 se convierte en E3D7::51F4:C8:C0A8:6420
- 3FFE:0501:0008:0000:0260:97FF:FE40:EFAB se convierte en 3FFE:501:8:0:260:97FF:FE40:EFAB se convierte en

  3FFE:501:8::260:97FF:FE40:EFAB

Notación decimal con puntos

Durante la transición de Internet de IPv4 a IPv6 será típico operar en entornos de doble direccionamiento (IPv4 e IPv6). Por este motivo se ha introducido una notación especial para expresar direcciones IPv6 que sean IPv4-mapeada o IPv4-compatible, representando los últimos 32 bits de la dirección IPv6 en el formato decimal con puntos usado en IPv4.

Por ejemplo, para 192.0.2.128 (C0.00.2.80), su dirección IPv6 del tipo Ipv4-mapeada

::ffff:c000:280

se puede representar en notación Ipv4_compatible (no se usa, aunque todavía en los RFC no se ha descartado su uso) como

::192.0.2.128

mostrando claramente la dirección IPv4 mapeada dentro de la IPv6.

Las máscaras, para identificar en routers subredes y rangos de direcciones Ipv6, son expresadas de la misma forma que en la notación CIDR utilizada en IPv4.

En IPv6 la longitud del **prefijo** indica un conjunto mínimo de bits comunes, que no se deben cambiar y que identifican unívocamente a cualquier "clase" de la DIRECCION Ipv6.

En las redes IPv6 el prefijo es siempre /64, es decir, las redes en IPv6 son de tamaño fijo.

Un prefijo de dirección IPv6 se representa con la siguiente notación:

direccion-ipv6 / longitud-prefijo, donde

direccion-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.

longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección. Así el router toma decisiones de por donde encaminar

CLASIFICACIÓN:

Las direcciones identifican interfaces individuales (no hosts)o conjuntos de interfaces. Se clasifican en tres tipos:

- **Unicast** identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Consideramos los siguientes tipos:
    - Dirección unicast local de enlace (privada): Para tareas internas.
    - Dirección unicast global (pública): Es única en el mundo, por lo que se pueden enrutar a nivel mundial sin ninguna modificación.
    - Dirección unicast local de sitio (privada): No es enrutable fuera de la red. Es el equivalente a la ipv4 privada. NO RECOMENDADO SU USO.
    - Dirección unicast local exclusiva. Sustituyen a la anterior.
- **Anycast** identifican a un conjunto de interfaces(TIPICAMENTE PERTENECEN A DISTINTOS NODOS). Un paquete enviado a una dirección anycast, (pensemos en un servidor dns) será entregado a una de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast, (la más próxima según las medidas de distancia del protocolo de encaminamiento). Nos permite crear ámbitos de redundancia, de forma que varias máquinas pueden ocuparse del mismo tráfico(según secuencia determinada por el routing) si una cae. En toda red tiene que conocerse la dirección anycast del router de subred ,que es la dirección de la subred y los últimos 64 bits a cero.

- **Multicast** identifican un grupo de interfaces(dispositivos). Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

DIFERENCIAS CON RESPECTO A IPV4:

- El prefijo nos permite conocer la ruta de encaminamiento, es decir donde esta conectada esa ip. A los clientes de los ISP se les asigna una /48, teniendo así 16 bits para subredes internas.
- No hay direcciones broadcast
- Las direcciones IPv6 se asignan a interfaces no a nodos. Dado que las interfaces pertenecen a nodos, podemos utilizar cualquier dirección unicast para referirnos al nodo.
- Todas las interfaces han de tener una dirección de enlace-local.
- Una interfaz puede tener varias direcciones Ipv6 de cualquier tipo(unicast, anycast, multicast) y ámbito
- En IPv4 sólo permite un nivel jerárquico: **netid** (parte para la red de la ip) y **hostid** (parte para hosts de la ip), pero IPv6 permite más niveles de jerarquía, no se habla de direcciones de host, sino no de direcciones de interfaces de un host. (pueden haber varias)

Cada dirección IPv6 comienza por un prefijo que indica qué tipo de dirección es:

Tipo de dirección	**Comienzo en binario**	**Comienzo en hexadecimal**	**Dirección**
Dirección indefinida	0000 0000	00	::/128
Unicast Global, documentación			2001:db8::/32
Unicast Global	001	2 ó 3	2000::/3
Unicast Enlace Local	1111 1110 10	FE8 hasta FEB	FE80::/10
Unicast Enlace de sitio	1111 1110 11	FEC0 hasta FEFF	FEC0::/10

Declarado obsoleto en RFC3879, aunque existe en la bibliografia.			
Unicast local exclusiva	1111 1101	FC00 hasta FDFF	FC00::/7
Multicast	1111 1111	FF	FF00::/8

DIRECCIÓN UNICAST GLOBAL DE DOCUMENTACIÓN

2001:db8::/32 Este prefijo está reservado para documentación. Estas direcciones deben usarse siempre que alguien quiera escribir un ejemplo de dirección IPv6, o se plasmen modelos de red

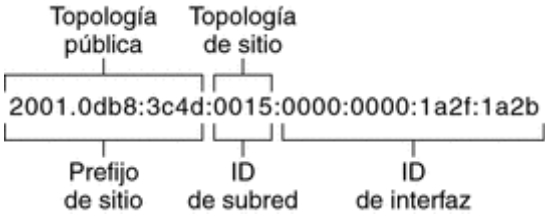
DIRECCIÓN UNICAST GLOBAL DE IPV6

Son las que utiliza una máquina conectada a Internet. Para que no sean tan grandes las tablas de enrutamiento ,se organizan las direcciones de forma jerárquica.

Las direcciones unicast globales normalmente están compuestas por un prefijo de enrutamiento global de 48 bits y un ID de subred de 16 bits. Las organizaciones individuales pueden utilizar un campo de subred de 16 bits para crear su propia jerarquía de direccionamiento local. Este campo permite a la organización utilizar hasta 65.535 subredes individuales.

La dirección unicast global actual asignada por IANA utiliza el rango de direcciones que comienzan con el valor binario 001 (2000::/3). Esto significa que las direcciones solo pueden comenzar por los números hexadecimales 2 o 3.

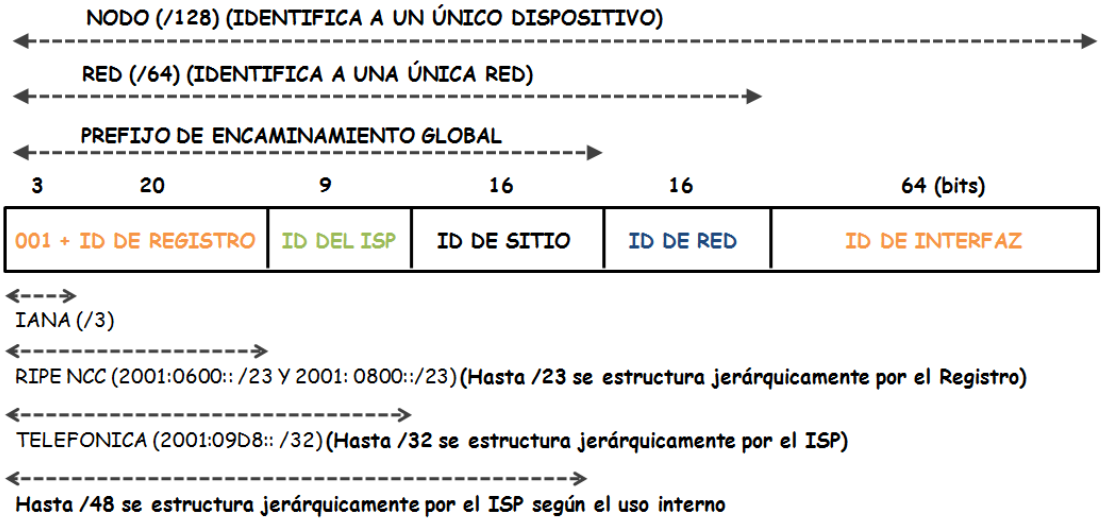
IANA está asignando espacio de direcciones IPv6 en los rangos de 2001::/16 a los cinco registros RIR (ARIN, RIPE, APNIC, LACNIC y AfriNIC). Ejemplo:



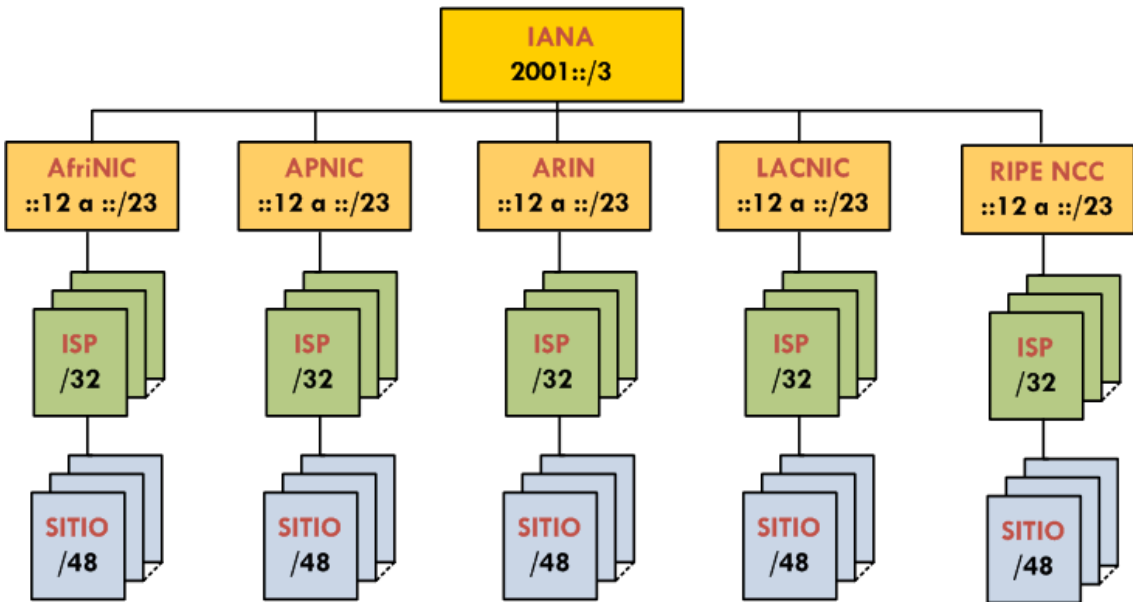
Permiten la autoconfiguración:

- Una máquina puede obtener el prefijo de red desde el router de su red.

- El identificador de interfaz se puede construir: a partir de la dirección MAC, o bien de forma aleatoria (Windows 10). Esto se puede fijar en la configuración de la máquina.



Lo general es que un ISP nivel 1 pueda otorgar una red de prefijo /48 a una entidad(cliente), pero se puede optar por solicitar una red de prefijo /32 directamente a RIPE. Este tamaño de prefijo se entrega normalmente a proveedores de servicios, sin embargo se otorga excepcionalmente a instituciones que puedan justificar su uso. Si obtenemos una red /48 podemos utilizar los siguientes 16 bits para hacer nuestras subredes (nuestro enrutamiento interno) y el resto hasta los 128 bits (64 bits) para los equipos.



Curiosidad: RIPE concedió a Jazztel un rango de direcciones IPv6, concretamente el 2a02:2e00::/27. Llama la atención su tamaño, puesto que normalmente los rangos asignados a los operadores son /32 y en el caso de Jazztel es /27. Con este bloque la operadora tiene espacio suficiente para 137.000 millones de rangos domésticos.

Cabe mencionar que en IPv6 a los routers domésticos(los ISP) no se les asigna una IP, sino un rango /64, con lo cual no es necesario hacer NAT, ya que cada router dispone (en su red) de millones de direcciones IP públicas.

DIRECCIONES UNICAST LOCAL (DE ENLACE, DE SITIO Y LOCAL EXCLUSIVA)

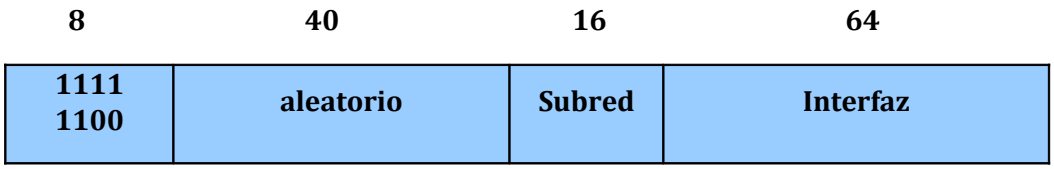
Se separó un bloque de direcciones IPv6 para direcciones privadas, igual que lo que se hizo con IPv4. Estas direcciones privadas son locales solamente en un enlace o sitio en particular y, por lo tanto, nunca se enrutan fuera de la red de una empresa particular. Las direcciones privadas tienen un primer valor de octeto de "FE" en la notación hexadecimal y el siguiente dígito hexadecimal es un valor de 8 a F.

Estas direcciones se subdividen en tres tipos, según su ámbito.

- Las direcciones locales de un sitio son direcciones similares a la asignación de direcciones para Internets privadas en IPv4. El ámbito de estas direcciones es un sitio o una organización completa. **Sin embargo, el uso de direcciones locales de un sitio es problemático y RFC 3879 lo desaprueba desde 2003**. En notación hexadecimal, las direcciones locales de un sitio comienzan con "FE" y el tercer dígito hexadecimal está entre "C" y "F". Es así como estas direcciones comienzan con "FEC", "FED", "FEE" o "FEF".

FEC0::<ID-SUBRED>:<ID-INTERFAZ>/10

- Las direcciones locales exclusivas comienzan por FC, seguidas de 40 bits pseudoaleatorios con el fin de que sean exclusivas en el universo, los siguientes 16 bits estarían destinados a subredes. Se utilizan para comunicaciones locales. Son enrutables solo dentro de un ámbito cooperativo (similar a los rangos de direcciones privadas `10/8`, `172.16/12`, y `192.168/16` en IPv4)

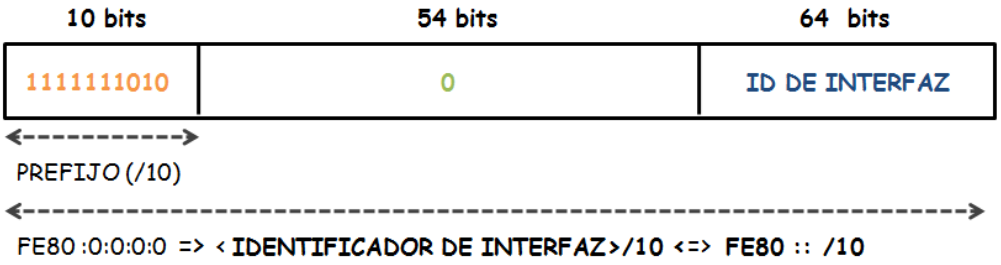


FC00::/7

- Las direcciones unicast de enlace local son nuevas dentro del concepto de direccionamiento con IP en la capa de red. Estas direcciones tienen un ámbito más pequeño que las direcciones locales de un sitio, ya que hacen referencia solamente a un enlace físico en particular (red física). No se enrutan ni siquiera dentro de la organización. Son útiles en redes sin routers. Se utilizan para comunicaciones de enlace, por ejemplo, configuración automática de direcciones, detección de vecinos

y detección de routers. Muchos protocolos de enrutamiento IPv6 también utilizan direcciones link-local. En notación hexadecimal, las direcciones link-local comienzan con "FE" y el tercer dígito hexadecimal es un valor entre "8" y "B". Así es como estas direcciones comienzan con "FE8", "FE9", "FEA" o "FEB".

FE80::<ID-INTERFAZ>/10



DIRECCIONES MULTICAST

Como se mencionó anteriormente en ipv6 no existe la dirección de broadcast o multidifusión, esta ha sido sustituida por un conjunto de direcciones multicast, usando una dirección multicast distinta para cada función, esto permite que si un host no quiere participar en una determinada acción ignorará este tipo de multidifusiones. (Por ejemplo, un mensaje de solicitud de router solo será respondido por los routers).

Solo pueden usarse como direcciones de destino y nunca como direcciones de origen

Formato general de dirección multicast

bits	8	4	4	112
campo	*prefix*	*flags*	*scope*	*group ID*
valor	11111111	0RPT	XXXX	

Comienzan por FF (=x11111111)

Le sigue los flags (0RPT), r, p reservados, t=0 bien conocido 1= temporal

Le sigue el indicador de Ámbito: (donde el paquete debe ser propagado)

- Nodo local (0001) (0x1)
- Enlace local (0010) (0x2)
- Sitio local (0101) (0x5)
- Organización (1000) (0x8)
- Global (1110) (0xE)

El protocolo de descubrimiento de vecino (NDP) tiene direcciones reservadas desde FF02::1:FF00:0 hasta FF02::1:FFFF:FFFF. Ejemplo: Se necesita averiguar la dirección MAC asociada con la dirección IPv6 2001::1:800:200E:8C6C se envía un mensaje ICMP

Neigbour Discovery a la dirección FF02::1:FF0E:8C6C (**Nodo solicitado multicast**). A este grupo se incluye un dispositivo cuando se asigna una dirección IP.

Formato de dirección multicast Solicited-node

bits	8	4	4	79	9	24
campo	*prefix*	*flags*	*scope*	*ceros*	*unos*	*dirección unicast*
valor	11111111	0000	0010	00000000...00000000	111111111	

Ejemplos de direcciones multicast:

(FF01 útil solo para la transmisión loopback del tráfico multicast)

Direcciones multicast de los routers: (un mensaje a esta direcciones será respondido por:)

- FF01::2 → routers del nodo local.
- FF02::2 → routers del enlace local.

Direcciones multicast de los computadores:

- FF01::1 → computador del nodo local (todos los interfaces del nodo local).
- FF02::1 → computadores del enlace local.

  (Ejemplo ff02::1:2 para buscar servidor dhcp6)

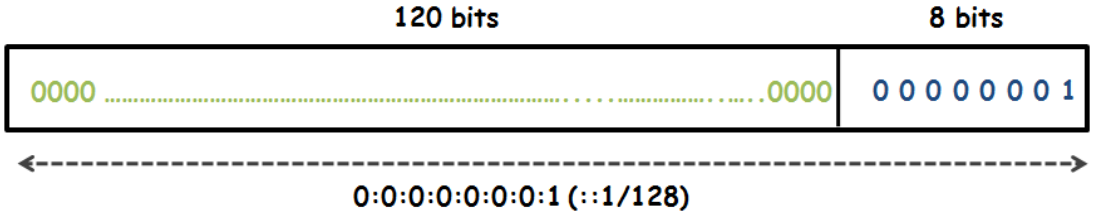
Todas estas direcciones se gestionan de forma trasparente para el administrador de sistemas. Por ejemplo esta es la salida parra la interfaz de un router, al que el administrador solo le ha configurado la ipv6. Nos fijamos en las direcciones multicast:

```
Router#SHOW IPV6 INTERFACE FASTETHERNET0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::202:4AFF:FEB2:7901
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:CAFE:8000::, subnet is 2001:DB8:CAFE:8000::/49
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FFB2:7901
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
```

DIRECCIÓN DE LOOPBACK

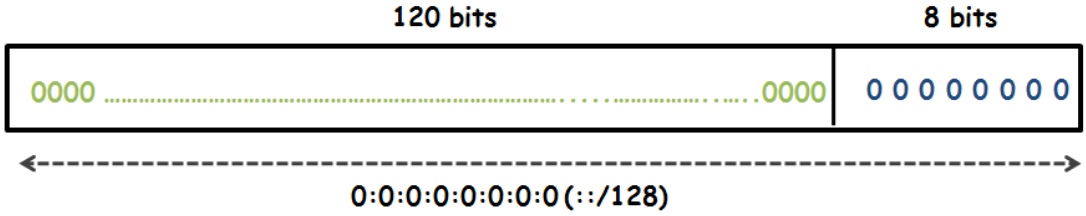
Igual que en IPv4, se hizo una reserva de una dirección especial de loop back IPv6 para hacer pruebas: los datagramas que se envían a esta dirección regresan al dispositivo

emisor y forman así un bucle de retorno o "loopback". Sin embargo, en IPv6 hay sólo una dirección y no todo un bloque para esta función. La dirección de loopback es 0:0:0:0:0:0:0:1, que normalmente se expresa mediante la compresión de ceros como "::1".



DIRECCIÓN NO ESPECIFICADA

En IPv4, una dirección IP compuesta únicamente por ceros tiene un significado especial: hace referencia al mismo host y se utiliza cuando un dispositivo no conoce su propia dirección. En IPv6, este concepto se formalizó y la dirección compuesta únicamente por ceros (0:0:0:0:0:0:0:0) se denomina dirección "no especificada". Normalmente se utiliza en el campo de origen de un datagrama que envía un dispositivo que desea configurar su dirección IP. Es posible aplicar compresión de direcciones en esta dirección, lo que la convierte simplemente en "::".



DIRECCIONES RESERVADAS

IETF reserva una parte del espacio de direcciones de IPv6 para diferentes usos, tanto presentes como futuros. Las direcciones reservadas representan 1 de 256 partes del espacio total de direcciones de IPv6. Algunos de los otros tipos de direcciones IPv6 provienen de este bloque. Por ejemplo la direccion de loopback.

DIRECCIONES ESPECIALES DE TRANSICIÓN

Son direcciones de transición de IPv4 a IPv6 ya que la mayoría de los routers son IPv4.

No se utilizan, aunque todavía se hace mención a ellas en la bibliografía.

Hay dos tipos de direcciones especiales de transición, las compatibles con IPv4 y las mapeadas a IPv4:

- **Ipv6 compatibles con Ipv4** (::IPv4/128): Para túneles automáticos sobre IPv4.Las maquinas destinatarias son IPv6 (p.ej, :: 138.10.9.16).
- **Ipv6 mapeados desde IPv4** (::FFFF: IPv4 /128): Para comunicar terminales con doble pila y utilizando direccionamiento IPv6 sobre redes IPv4. Se usa para enviar

tráfico desde un terminal IPv6 tráfico a un terminal IPv4. Las maquinas destinatarias son IPv4 (p.ej, ::FFFF: 138.10.9.16).

Hay otro tipo de direcciones de transición, las de Estrategia 6to4:

- **Estrategia 6to4** (2002:IPv4::/48): Para túneles automáticos sobre IPv4. La dirección IPv4 está en hexadecimal. (p.ej, 129.146.86.187 = 8192:56BB)

FORMATO URL

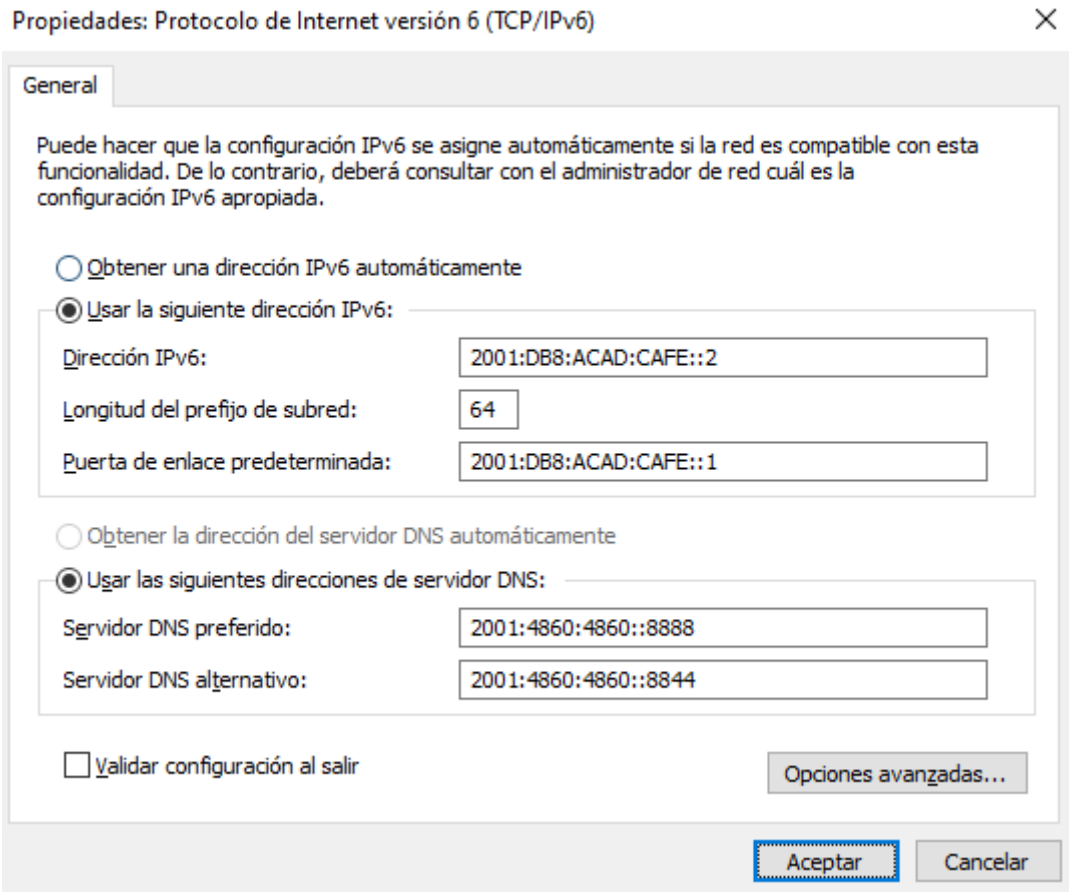
En una URL los dos puntos indican opcionalmente el número de puerto.

La dirección IPv6 debe ir contenida entre corchetes, Ejemplo:

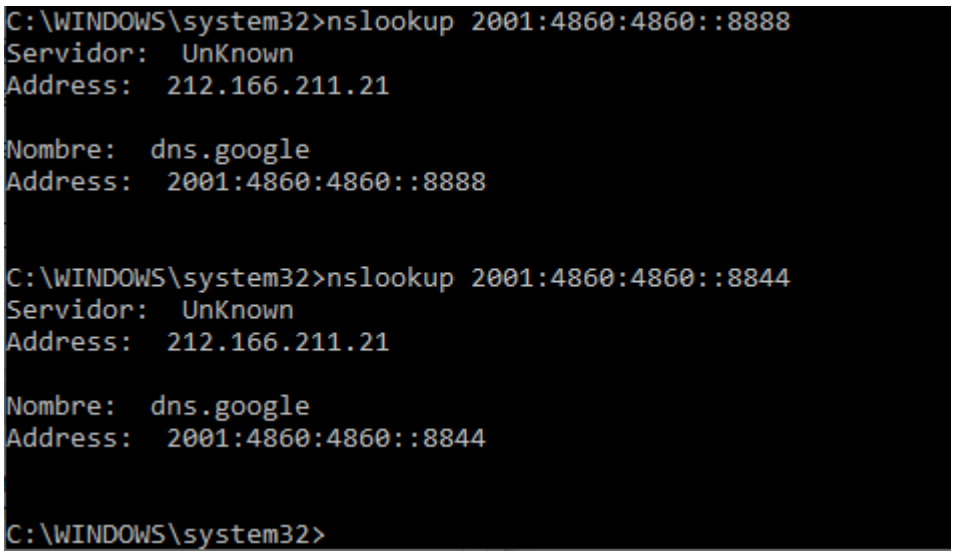
http://[2001:720::212:6BFF:FE11:1111]:80/index.html

ASIGNACIÓN DE IPV6

Asignación estática de toda la dirección: Una manera de asignar estáticamente una dirección IPv6 a un dispositivo consiste en asignar manualmente tanto el prefijo (red) como la porción del ID de la interfaz (host) de la dirección IPv6, es decir, indicar los 128 bits completos de la dirección ipv6.



Los DNS especificados son los de google



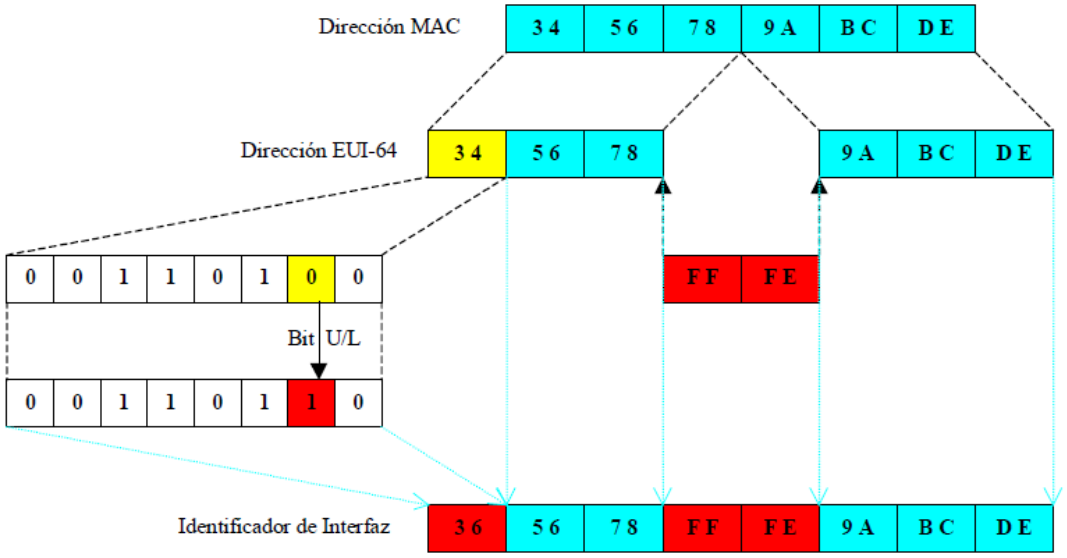
Asignación dinámica con ID de interfaz aleatoria

Por defecto es la de Windons 10, no así en el resto de sistemas. Esto se puede cambiar. Consultar:

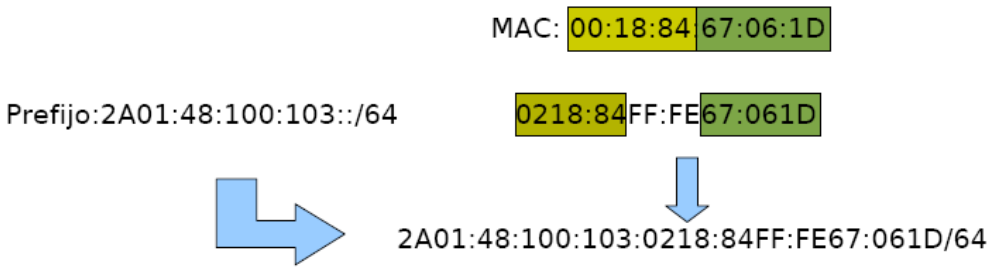
https://www.autoaprendizaje.es/2020/10/17/configuracion-automatica-de-direcciones-ipv6-en-windows-7-8-10-con-eui-64/

Asignación dinámica con ID de interfaz EUI-64 En este caso los primeros 64 bits corresponderán a la parte de red de la dirección (obtenidos del router de subred) y los últimos 64 bits corresponderán a la parte de interfaz. Para construir esta segunda mitad se divide la dirección MAC en dos mitades (Fabricante – Tarjeta) e inserta en medio la cadena

FF:FE, hasta aquí es fácil, pero además el formato EUI-64 exige que el septimo bit del primer byte sea 1 por lo que la dirección MAC se puede ver alterada.



En el siguiente ejemplo le añadimos el prefijo de red:



Configuración dinámica sin estado con EUI-64 (sin servidor DHCP) La información de estado es aquella que almacena un servidor DHCP en la que registra la ip asignada, caducidad, etc, es decir, una información con la que hace un seguimiento. En IPv6 no es necesario DHCP.

En IPv6 se supone que los dispositivos que no son PC, así como las terminales de computadoras, están conectados a la red. El mecanismo de configuración automática se introdujo para permitir networking plug-and-play de estos dispositivos a fin de lograr la reducción de los gastos administrativos.

El dispositivo aprende el prefijo /64 y calcula el resto de su ip utilizando eui-64. El proceso sería el siguiente:

1. El equipo se enciende y calcula su dirección local de enlace (que comenzará por fe80::/10)

2. El equipo envía un mensaje ICMPv6 de tipo NDP que será un mensaje de "solicitud de router" enviado a la dirección de multidifusión ff02::2 –todos los routers de la red—y remitido por el la ip local de enlace anterior.

3. el router de la red responderá con su dirección de enlace local con un mensaje de "publicación de router" a la dirección de multidifusión ff02::1 –todos los equipos de la red-- donde indicará con el prefijo de la red y la ip del el router predeterminado)

En ausencia del router, el equipo solo podrá generar la dirección de enlace local, aunque esto será suficiente para que haya comunicación con los demás equipos de la red.

Configuración automática sin estado (con servidor DHCPv6) El servidor DHCP no asigna las ips pero si aporta información adicional. Por tanto, los clientes del modo sin estado DHCPv6 usan DHCPv6 para obtener parámetros de configuración de red distintos de la dirección IPv6 (por ejemplo, direcciones de servidor DNS). En el caso anterior habrá un paso más:

4. el equipo construye su ipv6 y envia mensajes DHCPv6 a ff02::1:2 para pedir al servidor DHCPv6 el sevidor DNS y el dominio.

Configuración automática con estado (con servidor DHCPv6) En el modo con estado DHCPv6, los clientes obtienen la dirección IPv6 y otros parámetros de configuración de red mediante DHCPv6. Además el servidor DHCP recuerda las ip's asignadas. Este protocolo se puede utilizar por separado o de manera concurrente con la configuración automática de direcciones IPv6 sin estado para obtener parámetros de configuración.

Nota: la máscara de subred la proporcionan los anuncios de enrutador, no el servidor DHCPv6. En DHCPv6 también se permite a los clientes la solicitud de múltiples direcciones IPv6.

ICMPV6

Es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 sustituye funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP, IGMP o ARP y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

Los mensajes ICMPv6 son enviados dentro de paquetes IPv6

Paquete ICMPv6

Bit offset	0–7	8–15	16–31
0	Type	Code	Checksum
32	Message body		

Los paquetes ICMPv6 tienen el formato: Tipo, Código y Checksum.

Los 8 bits del campo Tipo indican el tipo de mensaje:

Si el bit de mayor peso tiene el valor 0 (valores entre 0 y 127) entonces es un mensaje de error, por el contrario

Si el bit de mayor peso es 1 (valores entre 128 y 255) entonces es un mensaje informativo.

Vemos una lista de valores del campo tipo sacada de:

https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-2

Escribe	Nombre	Referencia
0	Reservado	
1	Destino inalcanzable	[RFC4443]
2	Paquete demasiado grande	[RFC4443]
3	Tiempo excedido	[RFC4443]
4	Problema de parámetro	[RFC4443]
5-99	Sin asignar	
100	Experimentación privada	[RFC4443]
101	Experimentación privada	[RFC4443]
102-126	Sin asignar	
127	Reservado para la expansión de mensajes de error ICMPv6	[RFC4443]
128	Solicitud de eco	[RFC4443]
129	Respuesta de eco	[RFC4443]

Los 8 bits del campo Código dependen del tipo de mensaje, y son usados para crear un nivel adicional de clasificación de mensajes, de tal forma que los mensajes informativos en función del campo Código se pueden subdividir en varios tipos.

Vemos una lista de valores del campo codigo para un valor 1 del campo Tipo sacada de:

https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-2

Tipo 1 - Destino inalcanzable

Procedimiento (s) de registro
Acción de estándares o aprobación de IESG
Referencia
[RFC4443]
Formatos disponibles

CSV

Código	Nombre	Referencia
0	sin ruta al destino	
1	comunicación con destino administrativamente prohibida	
2	más allá del alcance de la dirección de origen	[RFC4443]
3	dirección inalcanzable	
4	puerto inalcanzable	
5	dirección de origen fallida política de entrada / salida	[RFC4443]
6	rechazar ruta a destino	[RFC4443]
7	Error en el encabezado de enrutamiento de origen	[RFC6550] [RFC6554]
8	Encabezados demasiado largos	[RFC8883]

El campo Checksum es usado para detectar errores en los mensajes ICMPv6 y en algunos de los mensajes IPv6.

Los mensajes de error de ICMPv6 son similares a los mensajes de error de ICMPv4. Se dividen en 4 categorías: destino inaccesible, paquete demasiado grande, tiempo excedido y problemas de parámetros.

El segundo tipo de mensajes ICMP son los mensajes informativos. Estos mensajes se subdividen en tres grupos: mensajes de diagnóstico, mensajes para la administración de grupos multicast (sustituye a IGMP que se utilizaba para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión) y mensajes de Neighbor Discovery (NDP entre otras funciones sustituye a ARP)

Observación:

Las funciones de ARP en ipv6 las realiza el protocolo “Neighbor Discovery Protocol”.

En ipv6 no exite la tabla arp, pues no utilizamos arp, en su lugar existe algo parecido la neighbor table.

Para visualizarla utilizar en windows:

```
netsh interface ipv6 show neighbors
```

en Linux:

```
ip nei
```

TRANSICIÓN DE IPV4 A IPV6

La transición de IPv4 no requiere que las actualizaciones de todos los nodos sean simultáneas. Hay muchos mecanismos de transición que permiten una integración fluida de IPv4 e IPv6. Hay otros mecanismos que permiten que los nodos IPv4 se comuniquen con nodos IPv6. Para diferentes situaciones se requieren diferentes estrategias.

Recuerde el consejo: "Use stack doble cuando pueda y tunneling cuando no tenga otra opción". Estos dos métodos son las técnicas más comunes de transición de IPv4 a IPv6.

El DNS tiene un nuevo tipo de registro “AAAA” para direcciones Ipv6. Un mismo nodo puede tener un registro “A” para su dirección IPv4, un registro “AAAA” para una dirección IPv6 pura y otro registro “AAAA” para una dirección “IPv6” compatible IPv4.

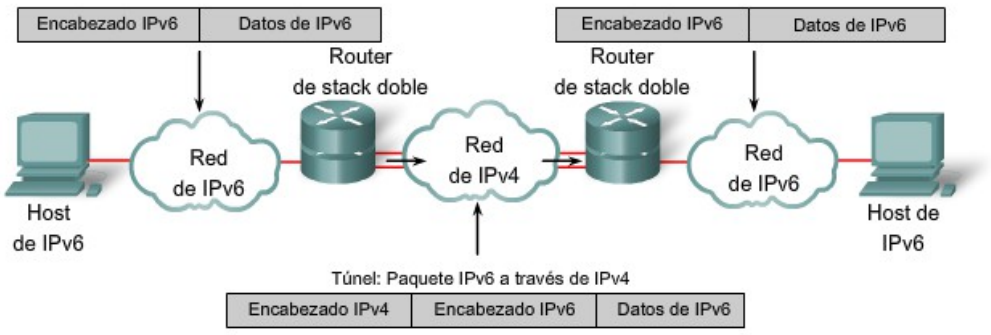
STACK DOBLE Ó DOBLE CAPA IP Ó DUAL STACK

El método de stack doble es un método de integración en el que un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Es la opción recomendada y requiere que se ejecuten IPv4 e IPv6 simultáneamente. El router y los switches se configuran para admitir ambos protocolos; el protocolo preferido es IPv6.

El enfoque de stack doble para la integración de IPv6, en el que los nodos tienen stacks de IPv4 e IPv6, será uno de los métodos de integración más comúnmente utilizados. Un nodo de stack doble elige qué stack utilizar en función de la dirección de destino del paquete. Un nodo de stack doble debe preferir utilizar IPv6 cuando esté disponible. Las aplicaciones antiguas que sólo admiten IPv4 siguen funcionando igual que antes. Las aplicaciones nuevas y las codificadas aprovechan las dos capas IP. Las desventajas son una disminución del desempeño de los equipos de red, que deben mantener tablas de direcciones y rutas independientes para cada protocolo

TUNNELING

La segunda técnica de transición más importante es el tunneling, consiste en encapsular los paquetes ipv6 dentro de otro protocolo por ejemplo ipv4. El tunneling es una técnica de integración y transición intermedia, y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa.



Existen varias técnicas de tunneling, entre ellas:

- Tunneling manual de IPv6 sobre IPv4: un paquete de IPv6 se encapsula dentro del protocolo IPv4. Este método requiere routers de stack doble.

- Tunneling dinámico 6to4: establece automáticamente la conexión de islas de IPv6 a través de la red IPv4, normalmente Internet. Aplica dinámicamente un prefijo IPv6 válido y único a cada isla de IPv6, lo que posibilita la implementación rápida de IPv6 en una red corporativa sin recuperación de direcciones de los ISP o los registros.

- Tunneling del protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP, Intra-Site Automatic Tunnel Addressing Protocol): mecanismo de tunneling de capa superior automática que utiliza la red IPv4 subyacente como capa de enlace para IPv6. Los túneles del ISATAP permiten que los hosts de stack doble individuales IPv4 o IPv6 de un sitio se comuniquen con otros hosts similares a través de un enlace virtual y creen así una red IPv6 mediante la infraestructura IPv4.

- Tunneling Teredo: tecnología de transición a IPv6 que proporciona tunneling automático de host a host en lugar de tunneling de gateway. Este enfoque transmite tráfico IPv6 unicast si hay hosts de stack doble (hosts que ejecutan tanto IPv6 como IPv4) detrás de una o varias NAT IPv4.

NAT-PT (NETWORK ADDRESS TRANSLATION – PROTOCOL TRANSLATION)

Es una técnica que transforma directamente paquetes IPv6 en paquetes IPv4 y viceversa. Es totalmente transparente desde el punto de vista de los nodos en una conexión, solo es necesario configurar un "router" que realiza la transformación de paquetes. Es más complejo que el tradicional protocolo NAT de IPv4, ya que es necesario modificar íntegramente cada paquete IPv4/IPv6. Solo se recomienda su uso como medida temporal, cuando no existe otra alternativa.

DIRECCIONAMIENTO A NIVEL DE TRANSPORTE

INTRODUCCIÓN

Las aplicaciones como clientes de correo electrónico, exploradores Web y clientes de mensajería instantánea permiten que las personas utilicen las computadoras y las redes para enviar mensajes y buscar información.

Los datos de cada una de estas aplicaciones se empaquetan, transportan y entregan al **daemon** de servidor o aplicación adecuados en el dispositivo de destino.

La capa de Transporte acepta los datos de la capa de Aplicación y los prepara para el direccionamiento en la capa de Red. La capa de Transporte es responsable de la transferencia de **extremo a extremo** general de los datos de aplicación.

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de las distintas cadenas de comunicación.

Las **funciones** principales que debe cumplir son:

Control de flujo

A medida que la **capa de transporte** envía segmentos de datos, trata de garantizar que los datos no se pierdan. Un host receptor que no puede procesar los datos tan rápidamente como llegan puede provocar una pérdida de datos. El host receptor se ve obligado a descartar los datos. El control de flujo evita el problema que se produce cuando un host que realiza la transmisión inunda los buffers del host destinatario. TCP suministra el mecanismo de control de flujo al permitir que el host emisor y el receptor se comuniquen. Luego los dos hosts establecen velocidades de transferencia de datos que sean aceptables para ambos.

Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando la capa de Transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación que envía reduzca la velocidad del flujo de datos. Esto se lleva a cabo en la capa de Transporte regulando la cantidad de datos que el origen transmite como grupo. El control del flujo puede prevenir la pérdida de segmentos en la red y evitar la necesidad de retransmisión

Seguimiento de Conversaciones individuales(Multiplexación)

Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de Transporte controlar estas comunicaciones, es decir, realizar el multiplexado.

Ya que las redes proveen rutas múltiples que pueden poseer distintos tiempos de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, la capa de Transporte puede asegurar que los mismos se reensamblen en el orden adecuado.

Segmentación de datos

Debido a que cada aplicación genera una cadena de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables. Los protocolos de la capa de Transporte describen los servicios que segmentan estos datos de la capa de Aplicación. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

La segmentación de los datos proporciona los medios para enviar y recibir datos cuando se ejecutan varias aplicaciones de manera concurrente en una computadora. Sin segmentación, sólo una aplicación, la corriente de vídeo por ejemplo, podría recibir datos. No se podrían recibir correos electrónicos, chats ni mensajes instantáneos ni visualizar páginas Web y ver un vídeo al mismo tiempo.

Para profundizar en la elección adecuada del tamaño de segmento:

https://netwgeeks.com/opciones-tcp-tamano-maximo-del-segmento-mss/

Reensamble de segmentos

En el host de recepción, cada sección de datos puede ser direccionada a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar una cadena completa de datos que sea útil para la capa de Aplicación.

Identificación de las aplicaciones

Para poder transferir las cadenas de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

La capa de Transporte acepta datos de distintas conversaciones y los transfiere a las capas inferiores para ser enviadas a través del medio.

Las aplicaciones no necesitan conocer los detalles de operación de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red.

DIFERENTES PROTOCOLOS DE TRANSPORTE.

Debido a que las distintas aplicaciones poseen distintos requerimientos, existen varios protocolos de la capa de Transporte. En algunos casos, todos los datos deben recibirse para ser utilizados por cualquiera de las mismas. En otros casos, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red.

En las redes actuales, las aplicaciones con distintas necesidades de transporte pueden comunicarse en la misma red. Los distintos protocolos de la capa de Transporte poseen distintas reglas que permiten que los dispositivos gestionen los diversos requerimientos de datos. Las aplicaciones, como bases de datos, las páginas Web y los e-mails, requieren que todos los datos enviados lleguen al destino en su condición original, de manera que los mismos sean útiles. Todos los datos perdidos pueden corromper una comunicación y dejarla incompleta o ilegible. Por lo tanto, estas aplicaciones se diseñan para utilizar un protocolo de capa de Transporte que implemente la confiabilidad. El uso de recursos de red adicionales se considera necesario para estas aplicaciones.

Los dos protocolos más comunes de la capa de Transporte del conjunto de protocolos TCP/IP son el Protocolo de control de transmisión (TCP) y el Protocolos de datagramas de usuario (UDP). Ambos protocolos gestionan la comunicación de múltiples aplicaciones. Las diferencias entre ellos son las funciones específicas que cada uno implementa.

TCP está orientado a conexión, UDP no. Aproximadamente un 80% del tráfico es TCP.

Ejemplos de uso de TCP: FTP, HTTP. Conectan únicamente dos y solo dos extremos, por tanto no son utilizados en comunicaciones broadcast ni multicast. Sus paquetes se denominan en la bibliografía segmentos.

Ejemplos de UDP: DNS, SIP(protocolo de telefonía ip), DHCP, videoconferencia, tráfico broadcast y multicast. Sus paquetes se denominan en la bibliografía datagramas.

TCP

TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad. Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura

(gracias al sistema de acuse de recibo del protocolo TCP, orientado a conexión) independientemente de las capas inferiores.

Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman *segmentos*

Segmento de TCP

UDP

Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones de datos perdidos por los estrictos requisitos de retardo que se tiene en estos casos.

Datagrama de UDP

COMPARATIVA ENTRE UDP Y TCP

UDP: es un protocolo no orientado a conexión. Es decir cuando una maquina A envía paquetes a una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber realizado previamente una conexión con la maquina de destino (maquina B), y el destinatario recibirá los datos sin enviar una confirmación al emisor (la maquina A).

Proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade la información necesaria para la comunicación extremo a extremo al paquete que envía al nivel inferior.

Sobretodo se emplea en tareas de control y en la transmisión de audio y vídeo a través de una red. No introduce retardos para establecer una conexión, no mantiene estado de conexión alguno y no realiza seguimiento de estos parámetros.

Así, un servidor dedicado a una aplicación particular puede soportar más clientes activos cuando la aplicación corre sobre UDP en lugar de sobre TCP.

TCP: Contrariamente a UDP, el protocolo TCP está orientado a conexión. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de datos, y confirma su buena recepción. Aquí interviene el control CRC de datos que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que vuelvan a enviar los datos corruptos, es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones.

Está pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, pérdida de paquetes, orden en el que llegan los paquetes, duplicados de paquetes...) que gestiona el propio protocolo.

Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes que enviar.

Debido a que los paquetes para enviar tienen un tamaño máximo, cuanta más información añada el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete (el segmento TCP tiene una sobrecarga de 20 bytes en cada segmento, mientras que UDP solo añade 8 bytes). Por eso, cuando es más importante la velocidad que la fiabilidad, se utiliza UDP. En cambio, TCP asegura la recepción en destino de la información para transmitir.

DIRECCIONAMIENTO DEL PUERTO

Considere el ejemplo de una computadora que recibe y envía e-mails, mensajes instantáneos, páginas Web y llamadas telefónicas VoIP de manera simultánea.

Los servicios basados en TCP y UDP mantienen un seguimiento de las varias aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones. Estos identificadores únicos son los números de los puertos.

En el encabezado de cada segmento o datagrama hay un puerto de origen y destino. El número de puerto de origen es el número para esta comunicación asociado con la

aplicación que origina la comunicación en el host local. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino en el host remoto.

Los números de puerto se asignan de varias maneras, en función de si el mensaje es una solicitud o una respuesta. Mientras que los procesos en el servidor poseen números de puertos estáticos asignados a ellos, los clientes eligen un número de puerto de forma dinámica para cada conversación.

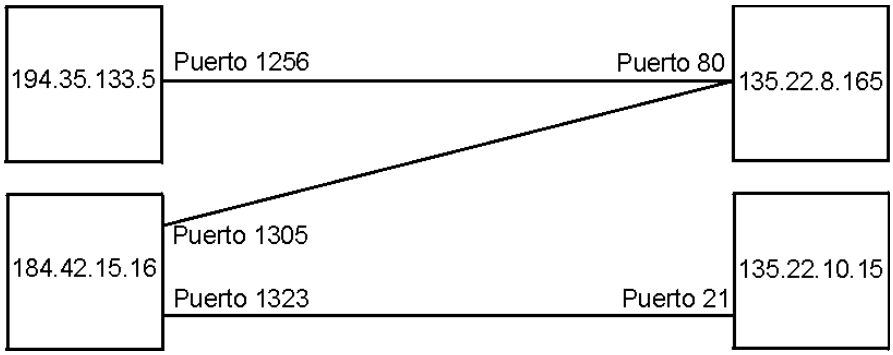
Cuando una aplicación de cliente envía una solicitud a una aplicación de servidor, el puerto de destino contenido en el encabezado es el número de puerto que se asigna al **daemon** de servicio que se ejecuta en el host remoto. El software del cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto. Este número de puerto de destino se puede configurar, ya sea de forma predeterminada o manual. Por ejemplo, cuando una aplicación de explorador Web realiza una solicitud a un servidor Web, el explorador utiliza TCP y el número de puerto 80 a menos que se especifique otro valor. Esto sucede porque el puerto TCP 80 es el puerto predeterminado asignado a aplicaciones de servidores Web. Muchas aplicaciones comunes tienen asignados **puertos predeterminados.**

El puerto de origen del encabezado de un segmento o datagrama de un cliente se genera de manera aleatoria. Siempre y cuando no entre en conflicto con otros puertos en uso en el sistema, el cliente puede elegir cualquier número de puerto. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de Transporte mantiene un seguimiento de este puerto y de la aplicación que generó la solicitud, de manera que cuando se devuelva una respuesta, pueda ser enviada a la aplicación correcta. El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.

La combinación del número de puerto de la capa de Transporte y de la dirección IP de la capa de Red asignada al host identifica de manera exclusiva un **proceso en particular que se ejecuta en un dispositivo host** específico. Esta combinación se denomina **socket.**

Eventualmente, los términos número de puerto y socket se utilizan en forma indistinta. En el contexto de este curso, el término socket hace referencia sólo a la combinación exclusiva de dirección IP y número de puerto. **Un par de sockets**, que consiste en las direcciones IP y los números de puerto de origen y de destino, también es exclusivo e **identifica la conversación** entre dos hosts.

Socket
194.35.133.5:1256
184.42.15.16:1305
184.42.15.16:1323



Nota: El comando NetStat muestra las conexiones abiertas en un ordenador, así como estadísticas de los distintos protocolos de Internet.

NÚMEROS DE PUERTOS

Existen distintos tipos de números de puerto:

Puertos bien conocidos (Números del 0 al 1023): estos números se reservan para servicios y aplicaciones. Por lo general, se utilizan para aplicaciones como HTTP (servidor Web), POP3/SMTP (servidor de e-mail) y Telnet. Al definir estos puertos conocidos para las aplicaciones del servidor, las aplicaciones del cliente pueden ser programadas para solicitar una conexión a un puerto específico y su servicio asociado.

Puertos Registrados (Números 1024 al 49151): estos números de puertos están asignados a procesos o aplicaciones del usuario. Estos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un puerto bien conocido. Cuando no se utilizan para un recurso del servidor, estos puertos también pueden utilizarse si un usuario los selecciona de manera dinámica como puerto de origen.

Puertos dinámicos o privados (Números del 49152 al 65535): también conocidos como puertos efímeros, suelen asignarse de manera dinámica a aplicaciones de **cliente** cuando se inicia una conexión. No es muy común que un cliente se conecte a un servicio (servidor) utilizando un puerto dinámico o privado de este (aunque algunos programas que comparten archivos punto a punto lo hacen).

Algunas aplicaciones pueden utilizar los dos protocolos: TCP y UDP. Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número 53 de puerto conocido es utilizado por ambos protocolos con este servicio.

ESTABLECIMIENTO DE LA CONEXIÓN TCP

Cuando dos hosts se comunican utilizando TCP, se establece una conexión antes de que puedan intercambiarse los datos. Una vez completa la comunicación, se cierran las sesiones y la conexión finaliza. Los mecanismos de conexión y de sesión habilitan la función de confiabilidad de TCP

Para establecer la conexión los hosts realizan un intercambio de señales de tres vías. Los bits de control en el encabezado TCP indican el progreso y estado de la conexión. Enlace de tres vías:

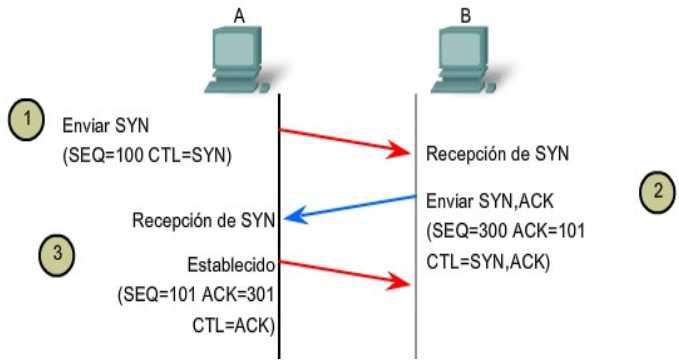
Establece que el dispositivo de destino esté presente en la red.

Verifica que el dispositivo de destino tenga un servicio activo y esté aceptando las peticiones en el número de puerto de destino que el cliente que lo inicia intente usar para la sesión.

Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en ese número de puerto.

En conexiones TCP, el host que brinde el servicio como cliente inicia la sesión al servidor. Los tres pasos para el **establecimiento de una conexión TCP** son:

Enviar SYN: El cliente que inicia la conexión envía un segmento que contiene un valor de secuencia inicial, que actúa como solicitud para el servidor para comenzar una sesión de comunicación.



Enviar SYN/ACK: El servidor responde con un segmento que contiene un valor de reconocimiento igual al valor de secuencia recibido más 1, además de su propio valor de secuencia de sincronización (Cabe recordar que la conversación entre el cliente y el servidor está compuesta en realidad por dos sesiones de una vía: una del cliente al servidor y la otra del servidor al cliente). El valor es uno mayor que el número de secuencia porque el ACK es siempre el próximo Byte u Octeto esperado. Este valor de reconocimiento permite al cliente unir la respuesta al segmento original que fue enviado al servidor.

Enviar ACK: El cliente que inicia la conexión responde con un valor de reconocimiento igual al valor de secuencia que recibió más uno. Esto completa el proceso de establecimiento de la conexión.

Para entender el proceso de enlace de tres vías, es importante observar los distintos valores que intercambian los dos hosts. Dentro del encabezado del segmento TCP, existen seis campos de 1 bit que contienen información de control utilizada para gestionar los procesos de TCP. Estos campos son los siguientes:

- URG: Urgente campo de señalizador significativo,
- ACK: Campo significativo de acuse de recibo,
- PSH: Función de empuje,
- RST: Reconfiguración de la conexión,
- SYN: Sincronizar números de secuencia,
- FIN: No hay más datos desde el emisor.

A estos campos se los denomina señaladores porque el valor de uno de estos campos es sólo de 1 bit, entonces tiene sólo dos valores: 1 ó 0. Si el valor del bit se establece en 1, indica la información de control que contiene el segmento.

Si se utiliza un proceso de cuatro pasos, los señalizadores se intercambian para finalizar la conexión TCP.

Finalización de la conexión TCP

Cuando el cliente no tiene más datos para enviar, envía un segmento con el señalizador FIN establecido.

El servidor envía un ACK para acusar recibo de Fin y terminar la sesión del cliente al servidor.

El servidor envía un FIN al cliente para finalizar la sesión del servidor al cliente.

El cliente responde con un ACK para dar acuse de recibo de FIN desde el servidor.

También es posible terminar la conexión mediante un enlace de tres vías. Cuando el cliente no posee más datos para enviar, envía un señalizador FIN al servidor. Si el servidor tampoco tiene más datos para enviar, puede responder con los señalizadores FIN y ACK, combinando dos pasos en uno. El cliente responde con un ACK.

ANEXO: ALGUNOS NÚMEROS DE PUERTOS CONOCIDOS.

Puerto/ protocolo	Descripción
20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	SSH, scp, SFTP
23/tcp	Telnet comunicaciones de texto inseguras
25/tcp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
37/tcp	time
53/tcp	DNS Domain Name System (Sistema de Nombres de Dominio)
53/udp	DNS Domain Name System (Sistema de Nombres de Dominio)
67/udp	BOOTP BootStrap Protocol (Server), también usado por DHCP
68/udp	BOOTP BootStrap Protocol (Client), también usado por DHCP
69/udp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
80/tcp	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de

	HiperTexto) (WWW)
88/tcp	Kerberos Agente de autenticación
110/tcp	POP3 Post Office Protocol (E-mail)
119/tcp	NNTP usado en los grupos de noticias de usenet
123/udp	NTP Protocolo de sincronización de tiempo
123/tcp	NTP Protocolo de sincronización de tiempo
137/tcp	NetBIOS Servicio de nombres
137/udp	NetBIOS Servicio de nombres
138/tcp	NetBIOS Servicio de envío de datagramas
138/udp	NetBIOS Servicio de envío de datagramas
139/tcp	NetBIOS Servicio de sesiones
139/udp	NetBIOS Servicio de sesiones
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/tcp	SNMP Simple Network Management Protocol
161/udp	SNMP Simple Network Management Protocol
162/tcp	SNMP-trap
162/udp	SNMP-trap
177/tcp	XDMCP Protocolo de gestión de displays en X11
177/udp	XDMCP Protocolo de gestión de displays en X11
389/tcp	LDAP Protocolo de acceso ligero a Bases de Datos
389/udp	LDAP Protocolo de acceso ligero a Bases de Datos
443/tcp	HTTPS/SSL usado para la transferencia segura de páginas web
445/tcp	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
445/udp	Microsoft-DS compartición de ficheros
500/udp	IPSec ISAKMP, Autoridad de Seguridad Local
520/udp	RIP
631/tcp	CUPS sistema de impresión de Unix

993/tcp	IMAP4 sobre SSL (E-mail)
995/tcp	POP3 sobre SSL (E-mail)
1433/tcp	Microsoft-SQL-Server
1434/tcp	Microsoft-SQL-Monitor
1434/udp	Microsoft-SQL-Monitor
1512/tcp	WINS
1521/tcp	Oracle listener por defecto
1701/udp	Enrutamiento y Acceso Remoto para VPN con L2TP.
1723/tcp	Enrutamiento y Acceso Remoto para VPN con PPTP.
1863/tcp	MSN Messenger
2049/tcp	NFS Archivos del sistema de red
3306/tcp	MySQL sistema de gestión de bases de datos
3389/tcp	RDP (Remote Desktop Protocol)
4662/tcp	eMule (aplicación de compartición de ficheros)
4672/udp	eMule (aplicación de compartición de ficheros)
4899/tcp	RAdmin (Remote Administrator), herramienta de administración remota (normalmente troyanos)
5631/tcp	PC-Anywhere protocolo de escritorio remoto
5632/udp	PC-Anywhere protocolo de escritorio remoto
5400/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5500/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5600/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5700/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5800/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5900/tcp	VNC protocolo de escritorio remoto (conexión normal)
6000/tcp	X11 usado para X-windows
6881/tcp	BitTorrent puerto por defecto
6969/tcp	BitTorrent puerto de tracker

7100/tcp	Servidor de Fuentes X11
7100/udp	Servidor de Fuentes X11
8000/tcp	iRDMI por lo general, usado erróneamente en sustitución de 8080. También utilizado en el servidor de streaming ShoutCast.
8080/tcp	HTTP HTTP-ALT ver puerto 80. Tomcat lo usa como puerto por defecto.
8118/tcp	privoxy
9009/tcp	Pichat peer-to-peer chat server
9898/tcp	Gusano Dabber (troyano/virus)
10000/tcp	Webmin (Administración remota web)