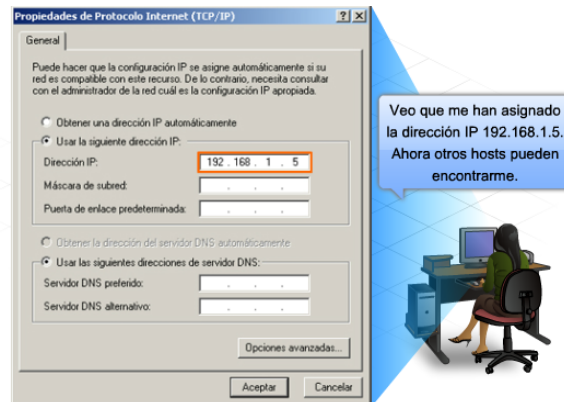


## DIRECCIONAMIENTO DE LA RED: IPv4

### INTRODUCCIÓN

El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente.



La versión IP 4 (IPv4) es la forma actual de direccionamiento utilizada en Internet.

### ESTRUCTURA DE UNA DIRECCIÓN Ipv4

Cada dispositivo de una red debe definirse en forma exclusiva. En la capa de red, es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, se aplica la lógica digital para su interpretación. Para quienes formamos parte de la red humana, una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato de decimal punteada.

#### Decimal punteada

Los patrones binarios que representan direcciones IPv4 se expresan mediante decimales punteados separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

Por ejemplo, la dirección:

10101100000100000000010000010100

se expresa como decimal punteada de la siguiente manera:

172.16.4.20

Tenga en cuenta que los dispositivos utilizan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

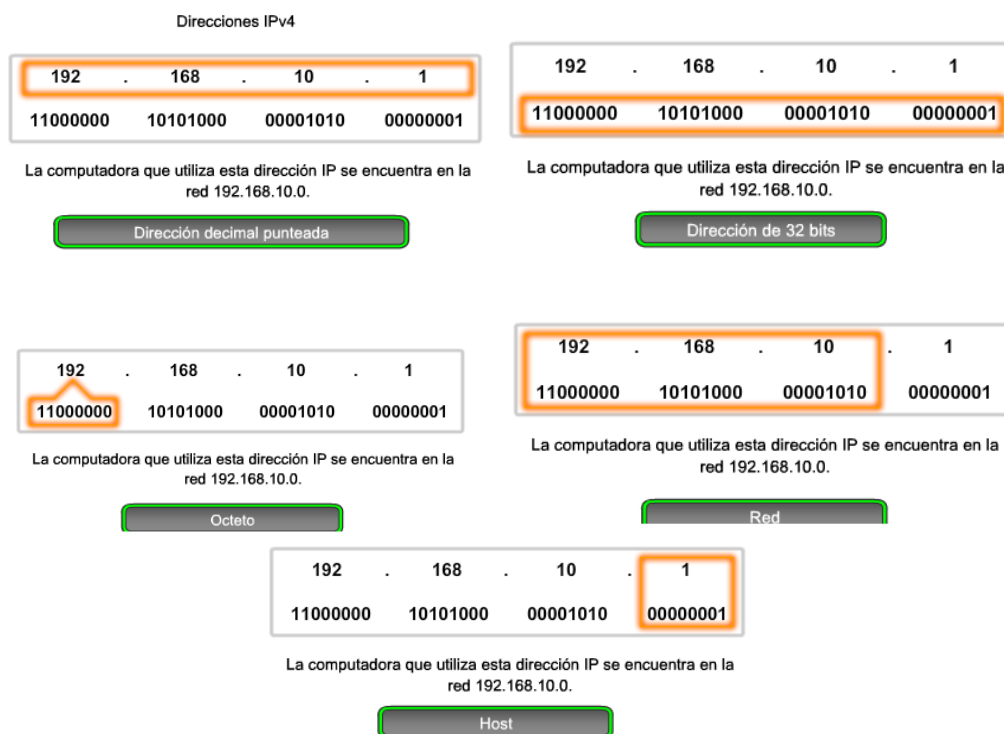
#### Porciones de red y de host

En cada dirección IPv4, alguna porción de los bits de orden superior representan la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones.

A pesar de que los 32 bits definen la dirección host IPv4, existe una cantidad variable de bits que conforman la porción de host de la dirección. La cantidad de bits usada en esta porción de host determina la cantidad de host que podemos tener dentro de la red.

Por ejemplo, si necesitamos tener al menos 200 hosts en una red determinada, necesitaríamos utilizar suficientes bits en la porción de host para poder representar al menos 200 patrones diferentes de bits.

Para asignar una dirección exclusiva a 200 hosts, se utilizará el último octeto entero. Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red.



### CONVERSIÓN DE BINARIO EN DECIMAL

Para comprender el funcionamiento de un dispositivo en una red, es necesario considerar las direcciones y otros datos de la manera en que lo hace un dispositivo: en notación binaria. Esto significa que es necesario ser hábil en la conversión de binario en decimal.

Los datos representados en el sistema binario pueden representar muchas formas diferentes de datos en la red humana. En este tema, se hace referencia al sistema binario por estar relacionado con el direccionamiento IPv4. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255.

### **Notación de posición**

Aprender a convertir el sistema binario a decimal requiere el conocimiento de los fundamentos matemáticos de un sistema de numeración denominado notación de posición. Notación de posición significa que un dígito representa diferentes valores según la posición que ocupa. Más específicamente, el valor que un dígito representa es el valor multiplicado por la potencia de la base o raíz representado por la posición que el dígito ocupa. Algunos ejemplos ayudarán a aclarar cómo funciona este sistema.

Para el número decimal 245, el valor que el 2 representa es  $2 \cdot 10^2$  (2 multiplicado por 10 elevado a la segunda potencia). El 2 se encuentra en lo que comúnmente llamamos la posición "100". La notación de posición se refiere a esta posición como posición base<sup>2</sup> porque la base o raíz es 10 y la potencia es 2.

Usando la notación de posición en el sistema de numeración con base 10, 245 representa:

$$245 = (2 \cdot 10^2) + (4 \cdot 10^1) + (5 \cdot 10^0)$$

o

$$245 = (2 \cdot 100) + (4 \cdot 10) + (5 \cdot 1)$$

### Sistema de numeración binaria

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa potencias incrementadas de 2. En números binarios de 8 bits, las posiciones representan estas cantidades:

$$2^7 \ 2^6 \ 2^5 \ 2^4 \ 2^3 \ 2^2 \ 2^1 \ 2^0$$

$$128 \ 64 \ 32 \ 16 \ 8 \ 4 \ 2 \ 1$$

El sistema de numeración de base 2 tiene solamente dos dígitos: 0 y 1.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esa posición representa si el dígito es 1 y no se obtiene la cantidad si el dígito es 0, como se muestra en la figura.

$$1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1$$

$$128 \ 64 \ 32 \ 16 \ 8 \ 4 \ 2 \ 1$$

Un 1 en cada posición significa que sumamos el valor para esa posición al total. Ésta es la suma cuando hay un 1 en cada posición de un octeto. El total es 255.

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$$

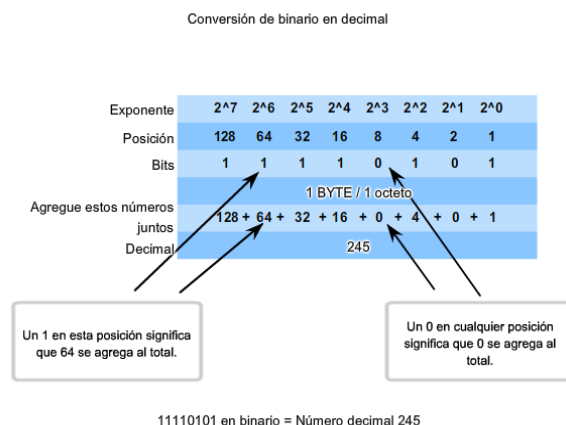
Un 0 en cada posición indica que no se suma el valor para esa posición al total. Un 0 en cada posición produce un total de 0.

$$0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$$

$$128 \ 64 \ 32 \ 16 \ 8 \ 4 \ 2 \ 1$$

$$0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0$$

En la figura que una combinación diferente de unos y ceros producirá un valor decimal diferente.



Observe la figura para obtener los pasos para convertir una dirección binaria en una dirección decimal.

En el ejemplo, el número binario:

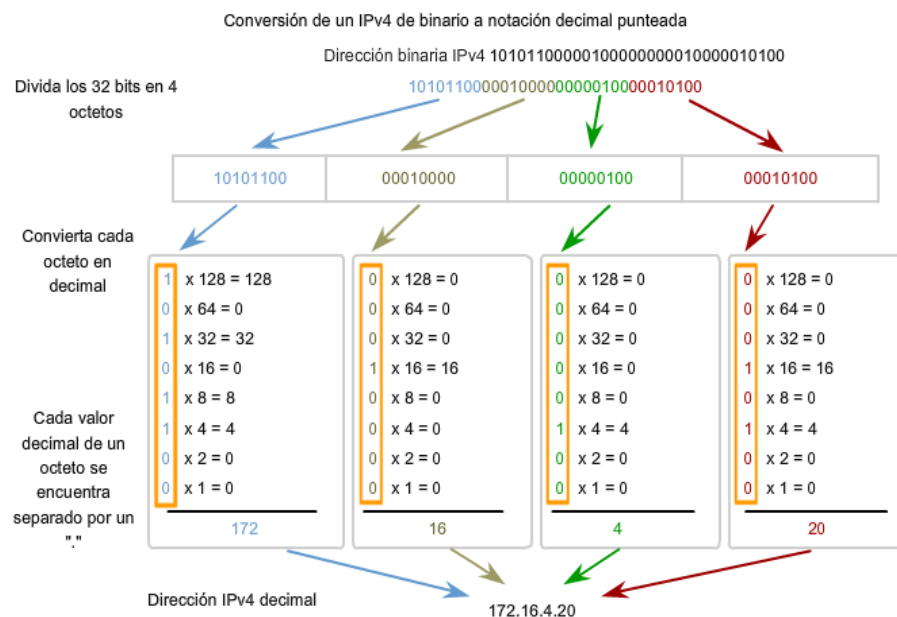
10101100000100000000010000010100

Se convierte en:

172.16.4.20

Tenga en cuenta estos pasos:

- Divida los 32 bits en 4 octetos.
- Convierta cada octeto a decimal.
- Agregue un "punto" entre cada decimal.



### CONVERSIONES DE DECIMALES EN BINARIO

No sólo es necesario poder realizar una conversión de binario a decimal, sino que también es necesario poder realizar una conversión de decimal a binario. Con frecuencia es necesario examinar un octeto individual de una dirección que se proporciona en notación decimal punteada. Tal es el caso cuando los bits de red y los bits de host dividen un octeto.

Por ejemplo, si un host 172.16.4.20 utilizara 28 bits para la dirección de red, sería necesario examinar los datos binarios del último octeto para descubrir que este host está en la red 172.16.4.16.

Los valores de la dirección están entre 0 y 255

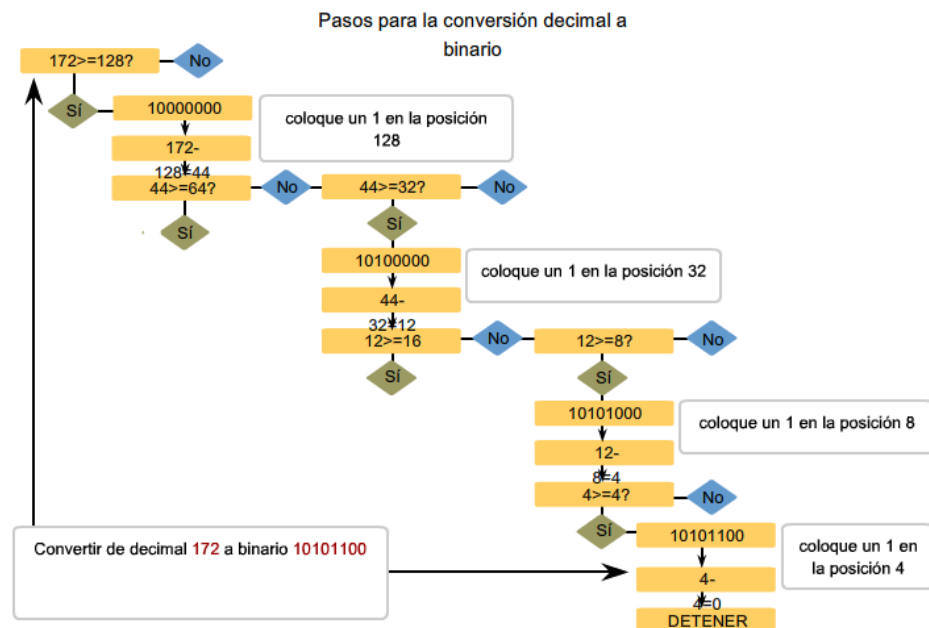
Examinaremos sólo el proceso de conversión binaria de 8 bits a valores decimales de 0 a 255 porque nuestra representación de direcciones está limitada a valores decimales para un solo octeto.

Para comenzar el proceso de conversión, empezaremos determinando si el número decimal es igual a o mayor que nuestro valor decimal más grande representado por el bit más significativo. En la posición más alta, se determina si el valor es igual o mayor que 128. Si el valor es menor que 128, se coloca un 0 en la posición de 128 bits y se mueve a la posición de 64 bits.

Si el valor en la posición de 128 bits es mayor o igual que 128, se coloca un 1 en la posición 128 y se resta 128 del número que se está convirtiendo. Luego se comparan los valores restantes de esta

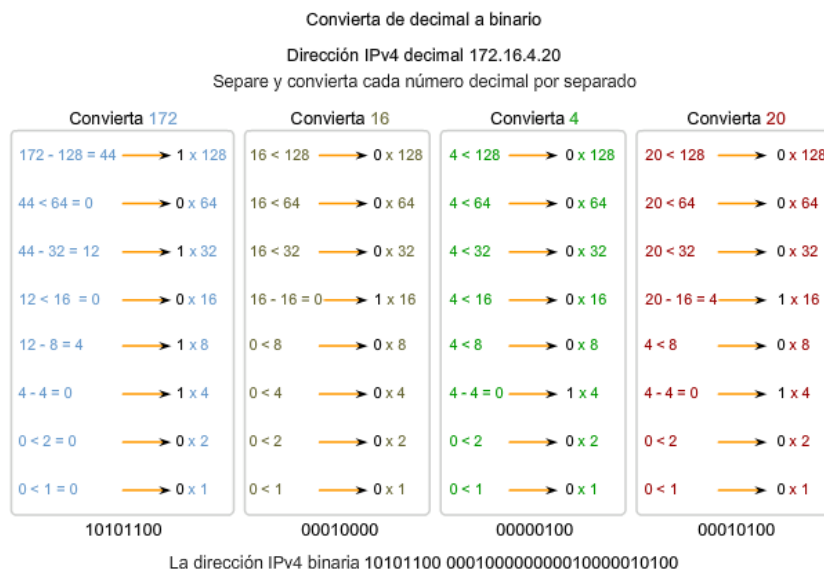
operación con el siguiente valor más pequeño, 64. Se continúa con este proceso para todas las posiciones de bits restantes.

En la figura se presenta un ejemplo de estos pasos. Se convierte 172 en 10101100.



### Resumen de conversión

En figura resume la conversión completa de 172.16.4.20 de notación decimal punteada a notación binaria.



## DIRECCIONES PARA DIFERENTES PROPÓSITOS

### 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.

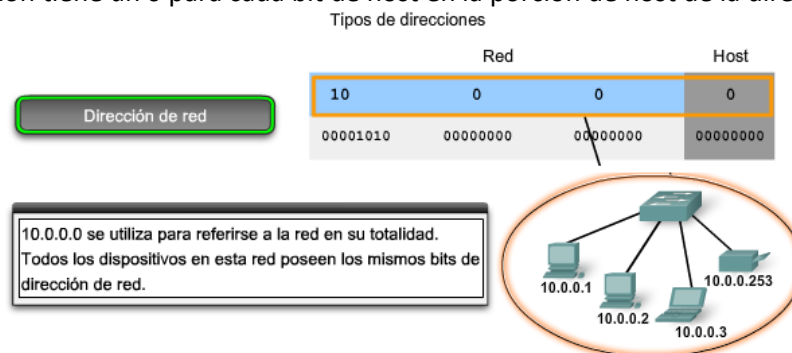
**Dirección de broadcast:** una dirección especial que se utiliza para enviar datos a todos los hosts de la red.

**Direcciones host:** las direcciones asignadas a los dispositivos finales de la red.

### Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como "red 10.0.0.0". Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

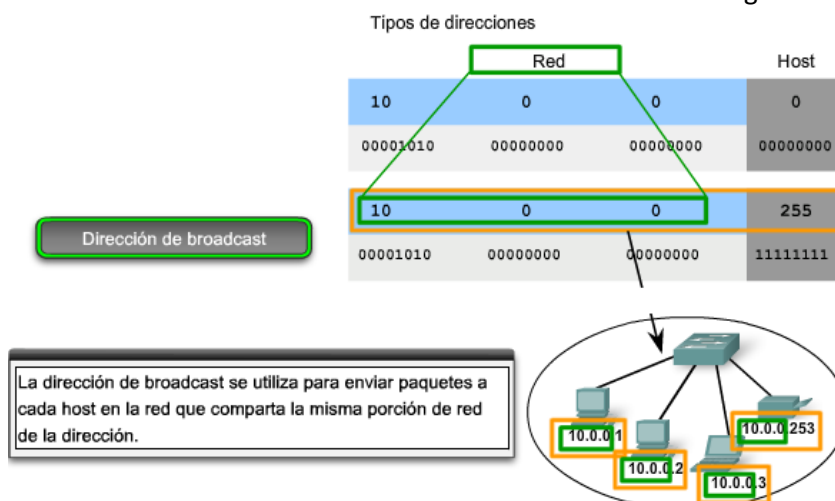
Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.



### Dirección de broadcast

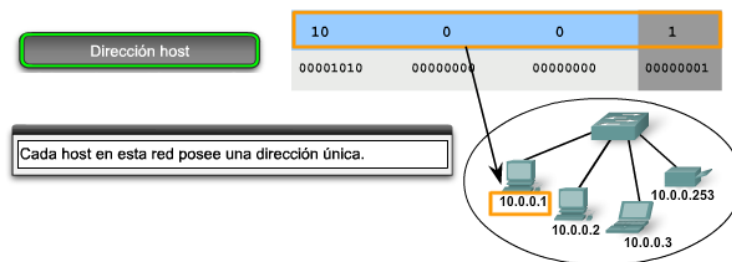
La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

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. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido.



### Direcciones host

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.



## TIPOS DE DIRECCIONES EN UNA RED IPv4

### Prefijos de red

Una pregunta importante es: ¿Cómo es posible saber cuántos bits representan la porción de red y cuántos bits representan la porción de host? Al expresar una dirección de red IPv4, se agrega una longitud de prefijo a la dirección de red. La longitud de prefijo es la cantidad de bits en la dirección que conforma la porción de red. Por ejemplo: en 172.16.4.0 /24, /24 es la longitud de prefijo e indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza unos y ceros para indicar qué bits de la dirección son bits de red y qué bits son bits de host.

No siempre se asigna un prefijo /24 a las redes. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes duraciones de prefijos. En esta figura puede ver también que la cantidad de host que puede ser direccionada a la red también cambia.

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de host (en rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
Representación binaria 24 bits de red	10101100.00010000. 00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000. 00000100.11111111
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

DIFERENTE CANTIDAD DE HOSTS PARA CADA PREFIJO  
254 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de host (en rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
Representación binaria 25 bits de red	10101100.00010000. 00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.01111110	10101100.00010000. 00000100.11111111
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

DIFERENTE CANTIDAD DE HOSTS PARA CADA PREFIJO  
126 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de host (en rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo zeros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
Representación binaria 26 bits de red	10101100.00010000. 00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000. 00000100.00111111
172.16.4.0 /27	172.16.4.0	10101100.00010000.00000100.00111110 172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

DIFERENTE CANTIDAD DE HOSTS PARA CADA PREFIJO  
62 hosts

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red Todos los bits de host (en rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo zeros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31
Representación binaria 27 bits de red	10101100.00010000. 00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000. 00000100.00111111

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

DIFERENTE CANTIDAD DE HOSTS PARA CADA PREFIJO  
30 hosts

### CÁLCULO DE DIRECCIONES HOST, DE RED y DE BROADCAST

Hasta ahora, el usuario podría preguntarse: ¿Cómo se calculan estas direcciones? Este proceso de cálculo requiere que el usuario considere estas direcciones como binarias.

En las divisiones de red de ejemplo, se debe considerar el octeto de la dirección donde el prefijo divide la porción de red de la porción de host. En todos estos ejemplos, es el último octeto. A pesar de que esto es frecuente, el prefijo también puede dividir cualquiera de los octetos.

Para comenzar a comprender este proceso de determinar asignaciones de dirección, se desglosarán algunos ejemplos en datos binarios.

Observe la figura para obtener un ejemplo de la asignación de dirección para la red 172.16.20.0 /25.

En el primer cuadro, se encuentra la representación de la dirección de red. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la dirección de red, todos estos bits de host son "0". Esto hace que el último octeto de la dirección sea 0. De esta forma, la dirección de red es 172.16.20.0 /25.

En el segundo cuadro, se observa el cálculo de la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.



El tercer cuadro muestra el cálculo de la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

El cuarto cuadro representa el cálculo de la dirección host más alta. La dirección host más alta de una red es siempre un número menor que la dirección de broadcast. Esto significa que el bit más bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

A pesar de que para este ejemplo se ampliaron todos los octetos, sólo es necesario examinar el contenido del octeto dividido.

#### Asignación de direcciones



### UNICAST, BROADCAST, MULTICAST: TIPOS DE COMUNICACIÓN

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

**Unicast:** el proceso por el cual se envía un paquete de un host a un host individual.

**Broadcast:** el proceso por el cual se envía un paquete de un host a todos los hosts de la red.

**Multicast:** el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

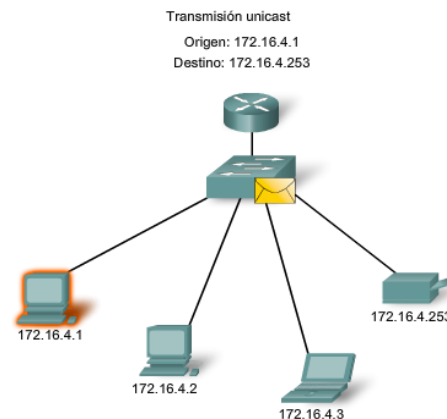
Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

#### **Tráfico unicast**

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internetwork.

En una red IPv4, a la dirección unicast aplicada a un dispositivo final se le denomina dirección host. En la comunicación unicast, las direcciones host asignadas a dos dispositivos finales se usan como direcciones IPv4 de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección host de origen y la

dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino. Es posible enviar la comunicación utilizando un paquete unicast por medio de una internetwork con las mismas direcciones.



### Transmisión de broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast.

La transmisión de broadcast se usa para ubicar servicios o dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe proporcionar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección
- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast.

De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local. Esta restricción depende de la configuración del router que bordea la red y del tipo de broadcast. Existen dos tipos de broadcasts: **broadcast dirigido y broadcast limitado**.

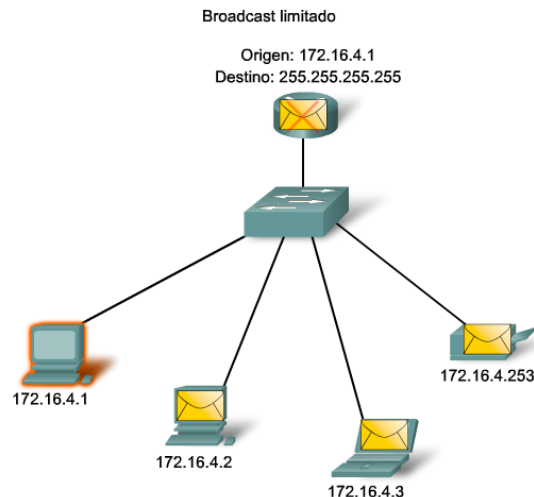
**Broadcast dirigido:** Un broadcast dirigido se envía a todos los hosts de una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red no local. Por ejemplo: para que un host fuera de la red se comunique con los hosts dentro de la red 172.16.4.0 /24, la dirección de destino del paquete sería 172.16.4.255. Esto se muestra en la figura. Aunque los routers no reenvían broadcasts dirigidos de manera predeterminada, se les puede configurar para que lo hagan.

**Broadcast limitado:** El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino 255.255.255.255. Los routers no envían estos broadcasts. Los paquetes dirigidos a la dirección de broadcast limitada sólo aparecerán

en la red local. Por esta razón, también se hace referencia a una red IPv4 como un dominio de broadcast. Los routers son dispositivos fronterizos para un dominio de broadcast.

A modo de ejemplo, un host dentro de la red 172.16.4.0 /24 transmitiría a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

Cuando se transmite un paquete, éste utiliza recursos de la red y de esta manera obliga a cada host de la red que lo recibe a procesar el paquete. Por lo tanto, el tráfico de broadcast debe limitarse para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan dominios de broadcast, subdividir las redes con tráfico de broadcast excesivo puede mejorar el rendimiento de la red.



### Transmisión de multicast

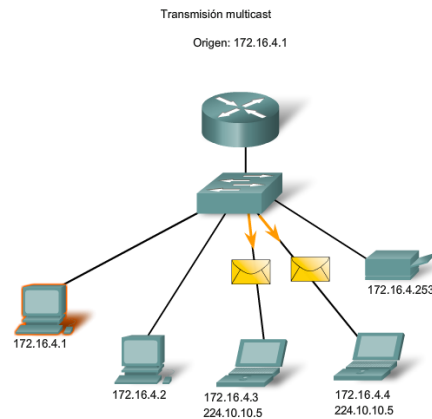
La transmisión de multicast está diseñada para conservar el ancho de banda de la red IPv4. Ésta reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino.

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
- Suministro de noticias

**Clientes multicast:** Los hosts que desean recibir datos multicast específicos se denominan clientes multicast. Los clientes multicast usan servicios iniciados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast exclusivamente asignada. Como se puede ver, IPv4 ha apartado un bloque especial de direcciones desde 224.0.0.0 hasta 239.255.255.255 para direccionamiento de grupos multicast.



### RANGOS DE DIRECCIONES IPv4 RESERVADAS

Expresado en formato de decimal punteada, el rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255. Como se pudo observar anteriormente, no todas estas direcciones pueden usarse como direcciones host para la comunicación unicast.

**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.

**Direcciones multicast:** Como se mostró antes, otro bloque importante de direcciones reservado con objetivos específicos es el rango de direcciones multicast IPv4 de 224.0.0.0 a 239.255.255.255. Además, el rango de direcciones multicast se subdivide en diferentes tipos de direcciones: direcciones de enlace local reservadas y direcciones agrupadas globalmente. Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de agrupamiento limitado.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones de enlace local reservadas. 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 las direcciones link-local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones agrupadas globalmente son de 224.0.1.0 a 238.255.255.255. Se les 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.

**Direcciones host:** Después de explicar los rangos reservados para las direcciones experimentales y las direcciones multicast, queda el rango de direcciones de 0.0.0.0 a 223.255.255.255 que podría usarse con hosts IPv4. Sin embargo, dentro de este rango existen muchas direcciones que ya están reservadas con objetivos específicos. A pesar de que se han tratado algunas de estas direcciones anteriormente, las principales direcciones reservadas se analizan en la siguiente sección.

Rangos de direcciones IPv4 reservadas

Tipo de dirección	Uso	Rango de direcciones IPv4 reservadas	RFC
Dirección host	utilizada en hosts IPv4	De 0.0.0.0 a 223.255.255.255	790
Direcciones multicast	utilizada en grupos multicast en una red local	De 224.0.0.0 a 239.255.255.255	1700
Direcciones experimentales	<ul style="list-style-type: none"><li>• utilizada para investigación o experimentación</li><li>• actualmente no se puede utilizar para los hosts en las redes IPv4</li></ul>	De 240.0.0.0 a 255.255.255.254	1700 3330

### DIRECCIONES PÚBLICAS y PRIVADAS

Aunque la mayoría de las direcciones host IPv4 son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan direcciones privadas.

#### **Direcciones privadas**

Los bloques de direcciones privadas son:

- de 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
- de 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
- de 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

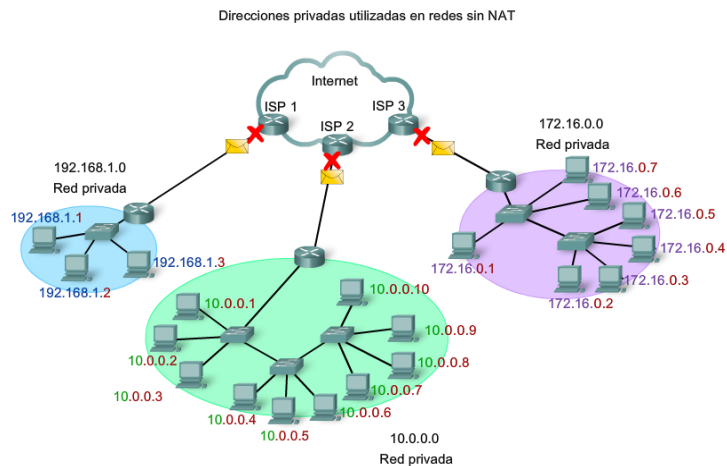
Los bloques de direcciones del espacio privado, como se muestra en la figura, se reservan para uso en redes privadas. No necesariamente el uso de estas direcciones debe ser exclusivo entre redes externas. Por lo general, los hosts que no requieren acceso a Internet pueden utilizar las direcciones privadas sin restricciones. Sin embargo, las redes internas aún deben diseñar esquemas de direcciones de red para garantizar que los hosts de las redes privadas utilicen direcciones IP que sean únicas dentro de su entorno de networking.

Muchos hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública. El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a llegar hasta Internet, los routers no tendrían rutas para reenviarlos a la red privada correcta.

**Traducción de direcciones de red (NAT):** Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

La NAT permite a los hosts de la red "pedir prestada" una dirección pública para comunicarse con redes externas. A pesar de que existen algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

**Direcciones públicas:** La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aún dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos.



### DIRECCIONAMIENTO IPv4 ESPECIALES

Hay determinadas direcciones que no pueden asignarse a los hosts por varios motivos. También hay direcciones especiales que pueden asignarse 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, respectivamente, la dirección de red y la dirección de broadcast.

**Ruta predeterminada:** Como se mostró anteriormente, la ruta predeterminada IPv4 se representa 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 de loopback IPv4 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 del stack de 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. Las direcciones dentro de este bloque no deben figurar en ninguna red.

**Direcciones link-local:** Las direcciones IPv4 del bloque de direcciones desde 169.254.0.0 hasta 169.254.255.255 (169.254.0.0 /16) se encuentran designadas como direcciones link-local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se puede usar en una red de punto a punto o para un host que no pudo obtener automáticamente una dirección de un servidor de protocolo de configuración dinámica de host (DHCP).

La comunicación mediante direcciones link-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 link-local IPv4 a ningún router para ser reenviado, y debería establecer el TTL de IPv4 para estos paquetes en 1.

Las direcciones link-local no proporcionan 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.

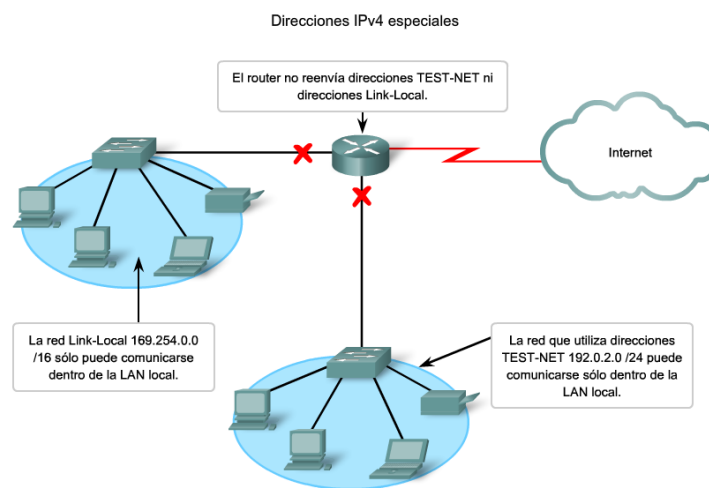
**Direcciones TEST-NET:** Se establece el bloque de direcciones de 192.0.2.0 a 192.0.2.255 (192.0.2.0 /24) para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas 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.

Enlaces:

Direcciones local-link <http://www.ietf.org/rfc/rfc3927.txt?number=3927>

Direcciones IPv4 de uso especial <http://www.ietf.org/rfc/rfc3330.txt?number=3330>

Ubicación multicast: <http://www.iana.org/assignments/multicast-addresses>



## DIRECCIONAMIENTO DE IPv4 DE LEGADO

**Clases de redes antiguas:** Históricamente, la RFC1700 agrupaba rangos de unicast en tamaños específicos llamados direcciones de clase A, de clase B y de clase C. También definía a las direcciones de clase D (multicast) y de clase E (experimental), anteriormente tratadas.

Las direcciones unicast de clases A, B y C definían redes de tamaños específicos, así como bloques de direcciones específicos para estas redes, como se muestra en la figura. Se asignó a una compañía u organización todo un bloque de direcciones de clase A, clase B o clase C. Este uso de espacio de dirección se denomina direccionamiento con clase.

**Bloques de clase A:** Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo /8 fijo, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host.

Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que sólo había 128 redes de clase A posibles, de 0.0.0.0 /8 a 127.0.0.0 /8, antes de excluir los bloques de direcciones reservadas. A pesar de que las direcciones de clase A reservaban la mitad del espacio de direcciones, debido al límite de 128 redes, sólo podían ser asignadas a aproximadamente 120 compañías u organizaciones.

**Bloques de clase B:** El espacio de direcciones de clase B fue diseñado para satisfacer las necesidades de las redes de tamaño moderado a grande con más de 65.000 hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones host. Al igual que con la clase A, debía reservarse espacio de direcciones para las clases de direcciones restantes.

Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran 10. De esta forma, se restringía el bloque de direcciones para la clase B a 128.0.0.0 /16 hasta 191.255.0.0 /16. La clase B tenía una asignación de direcciones un tanto más eficiente que la clase A debido a que dividía equitativamente el 25% del total del espacio total de direcciones IPv4 entre aproximadamente 16.000 redes.

**Bloques de clase C:** El espacio de direcciones de clase C era la clase de direcciones antiguas más comúnmente disponible. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts.

Los bloques de direcciones de clase C utilizaban el prefijo /24. Esto significaba que una red de clase C usaba sólo el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red.

Los bloques de direcciones de clase C reservaban espacio de direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0 /16 a 223.255.255.0 /16. A pesar de que ocupaba sólo el 12.5% del total del espacio de direcciones IPv4, podía suministrar direcciones a 2 millones de redes.

#### **Limitaciones del sistema basado en clases**

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. La asignación con clase de espacio de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4. Por ejemplo: una compañía con una red con 260 hosts necesitaría que se le otorgue una dirección de clase B con más de 65.000 direcciones.

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 duración del prefijo de acuerdo con la clase de dirección.

#### **Direccionamiento sin clase**

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



## Clases de direcciones IP

Clase de dirección	Rango del primer octeto (decimal)	Bits del primer octeto (los bits verdes no se modifican)	Partes de las direcciones de red (N) y de host (H)	Máscara de subred predeterminada (decimal y binaria)	Cantidad de posibles redes y hosts por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes ( $2^7$ ) 16777214 hosts por red ( $2^{24}-2$ )
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16384 redes ( $2^{14}$ ) 65534 hosts por red ( $2^{16}-2$ )
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2097150 redes ( $2^{21}-2$ ) 254 hosts por red ( $2^8-2$ )
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

\*\* Todos los ceros (0) y los unos (1) son direcciones hosts no válidas.

## ASIGNACIÓN DE DIRECCIONAMIENTO

PLANIFICACIÓN DEL DIRECCIONAMIENTO DE LA RED

Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red corporativa esté bien diseñada. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

- Evitar duplicación de direcciones
- Proporcionar y controlar el acceso
- Controlar seguridad y rendimiento

**Evitar duplicación de direcciones:** Como se sabe, cada host en una interwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

**Proporcionar y controlar el acceso:** Algunos hosts proporcionan recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. El acceso a estos recursos puede ser controlado por la dirección de la Capa 3. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Por ejemplo, si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a su dirección y es posible que los clientes no puedan ubicar este recurso.

**Controlar seguridad y rendimiento:** De igual manera, es necesario controlar la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

**Asignación de direcciones dentro de una red**

Como ya se ha explicado, los hosts se asocian con una red IPv4 por medio de una porción de red común de la dirección. Dentro de una red, existen diferentes tipos de hosts.

Algunos ejemplos de diferentes tipos de hosts son:

- Dispositivos finales para usuarios
- Servidores y periféricos
- Hosts a los que se accede desde Internet
- Dispositivos intermediarios

Cada uno de los diferentes tipos de dispositivos debe asignarse a un bloque lógico de direcciones dentro del rango de direcciones de la red.

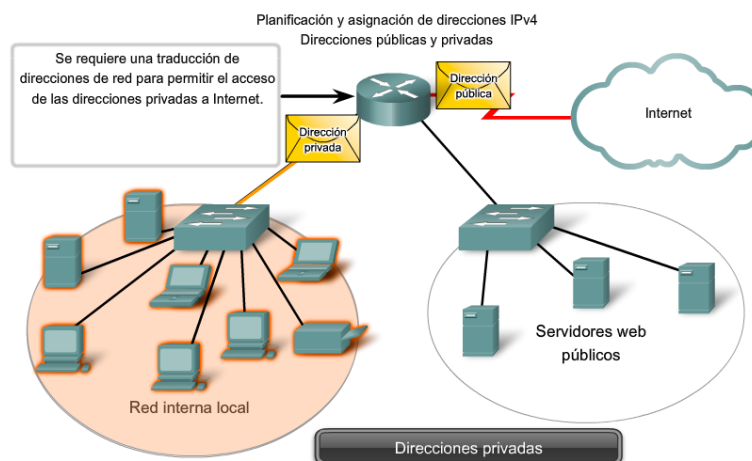


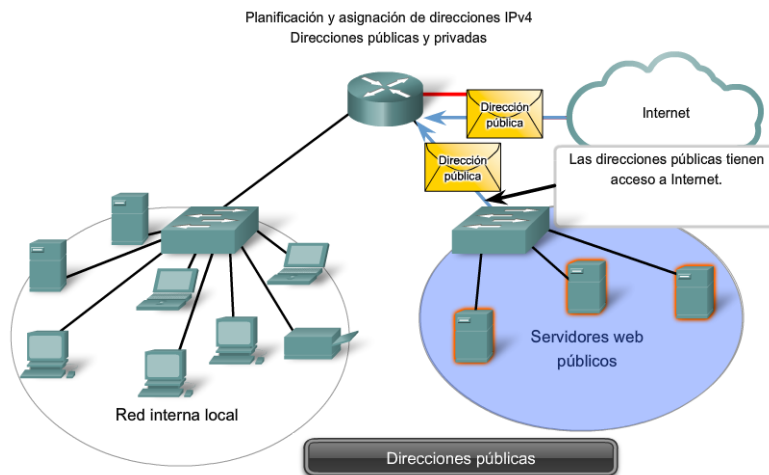
Una parte importante de la planificación de un esquema de direccionamiento IPv4 es decidir cuándo utilizar direcciones privadas y dónde se deben aplicar.

Se debe tener en cuenta lo siguiente:

- ¿Habrá más dispositivos conectados a la red que direcciones públicas asignadas por el ISP de la red?
- ¿Se necesitará acceder a los dispositivos desde fuera de la red local?
- Si los dispositivos a los que se pueden asignar direcciones privadas requieren acceso a Internet, ¿está la red capacitada para proporcionar el servicio de traducción de direcciones de red (NAT)?

Si hay más dispositivos que direcciones públicas disponibles, sólo los dispositivos que accederán directamente a Internet, como los servidores web, requieren una dirección pública. Un servicio NAT permitiría a esos dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.





### DIRECCIONAMIENTO ESTÁTICO o DINÁMICO PARA DISPOSITIVOS DE USUARIO FINAL

**Direcciones para dispositivos de usuario:** En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos IP, impresoras y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

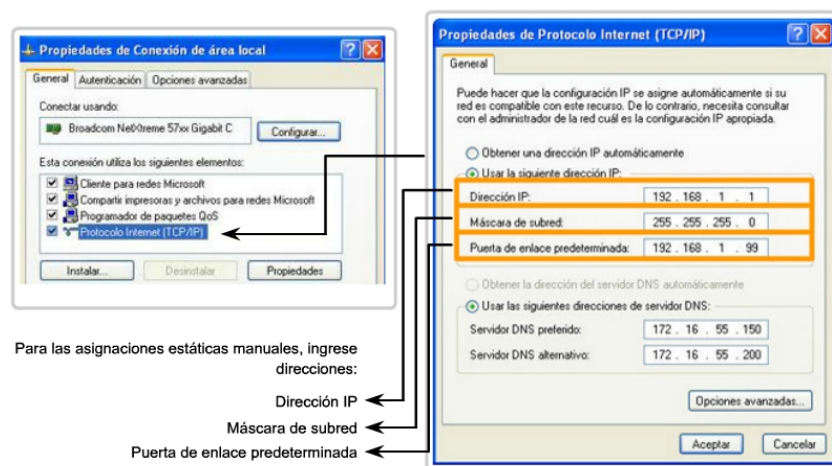
Las direcciones IP pueden asignarse de manera estática o dinámica.

**Asignación estática de direcciones:** Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host, como se muestra en la figura. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto.

Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red. Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocaría problemas si se cambiara esa dirección. Además, la asignación estática de información de direccionamiento puede proporcionar un mayor control de los recursos de red. Sin embargo, puede llevar mucho tiempo ingresar la información en cada host.

Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.

Direccionamiento de dispositivos finales

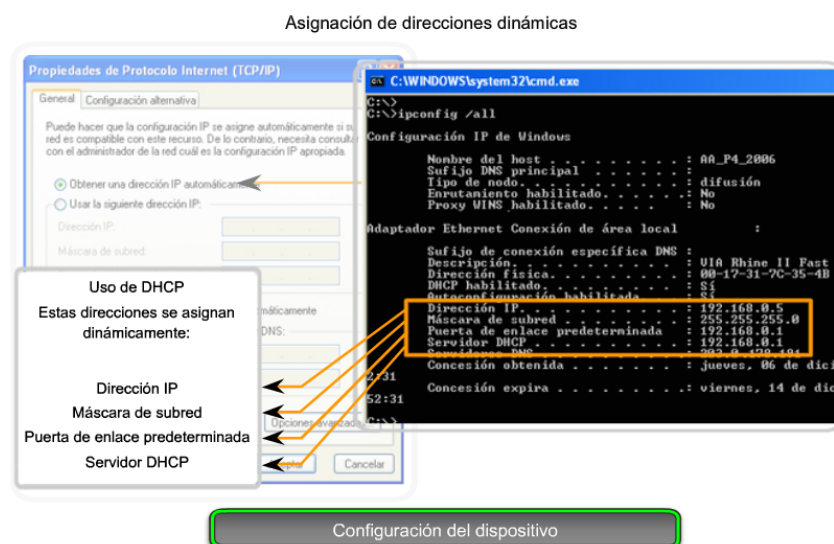


**Asignación dinámica de direcciones:** Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos de usuarios finales a menudo poseen direcciones que se asignan en forma dinámica utilizando el protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración. La configuración del servidor DHCP requiere definir un bloque de direcciones, denominado pool de direcciones, para asignarlo a los clientes DHCP en una red. Las direcciones asignadas a este pool deben ser planificadas de manera que se excluyan las direcciones utilizadas para otros tipos de dispositivos.

Generalmente, el DHCP es el método que se prefiere para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para el personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.



## ASIGNACIÓN DE DIRECCIONES A OTRO DISPOSITIVOS

**Direcciones para servidores y periféricos:** Cualquier recurso de red como un servidor o una impresora debe tener una dirección IPv4 estática, como se muestra en la figura. Los hosts clientes acceden a estos recursos utilizando las direcciones IPv4 de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos.

Los servidores y periféricos son un punto de concentración para el tráfico de la red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red debe poder identificar rápidamente estos dispositivos. Utilizar un sistema de numeración consistente para estos dispositivos facilita la identificación.

**Direcciones para hosts accesibles desde Internet:** En la mayoría de las internetworks, los hosts fuera de la empresa pueden acceder sólo a unos pocos dispositivos. En la mayoría de los casos, estos

dispositivos son normalmente algún tipo de servidor. Al igual que todos los dispositivos en una red que proporciona recursos de red, las direcciones IPv4 para estos dispositivos deben ser estáticas.

En el caso de los servidores a los que se puede acceder desde Internet, cada uno debe tener una dirección de espacio público asociada. Además, las variaciones en la dirección de uno de estos dispositivos hará que no se pueda acceder a éste desde Internet. En muchos casos, estos dispositivos se encuentran en una red numerada mediante direcciones privadas. Esto significa que el router o el firewall del perímetro de la red debe estar configurado para traducir la dirección interna del servidor en una dirección pública. Debido a esta configuración adicional del dispositivo que actúa como intermediario del perímetro, resulta aun más importante que estos dispositivos tengan una dirección predecible.

**Direcciones para dispositivos intermediarios:** Los dispositivos intermediarios también son un punto de concentración para el tráfico de la red. Casi todo el tráfico dentro redes o entre ellas pasa por alguna forma de dispositivo intermediario. Por lo tanto, estos dispositivos de red ofrecen una ubicación oportuna para la administración, el monitoreo y la seguridad de red.

A la mayoría de los dispositivos intermediarios se le asigna direcciones de Capa 3. Ya sea para la administración del dispositivo o para su operación. Los dispositivos como hubs, switches y puntos de acceso inalámbricos no requieren direcciones IPv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar, monitorear o resolver problemas de funcionamiento de la red, éstos deben tener direcciones asignadas.

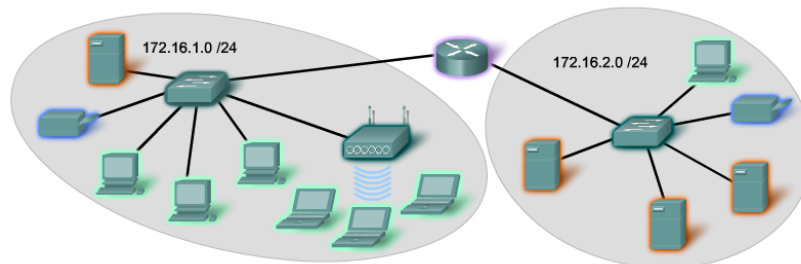
Debido a que es necesario saber cómo comunicarse con dispositivos intermediarios, éstos deben tener direcciones predecibles. Por lo tanto, típicamente, las direcciones se asignan manualmente. Además, las direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red que las direcciones de dispositivos de usuario.

**Routers y firewalls:** A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall un dirección IPv4 para cada interfaz. Cada interfaz se encuentra en una red diferente y funciona como gateway para los hosts de esa red. Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red. Esta asignación debe ser uniforme en todas las redes de la empresa, de manera que el personal de red siempre conozca la gateway de la red, independientemente de cuál sea la red en la que están trabajando.

Las interfaces de router y firewall son el punto de concentración del tráfico que entra y sale de la red. Debido a que los hosts de cada red usan una interfaz de dispositivo router o firewall como gateway para salir de la red, existe un flujo abundante de paquetes en estas interfaces. Por lo tanto, estos dispositivos pueden cumplir una función importante en la seguridad de red al filtrar los paquetes según las direcciones IPv4 de origen y destino. Agrupar los diferentes tipos de dispositivos en grupos de direccionamiento lógico hace que la asignación y el funcionamiento del filtrado de paquetes sea más eficiente.

Rangos de direcciones IP de los dispositivos

Uso	Primera dirección	Última dirección	Dirección de resumen
Dirección de red	172.16.x.0	.....	172.16.x.0 /25
Hosts de usuarios (pool de DHCP)	172.16.x.1	172.16.x.127	
Servidores	172.16.x.128	172.16.x.191	172.16.x.128 /26
Periféricos	172.16.x.192	172.16.x.223	172.16.x.128 /26
Dispositivos de networking	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



### ¿QUIEN ASIGNA LAS DIFERENTES DIRECCIONES?

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.

La Autoridad de números asignados de Internet (IANA) (<http://www.iana.net>) es un soporte maestro de direcciones IP. Las direcciones IP multicast 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), como se muestra en la figura. Cuando un RIR requiere más direcciones IP para distribuirlas o asignarlas dentro de su región, la IANA distribuye direcciones IPv6 a los RIR en función de sus necesidades establecidas.

Los principales registros son:

- AfriNIC (African Network Information Centre), región África <http://www.afrinic.net>
- APNIC (Asia Pacific Network Information Centre), región Asia/Pacífico <http://www.apnic.net>
- ARIN (American Registry for Internet Numbers), región América del Norte <http://www.arin.net>
- LACNIC (Regional Latin-American and Caribbean IP Address Registry), 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>

Enlaces:

Asignaciones de registros de direcciones IPv4:

- <http://www.ietf.org/rfc/rfc1466.txt?number=1466>
- <http://www.ietf.org/rfc/rfc2050.txt?number=2050>
- Asignación de direcciones IPV4: <http://www.iana.org/ipaddress/ip-addresses.htm>
- Búsqueda de direcciones IP: <http://www.arin.net/whois/>

Entidades que supervisan la asignación de direcciones IP

Global	IANA				
Registros de Internet regionales	AfriNIC Región de África	APNIC Asia/ Región del Pacífico	LACNIC Región de América Latina y el Caribe	ARIN Región de América del Norte	RIPE NCC Europa, Medio Oriente, Región de Asia Central

### PROVEEDORES DE SERVICIOS DE INTERNET (ISP)

**El papel del ISP:** La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio.

En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente.

**Servicios del ISP:** Para tener acceso a los servicios de Internet, tenemos que conectar nuestra red de datos a Internet usando un proveedor de servicios de Internet (ISP).

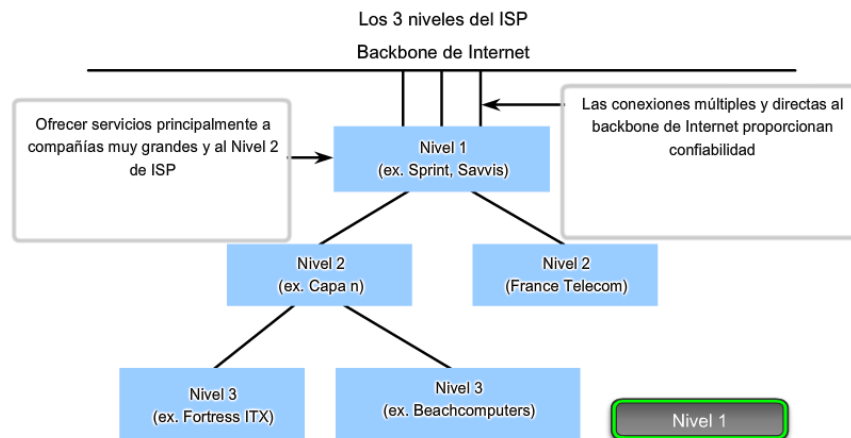
Los ISP poseen sus propios conjuntos de redes internas de datos para administrar la conectividad a Internet y proporcionar servicios relacionados. Entre los servicios que un ISP generalmente ofrece a sus clientes se encuentran los servicios DNS, servicios de correo electrónico y un sitio Web. Dependiendo del nivel de servicio requerido y disponible, los clientes usan diferentes niveles de un ISP.

**Niveles del ISP:** Los ISP se designan mediante una jerarquía basada en su nivel de conectividad al backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior, como se muestra en la figura.

#### Nivel 1

En la parte superior de la jerarquía de ISP están los ISP de nivel 1. Éstos son grandes ISP a nivel nacional o internacional que se conectan directamente al backbone de Internet. Los clientes de ISP de nivel 1 son ISP de menor nivel o grandes compañías y organizaciones. Debido a que se encuentran en la cima de la conectividad a Internet, ofrecen conexiones y servicios altamente confiables. Entre las tecnologías utilizadas como apoyo de esta confiabilidad se encuentran múltiples conexiones al backbone de Internet.

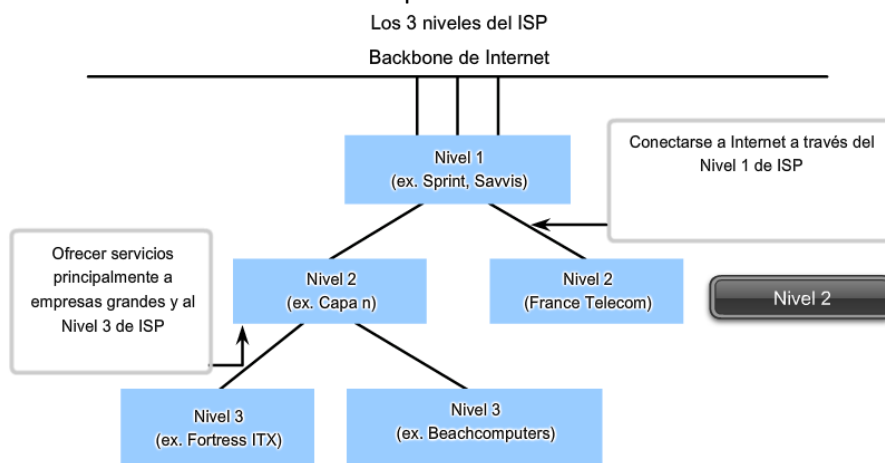
Las principales ventajas para los clientes de ISP de nivel 1 son la confiabilidad y la velocidad. Debido a que estos clientes están a sólo una conexión de distancia de Internet, hay menos oportunidades de que se produzcan fallas o cuellos de botella en el tráfico. La desventaja para los clientes de ISP de nivel 1 es el costo elevado.



### Nivel 2

Los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1. Los ISP de nivel 2 generalmente se centran en los clientes empresa. Los ISP de nivel 2 normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus propios servicios como DNS, servidores de correo electrónico y servidores web. Otros servicios ofrecidos por los ISP de nivel 2 pueden incluir desarrollo y mantenimiento de sitios web, e-commerce/e-business y VoIP.

La principal desventaja de los ISP de nivel 2, comparados con los ISP de nivel 1, es el acceso más lento a Internet. Como los IPS de Nivel 2 están al menos a una conexión más lejos de la red troncal de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1.

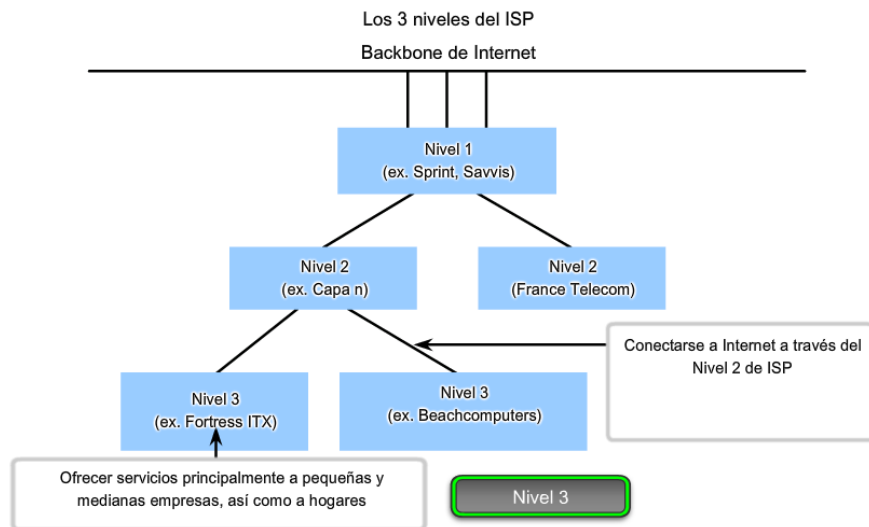


### Nivel 3

Los ISP de nivel 3 compran su servicio de Internet de los ISP de nivel 2. El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica. Típicamente, los clientes del nivel 3 no necesitan muchos de los servicios requeridos por los clientes del nivel 2. Su necesidad principal es conectividad y soporte.

Estos clientes a menudo tienen conocimiento escaso o nulo sobre computación o redes. Los ISP de nivel 3 suelen incluir la conectividad a Internet como parte del contrato de servicios de red y computación para los clientes. A pesar de que pueden tener un menor ancho de banda y menos confiabilidad que los proveedores de nivel 1 y 2, suelen ser buenas opciones para pequeñas y medianas empresas.





### DESCRIPCIÓN DE IPv6

A principios de los años noventa, el grupo de trabajo de ingeniería de Internet (IETF) centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo. Esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6.

Crear mayores capacidades de direccionamiento fue la motivación inicial para el desarrollo de este nuevo protocolo. También se consideraron otros temas durante el desarrollo de IPv6, como:

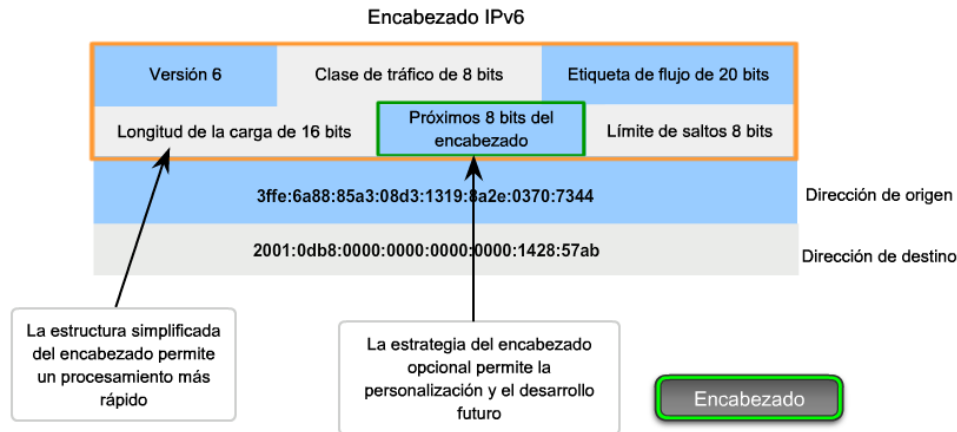
- Mejor manejo de paquetes
- Escalabilidad y longevidad mejoradas
- Mecanismos de QoS
- Seguridad integrada

Para proporcionar estas características, IPv6 ofrece:

- Direccionamiento jerárquico de 128 bits: para expandir las capacidades de direccionamiento
- Simplificación del formato de encabezado: para mejorar el manejo de paquetes
- Soporte mejorado para extensiones y opciones: para escalabilidad y longevidad mejoradas y mejor manejo de paquetes
- Capacidad de etiquetado de flujo: como mecanismos QoS
- Capacidades de autenticación y privacidad: para integrar la seguridad

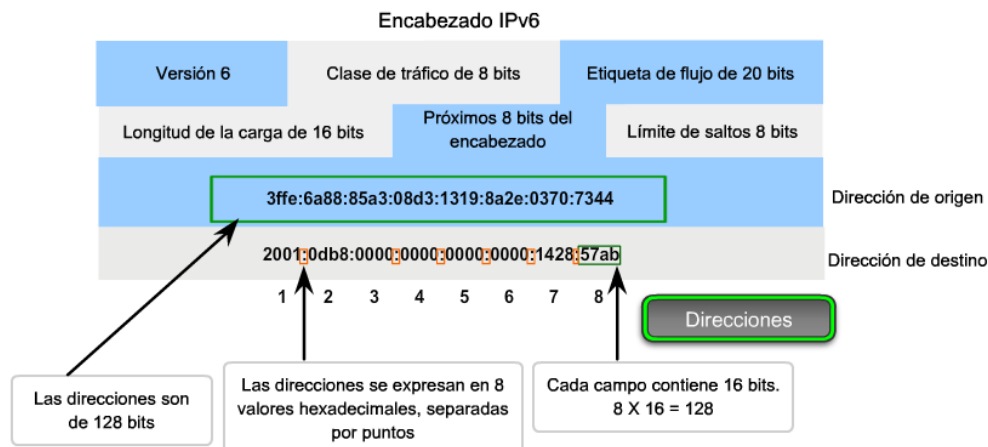
IPv6 no es simplemente un nuevo protocolo de Capa 3: es una nueva suite de protocolos. Se han desarrollado nuevos protocolos en varias capas del stack para admitir este nuevo protocolo. Hay un nuevo protocolo de mensajería (ICMPv6) y nuevos protocolos de enrutamiento. Debido al mayor tamaño del encabezado de IPv6, también repercute en la infraestructura de red subyacente.

**Transición a IPv6:** Como se puede ver en esta breve introducción, IPv6 ha sido diseñado con escalabilidad para permitir años de crecimiento de la internetwork. Sin embargo, IPv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro. Sin embargo, IPv6 podrá eventualmente reemplazar a IPv4 como protocolo de Internet dominante.



Enlaces:

- IPv6: <http://www.ietf.org/rfc/rfc2460.txt?number=2460>
- Direccionamiento IPv6: <http://www.ietf.org/rfc/rfc3513.txt?number=3513>
- Seguridad IPv6: <http://www.ietf.org/rfc/rfc2401.txt?number=2401>
- Seguridad IPv6: <http://www.ietf.org/rfc/rfc3168.txt?number=3168>
- Seguridad IPv6: <http://www.ietf.org/rfc/rfc4302.txt?number=4302>
- ICMPv6: <http://www.ietf.org/rfc/rfc4443.txt?number=4443>



**Bibliografía:**

- Cisco Systems: Academia de Networking de Cisco Systems: Guía del primer año. — 2ª ed. — Madrid: Pearson Educación, 2002. ISBN 8420532967
- Curso Cisco Systems: Academia de Networking de Cisco Systems – Versión 4.0
- Curso visual y práctico: Administrador de Redes Instalación y configuración de hardware y software. – USERS-CISCO.

**Sitios web:**

- Calculadora IP On-Line: <http://www.subnet-calculator.com/>
- ¿qué es Ipv6? - <http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx>