Conversión binaria y decimal.

Direcciones IPv4.

El sistema binario es un sistema numérico que consiste en los números 0 y 1, denominados bits. En comparación, el sistema numérico decimal consiste en 10 dígitos, que incluyen los números 0 a 9.

Es importante que comprendamos el sistema binario, ya que los hosts, los servidores y los dispositivos de red usan el direccionamiento binario. Específicamente, usan direcciones IPv4 binarias, como se muestra en la figura 1, para identificarse entre sí.

Cada dirección consta de una cadena de 32 bits, divididos en cuatro secciones denominadas octetos. Cada octeto contiene 8 bits (o 1 byte) separados por un punto. Por ejemplo, a la PC1 de la ilustración se le asignó la dirección IPv4 11000000.10101000.00001010.00001010. La dirección de gateway predeterminado sería la de la interfaz Gigabit Ethernet del R1, 11000000.10101000.00001010.00000001.

El trabajo con números binarios puede ser desafiante. Para que esto resulte más fácil, las direcciones IPv4 suelen expresarse mediante una notación decimal punteada, como se muestra en la figura 2. A la PC1 se le asignó la dirección IPv4 192.168.10.10, y la dirección de gateway predeterminado es 192.168.10.1.

Para tener una buena comprensión del direccionamiento de red, es necesario comprender el direccionamiento binario y obtener habilidades prácticas en la conversión entre direcciones IPv4 binarias y decimales punteadas.

En esta sección, se explica cómo convertir entre los sistemas de numeración de base dos y de base 10.

Notación de posición.

Para aprender a convertir de sistema binario a decimal, es necesario entender la notación de posición. El término "notación de posición" significa que un dígito representa diferentes valores según la "posición" que el dígito ocupa en la secuencia de números. Ya conoce el sistema de numeración más común, el sistema de notación decimal (de base 10).

El sistema de notación de posición decimal funciona como se describe en la figura 1. Haga clic en los títulos de las filas para ver una descripción de cada una. Para usar el sistema de posición, una un número dado con su valor de posición. En el ejemplo de la figura 2, se muestra cómo se usa la notación de posición con el número decimal 1234.

En comparación, la notación de posición binaria funciona como se describe en la figura 3. Haga clic en los títulos de las filas para ver una descripción de cada una.

En el ejemplo de la figura 4, se muestra cómo el número binario 11000000 corresponde al número 192. Si el número binario fuera 10101000, el número decimal correspondiente sería 168.

Base

La primera fila identifica la base numérica o la base. El sistema de notación decimal está basado en 10, por lo tanto, la base es 10.

Position in Number

La segunda fila toma en cuenta la posición del número decimal de derecha a izquierda, 0 (primera posición), 1 (segunda posición), 2 (tercera posición), 3 (cuarta posición). A su vez, estos números representan el valor exponencial que se usa para calcular el valor de posición (cuarta fila).

Cálculo

La tercera fila calcula el valor de posición al aumentar la base con el valor exponencial de la posición. Nota: n^0 es siempre = 1.

Valor de posición

La primera fila identifica la base numérica o la base. Por lo tanto, el valor que se indica, de izquierda a derecha, representa unidades de millares, centenas, decenas y unidades.

Base

El sistema de notación decimal está basado en 2, por lo tanto, la base es 2.

Position in Number

La segunda fila toma en cuenta la posición del número binario de derecha a izquierda, 0 (primera posición), 1 (segunda posición), 2 (tercera posición), 3 (cuarta posición). A su vez, estos números representan el valor exponencial que se usa para calcular el valor de posición (cuarta fila).

Cálculo

La tercera fila calcula el valor de posición al aumentar la base con el valor exponencial de la posición. Nota: n^0 es siempre = 1.

Valor de posición

La cuarta fila identifica el valor de posición, lo que significa que un dígito en dicha posición representa el valor de la unidad. Por lo tanto, el valor que se indica, de derecha a izquierda, representa unidades de uno, dos, cuatro, ocho, etc.

Conversión de sistema binario a decimal.

Para convertir una dirección IPv4 binaria a su equivalente decimal punteada, divida la dirección IPv4 en cuatro octetos de 8 bits. A continuación, aplique el valor de posición binario al primer octeto del número binario y calcule según corresponda.

Por ejemplo, suponga que 11000000.10101000.00001011.00001010 es la dirección IPv4 binaria de un host. Para convertir la dirección de sistema binario a decimal, comience con el primer octeto, como se muestra en la figura 1. Introduzca el número binario de 8 bits en el valor de posición de la fila 1 y, después, calcule para producir el número decimal 192. Este número entra en el primer octeto de la notación decimal punteada.

A continuación, convierta el segundo octeto como se muestra en la figura 2. El valor decimal resultante es 168 y entra en el segundo octeto.

Convierta el tercer octeto como se muestra en la figura 4 y el cuarto octeto como se muestra en la figura 5, con lo que se completa la dirección IP y se obtiene 192.168.11.10.

Conversión de sistema decimal a binario.

También es necesario comprender cómo convertir una dirección IPv4 decimal punteada a una binaria. La tabla de valores de posición binarios es una herramienta útil. A continuación, se muestra cómo usar la tabla para convertir de sistema decimal a binario:

- En la figura 1, se pregunta si el número decimal del octeto (n) es igual o superior al bit más significativo (128). Si no es así, introduzca un valor binario 0 en el valor de posición 128. Si es así, agregue un valor binario 1 al valor de posición 128 y reste 128 del número decimal.
- En la figura 2, se pregunta si el resto (n) es igual o superior al siguiente bit más significativo (64). Si no es así, agregue un valor binario 0 al valor de posición 64, de lo contrario, agregue el valor binario 1 y reste 64 del número decimal.
- En la figura 3, se pregunta si el resto (n) es igual o superior al siguiente bit más significativo (32). Si no es así, agregue un valor binario 0 al valor de posición 32, de lo contrario, agregue el valor binario 1 y reste 32 del número decimal.

En las figuras 4 a 8, continúe evaluando el número decimal hasta que se hayan introducido todos los valores de posición y se obtenga el valor binario equivalente.

Ejemplos de conversión de sistema decimal a binario.

Para poder comprender el proceso, considere la dirección IP 192.168.11.10. Mediante el proceso explicado anteriormente, comience con la tabla de valores de posición binarios y el primer número decimal 192.

En la figura 1, se muestra cómo se compara el número 192 para ver si es igual o mayor que el bit de valor superior 128. Como 192 es mayor que 128, agregue un 1 al valor de posición de valor superior para que represente 128. A continuación, reste 128 de 192 para obtener un resto de 64. En la figura 2, se compara el valor 64 con el siguiente bit de valor superior 64. Como son iguales, agregue un 1 al siguiente valor de posición de valor superior. Introduzca un valor binario 0 en el resto de los valores de posición, como se muestra en la figura 3. El valor binario del primer octeto es 11000000.

El siguiente octeto es 168. En la figura 4, se compara 168 con el bit de valor superior 128. Como 168 es mayor que 128, agregue un 1 al valor de posición de valor superior. A continuación, reste 128 de 168 para obtener un resto de 40. En la figura 5, se compara el valor 40 con el siguiente bit de valor superior 64. Como 40 es menor, agregue un 0 al siguiente valor de posición de valor superior 64. En la figura 6, se compara el siguiente bit de valor superior 32. Como 40 es mayor que 32, agregue un 1 al valor de posición y reste 32 de 40 para obtener un resto de 8. Ocho coincide con un valor de posición específico. Por lo tanto, introduzca un 0 para el valor de posición de 16 y agregue un 1 al valor de posición de 8, como se muestra en la figura 7. Agregue un 0 a todos los valores de posición restantes. Como se muestra en la figura 8, el valor binario del tercer octeto es 10101000.

El tercer octeto es 11. Es posible omitir el proceso de resta con números decimales menores o más pequeños. Por ejemplo, en la figura 9, se muestra el número binario convertido. Observe que sería bastante fácil calcular este número sin tener que pasar por el proceso de resta (8 + 2 + 1 = 11). El valor binario del segundo octeto es 00001011.

El cuarto octeto es 10 (8 + 2). Como se muestra en la figura 10, el valor binario del cuarto octeto es 00001010.

La conversión de sistema binario a decimal puede parecer un desafío inicialmente, pero con la práctica resulta más fácil.

Estructura de la dirección IPv4. Porciones de red y de host.

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Recuerde que una dirección IPv4 es una dirección jerárquica compuesta por una porción de red y una porción de host. Cuando se determina la porción de red en comparación con la porción de host, se debe observar la secuencia de 32 bits. Dentro de la secuencia de 32 bits, una porción de los bits identifica la red y una porción identifica el host, como se muestra en la ilustración.

Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Si dos hosts tienen el mismo patrón de bits en la porción de red especificada de la secuencia de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits identifica la red y qué porción identifica el host? Esa es la función de la máscara de subred.

La máscara de subred.

Como se muestra en la figura 1, se deben configurar tres direcciones IPv4 decimales punteadas cuando se asigna una configuración IPv4 al host.

- **Dirección IPv4:** dirección IPv4 única del host.
- **Máscara de subred:** se usa para identificar la porción de red/host de la dirección IPv4.
- **Gateway predeterminado:** identifica el gateway local (es decir, la dirección IPv4 de interfaz de router local) para llegar a redes remotas.

Cuando se asigna una dirección IPv4 a un dispositivo, la máscara de subred se usa para determinar la dirección de red a la que pertenece el dispositivo. La dirección de red representa todos los dispositivos de la misma red.

En la figura 2, se muestra la dirección decimal punteada y la máscara de subred de 32 bits. Observe que la máscara de subred es básicamente una secuencia de bits 1 seguida de una secuencia de bits 0.

Para identificar las porciones de red y de host de una dirección IPv4, se compara la máscara de subred con la dirección IPv4 bit por bit, de izquierda a derecha, como se muestra en la figura 3. Los 1 de la máscara de subred identifican la porción de red, mientras que los 0 identifican la porción de host. Se debe tener en cuenta que la máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice a la PC dónde buscar estas porciones en una dirección IPv4 dada.

El proceso real que se usa para identificar la porción de red y la porción de host se denomina AND.

AND lógico.

El AND lógico es una de las tres operaciones binarias básicas que se utilizan en la lógica digital. Las otras dos son OR y NOT. Si bien en las redes de datos se usan las tres, solo AND se usa para determinar la dirección de red. Por lo tanto, nuestro debate en este punto se limita a la operación lógica AND.

La operación lógica AND es la comparación de dos bits que producen los resultados que se muestran en la figura 1. Observe que solo mediante 1 AND 1 se obtiene 1.

Para identificar la dirección de red de un host IPv4, se recurre a la operación lógica AND para la dirección IPv4, bit por bit, con la máscara de subred. El uso de la operación AND entre la dirección y la máscara de subred produce la dirección de red.

Para demostrar cómo se usa AND para detectar una dirección de red, piense en un host con la dirección IPv4 192.168.10.10 y la máscara de subred 255.255.255.0. En la figura 2, se muestra la dirección de host IPv4 y la conversión a dirección binaria. En la figura 3, se agrega la dirección binaria de la máscara de subred del host.

En las secciones resaltadas en amarillo de la figura 4, se identifican los bits AND que produjeron un 1 binario en la fila de Resultados AND. Todas las demás comparaciones de bits producen 0 binarios. Observe cómo el último octeto ya no tiene bits 1 binarios.

Por último, en la figura 5, se muestra la dirección de red resultante 192.168.10.0 255.255.255.0. Por lo tanto, el host 192.168.10.10 está en la red 192.168.10.0 255.255.255.0.

La longitud de prefijo.

Puede ser difícil expresar direcciones de red y de host con la dirección de la máscara de subred decimal punteada. Afortunadamente, existe un método alternativo más simple para identificar una máscara de subred que se denomina "longitud de prefijo".

Específicamente, la longitud de prefijo es el número de bits fijados en 1 en la máscara de subred. Se escribe mediante la "notación de barra diagonal", es decir, una "/" seguida por el número de bits fijados en 1. Por lo tanto, cuente el número de bits en la máscara de subred y anteponga una barra diagonal.

Para ver un ejemplo, consulte la tabla de la ilustración. En la primera columna, se enumeran varias máscaras de subred que se pueden usar con una dirección de host. En la segunda columna, se muestra la dirección binaria de 32 bits convertida. En la última columna, se muestra la longitud de prefijo resultante.

Más adelante se analiza el uso de varios tipos de longitudes de prefijo. De momento, nos centraremos en la máscara de subred /24 (es decir, 255.255.255.0).

Direcciones de red, de host y de difusión.

Cada dirección de red contiene (o identifica) direcciones de host y una dirección de difusión, como se describe en la figura 1.

- En la figura 2, se enumeran y se describen las direcciones específicas dentro de la red 192.168.10.0 /24.
- Para ver otro ejemplo, consulte las figuras 3 a 7. En estas ilustraciones, observe cómo la porción de red de las direcciones se mantiene igual, al tiempo que la porción de host cambia.
- En la figura 3, se muestra la dirección de red 10.1.1.0 /24. Los bits de host son todos 0.
- En la figura 4, se muestra la dirección de host IPv4 10.1.1.10. Los bits de host son una mezcla de 0 y 1.
- En la figura 5, se muestra la primera dirección de host IPv4 10.1.1.1. Los bits de host son todos 0 con un 1. Observe que se asigna a la interfaz de router y, por lo tanto, se transformaría en el gateway predeterminado para todos los hosts en esa red.
- En la figura 6, se muestra la última dirección de host IPv4 10.1.1.254. Los bits de host son todos 1 con un 0.
- En la figura 7, se muestra la dirección de difusión 10.1.1.255. Los bits de host son todos 1.

Los conceptos que se debaten en este tema son fundamentales para comprender el direccionamiento IPv4. Asegúrese de entender cómo una dirección de red identifica una porción de red y una porción de host mediante la máscara de subred o la longitud de prefijo y la operación AND. También debe tomar nota de los diferentes tipos de direcciones de red dentro de una red.

Dirección de red

La dirección y la máscara de subred hacen referencia a una red. Todos los hosts dentro de la red comparten la misma dirección de red. La porción de host se compone solo de ceros.

Direcciones de Host

Direcciones IP únicas asignadas a los hosts y a los dispositivos. La porción de host siempre contiene ceros y unos combinados, pero nunca ceros o unos solamente.

Primera dirección de host

Primera dirección IP de host disponible en la red. La porción de host siempre se compone de todos ceros, excepto el último número, que es un uno.

Última dirección de host

Última dirección IP de host disponible en la red. La porción de host siempre se compone de todos números uno, excepto el último, que es un cero.

Dirección de difusión

Una dirección especial que se comunica con todos los hosts en una red, por ejemplo, cuando un host envía un paquete a la dirección IPv4 de difusión de la red, y todos los demás hosts de la red reciben el paquete. La dirección de difusión utiliza la dirección más alta en el rango de la red. La porción de host se compone solo de unos.

Dirección de red

La porción de host se compone solo de ceros (.00000000)

Direcciones de Host

La porción de host contiene ceros y unos (.00000001 a .11111110)

Primera dirección de host

La porción de host se compone de todos ceros, excepto el último número, que es un uno (.00000001)

Última dirección de host

La porción de host se compone de todos números uno, excepto el último, que es un cero (.11111110)

Dirección de difusión

La porción de host se compone solo de unos (.11111111)

Direcciones IPv4 de unidifusión, difusión y multidifusión.

Asignación de una dirección IPv4 dinámica a un host.

En la mayoría de las redes de datos, la mayor parte de los hosts incluyen PC, tabletas PC, teléfono inteligentes, impresoras y teléfonos IP. También suele ocurrir que la población de usuarios y los dispositivos cambian con frecuencia. No sería práctico comenzar a asignar direcciones IPv4 de manera estática a cada dispositivo. Por lo tanto, a estos dispositivos se les asignan direcciones IPv4 de manera dinámica con el protocolo DHCP.

Como se muestra en la ilustración, un host puede obtener la información de asignación de direcciones IPv4 de forma automática. El host es un cliente DHCP y solicita la información de dirección IPv4 de un servidor DHCP. El servidor DHCP proporciona una dirección IPv4, una máscara de subred, un gateway predeterminado y otra información de configuración.

En general, el protocolo DHCP es el método preferido para asignar direcciones IPv4 a los hosts en redes grandes. Un beneficio adicional de DHCP es que la dirección no se asigna permanentemente a un host, sino que solo se "presta" por un período. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta característica es muy útil para los usuarios móviles que entran a una red y salen de ella.

Asignación de una dirección IPv4 estática a un host.

Se pueden asignar direcciones IP a los dispositivos de manera estática o dinámica.

En las redes, algunos dispositivos necesitan una dirección IP fija. Por ejemplo, las impresoras, los servidores y los dispositivos de red necesitan una dirección IP que no cambie. Por este motivo, generalmente, se asigna a estos dispositivos una dirección IP estática.

Un host también se puede configurar con una dirección IPv4 estática como la que se muestra en la ilustración. En redes pequeñas, es aceptable asignar direcciones IP estáticas a los hosts. Sin embargo, en una red grande, introducir una dirección estática en cada host llevaría mucho tiempo. Es importante mantener una lista precisa de las direcciones IP estáticas asignadas a cada dispositivo.

Comunicación IPv4.

Un host conectado correctamente a una red puede comunicarse con otros dispositivos de alguna de estas tres maneras:

- **Unidifusión:** es el proceso de enviar un paquete de un host a otro host individual, como se muestra en la figura 1.
- **Difusión:** es el proceso de enviar un paquete de un host a todos los hosts de la red, como se muestra en la figura 2.
- **Multidifusión:** es el proceso de enviar un paquete de un host a un grupo seleccionado de hosts, probablemente en diferentes redes, como se muestra en la figura 3.

Estos tres tipos de comunicación se utilizan con distintos 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.

Transmisión de unidifusión.

La comunicación de unidifusión se usa para la comunicación normal de host a host, tanto en redes cliente/servidor como en redes punto a punto. Los paquetes de unidifusión usan la dirección del dispositivo de destino como la dirección de destino y pueden enrutarse en una interconexión de redes.

En una red IPv4, la dirección de unidifusión aplicada a un terminal se denomina "dirección de host". En la comunicación de unidifusión, las direcciones asignadas a los dos terminales se usan como las direcciones IPv4 de origen y de destino. Durante el proceso de encapsulamiento, el host de origen usa su dirección IPv4 como dirección de origen y la dirección IPv4 del host de destino como dirección de destino. Sin importar si en el destino se especificó un paquete como unidifusión, difusión o multidifusión, la dirección de origen de cualquier paquete siempre es la dirección de unidifusión del host de origen.

Nota: en este curso, todas las comunicaciones entre dispositivos es de unidifusión, a menos que se indique lo contrario.

Las direcciones de host IPv4 de unidifusión se encuentran en el intervalo de direcciones de 0.0.0.0 a 223.255.255.255. Sin embargo, dentro de este intervalo existen muchas direcciones reservadas para fines específicos. Estas direcciones con fines específicos se analizan más adelante en este capítulo.

Transmisión de difusión.

El tráfico de difusión se utiliza para enviar paquetes a todos los hosts en la red con la dirección de difusión para la red. En una difusión, el paquete contiene una dirección IPv4 de destino con todos los números uno (1) en la porción de host. Esto significa que todos los hosts de esa red local (dominio de difusión) reciben y ven el paquete. En gran parte de la tecnología impulsada por la red, como DHCP, se utilizan transmisiones por difusión. Cuando un host recibe un paquete enviado a la dirección de difusión de la red, el host procesa el paquete de la misma manera en la que procesaría un paquete dirigido a su dirección de unidifusión.

La difusión puede ser dirigida o limitada. Una difusión dirigida se envía a todos los hosts de una red específica. Por ejemplo, un host de la red 172.16.4.0/24 envía un paquete a la dirección 172.16.4.255. Se envía una difusión limitada a 255.255.255.255. De manera predeterminada, los routers no reenvían transmisiones por difusión.

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

Cuando se transmite un paquete por difusión, utiliza recursos de la red y hace que cada host receptor de la red procese el paquete. Por lo tanto, se debe limitar el tráfico de difusión para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan los dominios de difusión, la subdivisión de redes puede mejorar el rendimiento de la red al eliminar el exceso de tráfico de difusión.

Transmisión de multidifusión.

La transmisión de multidifusión reduce el tráfico al permitir que un host envíe un único paquete a un grupo seleccionado de hosts que estén suscritos a un grupo de multidifusión.

IPv4 reservó las direcciones de 224.0.0.0 a 239.255.255.255 como rango de multidifusión. Las direcciones IPv4 de multidifusión de 224.0.0.0 a 224.0.0.255 están reservadas para la multidifusión solo en la red local. Estas direcciones se utilizan con grupos de multidifusión en una red local. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo de multidifusión de una red local y no los sigue reenviando. Un uso típico de una dirección de multidifusión de una red local reservada son los Routing Protocols que usan la transmisión de multidifusión para intercambiar información de routing. Por ejemplo, 224.0.0.9 es la dirección de multidifusión que usa el protocolo de información de routing (RIP) versión 2 para comunicarse con otros routers RIPv2.

Los hosts que reciben datos de multidifusión específicos se denominan “clientes de multidifusión”. Los clientes de multidifusión utilizan servicios solicitados por un programa cliente para subscribirse al grupo de multidifusión.

Cada grupo de multidifusión está representado por una sola dirección IPv4 de destino de multidifusión. Cuando un host IPv4 se suscribe a un grupo de multidifusión, el host procesa los paquetes dirigidos a esta dirección de multidifusión y los paquetes dirigidos a la dirección de unidifusión asignada exclusivamente.

Direcciones IPv4 públicas y privadas

Las direcciones IPv4 públicas son direcciones que se enrutan globalmente entre los routers de los ISP (proveedores de servicios de Internet). Sin embargo, no todas las direcciones IPv4 disponibles pueden usarse en Internet. Existen bloques de direcciones denominadas *direcciones privadas* que la mayoría de las organizaciones usan para asignar direcciones IPv4 a los hosts internos.

A mediados de la década de 1990, se presentaron las direcciones IPv4 privadas debido a la reducción del espacio de direcciones IPv4. Las direcciones IPv4 privadas no son exclusivas y pueden usarse en una red interna.

Específicamente, los bloques de direcciones privadas son los siguientes:

- **10.0.0.0 /8** o **10.0.0.0** a **10.255.255.255**
- **172.16.0.0 /12** o **172.16.0.0 a 172.31.255.255**
- **192.168.0.0 /16** o **192.168.0.0 a 192.168.255.255**

Es importante saber que las direcciones dentro de estos bloques de direcciones no están permitidas en Internet y deben ser filtradas (descartadas) por los routers de Internet. Por ejemplo, en la ilustración, los usuarios de las redes 1, 2 o 3 envían paquetes a destinos remotos. Los routers del proveedor de servicios de Internet (ISP) detectan que las direcciones IPv4 de origen de los paquetes son de direcciones privadas y, por lo tanto, descartan los paquetes.

Nota: las direcciones privadas se definen en RFC 1918.

La mayoría de las organizaciones usan direcciones IPv4 privadas para los hosts internos. Sin embargo, estas direcciones RFC 1918 no se pueden enrutar en Internet y deben traducirse a direcciones IPv4 públicas. Se usa la traducción de direcciones de red (NAT) para traducir entre direcciones IPv4 privadas y públicas. En general, esto se hace en el router que conecta la red interna a la red del ISP.

Los routers domésticos brindan la misma funcionalidad. Por ejemplo, la mayoría de los routers domésticos asignan direcciones IPv4 a sus hosts cableados e inalámbricos desde la dirección privada 192.168.1.0 /24. A la interfaz de router doméstico que se conecta a la red del proveedor de servicios de Internet (ISP) se le asigna una dirección IPv4 pública para usar en Internet.

Direcciones IPv4 de uso especial

Existen determinadas direcciones que no pueden asignarse a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar 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.

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 al host local. Las direcciones dentro de este bloque no deben figurar en ninguna red.

Direcciones link-local

Las direcciones IPv4 del bloque de direcciones que va de 169.254.0.0 a 169.254.255.255 (169.254.0.0/16) se designan 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 pueden utilizar en una red punto a punto pequeña o para un host que no pudo obtener una dirección de un servidor de DHCP automáticamente.

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 tiempo de vida (TLL) 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

El bloque de direcciones que va de 192.0.2.0 a 192.0.2.255 (192.0.2.0/24) se reserva 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.

Direcciones experimentales

Las direcciones del bloque que va de 240.0.0.0 a 255.255.255.254 se indican como reservadas para uso futuro (RFC 3330). En la actualidad, estas direcciones solo se pueden utilizar para fines de investigación o experimentación, y no se pueden utilizar en una red IPv4. Sin embargo, según RFC 3330, podrían, técnicamente, convertirse en direcciones utilizables en el futuro.

Direccionamiento con clase antigua

Históricamente, RFC1700, Assigned Numbers (Números asignados), agrupaba rangos 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 y bloques de direcciones específicos para estas redes.

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. Todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que había solo 128 redes de clase A posibles, 0.0.0.0/8 a 127.0.0.0/8.

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 admitir las necesidades de redes de tamaño moderado a grande con hasta aproximadamente 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. Esto 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 ligeramente más eficaz que la clase A, debido a que dividía equitativamente el 25% del total del espacio total de direcciones IPv4 entre alrededor de 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 dirección utilizando un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringía el bloque de direcciones para la clase C a 192.0.0.0/24 hasta 223.255.255.0/24. A pesar de que ocupaba solo el 12,5% del total del espacio de direcciones IPv4, podía proporcionar direcciones a dos millones de redes.

En la figura 1, se ilustra cómo se dividen estas clases de direcciones.

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, cuando asigna una dirección IPv4 a una PC, el sistema operativo examina la dirección que se asigna, a fin de determinar si esta dirección es una dirección de clase A, de clase B o de clase C.

A continuación, el sistema operativo supone el prefijo utilizado por esa clase y lleva a cabo la asignación de la máscara de subred predeterminada.

Direccionamiento sin clase

El sistema que se utiliza en la actualidad se denomina “direccionamiento sin clase”. El nombre formal es “enrutamiento entre dominios sin clase” (CIDR, pronunciado “cider”). La asignación con clase de direcciones IPv4 era muy ineficaz, y permitía solo las duraciones de prefijo /8, /16 o /24, cada una de un espacio de dirección distinto. En 1993, el IETF creó un nuevo conjunto de estándares que permitía que los proveedores de servicios asignaran direcciones IPv4 en cualquier límite de bits de dirección (duración de prefijo) en lugar de solo con una dirección de clase A, B o C.

El IETF sabía que el CIDR era solo una solución temporal y que sería necesario desarrollar un nuevo protocolo IP para admitir el rápido crecimiento de la cantidad de usuarios de Internet. En 1994, el IETF comenzó a trabajar para encontrar un sucesor de IPv4, que finalmente fue IPv6.

Direccionamiento sin clase

El sistema que se utiliza en la actualidad se denomina “direccionamiento sin clase”. El nombre formal es “enrutamiento entre dominios sin clase” (CIDR, pronunciado “cider”). La asignación con clase de direcciones IPv4 era muy ineficaz, y permitía solo las duraciones de prefijo /8, /16 o /24, cada una de un espacio de dirección distinto. En 1993, el IETF creó un nuevo conjunto de estándares que permitía que los proveedores de servicios asignaran direcciones IPv4 en cualquier límite de bits de dirección (duración de prefijo) en lugar de solo con una dirección de clase A, B o C.

El IETF sabía que el CIDR era solo una solución temporal y que sería necesario desarrollar un nuevo protocolo IP para admitir el rápido crecimiento de la cantidad de usuarios de Internet. En 1994, el IETF comenzó a trabajar para encontrar un sucesor de IPv4, que finalmente fue IPv6.

Asignación de direcciones IP

Para que una compañía u organización tenga hosts de red, como servidores Web, a los que se pueda acceder desde Internet, dicha organización debe tener un bloque de direcciones públicas asignado. Se debe tener en cuenta que las direcciones públicas deben ser únicas, y el uso de estas direcciones públicas se regula y se asigna a cada organización de forma independiente. Esto es válido para las direcciones IPv4 e IPv6.

IANA y RIR

La Internet Assigned Numbers Authority (IANA) (http://www.iana.org) administra la asignación de direcciones IPv4 e IPv6. 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.

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

Proveedores de servicios de Internet (ISP)

Los RIR se encargan de asignar direcciones IP a los proveedores de servicios de Internet (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.

Las direcciones IPv6 se pueden obtener del ISP o, en algunos casos, directamente del RIR. Las direcciones IPv6 y los tamaños típicos de los bloques de direcciones se analizarán más adelante.

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 ofrecer servicios relacionados. Entre los demás servicios que los ISP suelen proporcionar a sus clientes se encuentran los servicios DNS, los 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 las ilustraciones.

Nivel 1

Como se muestra en la figura 1, en la cima de la jerarquía de ISP se encuentran los ISP de nivel 1.
Estos 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

Como se muestra en la figura 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

Como se muestra en la figura 3, los ISP de nivel 3 adquieren 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.