El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts, independientemente de si los hosts se encuentran en la misma red o en redes diferentes. Tanto el protocolo de Internet versión 4 (IPv4) como el protocolo de Internet versión 6 (IPv6) proporcionan direccionamiento jerárquico para los paquetes que transportan datos.

El diseño, la implementación y la administración de un plan de direccionamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente.

En este capítulo, se examina detalladamente la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP.

Para comprender el funcionamiento de los dispositivos en una red, debemos observar las direcciones y otros datos de la misma manera en que lo hacen los dispositivos: en notación binaria. La notación binaria es una representación de la información mediante unos y ceros solamente. Las PC se comunican mediante datos binarios. Los datos binarios se pueden utilizar para representar muchas formas distintas de datos. Por ejemplo, al pulsar letras en un teclado, esas letras aparecen en la pantalla de una manera que el usuario puede leer y comprender. Sin embargo, la PC traduce cada letra a una serie de dígitos binarios para su almacenamiento y transporte. Para traducir esas letras, la PC utiliza el Código Estadounidense Estándar para el Intercambio de Información (ASCII).

Mediante ASCII, la letra “A” se representa en forma de bit como “01000001”, mientras que la “a” minúscula se representa en forma de bit como “01100001”. Utilice el traductor de ASCII en la figura 1 para convertir los caracteres ASCII al sistema binario.

Si bien, por lo general, las personas no deben preocuparse por la conversión binaria de letras, es necesario comprender el uso del sistema binario para el direccionamiento IP. Cada dispositivo en una red se debe identificar de forma exclusiva mediante una dirección binaria. En redes IPv4, esta dirección se representa mediante una cadena de 32 bits (unos y ceros). A continuación, en la capa de red, los paquetes incluyen esta información de identificación única para los sistemas de origen y de destino. Por lo tanto, en una red IPv4, cada paquete incluye una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de capa 3.

Para la mayoría de las personas, una cadena de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por este motivo, representamos las direcciones IPv4 mediante el formato decimal punteado en lugar del binario. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255. Para entender cómo funciona esto, es necesario tener aptitudes para la conversión de sistema binario a decimal.

**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. En un sistema de notación de posición, la base numérica se denomina “raíz”. En el sistema de base 10, la raíz es 10. En el sistema binario, se utiliza una raíz de 2. Los términos “raíz” y “base” se pueden utilizar de manera indistinta. 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 ejemplo ayudarán a aclarar cómo funciona este sistema.

Para el número decimal 192, el valor que el 1 representa es 1\*10^2 (1 multiplicado por 10 elevado a la segunda potencia). El 1 se encuentra en lo que comúnmente llamamos la posición "100". La notación de posición se refiere a esta posición como posición base^2 porque la base o raíz es 10 y la potencia es 2. El 9 representa 9\*10^1 (9 multiplicado por 10 elevado a la primera potencia). En la figura 2, se muestra la notación de posición para el número decimal 192.

Usando la notación de posición en el sistema de numeración con base 10, 192 representa:

192 = (1 \* 10^2) + (9 \* 10^1) + (2 \* 10^0)

o

192 = (1 \* 100) + (9 \* 10) + (2 \* 1)

En IPv4, las direcciones son números binarios de 32 bits. Sin embargo, para facilitar el uso por parte de las personas, los patrones binarios que representan direcciones IPv4 se expresan en formato decimal punteado. Esto primero se logra separando cada byte (8 bits) del patrón binario de 32 bits, llamado “octeto”, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

La dirección binaria:

11000000 10101000 00001010 00001010

se expresa como decimal punteada de la siguiente manera:

192.168.10.10

En la figura 1, seleccione cada botón para ver cómo se representa la dirección binaria de 32 bits en octetos decimales punteados.

¿Pero de qué forma se determinan los equivalentes decimales reales?

**Sistema de numeración binaria**

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa aumentos en potencias 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 solo tiene 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.

En la figura 2, se ilustra la representación del número decimal 192 en sistema binario. Un 1 en una determinada posición significa que se agrega ese valor al total. Un 0 significa que no se agrega ese valor. El número binario 11000000 tiene un 1 en la posición 2^7 (valor decimal 128) y un 1 en la posición 2^6 (valor decimal 64). Los bits restantes son todos 0, de modo que no se agregan los valores decimales correspondientes. El resultado de agregar 128 + 64 es 192, el equivalente decimal de 11000000.

A continuación, se proporcionan dos ejemplos más:

**Ejemplo 1: un octeto compuesto solo por unos, 11111111**

Un 1 en cada posición significa que sumamos el valor para esa posición al total. Todos 1 significa que se incluyen los valores de cada posición en el total; por lo tanto, el valor de todos 1 en un octeto es 255.

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

**Ejemplo 2: un octeto compuesto solo por ceros, 00000000**

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

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

Una combinación distinta de unos y ceros arroja un valor decimal diferente.

Cada octeto está compuesto por 8 bits y cada bit tiene un valor, 0 o 1. Los cuatro grupos de 8 bits tienen el mismo conjunto de valores válidos en el rango de 0 a 255 inclusive. El valor de cada ubicación de bits, de derecha a izquierda, es 1, 2, 4, 8, 16, 32, 64 y 128.

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

* Si en esa posición hay un 0, no sume el valor.
* Si los 8 bits son 0, 00000000, el valor del octeto es 0.
* Si los 8 bits son 1, 11111111, el valor del octeto es 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1).
* Si los 8 bits están combinados, los valores se agregan juntos. Por ejemplo, el octeto 00100111 tiene un valor de 39 (32 + 4 + 2 + 1).

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

Utilizando la dirección IPv4 de 32 bits 11000000101010000000101000001010, convierta la representación binaria en decimal punteada mediante los siguientes pasos:

**Paso 1.** Divida los 32 bits en 4 octetos.

**Paso 2.** Convierta cada octeto a decimal.

**Paso 3.** Agregue un "punto" entre cada decimal.

Haga clic en Reproducir en la ilustración para ver cómo se convierte una dirección binaria en decimal punteada.

Además de poder convertir de sistema binario a decimal, también es necesario comprender cómo convertir de decimal a binario.

Dado que representamos las direcciones IPv4 mediante el formato decimal punteado, solo es necesario analizar el proceso de conversión de valores binarios de 8 bits a valores decimales de 0 a 255 para cada octeto en una dirección IPv4.

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 número de octeto es igual o superior a 128. Si el número de octeto es inferior a 128, se coloca un 0 en la posición de bit para el valor decimal 128 y se avanza a la posición de bit para el valor decimal 64.

Si el número de octeto en la posición de bit para el valor decimal 128 es mayor o igual que 128, se coloca un 1 en la posición de bit para el valor decimal 128 y se resta 128 del número de octeto que se está convirtiendo. A continuación, comparamos el resto de esta operación con el siguiente valor más pequeño, 64. Continuamos este proceso para todas las posiciones de bits restantes.

Haga clic en las figuras 1 a 6 para ver el proceso de conversión de 168 al equivalente binario de 10101000.

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Recuerde que una dirección IP es una dirección jerárquica que consta de dos partes: una porción de red y una porción de host. Pero al determinar la porción de red en comparación con la porción de host, es necesario analizar el stream de 32 bits, y no el valor decimal. Dentro del stream de 32 bits, una parte de los bits constituye la red y una porción de los bits constituye el host.

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. Independientemente de si los números decimales entre dos direcciones IPv4 coinciden, si dos hosts tienen el mismo patrón de bits en la porción de red especificada del stream de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits es red y qué porción es host? Esa tarea le corresponde a la máscara de subred.

Cuando se configura un host IP, se asigna una máscara de subred junto con una dirección IP. Como sucede con la dirección IP, la máscara de subred tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host.

La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host. Como se muestra en la figura 1, la máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa 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.

Como sucede con las direcciones IPv4, la máscara de subred se representa en formato decimal punteado por cuestiones de facilidad de uso. La máscara de subred se configura en un dispositivo host, junto con la dirección IPv4, y es necesaria para que el host pueda determinar a qué red pertenece. En la figura 2, se muestran las máscaras de subred válidas para un octeto IPv4.

**Prefijos de red**

La duración de prefijo es otra forma de expresar la máscara de subred. La duración de prefijo es la cantidad de bits establecidos en 1 en la máscara de subred. Se escribe en “notación con barras”, una “/” seguida de la cantidad de bits establecidos en 1. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits establecidos en 1 en la versión binaria de la máscara de subred, de modo que la duración de prefijo es 24 bits o /24. El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

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.

En las ilustraciones, se muestran distintos prefijos que utilizan la misma dirección 10.1.1.0. En la figura 1, se ilustran los prefijos /24 a /26. En la figura 2, se ilustran los prefijos /27 a /28.

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 las ilustraciones, puede ver que la cantidad de hosts que se pueden direccionar en la red también cambia.

Hay tres tipos de direcciones dentro del rango de direcciones de cada red IPv4:

* Dirección de red
* Dirección de host
* Dirección de broadcast

**Dirección de red**

La dirección de red es una manera estándar de hacer referencia a una red. Al referirse a la dirección de red, también es posible utilizar la máscara de subred o la duración de prefijo. Por ejemplo, la red que se muestra en la figura 1 podría indicarse como la red 10.1.1.0, la red 10.1.1.0 255.255.255.0 o la red 10.1.1.0/24. Todos los hosts en la red 10.1.1.0/24 tendrán los mismos bits de porción de red.

Como se muestra en la figura 2, dentro del rango de direcciones IPv4 de una red, la primera dirección 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. Todos los hosts dentro de la red comparten la misma dirección de red.

**Dirección de host**

Cada dispositivo final requiere una dirección única para comunicarse en la red. En direcciones IPv4, los valores entre la dirección de red y la dirección de broadcast se pueden asignar a los dispositivos finales en una red. Como se muestra en la figura 3, esta dirección tiene cualquier combinación de bits 0 y bits 1 en la porción de host de la dirección, pero no puede contener todos bits 0 o todos bits 1.

**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 en una red a la vez, un host puede enviar un único paquete dirigido a la dirección de broadcast de la red, y cada host en la red que recibe este paquete procesa su contenido.

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. Todos 1 en un octeto en forma binaria es igual al número 255 en forma decimal. Por lo tanto, como se muestra en la figura 4, para la red 10.1.1.0/24, en la cual se utiliza el último octeto para la porción de host, la dirección de broadcast sería 10.1.1.255. Observe que la porción de host no siempre es un octeto entero. A esta dirección se la conoce como broadcast dirigido.

Para asegurarse de que a todos los hosts en una red se les asigne una dirección IP única dentro de ese rango de red, es importante identificar la primera y la última dirección de host. Se pueden asignar direcciones IP dentro de este rango a los hosts dentro de una red.

**Primera dirección de host**

Como se observa en la figura 1, la porción de host de la primera dirección de host contiene todos bits 0 con un bit 1 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre un número mayor que la dirección de red. En este ejemplo, la primera dirección de host en la red 10.1.1.0/24 es 10.1.1.1. En muchos esquemas de direccionamiento, es común utilizar la primera dirección de host del router o la dirección de gateway predeterminado.

**Última dirección de host**

La porción de host de la última dirección de host contiene todos bits 1, con un bit 0 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre una menos que la dirección de broadcast. Como se observa en la figura 2, la última dirección de host en la red 10.1.1.0/24 es 10.1.1.254.

Cuando se asigna una dirección IPv4 a un dispositivo, ese dispositivo utiliza la máscara de subred para determinar a qué dirección de red pertenece. La dirección de red es la dirección que representa todos los dispositivos en la misma red.

Al enviar datos de red, el dispositivo utiliza esta información para determinar si puede enviar paquetes localmente o si debe enviarlos a un gateway predeterminado para la entrega remota. Cuando un host envía un paquete, compara la porción de red de su propia dirección IP con la porción de red de la dirección IP de destino, sobre la base de las máscaras de subred. Si los bits de la red coinciden, tanto el host de origen como el de destino se encuentran en la misma red, y el paquete puede ser enviado localmente. Si no coinciden, el host emisor reenvía el paquete al gateway predeterminado para que se envíe a otra red.

**La operación AND**

AND es una de las tres operaciones binarias básicas que se utilizan en la lógica digital. Las otras dos son OR y NOT. Mientras que las tres se usan en redes de datos, AND se usa para determinar la dirección de red. Por lo tanto, sólo se tratará aquí la lógica AND. La lógica AND es la comparación de dos bits que produce los siguientes resultados:

1 AND 1 = 1 (figura 1)

0 AND 1 = 0 (figura 2)

0 AND 0 = 0 (figura 3)

1 AND 0 = 0 (figura 4)

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

Si se aplica la lógica AND a cualquier bit de la dirección con valor de bit de 1 de la máscara de subred, da como resultado el valor de bit original de la dirección. Entonces, un 0 (de la dirección IPv4) AND 1 (de la máscara de subred) es 0. Un 1 (de la dirección IPv4) AND 1 (de la máscara de subred) es 1. Por lo tanto, el resultado de la aplicación de AND con un 0 en cualquier caso es 0. Estas propiedades de la operación AND se utilizan con la máscara de subred para “enmascarar” los bits de host de una dirección IPv4. Se aplica la lógica AND a cada bit de la dirección con el bit de máscara de subred correspondiente.

Debido a que todos los bits de la máscara de subred que representan bits de host son 0, la porción de host de la dirección de red resultante está formada por todos 0. Recuerde que una dirección IPv4 con todos 0 en la porción de host representa la dirección de red.

Asimismo, todos los bits de la máscara de subred que indican la porción de red son 1. Cuando se aplica la lógica AND a cada uno de estos 1 con el bit correspondiente de la dirección, los bits resultantes son idénticos a los bits de la dirección original.

Como se muestra en la ilustración, los bits 1 en la máscara de subred hacen que la porción de red de la dirección de red tenga los mismos bits que la porción de red del host. La porción de host de la dirección de red da como resultado todos 0.

En una dirección IP dada y su subred, se puede utilizar la operación AND para determinar a qué subred pertenece la dirección, así como qué otras direcciones pertenecen a la misma subred. Se debe tener en cuenta que si dos direcciones están en la misma red o subred, se considera que son locales una respecto de la otra y, por consiguiente, pueden comunicarse directamente entre sí. Las direcciones que no se encuentran en la misma red o subred se consideran remotas respecto de sí y, por lo tanto, deben tener un dispositivo de capa 3 (como un router o un switch de capa 3) entre ellas para comunicarse.

En la verificación o resolución de problemas de red, con frecuencia es necesario determinar si dos hosts se encuentran en la misma red local. Es necesario tomar esta determinación desde el punto de vista de los dispositivos de red. Debido a una configuración incorrecta, un host puede encontrarse en una red que no era la planificada. Esto puede hacer que el funcionamiento parezca irregular, a menos que se realice el diagnóstico mediante el análisis de los procesos de aplicación de AND utilizados por el host.

**Direcciones para dispositivos de usuario**

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales, como PC, tablet PC, smartphones, impresoras y teléfonos IP. Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts. A estos hosts se les asignan direcciones IP del rango de direcciones disponibles en la red. Estas direcciones IP pueden asignarse de manera estática o dinámica.

**Asignación estática**

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host. En la figura 1, se muestra la ventana de las propiedades del adaptador de red. Para configurar una dirección IPv4 estática, elija IPv4 en la pantalla del adaptador de red y, a continuación, introduzca la dirección estática, la máscara de subred y el gateway predeterminado. En la figura 2, se muestra la configuración estática mínima: la dirección IP, la máscara de subred y el gateway predeterminado del host.

El direccionamiento estático tiene varias ventajas. Por ejemplo, es útil para impresoras, servidores y otros dispositivos de red que no suelen cambiar la ubicación y que deben ser accesibles para los clientes en la red sobre la base de una dirección IP fija. 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. Por ejemplo, es posible crear filtros de acceso sobre la base del tráfico desde y hacia una dirección IP específica. Sin embargo, introducir el direccionamiento estático en cada host puede llevar mucho tiempo.

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.

**Asignación dinámica**

En las redes locales, es habitual que la población de usuarios cambie frecuentemente. Se agregan nuevos usuarios con computadoras portátiles, y esos usuarios requieren una conexión. Otros tienen estaciones de trabajo nuevas u otros dispositivos de red, como smartphones, que deben conectarse. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más simple que las direcciones IP se asignen automáticamente. Esto se realiza mediante un protocolo conocido como Protocolo de configuración dinámica de host (DHCP), como se muestra en la figura 1.

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 de DHCP requiere que se utilice un bloque de direcciones, denominado “conjunto de direcciones”, para la asignación a los clientes DHCP en una red. Las direcciones asignadas a este conjunto deben planificarse de modo que excluyan cualquier dirección estática que utilicen otros dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IPv4 a los hosts de grandes redes, dado que reduce la carga para al 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.

Si se habilita DHCP en un dispositivo host, se puede utilizar el comando **ipconfig** para ver la información de la dirección IP que asigna el servidor de DHCP, como se muestra en la figura 2.

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

* **Unicast:** proceso por el cual se envía un paquete de un host a un host individual.
* **Broadcast:** proceso por el cual se envía un paquete de un host a todos los hosts en la red.
* **Multicast:** proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts, posiblemente en redes distintas.

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.

**Tráfico unicast**

La comunicación unicast se usa para la comunicación normal de host a host, tanto en redes cliente/servidor como en redes punto a punto. Los paquetes unicast utilizan las direcciones del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork.

Reproduzca la animación para ver un ejemplo de transmisión unicast.

En una red IPv4, la dirección unicast aplicada a un dispositivo final se denomina “dirección de host”. En la comunicación unicast, las direcciones asignadas a dos dispositivos finales se usan como las 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 de origen y la dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino. Independientemente de si el destino especificado para un paquete es unicast, broadcast o multicast, la dirección de origen de cualquier paquete es siempre la dirección unicast del host de origen.

**Nota:** en este curso, todas las comunicaciones entre dispositivos son comunicaciones unicast, a menos que se indique lo contrario.

Las direcciones de host IPv4 son direcciones unicast y se encuentran en el rango de direcciones de 0.0.0.0 a 223.255.255.255. Sin embargo, dentro de este rango existen muchas direcciones reservadas para fines específicos. Estas direcciones con fines específicos se analizarán más adelante en este capítulo.

**Transmisión de broadcast**

El tráfico de broadcast se utiliza para enviar paquetes a todos los hosts en la red usando la dirección de broadcast para la red. Para broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esto significa que todos los hosts de esa red local (dominio de broadcast) recibirán y verán el paquete. Muchos protocolos de red, como DHCP, utilizan broadcasts. Cuando un host recibe un paquete enviado a la dirección de broadcast de red, el host procesa el paquete de la misma manera en la que procesaría un paquete dirigido a su dirección unicast.

Algunos ejemplos para utilizar una transmisión de broadcast son:

* Asignar direcciones de capa superior a direcciones de capa inferior
* Solicitar una dirección
* 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 del gateway 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 local. Por ejemplo, para que un host fuera de la red 172.16.4.0/24 se comunique con todos los hosts dentro de esa red, la dirección de destino del paquete sería 172.16.4.255. 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 siempre utilizan la dirección IPv4 de destino 255.255.255.255. Los routers no reenvían broadcasts limitados. 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.

Reproduzca la animación para ver un ejemplo de transmisión de broadcast limitado.

Cuando se transmite un paquete, utiliza recursos en la red y hace que cada host receptor en la red procese 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 las redes IPv4. Reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts que forman parte de un grupo multicast suscrito. 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. La responsabilidad de la internetwork es reproducir los flujos multicast en un modo eficaz para que alcancen solamente a los destinatarios.

Algunos ejemplos de transmisión de multicast son:

* Transmisiones de video y de audio
* Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
* Distribución de software
* Juegos remotos

**Direcciones multicast**

IPv4 tiene un bloque de direcciones reservadas para direccionar grupos multicast. Este rango de direcciones va de 224.0.0.0 a 239.255.255.255. El rango de direcciones multicast está subdividido en distintos 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. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo multicast de enlace local y nunca los reenvía nuevamente. Un uso común de las direcciones de 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, se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

**Clientes multicast**

Los hosts que reciben datos multicast específicos se denominan “clientes multicast”. Los clientes multicast utilizan servicios solicitados 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 asignada exclusivamente.

La animación muestra clientes que aceptan paquetes multicast.

Aunque la mayoría de las direcciones IPv4 de host 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:

10.0.0.0 a 10.255.255.255 (10.0.0.0/8)

172.16.0.0 a 172.31.255.255 (172.16.0.0/12)

192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Las direcciones privadas se definen en RFC 1918, Asignación de direcciones para redes de Internet privadas, y en ocasiones se hace referencia a ellas como direcciones RFC 1918. Los bloques de direcciones de espacio privado, como se muestra en la ilustración, se utilizan en redes privadas. Los hosts que no requieren acceso a Internet pueden utilizar direcciones privadas. Sin embargo, dentro de la red privada, los hosts aún requieren direcciones IP únicas dentro del espacio privado.

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.

En RFC 6598, IANA reservó otro grupo de direcciones conocidas como “espacio de dirección compartido”. Como sucede con el espacio de dirección privado definido en RFC 1918, las direcciones del espacio de dirección compartido no son enrutables globalmente. Sin embargo, el propósito de estas direcciones es solamente ser utilizadas en redes de proveedores de servicios. El bloque de direcciones compartido es 100.64.0.0/10.

**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. Aun dentro de estos bloques de direcciones IPv4, existen muchas direcciones designadas para otros fines específicos.

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.

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.

En la figura 2, se muestran los rangos de direcciones con clase.

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](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](http://www.afrinic.net/)
* APNIC (Asia Pacific Network Information Centre), región Asia/Pacífico [http://www.apnic.net](http://www.apnic.net/)
* ARIN (American Registry for Internet Numbers), región América del Norte [http://www.arin.net](http://www.arin.net/)
* LACNIC (Regional Latin-American and Caribbean IP Address Registry), América Latina y algunas islas del Caribe [http://www.lacnic.net](http://www.lacnic.net/)
* RIPE NCC (Reseaux IP Europeans), Europa, Medio Oriente y Asia Central [http://www.ripe.net](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 en este capítulo.

**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.

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un mayor espacio de direcciones de 128 bits, lo que proporciona 340 sextillones de direcciones. (Eso es el número 340 seguido de 36 ceros). Sin embargo, IPv6 es mucho más que una mera dirección más extensa. Cuando el IETF comenzó el desarrollo de una sucesora de IPv4, utilizó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras adicionales. Un ejemplo es el protocolo de mensajes de control de Internet versión 6 (ICPMv6), que incluye la resolución de direcciones y la configuración automática de direcciones, las cuales no se encuentran en ICMP para IPv4 (ICMPv4). ICMPv4 e ICMPv6 se analizarán más adelante en este capítulo.

**Necesidad de utilizar IPv6**

El agotamiento del espacio de direcciones IPv4 fue el factor que motivó la migración a IPv6. Debido al aumento de la conexión a Internet en África, Asia y otras áreas del mundo, las direcciones IPv4 ya no son suficientes para admitir este crecimiento. El lunes 31 de enero de 2011, la IANA asignó los últimos dos bloques de direcciones IPv4 /8 a los registros regionales de Internet (RIR). Diversas proyecciones indican que entre 2015 y 2020 se habrán acabado las direcciones IPv4 en los cinco RIR. En ese momento, las direcciones IPv4 restantes se habrán asignado a los ISP.

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas definidas en RFC 1918 junto con la traducción de direcciones de red (NAT) fueron un factor determinante para retardar el agotamiento del espacio de direcciones IPv4. La NAT tiene limitaciones que obstaculizan gravemente las comunicaciones punto a punto.

**Internet de las cosas**

En la actualidad, Internet es significativamente distinta de como era en las últimas décadas. Hoy en día, Internet es más que correo electrónico, páginas Web y transferencia de archivos entre PC. Internet evoluciona y se está convirtiendo en una Internet de las cosas. Los dispositivos que acceden a Internet ya no serán solamente PC, tablet PC y smartphones. Los dispositivos del futuro preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales. Imagine una reunión en la ubicación de un cliente que se programa en forma automática en la aplicación de calendario para que comience una hora antes de la hora en que normalmente comienza a trabajar. Esto podría ser un problema importante, en especial si olvida revisar el calendario o ajustar el despertador según corresponda. Ahora imagine que la aplicación de calendario comunica esta información directamente al despertador para usted y su automóvil. El automóvil calienta automáticamente para derretir el hielo del limpiaparabrisas antes de que usted ingrese y cambia la ruta hacia el lugar de la reunión.

Con una creciente población de Internet, un espacio limitado de direcciones IPv4, problemas con la NAT y con Internet de las cosas, llegó el momento de iniciar la transición a IPv6.

No hay una única fecha para realizar la transición a IPv6. En un futuro cercano, IPv4 e IPv6 coexistirán. Se espera que la transición demore años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de red a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

* **Dual-stack:** como se muestra en la figura 1, la técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. Los dispositivos dual-stack ejecutan stacks de protocolos IPv4 e IPv6 de manera simultánea.
* **Tunneling:** como se muestra en la figura 2, tunneling es un método para transportar paquetes IPv6 a través de redes IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.
* **Traducción:** como se muestra en la figura 3, la traducción de direcciones de red 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce en un paquete IPV4, y viceversa.

A diferencia de las direcciones IPv4, que se expresan en notación decimal punteada, las direcciones IPv6 se representan mediante valores hexadecimales. Usted observó que el formato hexadecimal se utiliza en el panel Packets Byte (Byte del paquete) de Wireshark. En Wireshark, el formato hexadecimal se utiliza para representar los valores binarios dentro de tramas y paquetes. El formato hexadecimal también se utiliza para representar las direcciones de control de acceso al medio (MAC) de Ethernet.

**Numeración hexadecimal**

El método hexadecimal ("Hex") es una manera conveniente de representar valores binarios. Así como el sistema de numeración decimal es un sistema de base diez y el binario es un sistema de base dos, el sistema hexadecimal es un sistema de base dieciséis.

El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras de la A a la F. En la figura 1, se muestran los valores hexadecimales, binarios y decimales equivalentes. Existen 16 combinaciones únicas de cuatro bits, de 0000 a 1111. El sistema hexadecimal de16 dígitos es el sistema de numeración perfecto para utilizar, debido a que cuatro bits cualesquiera se pueden representar con un único valor hexadecimal.

**Comprensión de los bytes**

Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 hasta 11111111 pueden representarse en valores hexadecimales como el intervalo 00 a FF. Se pueden mostrar los ceros iniciales para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se muestra en valor hexadecimal como 0A.

**Representación de valores hexadecimales**

**Nota:** en lo que respecta a los caracteres del 0 al 9, es importante distinguir los valores hexadecimales de los decimales.

Por lo general, los valores hexadecimales se representan en forma de texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un subíndice 16. Con menor frecuencia, pueden estar seguidos de una H, por ejemplo, 73H. Sin embargo, y debido a que el texto en subíndice no es reconocido en entornos de línea de comando o de programación, la representación técnica de un valor hexadecimal es precedida de "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como 0x0A y 0x73, respectivamente.

**Conversiones hexadecimales**

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16.

Con la práctica, es posible reconocer los patrones de bits binarios que coinciden con los valores decimales y hexadecimales. En la figura 2, se muestran estos patrones para valores seleccionados de 8 bits.

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen mayúsculas de minúsculas y pueden escribirse en minúscula o en mayúscula.

**Formato preferido**

Como se muestra en la figura 1, el formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

“Formato preferido” significa que la dirección IPv6 se escribe utilizando 32 dígitos hexadecimales. No significa necesariamente que es el método ideal para representar la dirección IPv6. En las siguientes páginas, veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

En la figura 2, se muestran ejemplos de direcciones IPv6 en el formato preferido.

La primera regla que permite reducir la notación de direcciones IPv6 es que se puede omitir cualquier 0 (cero) inicial en cualquier sección de 16 bits o hexteto. Por ejemplo:

* 01AB puede representarse como 1AB.
* 09F0 puede representarse como 9F0.
* 0A00 puede representarse como A00.
* 00AB puede representarse como AB.

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto “ABC” podría ser tanto “0ABC” como “ABC0”.

En las figuras 1 a 8, se muestran varios ejemplos de cómo se puede utilizar la omisión de ceros iniciales para reducir el tamaño de una dirección IPv6. Se muestra el formato preferido para cada ejemplo. Advierta cómo la omisión de ceros iniciales en la mayoría de los ejemplos da como resultado una representación más pequeña de la dirección.

La segunda regla que permite reducir la notación de direcciones IPv6 es que los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) compuestos solo por ceros.

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como “formato comprimido”.

Dirección incorrecta:

* 2001:0DB8::ABCD::1234

Expansiones posibles de direcciones comprimidas ambiguas:

* 2001:0DB8::ABCD:0000:0000:1234
* 2001:0DB8::ABCD:0000:0000:0000:1234
* 2001:0DB8:0000:ABCD::1234
* 2001:0DB8:0000:0000:ABCD::1234

Existen tres tipos de direcciones IPv6:

* **Unicast:** las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Como se muestra en la ilustración, las direcciones IPv6 de origen deben ser direcciones unicast.
* **Multicast:** las direcciones IPv6 multicast se utilizan para enviar un único paquete IPv6 a varios destinos.
* **Anycast:** las direcciones IPv6 anycast son direcciones IPv6 unicast que se pueden asignar a varios dispositivos. Los paquetes enviados a una dirección anycast se enrutan al dispositivo más cercano que tenga esa dirección. En este curso, no se analizan las direcciones anycast.

A diferencia de IPv4, IPv6 no tiene una dirección de broadcast. Sin embargo, existe una dirección IPv6 multicast de todos los nodos que brinda básicamente el mismo resultado.

Recuerde que es posible identificar el prefijo, o la porción de red, de una dirección IPv4 mediante una máscara de subred en formato decimal punteado o una duración de prefijo (notación con barras). Por ejemplo, la dirección IP 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

IPv6 utiliza la duración de prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/duración de prefijo.

La duración de prefijo puede ir de 0 a 128. Una duración de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete que se envía a una dirección unicast es recibido por la interfaz que tiene asignada esa dirección. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones unicast. Las direcciones IPv6 de destino pueden ser direcciones unicast o multicast.

Existen seis tipos de direcciones IPv6 unicast.

**Unicast global**

Las direcciones unicast globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones unicast globales pueden configurarse estáticamente o asignarse de forma dinámica. Existen algunas diferencias importantes con respecto a la forma en que un dispositivo recibe su dirección IPv6 dinámicamente en comparación con DHCP para IPv4.

**Link-local**

Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.

**Loopback**

Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Al igual que en el caso de una dirección IPv4 de loopback, se puede hacer ping a una dirección IPv6 de loopback para probar la configuración de TCP/IP en el host local. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado como ::1/128 o, simplemente, ::1 en el formato comprimido.

**Dirección sin especificar**

Una dirección sin especificar es una dirección compuesta solo por ceros representada como ::/128 o, simplemente, :: en formato comprimido. No puede asignarse a una interfaz y solo se utiliza como dirección de origen en un paquete IPv6. Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.

**Local única**

Las direcciones IPv6 locales únicas tienen cierta similitud con las direcciones privadas para IPv4 definidas en RFC 1918, pero también existen diferencias importantes. Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deben ser enrutables en la IPv6 global. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.

Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Esto se hace debido a la disponibilidad limitada de espacio de direcciones IPv4. Muchos sitios también utilizan la naturaleza privada de las direcciones definidas en RFC 1918 para ayudar a proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso que se pretendió dar a estas tecnologías, y el IETF siempre recomendó que los sitios tomen las precauciones de seguridad adecuadas en el router con conexión a Internet. Si bien IPv6 proporciona direccionamiento de sitio específico, no tiene por propósito ser utilizado para contribuir a ocultar dispositivos internos con IPv6 habilitado de Internet IPv6. El IETF recomienda que la limitación del acceso a los dispositivos se logre implementando medidas de seguridad adecuadas y recomendadas.

**Nota:** en la especificación IPv6 original, se definían las direcciones locales de sitio con un propósito similar y se utilizaba el rango de prefijos FEC0::/10. La especificación contenía varias ambigüedades, y el IETF dejó en desuso las direcciones locales de sitio en favor de direcciones locales únicas.

**IPv4 integrada**

El último tipo de dirección unicast es la dirección IPv4 integrada. Estas direcciones se utilizan para facilitar la transición de IPv4 a IPv6. En este curso, no se analizan las direcciones IPv4 integradas.

Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

A diferencia de las direcciones IPv4 link-local, las direcciones IPv6 link-local cumplen una función importante en diversos aspectos de la red. La dirección unicast global no constituye un requisito, pero toda interfaz de red con IPv6 habilitado debe tener una dirección link-local.

Si en una interfaz no se configura una dirección link-local de forma manual, el dispositivo crea automáticamente su propia dirección sin comunicarse con un servidor de DHCP. Los hosts con IPv6 habilitado crean una dirección IPv6 link-local incluso si no se asignó una dirección IPv6 unicast global al dispositivo. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

Las direcciones IPv6 link-local están en el rango de FE80::/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hexteto tiene un rango de 1111 1110 10**00 0000** (FE80) a 1111 1110 10**11 1111** (FEBF).

En la figura 1, se muestra un ejemplo de comunicación mediante direcciones IPv6 link-local.

En la figura 2, se muestra el formato de una dirección IPv6 link-local.

Los protocolos de enrutamiento IPv6 también utilizan direcciones IPv6 link-local para intercambiar mensajes y como la dirección del siguiente salto en la tabla de enrutamiento IPv6. Las direcciones link-local se analizan más detalladamente en un curso posterior.

**Nota:** por lo general, la dirección que se utiliza como gateway predeterminado para los otros dispositivos en el enlace es la dirección link-local del router, y no la dirección unicast global.

Las direcciones IPv6 unicast globales son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Internet Corporation for Assigned Names and Numbers (ICANN), el operador de la Internet Assigned Numbers Authority (IANA), asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones unicast y multicast.

**Nota:** la dirección 2001:0DB8::/32 se reservó para fines de documentación, incluido el uso en ejemplos.

En la figura 1, se muestra la estructura y el rango de una dirección unicast global.

Una dirección unicast global consta de tres partes:

* Prefijo de enrutamiento global
* ID de subred
* ID de interfaz

**Prefijo de enrutamiento global**

El prefijo de enrutamiento global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. En la actualidad, los RIR asignan a los clientes el prefijo de enrutamiento global /48. Esto incluye desde redes comerciales de empresas hasta unidades domésticas Para la mayoría de los clientes, este espacio de dirección es más que suficiente.

En la figura 2, se muestra la estructura de una dirección unicast global con el prefijo de enrutamiento global /48. Los prefijos /48 son los prefijos de enrutamiento global más comunes, y se utilizarán en la mayoría de los ejemplos a lo largo de este curso.

Por ejemplo, la dirección IPv6 2001:0DB8:ACAD::/48 tiene un prefijo que indica que los primeros 48 bits (3 hextetos) (2001:0DB8:ACAD) son la porción de prefijo o de red de la dirección. Los dos puntos dobles (::) antes de la duración de prefijo /48 significan que el resto de la dirección se compone solo de ceros.

**ID de subred**

Las organizaciones utilizan la ID de subred para identificar una subred dentro de su ubicación.

**ID de interfaz**

La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término “ID de interfaz” debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6.

**Nota:** a diferencia de IPv4, en IPv6 se pueden asignar las direcciones de host compuestas solo por ceros y unos a un dispositivo. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de broadcast. También se puede utilizar la dirección compuesta solo por ceros, pero se reserva como una dirección anycast de subred y router, y se debe asignar solo a routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hextetos. Como se muestra en la figura 3, en una dirección unicast global /64 los primeros cuatro hextetos son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hextetos restantes son para la ID de interfaz.

**Configuración del router**

La mayoría de los comandos de configuración y verificación IPv6 de Cisco IOS son similares a sus equivalentes de IPv4. En muchos casos, la única diferencia es el uso de **ipv6** en lugar de **ip** dentro de los comandos.

El comando **interface** que se utiliza para configurar una dirección IPv6 unicast global en una interfaz es **ipv6 address***dirección ipv6/duración de prefijo*.

Advierta que no hay un espacio entre *dirección ipv6* y *duración de prefijo*.

En la configuración de ejemplo, se utiliza la topología que se muestra en la figura 1 y estas subredes IPv6:

* 2001:0DB8:ACAD:0001:/64 (*o* 2001:DB8:ACAD:1::/64)
* 2001:0DB8:ACAD:0002:/64 (*o* 2001:DB8:ACAD:2::/64)
* 2001:0DB8:ACAD:0003:/64 (*o* 2001:DB8:ACAD:3::/64)

Como se muestra en la figura 2, los comandos requeridos para configurar la dirección IPv6 unicast global en la interfaz GigabitEthernet 0/0 de R1 serían los siguientes:

**Router(config)#interface GigabitEthernet 0/0**

**Router(config-if)#ipv6 address 2001:db8:acad:1::1/64**

**Router(config-if)#no shutdown**

**Configuración de host**

Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.

Como se muestra en la figura 3, la dirección de gateway predeterminado configurada para PC1 es 2001:DB8:ACAD:1::1, la dirección unicast global de la interfaz GigabitEthernet de R1 en la misma red.

Utilice el verificador de sintaxis de la figura 4 para configurar la dirección IPv6 unicast global.

Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de red en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Los dispositivos pueden obtener automáticamente una dirección IPv6 unicast global de dos maneras:

* Configuración automática de dirección sin estado (SLAAC)
* DHCPv6

**Configuración automática de dirección sin estado (SLAAC)**

La configuración automática de dirección sin estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un *router IPv6* sin utilizar un servidor de DHCPv6. Mediante SLAAC, los dispositivos dependen de los mensajes de anuncio de router (RA) de ICMPv6 del router local para obtener la información necesaria.

Los routers IPv6 envían mensajes de anuncio de router (RA) de ICMPv6 a todos los dispositivos en la red con IPv6 habilitado de forma periódica. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos a la dirección IPv6 de grupo multicast de todos los nodos. Los dispositivos IPv6 en la red no tienen que esperar estos mensajes periódicos de RA. Un dispositivo puede enviar un mensaje de solicitud de router (RS) utilizando la dirección IPv6 de grupo multicast de todos los routers. Cuando un router IPv6 recibe un mensaje de RS, responde inmediatamente con un anuncio de router.

Si bien es posible configurar una interfaz en un router Cisco con una dirección IPv6, esto no lo convierte en un “router IPv6”. Un router IPv6 es un router que presenta las siguientes características:

* Reenvía paquetes IPv6 entre redes.
* Puede configurarse con rutas estáticas IPv6 o con un protocolo de enrutamiento dinámico IPv6.
* Envía mensajes RA ICMPv6.

El enrutamiento IPv6 no está habilitado de manera predeterminada. Para habilitar un router como router IPv6, se debe utilizar el comando de configuración global**ipv6 unicast-routing**.

**Nota:** los routers Cisco están habilitados como routers IPv4 de manera predeterminada.

El mensaje de RA de ICMPv6 contiene el prefijo, la duración de prefijo y otra información para el dispositivo IPv6. El mensaje de RA también informa al dispositivo IPv6 cómo obtener la información de direccionamiento. El mensaje de RA puede contener una de las siguientes tres opciones, como se muestra en la ilustración:

* **Opción 1, SLAAC solamente:** el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. No se encuentra disponible ninguna otra información de un servidor de DHCPv6.
* **Opción 2, SLAAC y DHCPv6:** el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. Existe otra información disponible de un servidor de DHCPv6, como la dirección del servidor DNS. El dispositivo obtiene esta información adicional mediante el proceso normal de descubrimiento y consulta a un servidor de DHCPv6. Esto se conoce como DHCPv6 sin estado, debido a que el servidor de DHCPv6 no necesita asignar ni realizar un seguimiento de ninguna asignación de direcciones IPv6, sino que solo proporciona información adicional, tal como la dirección del servidor DNS.
* **Opción 3, DHCPv6 solamente:** el dispositivo no debe utilizar la información incluida en el mensaje de RA para obtener la información de direccionamiento. En cambio, el dispositivo utiliza el proceso normal de descubrimiento y consulta a un servidor de DHCPv6 para obtener toda la información de direccionamiento. Esto incluye una dirección IPv6 unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de los servidores DNS. En este caso, el servidor de DHCPv6 actúa como un servidor de DHCP sin estado, de manera similar a DHCP para IPv4. El servidor de DHCPv6 asigna direcciones IPv6 y realiza un seguimiento de ellas, a fin de no asignar la misma dirección IPv6 a varios dispositivos.

Los routers envían mensajes de RA de ICMPv6 utilizando la dirección link-local como la dirección IPv6 de origen. Los dispositivos que utilizan SLAAC usan la dirección link-local del router como su dirección de gateway predeterminado.

**DHCPv6**

El protocolo de configuración dinámica de host para IPv6 (DHCPv6) es similar a DHCP para IPv4. Los dispositivos pueden recibir de manera automática la información de direccionamiento, incluso una dirección unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de servidores DNS, mediante los servicios de un servidor de DHCPv6.

Los dispositivos pueden recibir la información de direccionamiento IPv6 en forma total o parcial de un servidor de DHCPv6 en función de si en el mensaje de RA de ICMPv6 se especificó la opción 2 (SLAAC y DHCPv6) o la opción 3 (DHCPv6 solamente). Además, el OS host puede optar por omitir el contenido del mensaje de RA del router y obtener su dirección IPv6 y otra información directamente de un servidor de DHCPv6.

Antes de implementar dispositivos IPv6 en una red, se recomienda primero verificar si el host observa las opciones dentro del mensaje ICMPv6 de RA del router.

Un dispositivo puede obtener la dirección IPv6 unicast global dinámicamente y también estar configurado con varias direcciones IPv6 estáticas en la misma interfaz. IPv6 permite que varias direcciones IPv6 (que pertenecen a la misma red IPv6) se configuren en la misma interfaz.

También se puede configurar un dispositivo con más de una dirección IPv6 de gateway predeterminado. Para obtener más información sobre cómo se toma la decisión respecto de cuál es la dirección que se usa como la dirección IPv6 de origen o cuál es la dirección de gateway predeterminado que se utiliza, consulte RFC 6724, Default Address Selection for IPv6 (Selección de direcciones predeterminada para IPv6).

**ID de interfaz**

Si el cliente no utiliza la información incluida en el mensaje de RA y depende exclusivamente de DHCPv6, el servidor de DHCPv6 proporciona la dirección IPv6 unicast global completa, incluidos el prefijo y la ID de interfaz.

Sin embargo, si se utiliza la opción 1 (SLAAC solamente) o la opción 2 (SLAAC con DHCPv6), el cliente no obtiene la porción de ID de interfaz real de la dirección mediante este estos procesos. El dispositivo cliente debe determinar su propia ID de interfaz de 64 bits, ya sea mediante el proceso EUI-64 o generando un número aleatorio de 64 bits.

**Proceso EUI-64**

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

* **Identificador único de organización (OUI):** el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna el IEEE.
* **Identificador de dispositivo:** el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.

Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

* OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto significa que si el séptimo bit es un 0, se convierte en 1, y viceversa.
* Valor de 16 bits FFFE introducido (en formato hexadecimal)
* Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura 1, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

**Paso 1:** Dividir la dirección MAC entre el OUI y el identificador de dispositivo

**Paso 2:** Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110

**Paso 3:** Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit) En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es una ID de interfaz de FE99:47FF:FE75:CEE0 generada mediante EUI-64.

**Nota:** el uso del bit U/L y los motivos para invertir su valor se analizan en RFC 5342.

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

**ID de interfaz generadas aleatoriamente**

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, comenzando con Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y sistemas operativos Windows anteriores utilizaban EUI-64.

Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz, como se muestra en la figura 2.

Después de que se establece una ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 para crear una dirección unicast global o una dirección link-local.

* **Dirección unicast global:** al utilizar SLAAC, el dispositivo recibe su prefijo del mensaje de RA de ICMPv6 y lo combina con la ID de interfaz.
* **Dirección link-local:** los prefijos link-local comienzan con FE80::/10. Los dispositivos suelen utilizar FE80::/64 como prefijo o duración de prefijo, seguido de la ID de interfaz.

Al utilizar SLAAC (SLAAC solamente o SLAAC con DHCPV6), los dispositivos reciben el prefijo y la duración de prefijo del mensaje de RA de ICMPv6. Debido a que el mensaje de RA designa el prefijo de la dirección, el dispositivo debe proporcionar únicamente la porción de ID de interfaz de su dirección. Como se indicó anteriormente, la ID de interfaz se puede generar de forma automática mediante el proceso EUI-64, o, según el OS, se puede generar de forma aleatoria. Con la información del mensaje de RA y la ID de interfaz, el dispositivo puede establecer su dirección unicast global.

Después de que se asigna una dirección unicast global a una interfaz, el dispositivo con IPv6 habilitado genera la dirección link-local automáticamente. Los dispositivos con IPv6 habilitado deben tener, como mínimo, la dirección link-local. Recuerde que una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en la misma subred.

Las direcciones IPv6 link-local se utilizan para diversos fines, incluidos los siguientes:

* Los hosts utilizan la dirección link-local del router local para obtener la dirección IPv6 de gateway predeterminado.
* Los routers intercambian mensajes de protocolo de enrutamiento dinámico mediante direcciones link-local.
* Las tablas de enrutamiento de los routers utilizan la dirección link-local para identificar el router del siguiente salto al reenviar paquetes IPv6.

Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

**Dirección link-local asignada dinámicamente**

La dirección link-local se crea dinámicamente mediante el prefijo FE80::/10 y la ID de interfaz.

De manera predeterminada, los routers en los que se utiliza Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red. Sin embargo, una desventaja de utilizar direcciones link-local asignadas dinámicamente es su longitud, que dificulta identificar y recordar las direcciones asignadas.

**Dirección Link-Local estática**

Configurar la dirección link-local de forma manual permite crear una dirección reconocible y más fácil de recordar.

Las direcciones link-local pueden configurarse manualmente mediante el mismo comando interface que se utiliza para crear direcciones IPv6 unicast globales, pero con un parámetro adicional:

**Router(config-if)#ipv6 address link-local-address link-local**

En la figura 1, se muestra que una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hexteto (segmento de 16 bits), el parámetro link-local debe seguir la dirección.

En la figura 2, se muestra la configuración de una dirección link-local mediante el comando **ipv6 address interface**. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces de R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar a R1, el router R2 se configuraría con FE80::2 como la dirección IPv6 link-local en todas sus interfaces.

Como se muestra en la figura 1, el comando para verificar la configuración de la interfaz IPv6 es similar al comando que se utiliza para IPv4.

El comando **show interface** muestra la dirección MAC de las interfaces Ethernet. EUI-64 utiliza esta dirección MAC para generar la ID de interfaz para la dirección link-local. Además, el comando **show ipv6 interface brief** muestra un resultado abreviado para cada una de las interfaces. El resultado[up/up] en la misma línea que la interfaz indica el estado de interfaz de capa 1/capa 2. Esto es lo mismo que las columnas Status (Estado) y Protocol (Protocolo) en el comando IPv4 equivalente.

Advierta que cada interfaz tiene dos direcciones IPv6. La segunda dirección para cada interfaz es la dirección unicast global que se configuró. La primera dirección, la que comienza con FE80, es la dirección unicast link-local para la interfaz. Recuerde que la dirección link-local se agrega automáticamente a la interfaz cuando se asigna una dirección unicast global.

Además, advierta que la dirección link-local serial 0/0/0 de R1 es igual a la interfaz GigabitEthernet 0/0. Las interfaces seriales no tienen una dirección MAC de Ethernet, de modo que Cisco IOS utiliza la dirección MAC de la primera interfaz Ethernet disponible. Esto es posible porque las interfaces link-local solo deben ser únicas en ese enlace.

La dirección link-local de la interfaz del router suele ser la dirección de gateway predeterminado para los dispositivos en ese enlace o red.

Como se muestra en la figura 2, el comando **show ipv6 route** puede utilizarse para verificar si las redes IPv6 y las direcciones específicas de la interfaz IPv6 se instalaron en la tabla de enrutamiento IPv6. El comando **show ipv6 route** muestra solamente redes IPv6, no redes IPv4.

Dentro de la tabla de la ruta, una C junto a una ruta indica que se trata de una red conectada directamente. Cuando la interfaz del router se configura con una dirección unicast global y su estado es “up/up”, se agrega el prefijo y la duración de prefijo IPv6 a la tabla de enrutamiento IPv6 como una ruta conectada.

La dirección IPv6 unicast global configurada en la interfaz también se instala en la tabla de enrutamiento como una ruta local. La ruta local tiene un prefijo /128. La tabla de enrutamiento utiliza las rutas locales para procesar eficazmente paquetes cuya dirección de destino es la dirección de la interfaz del router.

El comando **ping** para IPv6 es idéntico al comando que se utiliza con IPv4, excepto que se usa una dirección IPv6. Como se muestra en la figura 3, el comando se utiliza para verificar la conectividad de capa 3 entre R1 y PC1. Al hacer ping a una dirección link-local desde un router, Cisco IOS solicita al usuario la interfaz de salida. Dado que la dirección link-local de destino puede estar en uno o más de los enlaces o redes, el router debe saber qué interfaz utilizar para enviar el ping.

Utilice el verificador de sintaxis de la figura 4 para verificar la configuración de la dirección IPv6.

Las direcciones IPv6 multicast son similares a las direcciones IPv4 multicast. Recuerde que las direcciones multicast se utilizan para enviar un único paquete a uno o más destinos (grupo multicast). Las direcciones IPv6 multicast tienen el prefijo FF00::/8.

**Nota:** las direcciones multicast solo pueden ser direcciones de destino, no de origen.

Existen dos tipos de direcciones IPv6 multicast:

* Dirección multicast asignada
* Dirección multicast de nodo solicitado

**Dirección multicast asignada**

Las direcciones multicast asignadas son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones multicast asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

Dos grupos comunes de direcciones multicast IPv6 asignadas incluyen los siguientes:

* **Grupo multicast de todos los nodos FF02::1:** grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de broadcast en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección multicast de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo multicast de todos los nodos. El mensaje de RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la duración de prefijo y el gateway predeterminado.
* **Grupo multicast de todos los routers FF02::2:** grupo multicast al que se unen todos los routers con IPv6 habilitado. Un router se convierte en un miembro de este grupo cuando se habilita como router IPv6 mediante el comando de configuración global **ipv6 unicast-routing**. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección multicast de todos los routers. El mensaje de RS solicita un mensaje de RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.

Las direcciones multicast de nodo solicitado son similares a las direcciones multicast de todos los nodos. Recuerde que la dirección multicast de todos los nodos es esencialmente lo mismo que una dirección IPv4 de broadcast. Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección multicast de nodo solicitado.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz.

Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección IPv6 multicast de nodo solicitado se crea combinando un prefijo especial FF02:0:0:0:0:1:FF00::/104 con los 24 bits de su dirección unicast que se encuentran en el extremo derecho.

La dirección multicast de nodo solicitado consta de dos partes:

* **Prefijo multicast FF02:0:0:0:0:1:FF00::/104:** los primeros 104 bits de la dirección multicast de todos los nodos solicitados.
* **24 bits menos significativos:** los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo.

Es posible que varios dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien es poco común, esto puede suceder cuando los dispositivos tienen los mismos 24 bits que se encuentran más hacia la derecha en sus ID de interfaz. Esto no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión.

Si bien IP no es un protocolo confiable, la suite TCP/IP proporciona los mensajes que se deben enviar en caso de que se produzcan determinados errores. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP bajo determinadas condiciones, no es hacer que el IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Existen muchos tipos de mensajes de ICMP y muchos motivos por los cuales se envían estos mensajes. Analizaremos algunos de los mensajes más comunes.

Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente:

* Confirmación de host
* Destino o servicio inaccesible
* Tiempo superado
* Redireccionamiento de ruta

**Confirmación de host**

Se puede utilizar un mensaje de eco de ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. En la ilustración, haga clic en el botón Reproducir para ver una animación de la solicitud de eco o de la respuesta de eco de ICMP. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

**Destino o servicio inaccesible**

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje de destino inalcanzable de ICMP para notificar al origen que el destino o el servicio es inalcanzable. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

* 0: red inalcanzable
* 1: host inalcanzable
* 2: protocolo inalcanzable
* 3: puerto inalcanzable

**Nota:** los códigos de ICMPv6 para los mensajes de destino inalcanzable son similares, pero presentan algunas diferencias.

**Tiempo superado**

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo Tiempo de vida (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. IPv6 no tiene un campo TTL, por lo que utiliza el campo de Límite de saltos para determinar si el paquete caducó.

**Redireccionamiento de ruta**

Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways.

Tanto ICMPv4 como ICMPv6 utilizan mensajes de redireccionamiento de ruta.

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4.

ICMPv6 incluye cuatro nuevos protocolos como parte del protocolo ND o NDP (Neighbor Discovery Protocol, protocolo de descubrimiento de vecinos):

* Mensaje de solicitud de router
* Mensaje de anuncio de router
* Mensaje de solicitud de vecino
* Mensaje de anuncio de vecino

**Mensajes de solicitud y de anuncio de router**

Los dispositivos con IPv6 habilitado pueden dividirse en dos categorías: routers y hosts. Los mensajes de solicitud de router y de anuncio de router se envían entre hosts y routers.

* **Mensaje de solicitud de router (RS):** cuando un host está configurado para obtener la información de direccionamiento de forma automática mediante la configuración automática de dirección sin estado (SLAAC), el host envía un mensaje de RS al router. El mensaje de RS se envía como un mensaje IPv6 multicast de todos los routers.
* **Mensaje de anuncio de router (RA):** los routers envían mensajes de RA para proporcionar información de direccionamiento a los hosts mediante SLAAC. El mensaje de RA puede incluir información de direccionamiento para el host, como el prefijo y la duración de prefijo. Los routers envían mensajes de RA de forma periódica o en respuesta a un mensaje de RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes de RA se envían a la dirección IPv6 multicast de todos los nodos. Los hosts que utilizan SLAAC establecen su gateway predeterminado en la dirección link-local del router que envió el mensaje de RA.

El protocolo de descubrimiento de vecinos de ICMPv6 incluye dos tipos de mensajes adicionales: mensaje de solicitud de vecino (NS) y mensaje de anuncio de vecino (NA).

Los mensajes de solicitud y de anuncio de vecino se utilizan para lo siguiente:

* Resolución de direcciones
* Detección de direcciones duplicadas (DAD)

**Resolución de direcciones**

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 unicast de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que tiene la dirección IPv6 objetivo responde con un mensaje de NA que contiene la dirección MAC de Ethernet.

**Detección de direcciones duplicadas**

Cuando se asigna una dirección unicast global o una dirección unicast link-local a un dispositivo, se recomienda llevar a cabo la detección de direcciones duplicadas (DAD) en la dirección para asegurarse de que sea única. Para revisar si una dirección es única, el dispositivo envía un mensaje de NS con su propia dirección IPv6 como la dirección IPv6 objetivo. Si otro dispositivo en la red tiene esta dirección, responde con un mensaje de NA. Este mensaje de NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje de NA correspondiente dentro de determinado período, la dirección unicast es única y su uso es aceptable.

**Nota:** la DAD no es obligatoria, pero en RFC 4861 se recomienda que se realice la DAD en direcciones unicast.

Ping es una utilidad de prueba que utiliza mensajes de solicitud y de respuesta de eco de ICMP para probar la conectividad entre hosts. Ping funciona tanto con IPv4 y con hosts IPv6.

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección de host mediante el comando **ping**. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esta puede ser una medida del rendimiento de la red.

Ping posee un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, ping proporciona un mensaje que indica que no se recibió una respuesta. Generalmente, esto indica que existe un problema, pero también podría indicar que se habilitaron características de seguridad que bloquean mensajes ping en la red.

Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

**Ping del loopback local**

Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna de IPv4 o de IPv6 en el host local. Para realizar esta prueba, se debe hacer ping a la dirección de loopback de 127.0.0.1 para IPv4 (::1 para IPv6). En la ilustración, se muestra la prueba de la dirección IPv4 de loopback.

Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior del stack de red. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el TCP/IP no funciona en el host.

También es posible utilizar ping para probar la capacidad de comunicación del host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host. Un ping al gateway indica que la interfaz del host y la interfaz del router que cumplen la función de gateway funcionan en la red local.

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

Si el gateway u otro host responden, los hosts locales pueden comunicarse correctamente a través de la red local. Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway.

Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping.

También se puede utilizar ping para probar la capacidad de un host local para comunicarse a través de una internetwork. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la internetwork. Un ping correcto a través de la internetwork confirma la comunicación en la red local, el funcionamiento del router que funciona como gateway y el funcionamiento de todos los otros routers que podrían estar en la ruta entre la red local y la red del host remoto.

Además, es posible verificar la funcionalidad del host remoto. Si el host remoto no podía comunicarse fuera de la red local, no hubiera respondido.

**Nota:** muchos administradores de red limitan o prohíben la entrada de mensajes de ICMP a la red corporativa; motivo por el cual la ausencia de una respuesta de ping podría deberse a restricciones de seguridad.

Ping se utiliza para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (tracert) es una utilidad que genera una lista de saltos que se alcanzaron correctamente a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la resolución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

**Tiempo de ida y vuelta (RTT)**

El uso de traceroute proporciona el tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta es el tiempo que le lleva a un paquete llegar al host remoto y el tiempo que la respuesta del host demora en regresar. Se utiliza un asterisco (\*) para indicar un paquete perdido o sin respuesta.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

**Tiempo de vida (TTL) de IPv4 y Límite de saltos de IPv6**

Traceroute utiliza una función del campo TTL en IPv4 y del campo Límite de saltos en IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.

Reproduzca la animación en la figura para ver cómo Traceroute aprovecha el TTL.

La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router luego responde con un mensaje de ICMPv4. Traceroute ahora posee la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes expiran el límite de tiempo a lo largo del camino. El campo TTL continúa aumentando hasta que se llega a destino o hasta un máximo predefinido.

Una vez que se llega al destino final, el host responde con un mensaje de puerto inalcanzable de ICMP o un mensaje de respuesta de eco de ICMP, en lugar de hacerlo con un mensaje de tiempo superado de ICMP.

Las direcciones IP son jerárquicas y tienen porciones de red, subred y host. Una dirección IP puede representar una red completa, un host específico o la dirección de broadcast de la red.

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Los bits dentro de la porción de red de la dirección IP deben ser idénticos para todos los dispositivos que residen en la misma red. La máscara de subred o el prefijo se utilizan para determinar la porción de red de una dirección IP. Las direcciones IP pueden asignarse de manera estática o dinámica. 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.

Los hosts IPv4 pueden comunicarse de una de tres maneras diferentes: por unicast, broadcast y multicast. Además, los bloques de direcciones que se utilizan en redes que requieren acceso limitado o inexistente a Internet se denominan “direcciones privadas”. Los bloques de direcciones IPv4 privadas son los siguientes: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

La migración a IPv6 está motivada por el agotamiento del espacio de direcciones IPv4. Cada dirección IPv6 tiene 128 bits, en comparación con los 32 bits que poseen las direcciones IPv4. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el siguiente formato: dirección IPv6/duración de prefijo.

Hay tres tipos de direcciones IPv6: unicast, multicast y anycast. Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete. Las direcciones IPv6 link-local están en el rango de FE80::/10.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional.

Una vez implementada, la red IP se debe probar para verificar la conectividad y el rendimiento operativo.