

## 13.0 Introducción

Desplázate para empezar

### 13.0.1 ¿Por qué debería tomar este módulo?

Bienvenido a ICMP!

Imagina que tienes un intrincado juego de tren modelo. Sus vías y trenes están conectados, encendidos y listos para funcionar. Tú lanzas el interruptor. El tren va a la mitad de la pista y se detiene. Usted sabe de inmediato que el problema se encuentra muy probablemente donde el tren se ha detenido, así que mira allí primero. No es tan fácil visualizar esto con una red. Afortunadamente, hay herramientas para ayudarle a localizar áreas problemáticas en su red, ¡Y funcionan con redes IPv4 e IPv6! Usted estará feliz de saber que este módulo tiene un par de actividades Packet Tracer para ayudarle a practicar el uso de estas herramientas, así que vamos a probar!

### 13.0.2 ¿Qué aprenderé en este módulo?

**Título del módulo:** ICMP

**Objetivos del módulo:** Utilice varias herramientas para probar la conectividad de red.

## 13.1 Mensajes ICMP

Desplázate para empezar

### 13.1.1 Mensajes ICMPv4 e ICMPv6

En este tema, aprenderá acerca de los diferentes tipos de protocolos de mensajes de control de Internet (ICMP) y las herramientas que se utilizan para enviarlos.

Aunque IP es sólo un protocolo de mayor esfuerzo, el conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP. 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 en determinadas condiciones, no es hacer que 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.

Los tipos de mensajes ICMP y las razones por las que se envían son extensos. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 y discutidos en este módulo incluyen:

- Accesibilidad al host
- Destino o servicio inaccesible
- Tiempo superado

## 13.1.2 Accesibilidad al host

Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP. El host local envía una solicitud de eco 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/respuesta de eco ICMP. Este uso de los mensajes ICMP Echo es la base de la **ping** utilidad.

animación del host 1 enviando una solicitud de eco ICMP ping al host 2 y la respuesta de eco ICMP del host 2 al host 1

Sí, aquí estoy.

ping 192.168.30.1

play\_circle\_filled

## 13.1.3 Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. 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

Algunos de los códigos de destino inalcanzable para ICMPv6 son los siguientes:

- 0 - No hay ruta para el destino
- 1 - La comunicación con el destino está prohibida administrativamente (por ejemplo, firewall)
- 2 — Más allá del alcance de la dirección de origen
- 3 - No se puede alcanzar la dirección
- 4 - Puerto inalcanzable

**Nota:** ICMPv6 tiene códigos similares pero ligeramente diferentes para los mensajes de destino inalcanzable.

## 13.1.4 Tiempo excedido

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de tiempo de duración (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. En lugar del campo TTL de IPv4, ICMPv6 usa el campo Límite de salto de IPv6 para determinar si el paquete ha expirado.

La **Nota:** herramienta utiliza los mensajes de **traceroute** tiempo excedido.

## 13.1.5 Mensajes ICMPv6

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. Los mensajes ICMPv6 están encapsulados en IPv6.

ICMPv6 incluye cuatro mensajes nuevos como parte del protocolo de detección de vecino (ND o NDP).

Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, son los siguientes:

- Mensaje de solicitud de router (RS)
- Mensaje de anuncio de router (RA)

Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son los siguientes:

- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

**Nota:** ICMPv6 ND también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

Haga clic en cada una para obtener una ilustración y una explicación de los mensajes ICMPv6.

Mensaje de RA

Mensaje RS

Mensaje NS

Mensaje de NA

Los enrutadores habilitados para IPv6 envían mensajes de RA cada 200 segundos para proporcionar información de direccionamiento a los hosts habilitados para IPv6. El mensaje RA puede incluir información de direccionamiento para el host, como el prefijo, la longitud del prefijo, la dirección DNS y el nombre de dominio. Un host que utiliza la Configuración automática de direcciones sin estado (SLAAC) establecerá su puerta de enlace predeterminada en la dirección de enlace local del enrutador que envió el RA.

R1 envía un mensaje de anuncio de enrutador RA a FF02::1 la dirección de multidifusión de todos los nodos que llegará a PC1.

2001:db8:acad:1::1/64PC12001:db8:acad:1::1/64fe80::1R1

Mensaje de RA

*R1 envía un mensaje de RA, «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1::/64. Por cierto, use mi dirección local de enlace fe80::1 como su puerta de enlace predeterminada. »*

## 13.2 Pruebas de ping y traceroute

Desplázate para empezar

### 13.2.1 Ping - Prueba de Conectividad

En el tema anterior, se le presentó a las herramientas **ping** y **traceroute (tracert)**. En este tema, aprenderá acerca de las situaciones en las que se usa cada herramienta y cómo usarlas. Ping es una utilidad de prueba de IPv4 e IPv6 que utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts.

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección del host utilizando 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 sobre el tiempo entre el momento en que se envió la solicitud y el momento en que se recibió la respuesta. Esto puede ser una medida del rendimiento de la red.

El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta. Esto puede indicar que hay un problema, pero también podría indicar que las funciones de seguridad que bloquean los mensajes de ping se han habilitado en la red. Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la solicitud de eco ICMP.

Después de enviar todas las solicitudes, la **ping** utilidad proporciona un resumen que incluye la tasa de éxito y el tiempo promedio de ida y vuelta al destino.

Los tipos de pruebas de conectividad que se realizan con **ping** son los siguientes:

- Hacer ping al loopback local
- Hacer ping a la puerta de enlace predeterminada
- Hacer ping al host remoto

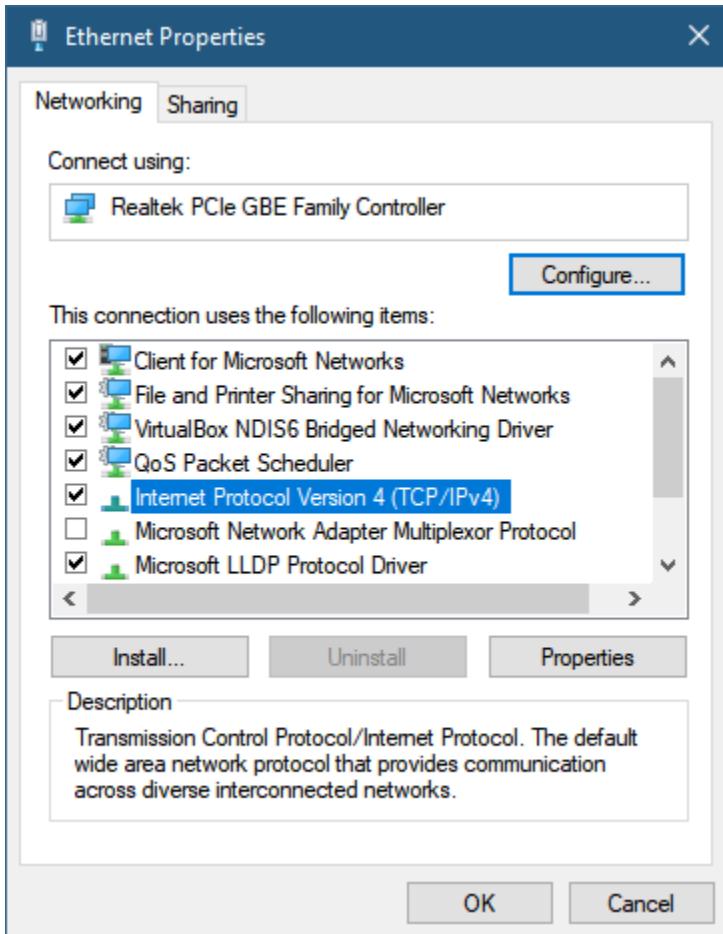
## 13.2.2 Hacer ping al loopback

Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Para realizar esta prueba, **ping** a dirección de bucle de retorno local de 127.0.0.1 para IPv4 (:: 1 para IPv6).

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 es una indicación de que las direcciones, máscaras o puertas de enlace estén configuradas correctamente. Tampoco indica nada acerca del estado de la capa inferior de la pila de red. Simplemente, prueba el protocolo IP en la capa de red de dicho protocolo. Un mensaje de error indica que TCP/IP no funciona en el host.

muestra el cuadro de diálogo Propiedades Ethernet muestra que el Protocolo de Internet versión 4 (TCP/IPv4) está instalado y activo, lo que se demuestra con un ping a 127.0.0.1

```
C:\>ping 127.0.0.1
```



- *Hacer ping al host local permite confirmar que el protocolo TCP/IP se encuentra instalado en el host y que funciona.*
- *Hacer ping a 127.0.0.1 ocasiona que un dispositivo se haga ping a sí mismo.*

### 13.2.3 Hacer ping al gateway predeterminado

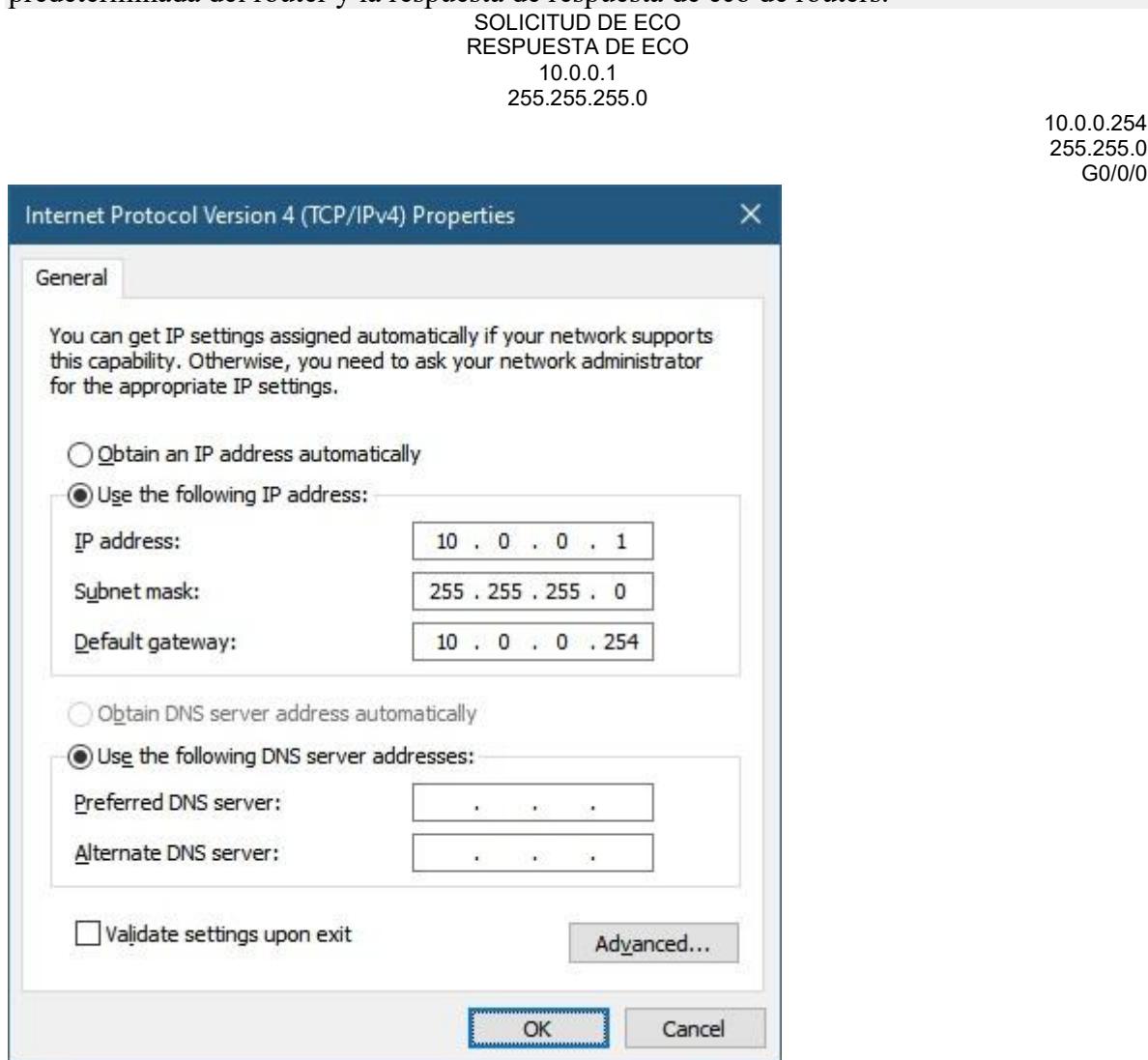
También puede usar para **ping** probar la capacidad de un host para comunicarse en la red local. Esto generalmente se hace haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un éxito en la **ping** puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirve como puerta de enlace predeterminada están operativos en la red local.

Para esta prueba, la dirección de puerta de enlace predeterminada se usa con mayor frecuencia porque el enrutador normalmente siempre está operativo. Si la dirección de la puerta de enlace predeterminada no responde, **ping** se puede enviar a la dirección IP de otro host en la red local que se sabe que está operativa.

Si la puerta de enlace predeterminada u otro host responde, entonces el host local puede comunicarse con éxito a través de la red local. Si la puerta de enlace predeterminada no responde pero otro host sí, esto podría indicar un problema con la interfaz del enrutador que funciona como la puerta de enlace predeterminada.

Una posibilidad es que se haya configurado una dirección de puerta de enlace predeterminada 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 solicitudes de ping.

El gráfico muestra el cuadro de diálogo de propiedades Ethernet configurado con una dirección IP estática, una máscara de subred y una puerta de enlace predeterminada. La topología muestra la PC que envía una solicitud de eco a la puerta de enlace predeterminada del router y la respuesta de respuesta de eco de routers.



*El host hace ping a su puerta de enlace predeterminada, enviando una solicitud de eco ICMP. La puerta de enlace predeterminada envía una respuesta de eco confirmando la conectividad.*

## 13.2.4 Hacer ping a un Host Remoto

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración. El router utiliza su tabla de enrutamiento IP para reenviar los paquetes.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un éxito en **ping** toda la red confirma la comunicación en la red local, el funcionamiento del enrutador que sirve como puerta de enlace predeterminada y el funcionamiento de todos los demás enrutadores que podrían estar en la ruta entre la red local y la red del host remoto.

De manera adicional, se puede verificar la funcionalidad del módulo remoto de E/S. Si el módulo remoto de E/S no podía comunicarse fuera de la red local, no hubiera respondido.

**Nota:** Muchos administradores de red limitan o prohíben la entrada de mensajes ICMP en la red corporativa; **ping** por lo tanto, la falta de respuesta podría deberse a restricciones de seguridad.

La animación muestra una solicitud de eco de ping a una red remota que se enruta a través de un router respuesta de eco que se enruta desde la red remota

Solicitud de eco  
Respuesta de eco  
Tabla de Enrutamiento IP

play\_circle\_filled

## 13.2.5 Traceroute - Prueba el Camino

El comando ping se usa 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 con éxito a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la solución 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 tiempo de ida y vuelta para cada salto a lo largo del camino e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Se utiliza un asterisco (\*) para indicar un paquete perdido o no respondido.

Esta información se puede usar para localizar un enrutador problemático en la ruta o puede indicar que el enrutador está configurado para no responder. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

### TTL de IPv4 y Límite de Saltos en IPv6

Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de salto en IPv6 en los encabezados de Capa 3, junto con el mensaje ICMP Time Exceeded.

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

La animación muestra una ruta de seguimiento a una red remota que cruza tres routers. El traceroute tomará 4 solicitudes de eco para llegar a su destino

Respuesta de Eco ICMP  
ICMP  
Tiempo Excedido  
ICMP  
Tiempo Excedido  
ICMP  
Tiempo Excedido  
**Traceroute**  
**192.168.1.2**  
**(TTL = 4)**  
**Traceroute**  
**192.168.1.2**  
**(TTL = 3)**  
**Traceroute**  
**192.168.1.2**  
**(TTL = 2)**  
**Traceroute**  
**192.168.1.2**  
**(TTL = 1)**

 play\_circle\_filled

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 enrutador responde con un mensaje ICMPv4 Tiempo excedido. Traceroute ahora tiene la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. Esto proporciona el rastro con la dirección de cada salto a medida que los paquetes caducan más adelante en la ruta. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.

Una vez que se alcanza el destino final, el host responde con un mensaje de puerto inalcanzable ICMP o un mensaje de respuesta de eco ICMP en lugar del mensaje de tiempo excedido ICMP.

## 13.3 Práctica del Módulo y Cuestionario

Desplázate para empezar

### 13.3.1 Packet Tracer - Utilice ICMP para probar y corregir la conectividad de red

En este laboratorio utilizará ICMP para probar la conectividad de red y localizar problemas de red. También corregirá problemas de configuración simples y restaurará la conectividad a la red.

Use ICMP para localizar problemas de conectividad.

Configure los dispositivos de red para corregir problemas de conectividad.

**description** Utilice ICMP para probar y corregir la conectividad de red  
**file\_download** Utilice ICMP para probar y corregir la conectividad de red

### 13.3.2 Laboratorio - Use Ping y Traceroute para probar la conectividad de red.

Oportunidad de Práctica de habilidades

Usted tiene la oportunidad de practicar las siguientes habilidades:

- Part 1: Construcción y configuración de la red
- Part 2: Utilizar el comando ping para realizar pruebas de red básicas
- Part 3: Utilizar los comandos tracert y traceroute para realizar pruebas de red básicas
- Part 4: Solucionar problemas de la topología

Puede practicar estas habilidades utilizando el Packet Tracer o el equipo de laboratorio, si está disponible.

## Packet Tracer Physical Mode (PTPM)

**description** Usar Ping y Traceroute para probar la conectividad de red - Modo

Físico **file\_download** Usar Ping y Traceroute para probar la conectividad de red -  
Modo Físico

## Equipo de Laboratorio

**description** Use Ping y Traceroute para probar la conectividad de red

## 13.3.3 ¿Qué aprenderé en este módulo?

### Mensajes ICMP

El conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP. Estos mensajes se envían usando ICMP. El propósito de estos mensajes es proporcionar comentarios sobre problemas relacionados con el procesamiento de paquetes IP bajo ciertas condiciones. Los mensajes ICMP comunes a ICMPv4 e ICMPv6 son: Accesibilidad del host, Destino o Servicio inalcanzable y Tiempo excedido. Un mensaje ICMP Echo prueba la accesibilidad de un host en una red IP. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. Esta es la base de la **ping** utilidad. Cuando un host o puerta de enlace recibe un paquete que no puede entregar, puede usar un mensaje ICMP Destination Unreachable para notificar a la fuente. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete. Un enrutador utiliza un mensaje ICMPv4 Tiempo excedido para indicar que no se puede reenviar un paquete porque el campo Tiempo de vida (TTL) del paquete se redujo a cero. Si un enrutador recibe un paquete y disminuye el campo TTL a cero, descarta el paquete y envía un mensaje de Tiempo excedido al host de origen. ICMPv6 también envía un Tiempo Excedido en esta situación. ICMPv6 usa el campo de límite de salto de IPv6 para determinar si el paquete ha expirado. La **traceroute** herramienta utiliza los mensajes de tiempo excedido. Los mensajes entre un enrutador IPv6 y un dispositivo IPv6, incluida la asignación dinámica de direcciones, incluyen RS y RA. Los mensajes entre dispositivos IPv6 incluyen el redireccionamiento (similar a IPv4), NS y NA.

### Prueba con Ping y Traceroute

Ping (utilizado por IPv4 e IPv6) utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts. Para probar la conectividad con otro host de 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, el comando ping

proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. 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 viaje de ida y vuelta al destino. Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local. Haga ping a la dirección de bucle de retorno local de 127.0.0.1 para IPv4 (:: 1 para IPv6). Utilícelo **ping** para probar la capacidad de un host para comunicarse en la red local, haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. Un ping exitoso a la puerta de enlace predeterminada indica que el host y la interfaz del enrutador que sirven como puerta de enlace predeterminada están operativos en la red local. También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede ser un **ping** host IPv4 operativo de una red remota. Traceroute (tracert) genera una lista de saltos que se alcanzaron con éxito a lo largo del camino. Esta lista proporciona información de verificación y solución 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. El tiempo de ida y vuelta es el tiempo que tarda un paquete en llegar al host remoto y que la respuesta del host regrese. Traceroute utiliza una función del campo TTL en IPv4 y del campo límite de saltos de IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.