Packet Tracer - Use Ping y Traceroute para probar la conectividad de red - Modo Físico

Topología

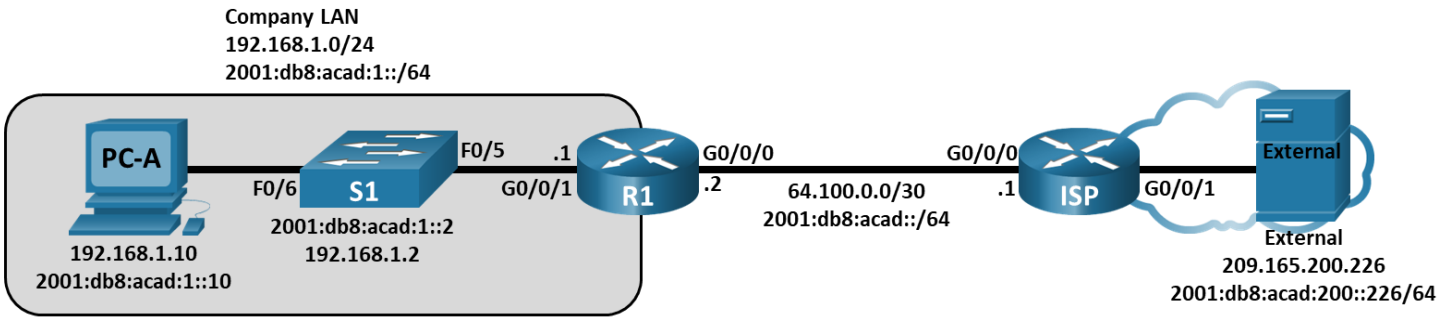

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1	G0/0/0	64.100.0.2 /30	N/D
		2001:db8:acad: :2 /64	
		fe80::2	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0/0	64.100.0.1 /30	N/A
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	209.165.200.225 /27	
		2001:db8:acad:200: :225 /64	
		fe80: :225	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001:db8:acad:1::2 /64	fe80::1
		fe80::2	
PC-A	NIC	2001:db8:acad:1: :10 /64	fe80::1
		192.168.1.10 /24	192.168.1.1

Dispositivo	Interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
Externo	NIC	209.165.200.226 /27	209.165.200.225
		2001:db8:acad:200::226 /64	fe80: :225

Objetivos

Parte 1: Utilizar el comando Ping para realizar pruebas de red básicas

Parte 2: Utilizar los comandos Tracert y Traceroute para realizar pruebas de red básicas

Parte 3: Solucionar problemas de la topología

Aspectos básicos/Situación

Ping y traceroute son dos herramientas imprescindibles para probar la conectividad de red TCP/IP. Ping es una utilidad de administración de redes que se utiliza para probar la accesibilidad de un dispositivo en una red IP. Esta utilidad también mide el tiempo de viaje de ida y vuelta para los mensajes que se envían desde el host de origen hasta un host de destino.

La utilidad traceroute es una herramienta de diagnóstico de red para mostrar la ruta y medir las demoras en el tránsito de los paquetes que viajan por una red IP.

En esta actividad de Packet Tracer de Modo Físico (PTPM), se examinan los comandos **ping** y **traceroute**, y se exploran las opciones de comandos para modificar el comportamiento de ambos. En esta actividad se utilizan dispositivos Cisco y PC para explorar los comandos. Las opciones disponibles para los comandos **ping** y **tracert** están limitadas en Packet Tracer. En esta actividad, se proporcionan las configuraciones necesarias para los dispositivos Cisco.

Instrucciones

Part 1: Utilizar el comando ping para realizar pruebas de red básicas

En esta parte de la actividad, utilice el comando **ping** para verificar la conectividad de extremo a extremo. Ping funciona mediante el envío de paquetes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP) al host de destino y la espera de una respuesta del ICMP. Puede registrar el tiempo de ida y vuelta y cualquier pérdida de paquetes o loops de enrutamiento.

Los paquetes IP tienen una vida útil limitada en la red. Los paquetes IPv4 utilizan un tiempo de vida (TTL) de 8 bits. Los paquetes IPv6 utilizan un valor de campo del encabezado Hop Limit (límite de salto). El TTL y el Hop Limit especifican el número máximo de saltos de Capa 3 que se pueden recorrer en la ruta hasta su destino. Cada host en una red establecerán el valor de 8 bits con un valor máximo de 255.

Cada vez que un paquete IP llega a un dispositivo de red de Capa 3, este valor se reduce en uno antes de que se reenvíe a su destino. Si este valor eventualmente llega a cero antes de alcanzar su destino, el paquete IP se descarta.

Examinará los resultados del comando **ping** y las opciones de ping adicionales que están disponibles en las PC de Packet Tracer y en los dispositivos Cisco.

Step 1: Pruebe la conectividad de red hacia R1 utilizando la PC-A.

Todos los pings desde la **PC-A** a otros dispositivos en la topología deberían ser exitosos. De lo contrario, revise la topología y el cableado, así como la configuración de los dispositivos Cisco y de las PC.

a. Desde la **PC-A**, haga ping al gateway predeterminado utilizando la dirección IPv4 (interfaz GigabitEthernet 0/0/1 de R1).

```
C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En este ejemplo, se enviaron cuatro solicitudes ICMP que tienen 32 bytes cada una. Las respuestas se recibieron en menos de un milisegundo sin pérdida de paquetes. El tiempo de transmisión y respuesta aumenta a medida que se procesan las solicitudes y respuestas de ICMP en más dispositivos a lo largo del trayecto hasta el destino final y desde él.

Esto también se puede hacer usando la dirección IPv6 del gateway predeterminado (interfaz GigabitEthernet 0/0/1 de R1).

```
C:\> ping 2001:db8:acad:1::1

Pinging 2001:db8:acad:1::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. Desde la **PC-A**, haga ping a las direcciones que figuran en la siguiente tabla y registre el tiempo promedio de ida y vuelta y el TTL de IPv4 o Hop Limit de IPv6.

Destino	Tiempo promedio de ida y vuelta (ms)	TTL/Límite de saltos
192.168.1.10		
2001:db8:acad:1: :10		
192.168.1.1 (**R1**)		
2001:db8:acad:1::1 (**R1**)		
192.168.1.2 (**S1**)		
2001:db8:acad:1::2(**S1**)		
64.100.0.2 (**R1**)		

Destino	Tiempo promedio de ida y vuelta (ms)	TTL/Límite de saltos
2001:db8:acad::2 (**R1**)		
64.100.0.1 (**ISP**)		
2001:db8:acad::1 (**ISP**)		
209.165.200.225 (**ISP** G0/0/1)		
2001:db8:acad:200::225 (**ISP** G0/0/1)		
209.165.200.226 (**External**)		
2001:db8:acad:200::226 (**External**)		

Step 2: Realice pings de S1 a External.

Desde **S1**, intente hacer ping a **ISP** y **External** usando direcciones IPv4 e IPv6.

¿Cuáles son los resultados de ping de S1 a ISP y External?

Part 2: Utilizar los comandos Tracert y Traceroute para realizar pruebas de red básicas

En las PC y los dispositivos de red, existen comandos para rastrear las rutas. En las PC con Windows, el comando **tracert** utiliza mensajes de ICMP para rastrear la ruta hacia el destino final. En dispositivos Cisco y PC del estilo de Unix, el comando **traceroute** utiliza los datagramas del Protocolo de Datagramas de Usuario (UDP) para rastrear las rutas hacia el destino final.

En esta parte, examinará los comandos traceroute y determinará la ruta de un paquete hasta el destino final. Utilizará el comando **tracert** en las PCs y el comando **traceroute** en los dispositivos Cisco. También examinará las opciones disponibles para ajustar los resultados de traceroute.

Step 1: Desde la PC-A, use el comando tracert a External.

a. En el Command Prompt (Símbolo del sistema) de **PC-A**, escriba **tracert 209.165.200.226**.

```
C:\ > tracert 209.165.200.226

Tracing route to 209.165.200.226 over a maximum of 30 hops:

  1 * * 1 ms 192.168.1.1
  2 * 0 ms 0 ms 64.100.0.1
  3 0 ms * 0 ms 64.100.0.1
  4 * 11 ms * Request timed out.
  5 0 ms * 0 ms 64.100.0.1
Control-C
^C
C:\>
```

Nota: Puede detener el trace route presionando **Ctrl-C**.

Los resultados de **tracert** indican la ruta desde PC-A a External va de PC-A a R1 a ISP y no logra llegar a Eternal. Los resultados del **tracert** indican un problema en el router ISP.

b. Repita el comando tracert utilizando la dirección IPv6. En el command prompt (símbolo del sistema), escriba **tracert 2001:db8:acad:200::226**.

Step 2: Utilice el comando traceroute del switch S1 a External.

Desde**S1**, escriba **traceroute 209.165.200.226** o **traceroute 2001:db8:acad:200::226**.

Nota: Para detener el **traceroute**, pulse **Ctrl-Shift-6**.

```
S1# traceroute 209.165.200.226
```

El comando **traceroute** tiene opciones adicionales. Puede utilizar el símbolo **?** o, simplemente, presione **Enter** después de escribir **traceroute** en la petición de entrada para explorar estas opciones.

Nota: Las opciones disponibles están limitadas en Packet Tracer.

En el siguiente enlace, se proporciona más información sobre los comandos **ping** y **traceroute** para dispositivos Cisco:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Part 3: Corrija el problema de conectividad de red en el ISP.

Step 1: Acceda a la ubicación de red donde se está produciendo el problema de conectividad.

A partir de los pasos anteriores, había determinado que había un problema en el router **ISP** usando los comandos **ping** y **traceroute**. Tiene acceso SSH remoto a todos los dispositivos de red utilizando nombre de usuario **admin** y contraseña **class**.

a. Desde el terminal de **S1**, haga SSH al router **ISP** usando la interfaz G0/0/0 para corregir el problema.

```
C:\> ssh -l admin 64.100.0.1
```

b. Utilice los comandos **show** para examinar las configuraciones en ejecución del router **ISP**.

Los resultados de los comandos **show run** y **show ip interface brief** indican que el estado de la interfaz GigabitEthernet 0/0/1 es up/up (activo/activo), pero se configuró con una dirección IP incorrecta.

c. Corrija los problemas encontrados. Desde el símbolo del sistema en **PC-A**, copie y pegue la siguiente configuración en el router **ISP** para corregir el problema en la sesión SSH en el router **ISP** .

```
configure terminal
interface g0/0/1
 no ip address 192.168.8.1 255.255.255.0
 ip address 209.165.200.225 255.255.255.224
 no ipv6 address 2001:db8:acad:201::225/64
 ipv6 address 2001:db8:acad:200::225/64
 ipv6 address fe80::225 link-local
no shutdown
```

d. Salga de la sesión SSH cuando termine.

Step 2: Verifique la conectividad de extremo a extremo

Desde el símbolo del sistema de **PC-A** , utilice los comandos **ping** y **tracert** para verificar la conectividad de extremo a extremo con el servidor externo en 209.165.200.226 y 2001:db8:acad:200:: 226.

Part 4: Uso de los comandos de ping extendido

Step 1: Use el comando ping extendido en la PC-A.

El comando **ping** predeterminado envía cuatro solicitudes de 32 bytes cada una. Espera 4000 milisegundos (4 segundos) la devolución de cada respuesta y, luego, muestra el mensaje “Request timed out (Tiempo de espera agotado)”. Se puede ajustar el comando **ping** para resolver los problemas de una red.

a. En el símbolo del sistema, escriba **ping** y presione **Enter**.

```
C:\ > ping
```

b. Mediante la opción **–t**, haga ping a External para verificar que External sea accesible. La opción **-t** hará ping continuamente al objetivo hasta que sea detenido. Utilicen **Ctrl+C** para detener el ping.

```
C:\> ping –t 209.165.200.226
```

c. Para ilustrar los resultados cuando no se puede acceder a un host, apague la interfaz GigabitEthernet 0/0/1 en el router **ISP**. Desde el switch **S1**, haga SSH a la interfaz G0/0/0 de **ISP**. Use la contraseña **class**

```
S1# ssh -l admin 64.100.0.1
```

d. Utilice el comando **shutdown** para desactivar la interfaz GigabitEthernet 0/0/1 en el router **ISP**.

Mientras la red funciona correctamente, el comando**ping** puede determinar si el destino respondió y cuánto tardó en recibir una respuesta del destino. Si existe un problema de conectividad de red, el comando **ping** muestra un mensaje de error.

e. Active la interfaz GigabitEthernet 0/0/1 en el router **ISP** (utilizando el comando **no shutdown**) antes de pasar al siguiente paso. Después de 30 segundos aproximadamente, el ping debería volver a ser correcto.

f. Presione **Ctrl+C** para detener el comando **ping**.

g. Los pasos anteriores se pueden repetir para la dirección IPv6 para obtener el mensaje de error ICMP.

¿Qué mensajes de error de ICMP recibió?

h. Active la interfaz GigabitEthernet 0/0/1 en el router **ISP** (utilizando el comando **no shutdown**) antes de pasar al siguiente paso. Después de 30 segundos aproximadamente, el ping debería volver a ser correcto.

Step 2: Probar la conectividad de red desde R1 por medio de dispositivos Cisco.

El comando **ping** también está disponible en los dispositivos Cisco. En este paso, el comando **ping** se examina usando el **R1** y **S1**.

a. Desde **R1**, haga ping a **External** en la red externa usando la dirección IP 209.165.200.226

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

El signo de exclamación (**!**) indica que el ping se realizó correctamente desde el router **R1** a **External**. El viaje de ida y vuelta dura un promedio de 1 ms sin pérdida de paquetes, como indica una tasa de éxito del 100%.

b. Debido a que se configuró una tabla de host local en **R1**, puede hacerle ping a **Externalv4** en la red externa utilizando el nombre de host configurado desde **R1**.

```
R1# ping Externalv4
```

¿Cuál es la dirección IP utilizada?

c. En el modo EXEC privilegiado, hay más opciones disponibles para el comando **ping**. En el símbolo del sistema, escriba **ping** y presione **Enter**. Use **ipv6** como protocolo. Escriba **2001:DB8:ACAD:200::226** o **External** para la dirección IPv6 de destino. Presione **Enter** para aceptar el valor predeterminado para las otras opciones.

```
R1# ping
Protocol [ip]: ipv6
Dirección IPv6 de destino: 2001:db8:acad:200: :226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:200::226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

d. Puede utilizar un ping extendido para observar cuando hay un problema de red. Inicie el comando **ping** a 209.165.200.226 con un conteo de repetición de 500. A continuación, apague la interfaz GigabitEthernet 0/0/1 en el router **ISP** .

Desde la sesión SSH al **ISP** en el switch **S1**, deshabilite la interfaz GigabitEthernet 0/0/1 en el **ISP**.

e. Desde la sesión SSH, encienda la interfaz GigabitEthernet 0/0/1 en **ISP** despues de que los signos de exclamación (**!**) hayan sido reemplazado por la letra **U** y puntos (**.**). Después de 30 segundos aproximadamente, el ping debería volver a ser correcto. Presione **Ctrl+Shift+6** para detener el comando **ping**.

```
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 50000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.U.
U.U.................!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
```

```
Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms
```

La letra **U** en los resultados indica que el destino es inaccesible. **R1**recibió un PDU de error. Cada punto (**.**) en el resultado indica que el ping agotó el tiempo de espera mientras esperaba una respuesta de **External**. En este ejemplo, el 1% de los paquetes se perdieron durante la interrupción de la red simulada.

El comando **ping** es extremadamente útil para solucionar problemas en la conectividad de red. Sin embargo, el comando **ping** no puede indicar la ubicación del problema cuando un **ping** no es exitoso . El comando **tracert** (o **traceroute**) puede mostrar la latencia de la red y la información sobre la ruta.

f. En la ventana de actividad PT, haga clic en **Comprobar resultados para comprobar** que todos los elementos de evaluación y las pruebas de conectividad son correctos.

Preguntas de reflexión

1. ¿Qué podría evitar que las respuestas de los comandos **ping** o **traceroute** regresen al dispositivo de origen, además de problemas de conectividad de red?

2. Si hace **ping** a una dirección inexistente en la red remota, como 209.165.200.227, ¿cuál es el mensaje que muestra el comando **ping**? ¿Qué significa esto? Si hace **ping** a una dirección de host válida y recibe esta respuesta, ¿qué debe revisar?

3. Si hace **ping** a una dirección que no existe en ninguna red de su topología, como 192.168.5.2, desde una PC con Windows ¿cuál es el mensaje que muestra el comando **ping**? ¿Qué significa este mensaje?