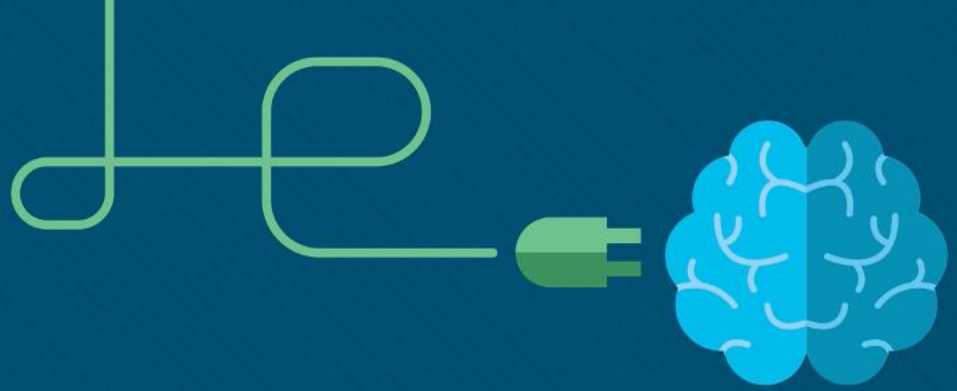


Módulo 29: ICMP

Fundamentos de Redes 3.0

Objetivos del Módulo

Título del Módulo: ICMP

Objetivo del Módulo: Usar varias herramientas para probar la conectividad de la red.

Título del Tema	Objetivo del Tema
Mensajes ICMP	Explicar la forma en que se usa ICMP para probar la conectividad de red.
Pruebas de Ping y Traceroute	Utilizar las utilidades ping y traceroute para probar la conectividad de red.

29.1 Mensajes ICMP

Mensajes ICMPv4 e ICMPv6

- Aunque IP es sólo un protocolo de mejor 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 y el propósito de estos mensajes es proporcionar comentarios sobre problemas relacionados con el procesamiento de paquetes IP bajo ciertas condiciones.

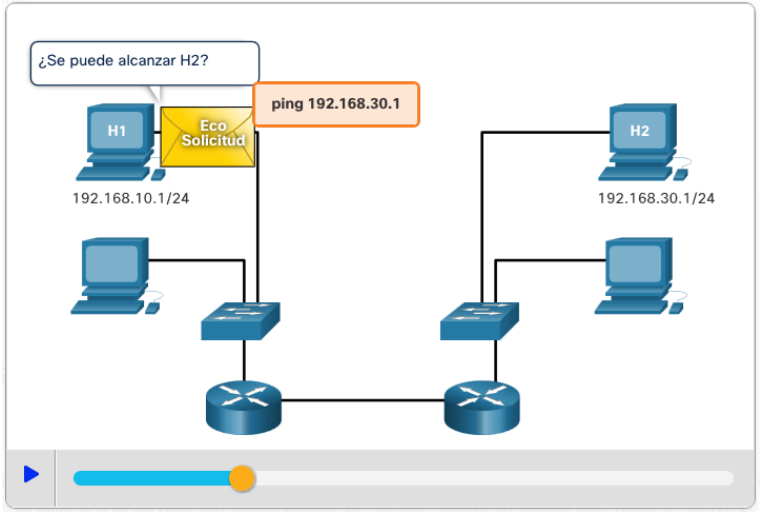
- Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

- 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.

- Los mensajes ICMP comunes a ICMPv4 e ICMPv6 y discutidos en este módulo incluyen:
  - Accesibilidad al Host
  - Destino o Servicio Inalcanzable
  - Tiempo Excedido

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 de Eco de ICMP es la base de la utilidad **ping**.



Destino o Servicio Inalcanzable

- Cuando un host o puerta de enlace 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 - Dirección inalcanzable
  - 4 - Puerto inalcanzable

Tiempo Excedido

- Los enrutadores utilizan los mensajes de Tiempo Excedido 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 enrutador 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 excedido si el enrutador 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.

Nota: Los mensajes de Tiempo Excedido son utilizados por la herramienta **traceroute**.

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.

- Los mensajes ICMPv6 están encapsulados en IPv6.

- ICMPv6 incluye cuatro mesajes 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:
  - Mensaje de Solicitud de Router (RS)
  - Mensaje de Anuncio de Router (RA)

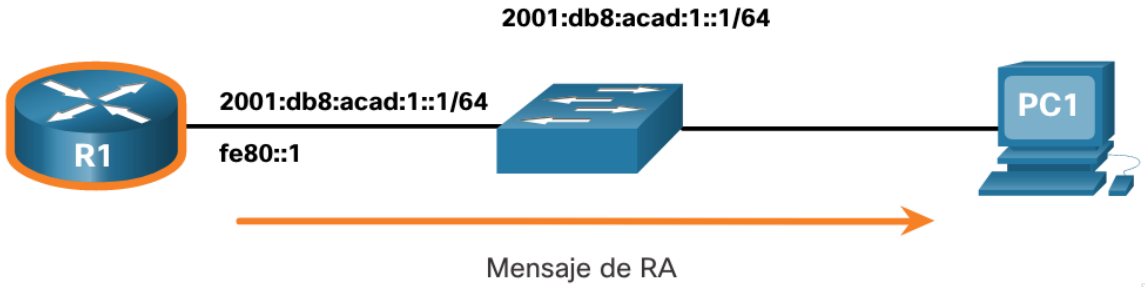
- Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son:
  - Mensaje de Solicitud de Vecino (NS)
  - Mensaje de Anuncio de Vecino (NA)

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

Mensajes ICMPv6 (continuación)

Mensaje de RA

- 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 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.»



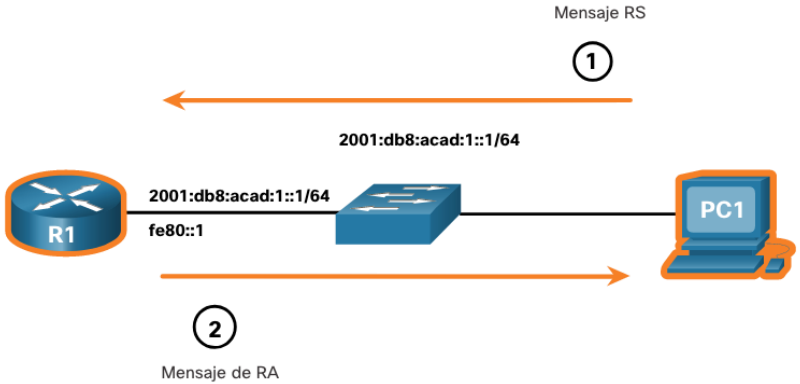
Mensajes ICMPv6 (continuación)

Mensaje de RS

- Un enrutador habilitado para IPv6 también enviará un mensaje RA en respuesta a un mensaje RS.
- En la figura, PC1 envía un mensaje RS para determinar cómo recibir dinámicamente su información de dirección IPv6.

- R1 responde a la RS con un mensaje de RA.
  1. PC1 envía un mensaje RS: «Hola, acabo de arrancar. ¿Hay un router IPv6 en la red? Necesito saber cómo obtener la información de mi dirección IPv6 de forma dinámica».

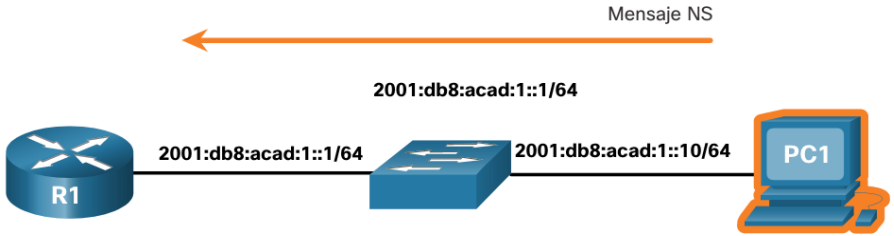
  2. R1 responde con un mensaje de RA. «Hola a todos los dispositivos habilitados para IPv6. Soy R1 y puedes usar SLAAC para crear una dirección de unidifusión global IPv6. El prefijo es 2001:db8:acad:1::/64. Por cierto, use mi dirección local de enlace fe80::1 como su puerta de enlace predeterminada.»



Mensajes ICMPv6 (continuación)

Mensaje de NS

- Cuando a un dispositivo se le asigna una dirección de unidifusión global IPv6 o unidifusión de enlace local, puede realizar una detección de dirección duplicada (DAD) para garantizar que la dirección IPv6 sea única.
- Para verificar la unicidad de una dirección, el dispositivo enviará un mensaje NS con su propia dirección IPv6 como la dirección IPv6 objetivo, como se muestra en la figura.
- Si otro dispositivo de la red tiene esta dirección, responderá con un mensaje NA.
- Este mensaje NA notifica al dispositivo emisor que la dirección está en uso.
- Si no se devuelve un mensaje NA correspondiente dentro de un cierto período de tiempo, la dirección de unidifusión es única y aceptable para su uso.



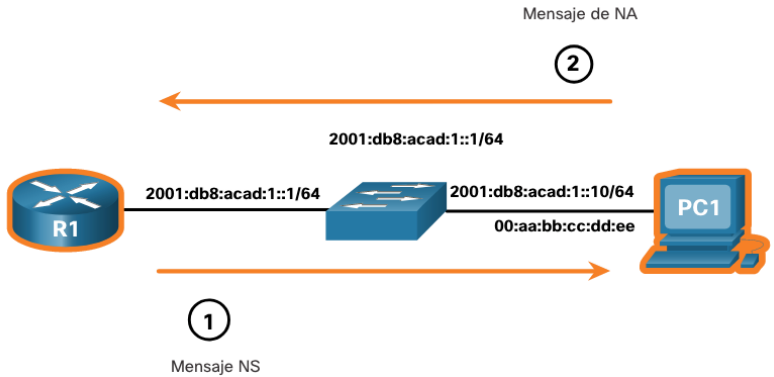
- PC1 envía un mensaje NS para comprobar que una dirección sea única, «¿Quién tenga la dirección IPv6 2001:db8:acad:1::10, envíeme su dirección MAC?»

Mensajes ICMPv6 (continuación)

Mensaje de NA

- La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de unidifusión 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 se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet.

- En la figura, R1 envía un mensaje NS a 2001:db8:acad:1: :10 pidiendo su dirección MAC.
  1. R1 envía un mensaje NS de resolución de dirección. «¿Quién tenga la dirección IPv6 2001:db8:acad:1::10, envíeme su dirección MAC?»
  2. PC1 responde con un mensaje NA. «Soy 2001:db8:acad:1::10 y mi dirección MAC es 00:aa:bb:cc:dd:ee.»



29.2 Pruebas de Ping y Traceroute

Ping - Prueba de Conectividad

- Ping es una utilidad de prueba de IPv4 e IPv6 que utiliza los mensajes de ICMP solicitud de eco y 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.
- Esto puede ser una medida del rendimiento de la red.

Ping - Prueba de Conectividad (continuación)

- 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.

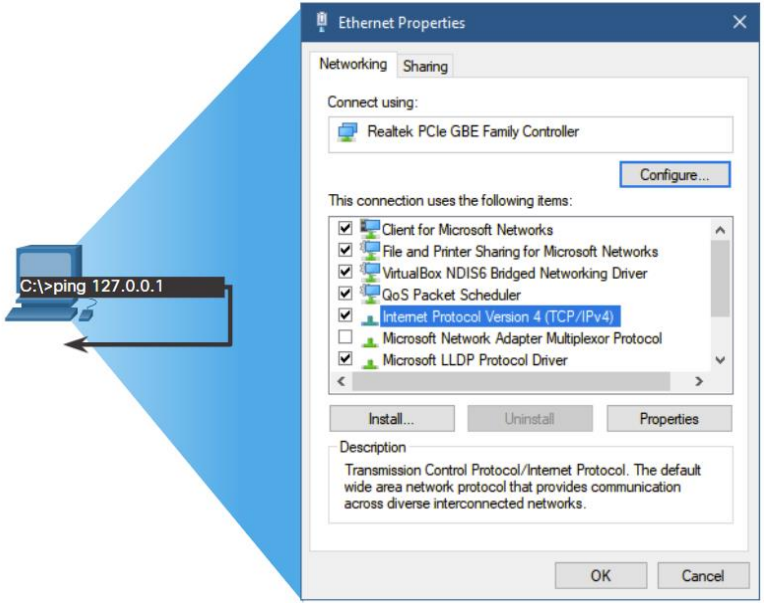
- Es común que el primer ping se agote si es necesario realizar la resolución de direcciones (ARP o ND) antes de enviar la Solicitud de Eco ICMP.

- 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.

- Los tipos de pruebas de conectividad que se realizan con **ping** son los siguientes:
  - Hacer ping al bucle invertido
  - Hacer ping a la puerta de enlace predeterminada
  - Hacer ping al host remoto

Ping al Bucle Invertido

- Ping se puede usar para probar la configuración interna de IPv4 o IPv6 en el host local.
- Para realizar esta prueba, se debe hacer ping a la dirección de bucle invertido local 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 y no es una indicación de que las direcciones, las máscaras o las puertas de enlace estén configuradas correctamente.
- Tampoco indica nada acerca del estado de la capa inferior de la pila de red.
- Un mensaje de error indica que TCP/IP no funciona en el host.
- 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.

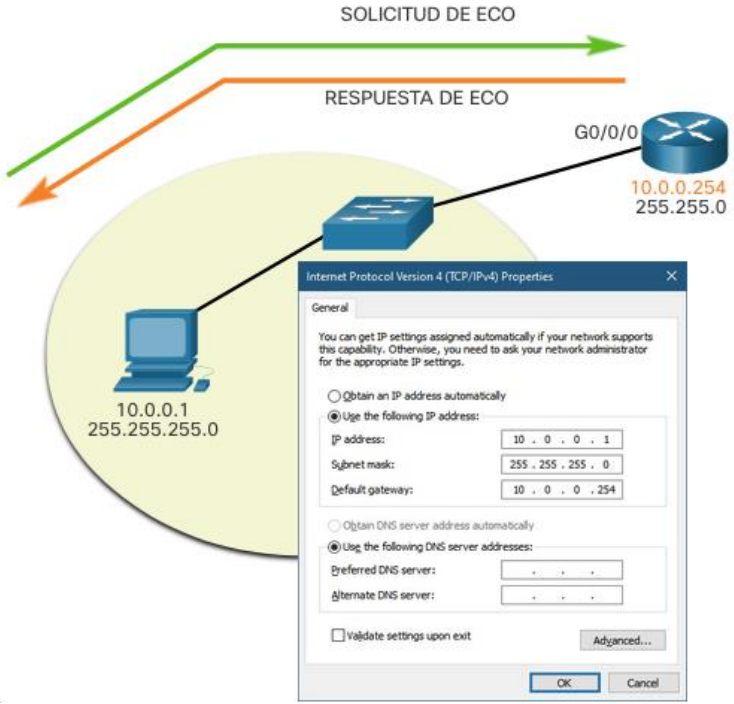


Ping a la Puerta de Enlace Predeterminada

- **Ping** también se puede usar 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 router que sirven 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 router normalmente siempre está operativo.
- Si la dirección de puerta de enlace predeterminada no responde, se puede enviar un **ping** a la dirección IP de otro host en la red local que se sabe que está operativo.
- Si la puerta de enlace predeterminada u otro host responde, entonces el host local puede comunicarse con éxito a través de la red local.

Ping a la Puerta de Enlace Predeterminada (continuación)

- 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 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.



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.
- 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 **ping** exitoso a través de 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.
- Además, se puede verificar la funcionalidad del host remoto.
- Si el host remoto no pudiera comunicarse fuera de su red local, no habría respondido.

Nota: Muchos administradores de redes limitan o prohíben la entrada de mensajes ICMP a la red de la empresa; por lo tanto, la falta de una respuesta de **ping** puede ser por razones de seguridad.

Traceroute - Probar el Camino

- 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 el tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si un salto no responde.
  - Es el tiempo que tarda un paquete en llegar al host remoto y para que regrese la respuesta del host.
  - Un asterisco (*) indica un paquete perdido o sin respuesta y se puede usar para ubicar 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.

Traceroute - Probar el Camino (continuación)

- **TTL de IPv4 y Límite de Saltos de IPv6**
  - Traceroute utiliza una función del campo TTL en IPv4 y el campo Límite de Saltos en IPv6 en los encabezados de la capa 3, junto con el mensaje ICMP Tiempo Excedido.
  - 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 enrutador.
  - Este router responde con un mensaje ICMPv4 Tiempo Excedido.
  - Traceroute ahora tiene la dirección del primer salto.
  - Luego, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes, proporcionando al rastreo la dirección de cada salto a medida que los paquetes se agotan más adelante en la ruta.
  - El campo TTL continúa incrementándose hasta que se alcanza el destino, o se incrementa hasta un máximo predefinido.
  - Una vez que se alcanza el destino final, el host responde con un mensaje ICMP Puerto Inalcanzable o un mensaje ICMP Respuesta de Eco en lugar del mensaje ICMP Tiempo Excedido.

Packet Tracer - Verifique el Direccionamiento IPv4 e IPv6

En esta actividad, cumplirá los siguientes objetivos:

- Pruebe y restaure la conectividad IPv4
- Pruebe y restaure la conectividad IPv6

Packet Tracer - Use Ping y Traceroute para Probar la Conectividad de Red

En esta actividad, cumplirá los siguientes objetivos:

- Completar la documentación de la tabla de direccionamiento
- Probar la conectividad mediante el comando ping
- Descubrir la ruta mediante su rastreo

29.3 Resumen de ICMP

Packet Tracer - Utilice ICMP para Probar y Corregir la Conectividad de Red

En esta actividad de Packet Tracer, completará los siguientes objetivos:

- Use ICMP para localizar problemas de conectividad.
- Configure los dispositivos de red para corregir problemas de conectividad.

¿Qué Aprendí en este Módulo?

- Aunque IP es sólo un protocolo de mejor esfuerzo, el conjunto TCP/IP proporciona mensajes de error y mensajes informativos cuando se comunica con otro dispositivo IP.
- El protocolo de mensajes para IPv4 es ICMPv4.
- ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional.
- Se puede utilizar un mensaje de eco ICMP para probar la accesibilidad de un host en una red IP.
- Si el host se encuentra disponible, el host de destino responde con una respuesta de eco.
- Cuando un host o puerta de enlace recibe un paquete que no puede entregar, puede usar un mensaje de destino inalcanzable de ICMP para notificar a la fuente que el destino o servicio es inalcanzable e incluye un código que indica por qué no se pudo entregar el paquete.
- Los enrutadores utilizan los mensajes de Tiempo Excedido 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 enrutador recibe un paquete y disminuye el campo TTL del paquete IPV4 a cero, descarta el paquete y envía un mensaje de Tiempo Excedido al host de origen.
- ICMPv6 también envía un mensaje de Tiempo Excedido si el enrutador no puede reenviar un paquete IPv6 debido a que el paquete caducó.
- ICMPv6 es muy similar a los mensajes de control y error implementados por ICMPv4, pero ICMPv6 incluye cuatro nuevos protocolos como parte de ND o NDP: mensaje RS, mensaje RA, mensaje NS y mensaje NA.

¿Qué Aprendí en este Módulo? (continuación)

- 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.
- Esto puede ser una medida del rendimiento de la red.
- 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.
- El tipo de pruebas de conectividad realizadas con ping incluye hacer ping al bucle invertido local, hacer ping en la puerta de enlace predeterminada y hacer ping en el host remoto.
- **tracert** es una utilidad que genera una lista de saltos que se alcanzaron con éxito a lo largo de la ruta, lo que brinda información importante de verificación y resolución de problemas.
- Si los datos alcanzan el destino, el rastreo lista la interfaz de cada enrutador en el camino entre los hosts.
- Si los datos fallan en algún salto en el camino, la dirección del último enrutador que respondió al rastreo puede proporcionar una indicación de dónde se encuentran el problema o las restricciones de seguridad.
- 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.