

UD1. Comandos

Índice

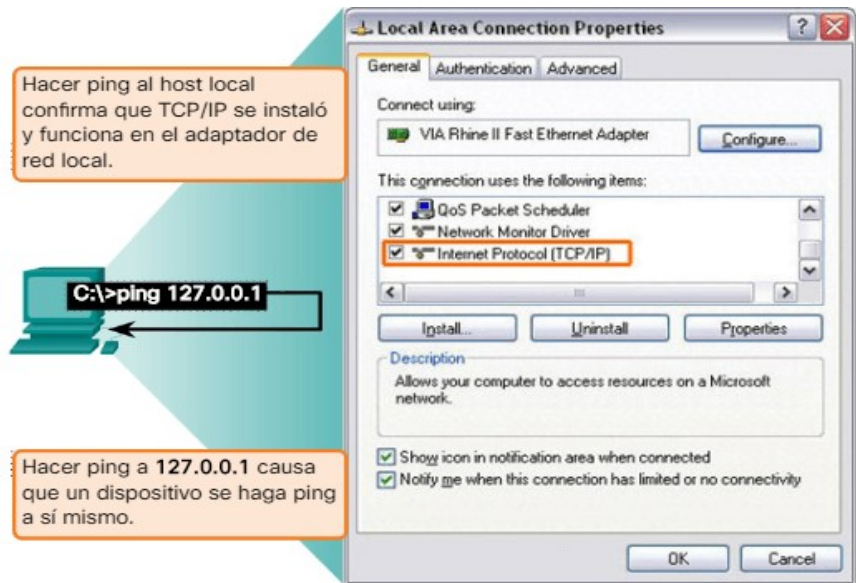
ping.....	2
Prueba de loopback.....	2
Ping extendido.....	3
Traceroute.....	4
ipconfig.....	5
arp.....	6

ping

El comando ping es una manera eficaz de probar la conectividad. Por lo general, a esta prueba se la conoce como “prueba del stack de protocolos”, porque el comando ping va desde la capa 3 del modelo OSI hasta la capa 2 y, luego, hasta la capa 1. Este comando utiliza el protocolo ICMP para verificar la conectividad.

El comando ping no siempre identifica la naturaleza de un problema, pero puede contribuir a identificar su origen, un primer paso importante en la resolución de problemas de una falla de red.

El comando ping proporciona un método para probar el stack de protocolos y la configuración de direcciones IPv4 en un host, así como para probar la conectividad a los hosts de destino local o remoto, como se muestra en la ilustración.



Un **ping** emitido desde el IOS de CISCO tiene como resultado una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:

- **!** (signo de exclamación): indica la recepción de un mensaje de respuesta de eco ICMP. Indica que el ping se completó correctamente y verifica la conectividad de capa 3.
- **.** (punto): indica que se agotó el tiempo mientras se esperaba un mensaje de respuesta de eco ICMP. Puede indicar problemas en la comunicación. Puede señalar que se produjo un problema de conectividad en alguna parte de la ruta. También puede indicar que un router de la ruta no contaba con una ruta hacia el destino y no envió un mensaje de ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo.
- **U**: se recibió un mensaje ICMP inalcanzable. Indica que un router de la ruta no contaba con una ruta hacia la dirección de destino o que se bloqueó la solicitud de ping y se respondió con un mensaje de ICMP de destino inalcanzable.

Prueba de loopback

El comando ping se utiliza para verificar la configuración IP interna en el host local. Recuerde que esta prueba se realiza utilizando el comando ping en una dirección reservada denominada “**dirección de loopback**” (127.0.0.1). Esto verifica que el stack de protocolos funcione correctamente desde la capa de red hasta la capa física y viceversa, sin colocar realmente una señal en los medios.

Los comandos ping se introducen en una línea de comandos.

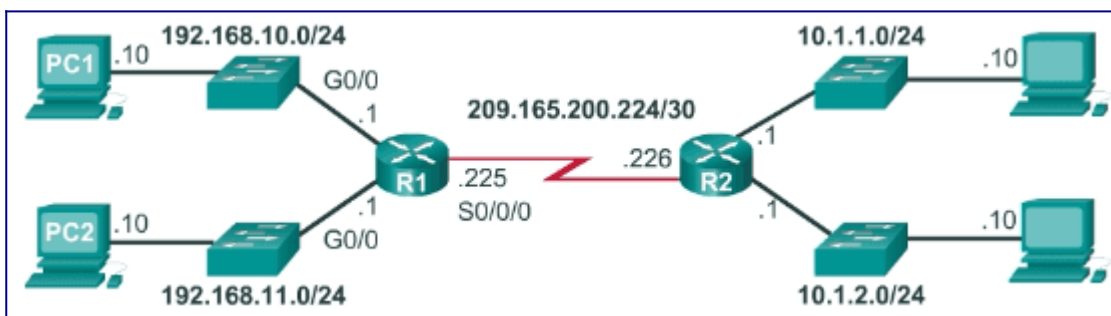
Utilice la siguiente sintaxis para hacer ping a la dirección de loopback: **c:\> ping 127.0.0.1**

El resultado indica por cada línea que se envió un paquete de prueba de 32 bytes desde el host 127.0.0.1 y se devolvieron a este en un tiempo de menos de 1 ms. TTL son las siglas de tiempo de vida, que define la cantidad de saltos que le restan al paquete ping antes de que se descarte.

Ping extendido

Cisco IOS ofrece un modo “extendido” del comando **ping**.

- Se ingresa a este modo escribiendo **ping** en el modo EXEC privilegiado sin una dirección IP de destino.
- Luego, se presenta una serie de peticiones de entrada, como se muestra en el siguiente ejemplo.
- Al presionar Intro se aceptan los valores predeterminados indicados.



El siguiente ejemplo muestra cómo forzar que la dirección de origen para un ping sea 10.1.1.1 (observe el R2 en la ilustración); la dirección de origen para un ping estándar sería 209.165.200.226.

De esta manera, el administrador de red puede verificar de forma remota (desde el R2) que el R1 tenga la ruta 10.1.1.0/24 en su tabla de enrutamiento.

```
R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms
```

traceroute

Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red. La forma del comando depende de dónde se emita el comando.

Cuando lleve a cabo el rastreo desde un equipo Windows, utilice **tracert**. Cuando lleve a cabo el rastreo desde la CLI de un router o desde un equipo linux, utilice **traceroute**.

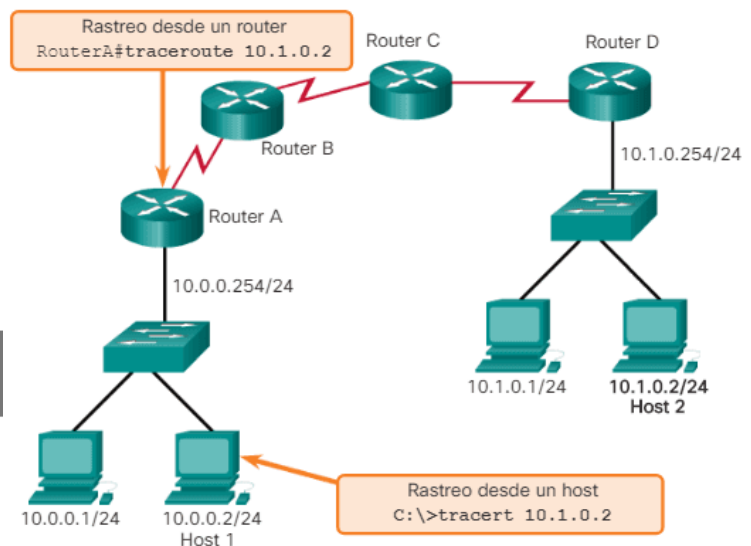
Al igual que los comandos ping, los comandos trace se introducen en la línea de comandos y llevan una dirección IP como argumento.

Aquí, sobre la base de que el comando se emite desde un equipo Windows, se utiliza la forma tracert:

```
C:\> tracert 10.1.0.2
```

Y a continuación el resultado por ejemplo:

```
1 2 ms 2 ms 2 ms 10.0.0.254
2 * * * Tiempo de espera agotado.
3 * * * Tiempo de espera agotado.
4 ^C
```



La única respuesta correcta fue la del gateway del router A. El tiempo de espera para las solicitudes de trace se agotó, lo que significa que el router de siguiente salto no respondió. Los resultados del comando trace indican que la falla entonces se encuentra en la internetwork más allá de la LAN.

ipconfig

La dirección IP de un host se puede ver emitiendo el comando **ipconfig** en la línea de comandos de un equipo Windows o **ip a** desde un equipo linux

El servicio del cliente DNS en las PC de Windows optimiza el rendimiento de la resolución de nombres DNS almacenando previamente los nombres resueltos en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows.




```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

Leyenda

-  Dirección IP para este equipo host
-  Máscara de subred de la red local
-  Dirección de gateway predeterminado para este equipo host

Una herramienta para analizar la dirección MAC de una PC es **ipconfig /all**. Observe que, la dirección MAC de la PC ahora aparece junto con varios detalles relacionados con el direccionamiento de capa 3 del dispositivo.

Además, se puede identificar el fabricante de la interfaz de red en la PC mediante la porción de OUI de la dirección MAC. Esto se puede investigar en Internet.

```
C:\>ipconfig /all

Ethernet adapter Network Connection:

    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                             2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                             2007 6:57:11 AM

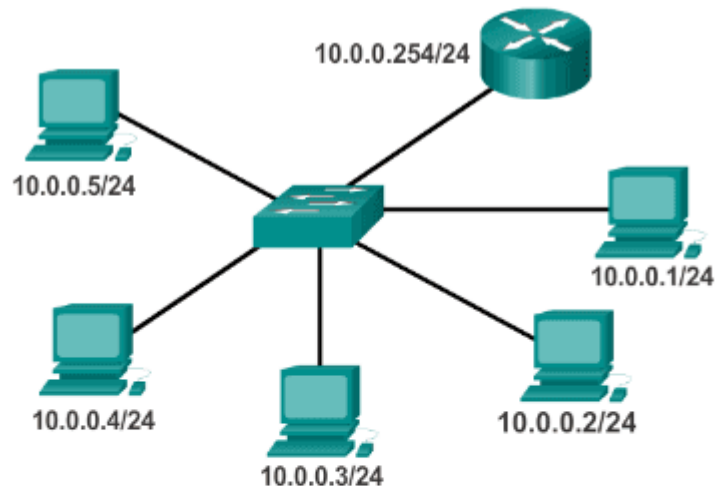
C:\>
```

arp

El comando arp permite crear, editar y mostrar las asignaciones de direcciones físicas a direcciones IPv4 conocidas. Este comando se ejecuta desde el símbolo del sistema de Windows.

Para ejecutar un comando arp, introduzca lo siguiente en el símbolo del sistema de un host:

```
C:\host1> arp -a
```



```
c:\>arp -a
Internet Address Physical Address Type
10.0.0.2          00-08-a3-b6-ce-04 dynamic
10.0.0.3          00-0d-56-09-fb-d1 dynamic
10.0.0.4          00-12-3f-d4-6d-1b dynamic
10.0.0.254       00-10-7b-e7-fa-ef dynamic
```

Par de direcciones IP
y MAC

El comando **arp -a** enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché mediante el comando **arp -d** en caso de que el administrador de red desee volver a llenarla con información actualizada.

Route

Trabaja con la tabla de enrutamiento

en windows:

route [/f] [/p] [<command>] [<destination>] [mask <netmask>] [<gateway>] [metric <metric>]] [if <interface>]]

<command>

- **add:** agrega una ruta.
- **change:** modifica una ruta existente.
- **delete:** elimina una o varias rutas.
- **print:** imprime una o varias rutas.

<destination> Especifica el destino de red de la ruta. El destino puede ser una dirección de red IP (donde los bits de la dirección de red se establecen en 0), una dirección IP para una ruta de host, o 0.0.0.0 para la ruta predeterminada.

En linux

```
route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.1.1 dev enp0s3
```

Route print imprime la tabla de enrutamiento en windows **route -n** en linux

netstat

Muestra las conexiones TCP activas, los puertos en los que escucha el equipo, las estadísticas de Ethernet, la tabla de enrutamiento IP, las estadísticas IPv4 (para los protocolos IP, ICMP, TCP y UDP) y las estadísticas de IPv6 (para los protocolos IPv6, ICMPv6, TCP a través de IPv6 y UDP a través de IPv6). Se usa sin parámetros; este comando muestra conexiones TCP activas.

Parámetro	Descripción
-a	Muestra todas las conexiones TCP activas y los puertos TCP y UDP en los que escucha el equipo.
-b	Muestra el ejecutable implicado en la creación de cada conexión o puerto de escucha.
-E	Muestra estadísticas Ethernet, como el número de bytes y paquetes enviados y recibidos. Este parámetro se puede combinar con -s .
-n	Muestra las conexiones TCP activas, pero las direcciones y los números de puerto se expresan en forma de número y no se intenta determinar los nombres.
-o	Muestra las conexiones TCP activas e incluye el identificador de proceso (PID) para cada conexión. Este parámetro se puede combinar con -a , -n y -p .
-r	Muestra el contenido de la tabla de enrutamiento de IP. Esto equivale al comando route print.

