Práctica de laboratorio: Herramientas de resolución de problemas de red

Objetivos

Parte 1: Iniciar la máquina virtual de DEVASC.

Parte 2: Explorar la herramienta de solución de problemas ifconfig

Parte 3: Explorar la herramienta de solución de problemas de ping

Parte 4: Explorar la herramienta de solución de problemas de traceroute

Parte 5: Explorar la herramienta de solución de problemas de nslookup

Aspectos básicos/Situación

En el esfuerzo por solucionar problemas de conexión de red, es importante que un desarrollador comprenda cómo usar las herramientas básicas de solución de problemas de red. Estas herramientas se utilizan para determinar cuál podría ser el problema de conexión.

Recursos necesarios

- Una computadora con el sistema operativo de su elección.
- VirtualBox o VMware.
- Máquina virtual (Virtual Machine) DEVASC.

Instrucciones

Parte 1: Inicie la máquina virtual de DEVASC.

Si aún no ha completado el **Laboratorio: Instale el Entorno de Laboratorio de Máquina Virtual**, hágalo ahora. Si ya ha completado el laboratorio, inicie la **Máquina virtual (Virtual Machine) DEVASC**

Parte 2: Explore la herramienta de solución de problemas ifconfig

La herramienta **ifconfig** es una aplicación para su uso con sistemas operativos basados en UNIX como Linux. Una utilidad similar está disponible en Windows llamada ipconfig. Estas aplicaciones se utilizan para administrar interfaces de red desde la línea de comandos. Puede usar ifconfig para lograr lo siguiente:

- Configurar la dirección IP y la máscara de subred para una interfaz.
- Recuperar el estado de las interfaces de red.
- Habilitar o deshabilitar interfaces de red.
- Cambiar la dirección MAC de una interfaz de red.

Paso 1: Ver las opciones ifconfig.

La herramienta **ifconfig** tiene muchas opciones diferentes que se pueden agregar al comando para realizar tareas específicas.

a. Abra una ventana de terminal directamente desde el escritorio o dentro de VS Code.

b. Escriba **ifconfig —help** para ver todas las opciones disponibles para el comando.

```
devasc @labvm: ~$ ifconfig —help
Uso:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast [<address>]] [[-] puntopunto [<address>]]
  [netmask <address>] [dstaddr <address>] [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>] [mtu <NN>]
  [[-] remolques] [[-] arp] [[-] allmulti]
  [multidifusión] [[-] promisc]
  [mem_start <NN>] [io_addr <NN>] [irq <NN>] [medios <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...
```

Esta es una visión general de algunas de las opciones más utilizadas;

- **add** or **del** - Esta opción le permite agregar o eliminar direcciones IP y su máscara de subred (longitud del prefijo).
- **hw ether** - Esto se utiliza para cambiar la dirección MAC física. Esto podría ser útil, por ejemplo, para cambiarlo a un nombre fácilmente reconocible para que se destaque en los registros para solucionar problemas.
- **arriba** y **abajo** - Estas opciones se utilizan para habilitar y deshabilitar interfaces. Asegúrese de qué interfaz está deshabilitando. Si es el que está utilizando para conectarse de forma remota a un dispositivo, ¡se desconectará!

Paso 2: Vea el estado de todas las interfaces.

a. Mostrar el estado de todas las interfaces de red en uso mediante la ejecución del comando **ip addr** por sí mismo.

```
devasc @labvm: ~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 08:00:27:e9:3d:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85901sec preferred_lft 85901sec
    inet6 fe80::a00:27ff:fee9:3de6/64 scope link
       valid_lft forever preferred_lft forever
3: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/ether e2:2b:24:96:98:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/32 scope global dummy0
       valid_lft forever preferred_lft forever
```

```
    inet 192.0.2.1/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet 192.0.2.3/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet 192.0.2.4/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet 192.0.2.5/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::e02b:24ff:fe96:98b8/64 scope link
       valid_lft forever preferred_lft forever
devasc@labvm:~$
```

A partir de este resultado, podemos decir mucho acerca de las interfaces de VM:

- Hay 3 interfaces, la interfaz de bucle invertido (**lo**), **enp0s3**y **dummy0**.
- **ether** muestra la dirección MAC y que Ethernet es la encapsulación del enlace.
- **inet** es la dirección IP, la máscara de subred se muestra en notación diagonal y **brd** es la dirección de difusión.
- **ARRIBA** indica que la interfaz está habilitada.
- **mtu** es la unidad máxima de transmisión que especifica el número máximo de bytes que la trama puede transmitirse en este medio antes de ser fragmentada.

Parte 3: Explore la herramienta de resolución de problemas de ping

La herramienta **ping** es una aplicación que se utiliza para probar la conectividad de red entre dispositivos. ping utiliza el Protocolo de mensajes de control de Internet (ICMP) para enviar paquetes a un dispositivo de la red y espera a que el dispositivo responda. Ping informa errores de red, pérdida de paquetes y tiempo de vida (TTL), entre otras estadísticas.

Paso 1: Ver las opciones de ping.

El ping sólo está disponible en una ventana de terminal o en un símbolo del sistema.

a. Escriba **ping -help** para ver todas las opciones disponibles para el comando.

```
devasc @labvm: ~$ ping -help

Uso
  ping [options] <destination>

Options
  <destination> nombre dns o dirección IP
  -a uso ping audible
  -a uso ping adaptativo
  -B dirección de origen pegajosa
  -c <count> detener después de que<count> responda
  -D imprimir marcas de tiempo(print timestamps)
  -d usar la opción SO_DEBUG socket
  -f flood ping
  -h ayuda de impresión y salida
  <interface>-O bien nombre de interfaz o dirección
  -i <interval> segundos entre el envío de cada paquete
```

```
  -L suprimir el bucle de retorno de paquetes de multidifusión
  -l enviar <preload> el número de paquetes mientras espera respuestas
  -m <mark>etiquetar los paquetes que salen
  -M <pmtud opt> define el descubrimiento de MTU, puede ser uno de <do|dont|want>
  -n sin resolución de nombres dns
  -O informe respuestas pendientes
  -p <pattern> contenido del byte de relleno
  -q salida silenciosa
  -Q <tclass> uso de la calidad de los <tclass> bits de servicio
  -s usan <size> como número de bytes de datos a enviar
  -S usar <size> como valor de opción de socket SO_SNDBUF
  -t <ttl> definir el tiempo para vivir
  -U impresión latencia de usuario a usuario
  -v salida verbosa
  -V versión de impresión y salida
  -w <deadline> respuesta espera <deadline> en segundos
  -W <timeout> tiempo para esperar la respuesta

Opciones IPv4:
  -4 utilizar IPv4
  -b permitir la emisión de ping
  -R ruta de registro
  -T <timestamp> define marca de tiempo, puede ser una de <tsonly|tsandaddr|tsprespec>

Opciones de IPv6:
  -6 usar IPv6
  -F <glowlabel> define la etiqueta de flujo, el valor predeterminado es aleatorio
  -N <nodeinfo opt> use la consulta de información de nodo icmp6, intente <help> como
argumento

Para más detalles vea ping
devasc @labvm: ~$
```

Paso 2: Hacer ping a un host.

La herramienta **ping** tiene muchas opciones diferentes que se pueden seleccionar para personalizar cómo debe tener lugar la comunicación. Algunas de las opciones que puede especificar incluyen:

- Especifique cuántas solicitudes de eco ICMP desea enviar.
- Identifique la dirección IP de origen si hay varias interfaces en el dispositivo.
- Indique la cantidad de tiempo que debe esperar a una respuesta.
- Tamaño del paquete, si desea enviar tamaños de paquete mayores que los 64 bytes predeterminados. Esto puede ayudar a determinar cuál es la unidad de transmisión máxima (MTU).

a. ping www.cisco.com para ver si es accesible.

```
devasc @labvm: ~$ ping -c 5 www.cisco.com
PING e2867.dsca.akamaiedge.net (23.66.161.25) 56(84) bytes de datos.
64 bytes de a23-66-161-25.deploy.static.akamaitechnologies.com (23.66.161.25):
icmp_seq=1 ttl=49 time=58.4 ms
64 bytes de a23-66-161-25.deploy.static.akamaitechnologies.com (23.66.161.25):
icmp_seq=2 ttl=49 time=63.1 ms
```

```
64 bytes de a23-66-161-25.deploy.static.akamaitechnologies.com (23.66.161.25):
icmp_seq=3 ttl=49 tiempo=61.2 ms
64 bytes de a23-66-161-25.deploy.static.akamaitechnologies.com (23.66.161.25):
icmp_seq=4 ttl=49 tiempo=57,7 ms
64 bytes de a23-66-161-25.deploy.static.akamaitechnologies.com (23.66.161.25):
icmp_seq=5 ttl=49 tiempo=57,6 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
5 packets transmitidos, 5 recibidos, 0% sw packet perdidos, tiempo 8153ms
rtt min/avg/max/mdev = 57.597/59.605/63.145/2.205 ms
devasc @labvm: ~$
```

Este ping especificó un recuento de 5 paquetes.

La herramienta **ping** realiza automáticamente la resolución DNS, devolviendo 23.66.161.25 (su dirección IP devuelta puede ser diferente). También se muestra el tiempo de vida (TTL) para las respuestas de eco recibidas y los tiempos de ida y vuelta. Las estadísticas finales confirman que se han transmitido 5 paquetes de solicitud de eco ICMP y se han recibido 5 paquetes de respuesta de eco ICMP, logrando una pérdida de paquetes del 0%. También se muestran estadísticas sobre la desviación mínima, media, máxima y estándar del tiempo que tardaron los paquetes en llegar al destino y regresar.

Si no recibe ninguna respuesta del destino no significa necesariamente que el host esté sin conexión o no esté accesible. Podría significar que los paquetes ICMP están siendo bloqueados por un firewall. Es una práctica recomendada exponer solo los servicios necesarios para estar disponibles en los hosts de la red.

Para IPv6 existe una utilidad similar que se llama **ping6** y también está disponible en la mayoría de los sistemas operativos.

Parte 4: Explore la herramienta de solución de problemas de trazar la ruta(traceroute)

La herramienta **traceroute** muestra la ruta que toman los paquetes en su camino a un destino. La alternativa de Microsoft Windows se llama **tracert**. La observación de la ruta de tráfico de red lleva desde el origen hasta el destino es importante para la solución de problemas, ya que los bucles de enrutamiento y las rutas no óptimas se pueden detectar y corregir.

Traceroute utiliza paquetes ICMP para determinar la ruta al destino. El campo Tiempo de vida (TTL) en el encabezado del paquete IP se utiliza para evitar bucles infinitos en la red. Para cada salto o router por el que pasa un paquete IP, el campo TTL se reduce en uno. Cuando el valor del campo TTL alcanza 0, el paquete se descarta evitando bucles infinitos. Por lo general, el campo TTL se establece en su valor máximo, 255, en el origen del tráfico, porque el host está tratando de maximizar las posibilidades de que ese paquete llegue a su destino. traceroute invierte esta lógica, e incrementa gradualmente el valor TTL, de 1 y sigue añadiendo 1 al campo TTL en el siguiente paquete y así sucesivamente. Establece un valor TTL de 1 para el primer paquete, significa que el paquete se descartará en el primer enrutador. De forma predeterminada, la mayoría de los routers envían de vuelta al origen del tráfico un paquete ICMP Time Exceeded informándole de que el paquete ha alcanzado un valor TTL de 0 y tuvo que descartarse. Traceroute utiliza la información recibida del router para averiguar su dirección IP y nombre de host, así como los tiempos de ida y vuelta.

Para IPv6 hay una alternativa llamada traceroute6 para sistemas operativos basados en UNIX y tracert6 para sistemas basados en Microsoft Windows.

Paso 1: Ver las opciones de traceroute.

a. Escriba **traceroute —help** para ver todas las opciones disponibles para el comando.

```
devasc @labvm: ~$ traceroute —help
Uso: traceroute [OPTION...] HOST
Imprima el seguimiento de paquetes de ruta al host de red.
```

```
  -f, —first hop=NUM establece la distancia inicial del salto, es decir, tiempo de
vida
  -g, —gateways=Lista de puertas de enlace para enrutamiento de fuentes sueltas
  -I, —icmp usa ICMP ECHO como sonda
  -m, —max-hop=Núm establecido conteo máximo de saltos (predeterminado: 64)
  -M, —TYPE=MÉTODO use METODO (`icmp' o `udp') para traceroute
       operaciones, por defecto a `udp'
  -p, —PORT=Puerto utilizar puerto puerto de destino (predeterminado: 33434)
  -q, —tries=Núm enviar paquetes de sondeo NUM por salto (predeterminado: 3)
      —resolver nombres de host resolver nombres de host
  -t, —tos=NUM establece el tipo de servicio (TOS) en NUM
  -w, —wait=NUM espera NUM segundos para la respuesta (predeterminado: 3)
  -?, —help dar esta lista de ayuda
      —uso da un mensaje de uso corto
  -V, —version versión del programa de impresión

Los argumentos obligatorios u opcionales para las opciones largas también son
obligatorios u opcionales
para las opciones cortas correspondientes.

Informe de errores a < bug-inetutils@gnu.org >.
devasc @labvm: ~$
```

Hay varias opciones disponibles con **traceroute**, incluyendo:

- Especifique el valor TTL del primer paquete enviado, 1 de forma predeterminada.
- Especifique el valor TTL máximo. De forma predeterminada, aumentará el valor TTL hasta 64 o hasta que se alcance el destino.
- Especifique la dirección de origen en caso de que haya varias interfaces en el dispositivo.
- Especifique el valor de calidad de servicio (QoS) en el encabezado IP.
- Especifique la longitud del paquete.

Paso 2: Utilice traceroute para encontrar la ruta de acceso a un servidor web.

Debido a la forma en que Virtual Box implementa una red NAT, no puede rastrear fuera de la máquina virtual. Tendría que cambiar su VM a Bridged. Pero entonces, no sería capaz de comunicarse con el CSR1000v en otros laboratorios. Por lo tanto, recomendamos dejar la VM en modo NAT.

Sin embargo, debería poder utilizar el comando **traceroute** en el host local. Para los hosts Mac y Linux, utilice el comando **traceroute**. Para los hosts de Windows, utilice el comando **tracert**, como se muestra a continuación. Abra un símbolo del sistema en su host local y rastree la ruta a www.netacad.com para ver cuántos saltos y cuánto tiempo tarda en llegar a él. Su salida será diferente.

```
C:\> tracert www.netacad.com

Rastreo de ruta a e7792.dsca.akamaiedge.net [2600:1406:22:183:: 1e70]
sobre un máximo de 30 saltos:

  1 43 ms 38 ms 36 ms hsrp-2001-420-c0c8-1.cisco.com [2001:420:c0c8:: 1]
  2 48 ms 54 ms 40 ms sjc05-sbb-gw1-twe1-0-13.cisco.com [2001:420:280:1 aa::]
```

```
  3 39 ms 37 ms 38 ms sjc05-rbb-gw1-por20.cisco.com [2001:420:41:116¤]
  4 37 ms 38 ms sjc12-corp-gw1-ten1-3-0.cisco.com [2001:420:41:11 c¤ 1]
  5 39 ms 39 ms 45 ms sjc12-dmzbb-gw1-vla777.cisco.com [2001:420:82:2¤ d]
  6 51 ms 39 ms 37 ms sjc5-cbb-gw1-be92.cisco.com [2001:420:82:4 e¤]
  7 39 ms 39 ms 38 ms sjc12-isp-gw2-ten0-0-0.cisco.com [2001:420:82:f¤]
  8 78 ms 57 ms 65 ms 2001:1890:c 00:6 c01¤ eee7:a12
  9 44 ms 42 ms 47 ms sj2ca81crs.ipv6.att.net [2001:1890:ff:ffff: 12:122:110:62]
 10 46 ms 46 ms 47 ms 2001:1890:ff:ffff: 12:122:149:225
 11 43 ms 41 ms 43 ms scaca401cts.ipv6.att.net [2001:1890:ff:ffff: 12:122:137:245]
 12 43 ms 43 ms 44 ms 2001:1890:fff: 2180:12:120:13:178
 13 53 ms 54 ms 45 ms 2001:1890:1 ff:2a 80:12:120:183:64
 14 52 ms 42 ms g2600-1406-0022-0183-0000-0000-0000-
1e70.deploy.static.akamaitechnologies.com [2600:1406:22:183¤ 1e70]

Trace complete.

devasc @labvm: ~$
```

La salida muestra que hay 14 saltos a lo largo de la ruta. También se muestran los tiempos de ida y vuelta.

Parte 5: Explore la herramienta de solución de problemas de nslookup

La herramienta **nslookup** utilizada para consultar el Sistema de nombres de dominio (DNS) para obtener la asignación de nombres de dominio a direcciones IP. Esta herramienta es útil para determinar si el servidor DNS configurado en un host específico está resolviendo nombres de host en direcciones IP.

Paso 1: Consulte un dominio.

Para utilizar nslookup, debe escribir el nombre de host que está intentando resolver en una dirección IP. Esto usará el servidor DNS configurado para encontrar la dirección IP. También puede especificar un servidor DNS para usar.

Uso: nslookup [HOST] [SERVER]

a. Escriba **nslookup www.cisco.com** para determinar la dirección IP del dominio.

```
devasc @labvm: ~$ nslookup www.cisco.com
Servidor: 127.0.0.53
Dirección: 127.0.0.53 #53

Respuesta no autoritativa:
www.cisco.com canonical name = origin-www.cisco.com.
Nombre: origin-www.cisco.com
Dirección: 173.37.145.84
Nombre: origin-www.cisco.com
Dirrección: 2001:420:1101:1::a

devasc @labvm: ~$
```

El comando devuelve la respuesta no autorizada y el nombre y la dirección IPv4 e IPv6. La respuesta no autorizada significa que el servidor no contiene los registros originales de la zona del dominio, sino que se crea a partir de búsquedas DNS anteriores.

Nota: Lo más probable es que su salida sea diferente. Sin embargo, debería ver una dirección IPv4 e IPv6.

Paso 2: Consulte una dirección IP.

También puede buscar direcciones IP para descubrir el dominio asociado a él.

a. Consulte el servidor DNS para obtener la dirección IP 8.8.8.8.

```
devasc @labvm: ~$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa      name = dns.google.

Las respuestas autorizadas se pueden encontrar en:

devasc @labvm: ~$
```

Paso 3: Consulte un dominio mediante un servidor DNS específico.

a. Escriba **nslookup www.cisco.com 8.8.8.8** para determinar la dirección IP del dominio según el DNS de Google.

```
devasc @labvm: ~$ nslookup www.cisco.com 8.8.8
Server: 8.8.8
Dirección: 8.8.8.8 #53

Respuesta no autoritativa:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net   canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net      canonical name =
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net   canonical name =
e2867.dsca.akamaiedge.net.
Nombre:      e2867.dsca.akamaiedge.net
Dirección: 23.205.37.210
Nombre:      e2867.dsca.akamaiedge.net
Dirección: 2600:1406:22:182:: b33
Nombre:      e2867.dsca.akamaiedge.net
Dirección: 2600:1406:22:19 c:: b33

devasc @labvm: ~$
```

Observe que mediante este método, el servidor resolvió la dirección en tres direcciones IP diferentes, todas diferentes de la consulta DNS anterior. Estos servidores tienen una caché diferente de consultas DNS a www.cisco.com.