Laboratorio 5

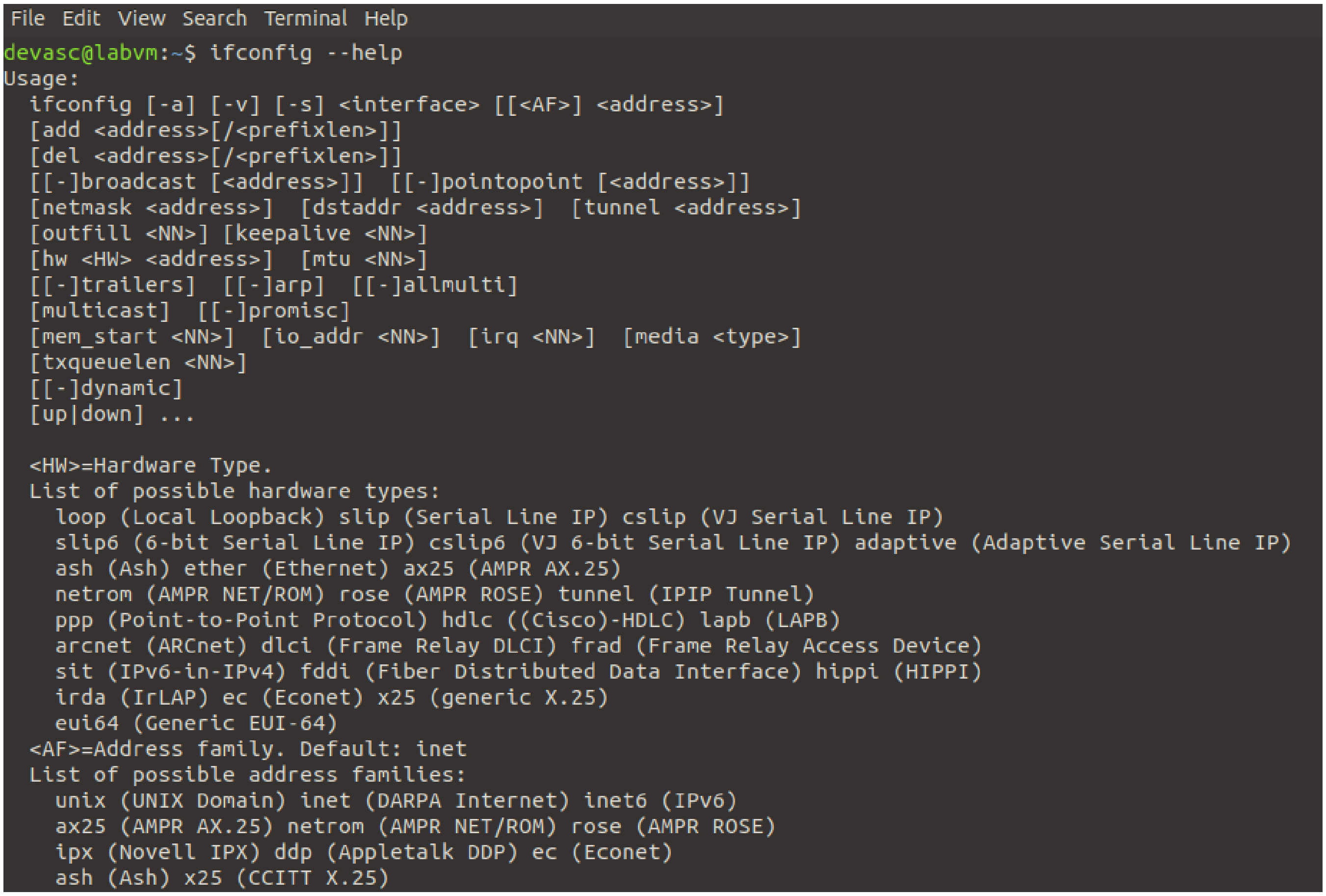
Network Troubleshooting Tools

Sergio Sebastian Pezo Jimenez - 20224087G

Parte 1: Inicializamos la VM de DEVASC.

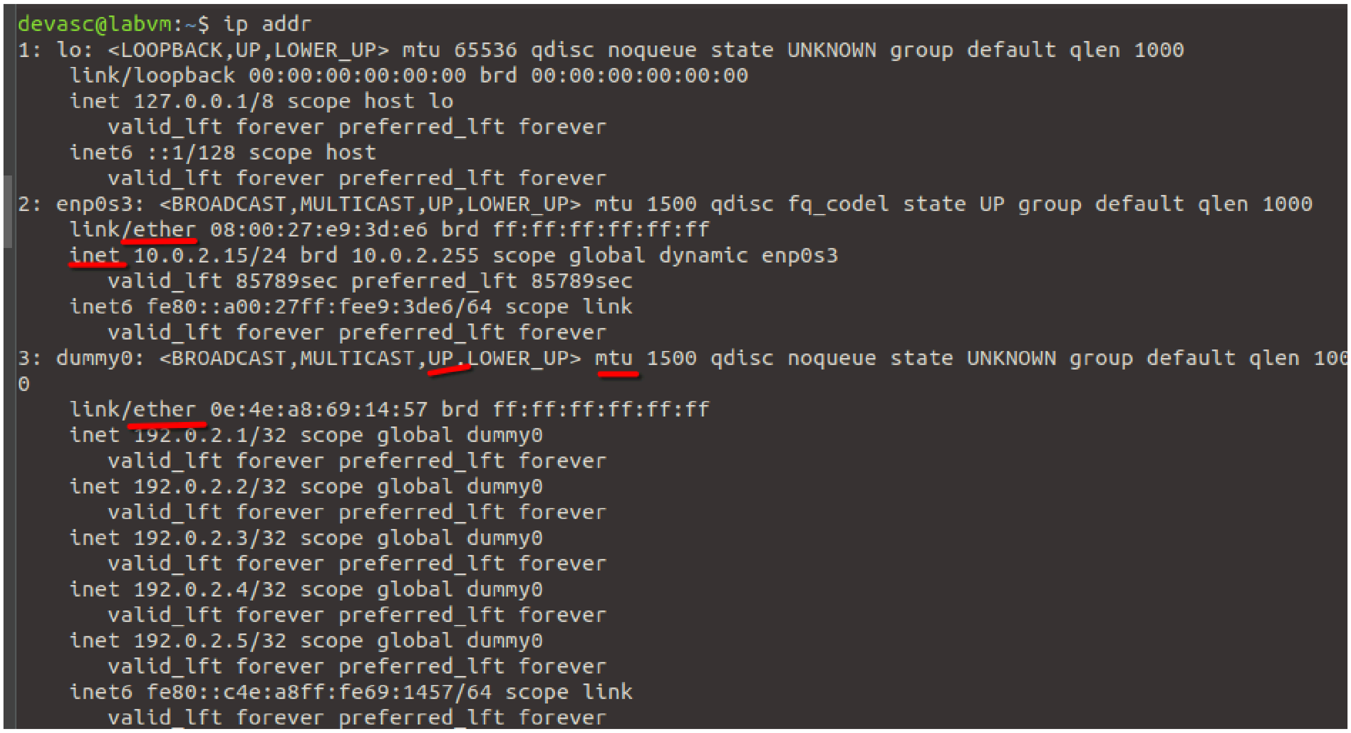
PARTE 2: Exploramos la `ifconfig` troubleshooting tool.

Así que primero observamos las diferentes opciones que nos brinda `ifconfig`.



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

  <HW>=Hardware Type.
  List of possible hardware types:
    loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
    slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
    ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
    arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
    sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) ec (Econet) x25 (generic X.25)
    eui64 (Generic EUI-64)
  <AF>=Address family. Default: inet
  List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
```

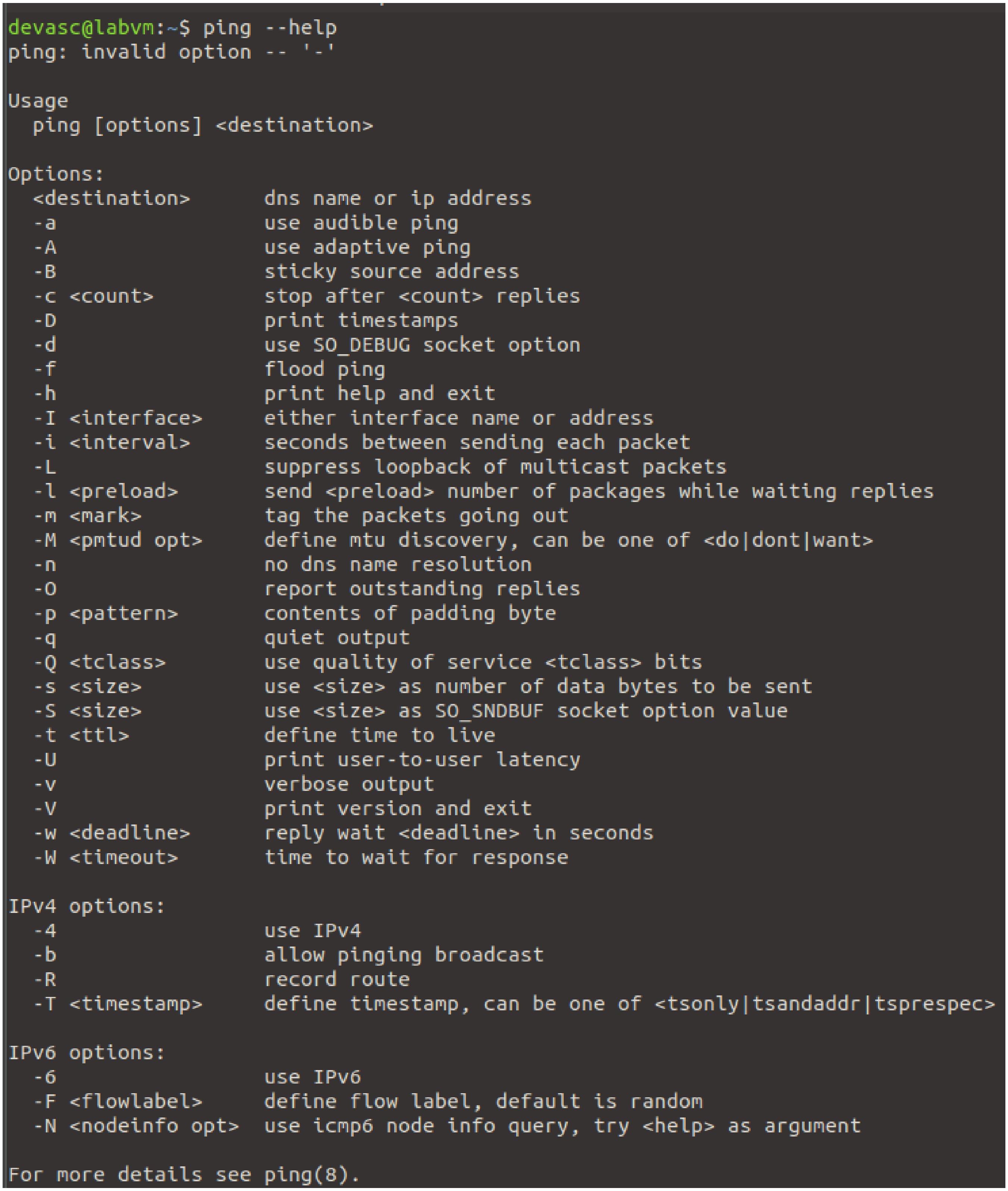
Ahora pasamos a ver el status de todas las interfaces.



```
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 85789sec preferred_lft 85789sec
    inet6 fe80::a00:27ff:fee9:3de6/64 scope link
       valid_lft forever preferred_lft forever
3: dummy0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 100
0
    link/ether 0e:4e:a8:69:14:57 brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.1/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet 192.0.2.2/32 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::c4e:a8ff:fe69:1457/64 scope link
       valid_lft forever preferred_lft forever
```

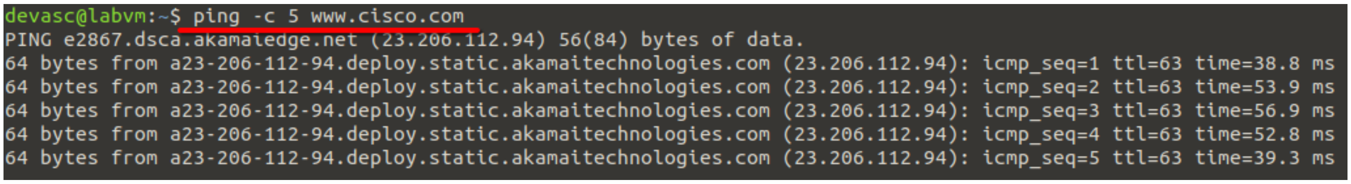
Parte 3: Exploramos la ping troubleshooting tool:

Observamos las opciones:



```
devasc@labvm:~$ ping --help
ping: invalid option -- '-'

Usage
  ping [options] <destination>

Options:
  <destination>      dns name or ip address
  -a                 use audible ping
  -A                 use adaptive ping
  -B                 sticky source address
  -c <count>         stop after <count> replies
  -D                 print timestamps
  -d                 use SO_DEBUG socket option
  -f                 flood ping
  -h                 print help and exit
  -I <interface>     either interface name or address
  -i <interval>      seconds between sending each packet
  -L                 suppress loopback of multicast packets
  -l <preload>       send <preload> number of packages while waiting replies
  -m <mark>          tag the packets going out
  -M <pmtud opt>     define mtu discovery, can be one of <do|dont|want>
  -n                 no dns name resolution
  -O                 report outstanding replies
  -p <pattern>       contents of padding byte
  -q                 quiet output
  -Q <tclass>        use quality of service <tclass> bits
  -s <size>          use <size> as number of data bytes to be sent
  -S <size>          use <size> as SO_SNDBUF socket option value
  -t <ttl>           define time to live
  -U                 print user-to-user latency
  -v                 verbose output
  -V                 print version and exit
  -w <deadline>      reply wait <deadline> in seconds
  -W <timeout>       time to wait for response

IPv4 options:
  -4                 use IPv4
  -b                 allow pinging broadcast
  -R                 record route
  -T <timestamp>     define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6                 use IPv6
  -F <flowlabel>     define flow label, default is random
  -N <nodeinfo opt>  use icmp6 node info query, try <help> as argument

For more details see ping(8).
```

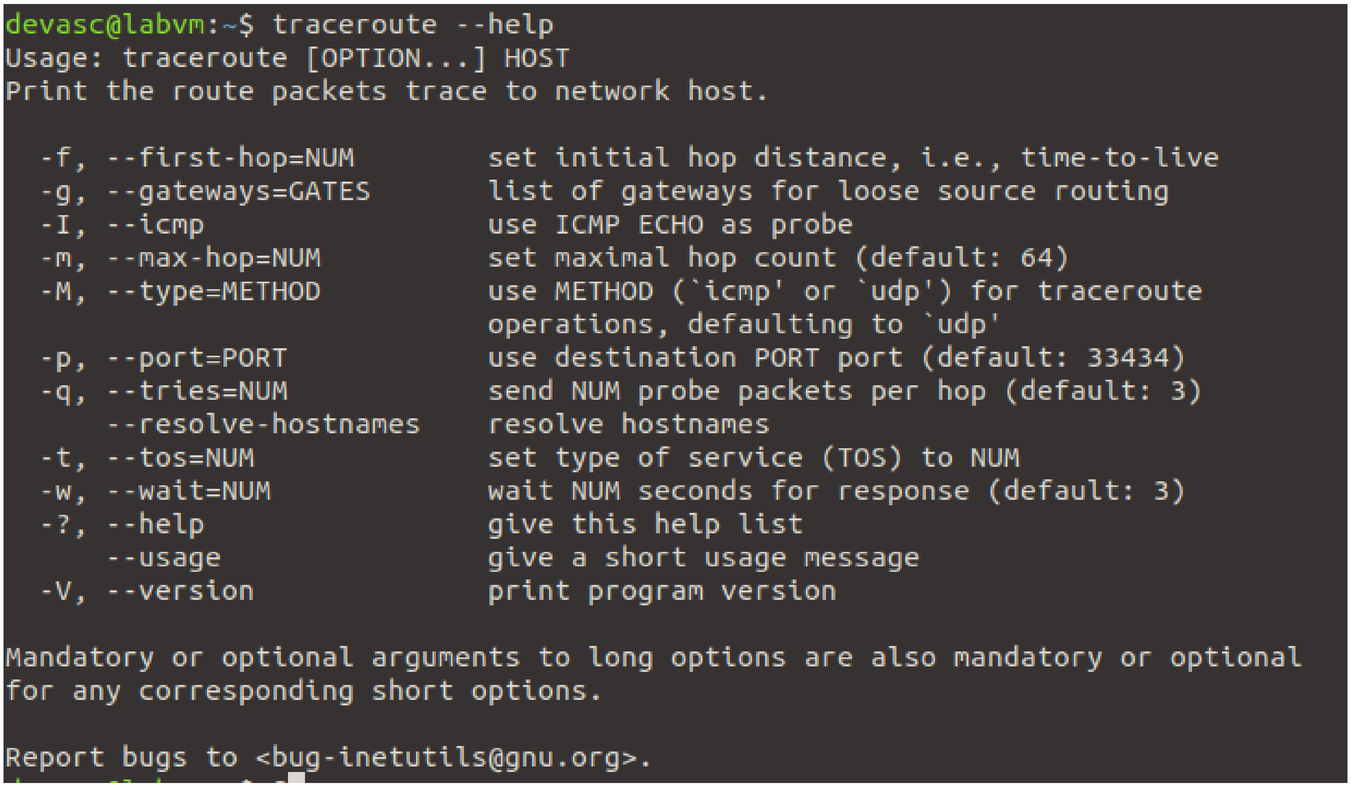
Nos comunicamos con `www.cisco.com` y especificamos realizar 5 peticiones.



```
devasc@labvm:~$ ping -c 5 www.cisco.com
PING e2867.dsca.akamaiedge.net (23.206.112.94) 56(84) bytes of data.
64 bytes from a23-206-112-94.deploy.static.akamaitechnologies.com (23.206.112.94): icmp_seq=1 ttl=63 time=38.8 ms
64 bytes from a23-206-112-94.deploy.static.akamaitechnologies.com (23.206.112.94): icmp_seq=2 ttl=63 time=53.9 ms
64 bytes from a23-206-112-94.deploy.static.akamaitechnologies.com (23.206.112.94): icmp_seq=3 ttl=63 time=56.9 ms
64 bytes from a23-206-112-94.deploy.static.akamaitechnologies.com (23.206.112.94): icmp_seq=4 ttl=63 time=52.8 ms
64 bytes from a23-206-112-94.deploy.static.akamaitechnologies.com (23.206.112.94): icmp_seq=5 ttl=63 time=39.3 ms
```

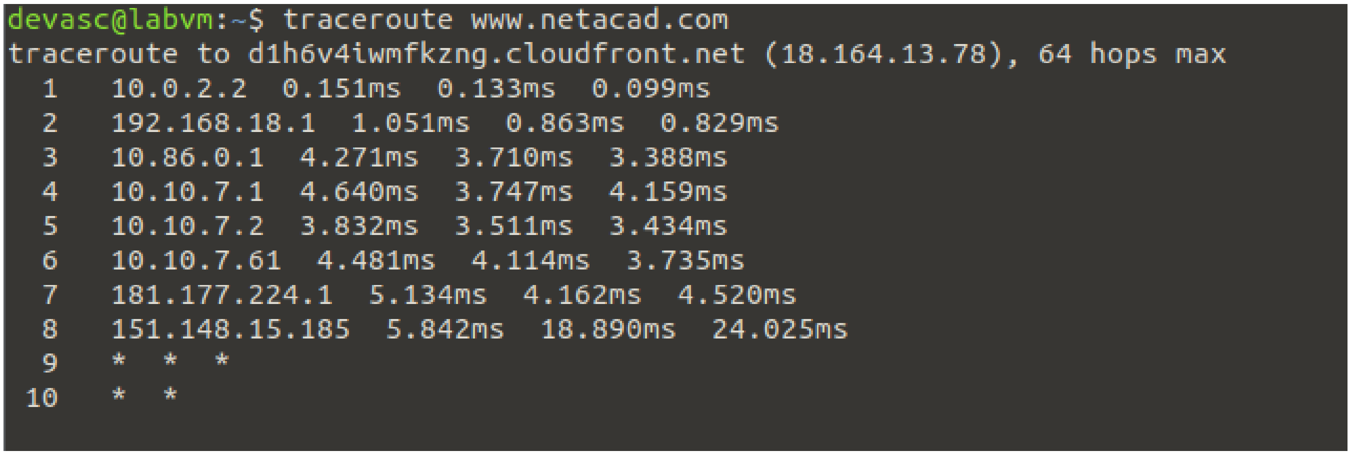
Parte 4: Exploramos el traceroute troubleshooting tool:

Observamos las opciones de traceroute.



```
devasc@labvm:~$ traceroute --help
Usage: traceroute [OPTION...] HOST
Print the route packets trace to network host.

  -f, --first-hop=NUM        set initial hop distance, i.e., time-to-live
  -g, --gateways=GATES       list of gateways for loose source routing
  -I, --icmp                 use ICMP ECHO as probe
  -m, --max-hop=NUM          set maximal hop count (default: 64)
  -M, --type=METHOD          use METHOD (`icmp' or `udp') for traceroute
                             operations, defaulting to `udp'
  -p, --port=PORT            use destination PORT port (default: 33434)
  -q, --tries=NUM            send NUM probe packets per hop (default: 3)
      --resolve-hostnames    resolve hostnames
  -t, --tos=NUM              set type of service (TOS) to NUM
  -w, --wait=NUM             wait NUM seconds for response (default: 3)
  -?, --help                 give this help list
      --usage                give a short usage message
  -V, --version              print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Report bugs to <bug-inetutils@gnu.org>.
```

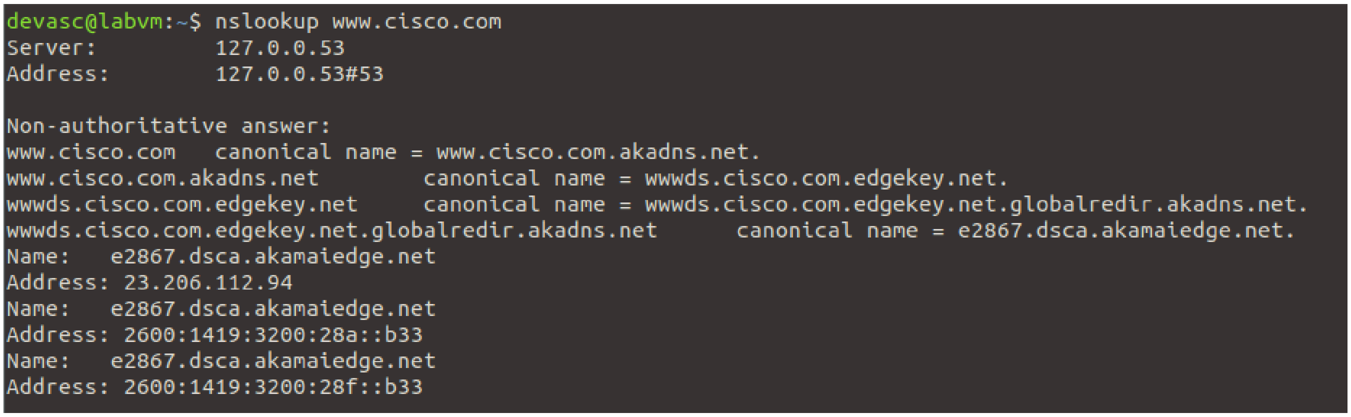
Usamos el comando para ver el camino a un servidor web.



```
devasc@labvm:~$ traceroute www.netacad.com
traceroute to d1h6v4iwmfkzng.cloudfront.net (18.164.13.78), 64 hops max
  1   10.0.2.2  0.151ms  0.133ms  0.099ms
  2   192.168.18.1  1.051ms  0.863ms  0.829ms
  3   10.86.0.1  4.271ms  3.710ms  3.388ms
  4   10.10.7.1  4.640ms  3.747ms  4.159ms
  5   10.10.7.2  3.832ms  3.511ms  3.434ms
  6   10.10.7.61  4.481ms  4.114ms  3.735ms
  7   181.177.224.1  5.134ms  4.162ms  4.520ms
  8   151.148.15.185  5.842ms  18.890ms  24.025ms
  9   *  *  *
 10   *  *
```

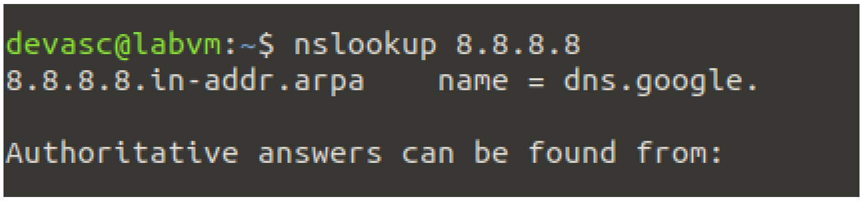
Parte 5: Exploramos nslookup troubleshooting tool:

Consultamos un dominio:



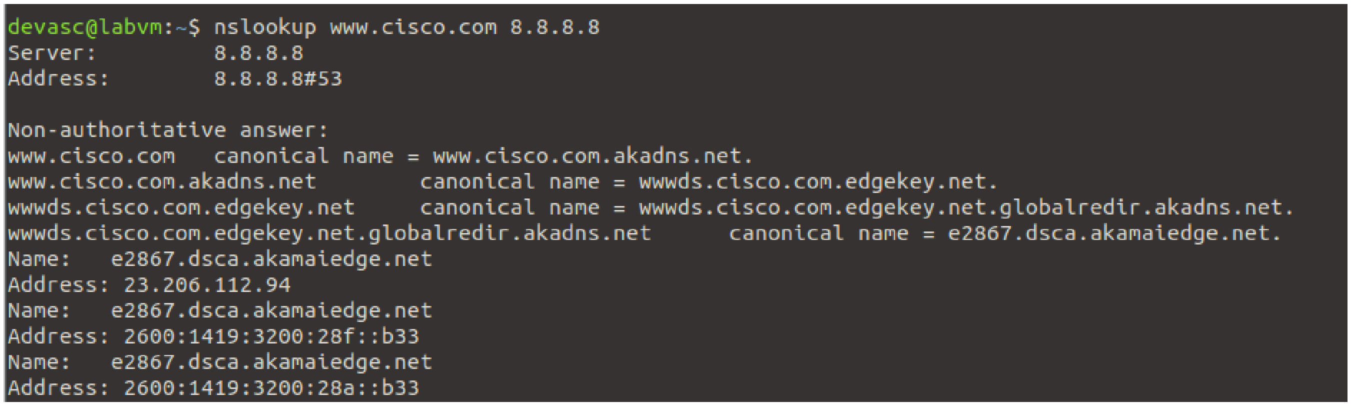
```
devasc@labvm:~$ nslookup www.cisco.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
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.
Name:   e2867.dsca.akamaiedge.net
Address: 23.206.112.94
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1419:3200:28a::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1419:3200:28f::b33
```

Ahora una dirección IP del DNS de google:



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

Authoritative answers can be found from:
```

Verificamos si el DNS de google contiene el dominio de cisco:



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

Non-authoritative answer:
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.
Name:   e2867.dsca.akamaiedge.net
Address: 23.206.112.94
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1419:3200:28f::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1419:3200:28a::b33
```

Y notamos que sí.

Finalizado.