

Universidad Tecnológica de Panamá
Sistemas Operativos I
Experiencia Práctica en Laboratorio No. 6
Interconectividad

Profesora Aris Castillo de Valencia

Objetivos:

- Probar y distinguir distintos comandos para realizar las siguientes actividades en el sistema operativo:

1. Verificar la interconectividad de mi computador con otros dispositivos en la red.
2. Verificar la información de configuración de los protocolos TCP/IP en mi equipo.
3. Buscar información en la red.

Metas:

Con esta experiencia práctica se espera que el estudiante sea capaz de realizar tareas sencillas de administración del sistema operativo Linux/GNU a través de comandos para configurar y monitorear servicios TCP/IP.

Contenidos:

- Comandos de red en Linux/GNU: ifconfig, ip, ping, arp, nslookup, dig, nestat, traceroute.

Metodología:

Se basa en métodos intuitivos, de experimentación y demostración en que se acerca al estudiante a situaciones reales de la práctica profesional de manera que resuelva las situaciones presentadas.

Evaluación:

- Se dará 50 puntos por el desarrollo de la práctica en el aula.
- Se dará 50 puntos por la entrega del informe escrito debidamente completado y por su nivel técnico.

Recursos:

- Hardware: computadora, conexión a Internet.
- Software: Sistema operativo Linux/GNU.

Procedimiento:

Lea cuidadosamente la guía; pruebe cada uno de los comandos listados prestando especial atención a los resultados obtenidos y a las variantes que le ofrecen las opciones de los comandos. Ponga en práctica los comandos aprendidos haciendo los ejercicios sugeridos. Llene la autoevaluación y retroalimentación y súbala a la plataforma Moodle.


Nota: más seguramente para ejecutar estos comandos debe tener una sesión de superusuario, root. Para pasarse a superusuario, ejecute el comando **su** seguido del usuario root.

Luego le pedirá la contraseña.

#su root

¿Cómo puedo saber la configuración de las interfaces de red?

Para conocer las configuraciones del protocolo TCP/IP en su máquina, puede utilizar el comando **ifconfig**. Al ejecutarlo, podrá visualizar cada una de las interfaces de red de su equipo, así como la siguiente información: dirección MAC, dirección IP, máscara de subred, etc. La siguiente figura muestra la salida.



```
aris@linux-9457:~  
File Edit View Terminal Help  
user privileges (eg. root).  
aris@linux-9457:~> su root  
Password:  
linux-9457:/home/aris # ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:21:CC:56:FA:02  
          UP BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)  
          Interrupt:28 Base address:0xe000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:820 (820.0 b)  TX bytes:820 (820.0 b)  
  
wlan0     Link encap:Ethernet  HWaddr 00:1B:B1:46:7B:E1  
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::21b:b1ff:fe46:7be1/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:55371 errors:39 dropped:0 overruns:0 frame:0  
          TX packets:5673 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:17688199 (16.8 Mb)  TX bytes:630089 (615.3 Kb)  
          Interrupt:17  
  
linux-9457:/home/aris #
```

| | |
|--------------------|---|
| eth0 | es la tarjeta de red Ethernet del equipo |
| lo-loopback | se refiere a la pila de protocolos TCP/IP en el equipo. Si hubiese problemas en la pila, basta con ejecutar el comando ping a la dirección 127.0.0.1 para comprobar que la pila de protocolos está funcionando mal. |
| wlan0 | es la tarjeta de red inalámbrica del equipo. |

Si existieran otras interfaces, serían desplegadas de la misma forma. Veamos ahora cada uno de los elementos desplegados por cada interfaz.

| | |
|-------------------|---|
| Link encap | Indica que el protocolo de la capa de enlace es Ethernet. |
| Hwaddr | Muestra la dirección MAC o física de la tarjeta de red del equipo. Cada interfaz de red tendrá un código MAC distinto, formado por el Serial del fabricante y un secuencia asignado por éste. |
| Inet addr | Es la dirección IP asignada. |
| Bcast | Es la dirección de broadcast. |
| Mask | Es la máscara de subred aplicada. |

Otra información es Rx packets para paquetes recibidos, Tx packets para paquetes enviados; número de interrupción y la dirección base de la rutina de servicio.

Ejercicio: Aplique el comando y anote la dirección IP, máscara de subred, dirección MAC y la dirección broadcast para cada interfaz desplegada.

```
[root@localhost-live liveuser]# ip addr show
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 08:00:27:0d:c2:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 85439sec preferred_lft 85439sec
    inet6 fe80::1539:1a7f:69a5:38c1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

1:

Dirección Ip y máscara subred:

```
inet 127.0.0.1/8 scope host lo
```

Dirección Broadcast:

```
inet6 ::1/128 scope host
```

2:

Dirección Ip y máscara subred:

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
```

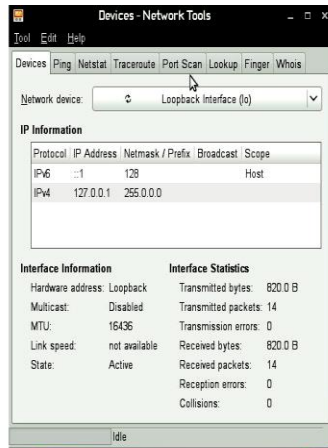
Dirección Mac:

```
link/ether 08:00:27:0d:c2:9e brd ff:ff:ff:ff:ff:ff
```

Dirección Broadcast:

```
inet6 fe80::1539:1a7f:69a5:38c1/64 scope link noprefixroute
```

Existe también una herramienta gráfica que permite revisar la información de configuración de las interfaces de red y configurarlas. Buscar en **System/System/Network_Tools**



¿Qué más debo saber sobre la configuración TCP/IP en mi máquina?

Es importante conocer sobre los archivos de configuración. Éstos contienen la información de configuración de las interfaces de red para poder comunicar el dispositivo con otros. Los archivos de configuración varían de acuerdo con la distribución de Linux. Algunos son los siguientes:

| | |
|--|---|
| /etc/resolv.conf | Contiene los servidores DNS para la resolución de nombres de dominio. Se debe colocar la dirección del servidor que convierte los nombres de dominio en direcciones IP. Ej. Cuando queremos entrar a un website externo, la petición irá primero al servidor DNS establecido en esta configuración. |
| /etc/hosts | Contiene los hosts a ser resueltos localmente, es decir, el sistema local en la red que no es el DNS. |
| /etc/nsswitch.conf | Contiene el orden de búsqueda de nombres en el host. Éste indica que para resolver un nombre de host se debe buscar primero en el archivo local del host y si no lo encuentra, entonces pasar la petición al servidor DNS. |
| /etc/protocols | Contiene la lista de todos los protocolos disponibles en el sistema operativo con su correspondiente número. |
| /etc/networks | Lista nombres y direcciones IP de la red local así como otras redes a las cuales nuestro equipo se conecta frecuentemente. |
| /etc/services | Lista todos los servicios de red existentes. Muestra el nombre del servicio, el número de puerto y el tipo de protocolo. |
| /etc/sysconfig/network | Contiene la configuración de red en RedHat/Fedora/CentOS |
| /etc/sysconfig/network-scripts/ifcfg-device | Contiene la información de TCP en RedHat/Fedora/CentOS |
| /etc/network/interfaces | Contiene la configuración de red en Ubuntu/Debian |

Ejercicio. Entre a estos archivos, usando el comando cat o un editor como vim, y tome datos de 5 protocolos, servicios y otra información relevante.

Ejecutando /etc/resolv.conf:

```
GNU nano 6.4 /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved>
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.
[ Read 23 lines ]
```

Ejecutando /etc/hosts

```
[root@localhost-live /]# cat /etc/hosts
# Loopback entries; do not change.
# For historical reasons, localhost precedes localhost.localdomain:
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
# See hosts(5) for proper format and other examples:
# 192.168.1.10 foo.mydomain.org foo
# 192.168.1.13 bar.mydomain.org bar
```

Ejecutando /etc/nsswitch.conf:

```
[root@localhost-live /]# cat /etc/nsswitch.conf
# Generated by authselect on Sat Nov  5 09:04:32 2022
# Do not modify this file manually, use authselect instead. Any user changes will
# be overwritten.
# You can stop authselect from managing your configuration by calling 'authselect
# opt-out'.
# See authselect(8) for more details.

# In order of likelihood of use to accelerate lookup.
passwd:      files sss systemd
shadow:      files
group:        files sss systemd
hosts:        files myhostname mdns4_minimal [NOTFOUND=return] resolve [!UNAVAIL=return] dns
services:     files sss
netgroup:     files sss
automount:    files sss

aliases:      files
ethers:        files
gshadow:       files
networks:      files dns
protocols:     files
publickey:     files
```

Ejecutando /etc/protocols:

```
[root@localhost-live /]# cat /etc/protocols
# /etc/protocols:
# $Id: protocols,v 1.12 2016/07/08 12:27 ovasik Exp $
#
# Internet (IP) protocols
#
#      from: @(#)protocols      5.1 (Berkeley) 4/17/89
#
# Updated for NetBSD based on RFC 1340, Assigned Numbers (July 1992).
# Last IANA update included dated 2011-05-03
#
# See also http://www.iana.org/assignments/protocol-numbers

ip      0      IP          # internet protocol, pseudo protocol number
hopopt  0      HOPOPT       # hop-by-hop options for ipv6
icmp    1      ICMP         # internet control message protocol
igmp    2      IGMP         # internet group management protocol
ggp     3      GGP          # gateway-gateway protocol
ipv4    4      IPv4         # IPv4 encapsulation
st      5      ST           # ST datagram mode
tcp     6      TCP          # transmission control protocol
cbt     7      CBT          # CBT, Tony Ballardie <A.Ballardie@cs.ucl.ac.uk>
egp     8      EGP          # exterior gateway protocol
```

Ejecutando /etc/services:

```
murray      1123/tcp      # Murray
murray      1123/udp      # Murray
hpvmcontrol 1124/tcp      # HP VMM Control
hpvmcontrol 1124/udp      # HP VMM Control
hpvmagent   1125/tcp      # HP VMM Agent
hpvmagent   1125/udp      # HP VMM Agent
hpvmdata    1126/tcp      # HP VMM Agent
hpvmdata    1126/udp      # HP VMM Agent
kwdb-commn  1127/udp      # KWDB Remote Communication
saphostctrl 1128/tcp      # SAPHostControl over SOAP/HTTP
saphostctrl 1128/udp      # SAPHostControl over SOAP/HTTP
saphostctrls 1129/tcp      # SAPHostControl over SOAP/HTTPS
saphostctrls 1129/udp      # SAPHostControl over SOAP/HTTPS
casp        1130/tcp      # CAC App Service Protocol
casp        1130/udp      # CAC App Service Protocol
caspsl      1131/tcp      # CAC App Service Protocol Encrypted
caspsl      1131/udp      # CAC App Service Protocol Encrypted
kvm-via-ip  1132/tcp      # KVM-via-IP Management Service
kvm-via-ip  1132/udp      # KVM-via-IP Management Service
dfn         1133/tcp      # Data Flow Network
dfn         1133/udp      # Data Flow Network
aplx        1134/tcp      # MicroAPL APLX
aplx        1134/udp      # MicroAPL APLX
omnivision  1135/tcp      # OmniVision Communication Service
```

Ejecutando /etc/sysconfig/network:

```
[root@localhost-live /]# cat /etc/sysconfig/network
cat: /etc/sysconfig/network: No such file or directory
```

Ejecutando /etc/sysconfig/network-scripts/ifcfg-device:

Tampoco me encuentra este directorio, lo intenté de varias maneras pero no me funciona.

Ejecutando /etc/network/interfaces:

¿Cómo cambio de configuración TCP/IP de alguna de las interfaces de red manualmente?

Se puede usar el comando **ip**.

Ejercicio. Despliegue el manual de ayuda del comando **ip**. Anote el procedimiento para cambiar la dirección de una interfaz. ¿Qué más le permite el comando?


```
[root@localhost-live /]# ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | amt | fou | help | ila | ioam | l2tp |
                  link | macsec | maddress | monitor | mptcp | mroute | mrule |
                  neighbor | neighbour | netconf | netns | nexthop | ntable |
                  ntbl | route | rule | sr | tap | tcpmetrics |
                  token | tunnel | tuntap | vrf | xfrm }
      OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                  -h[uman-readable] | -iec | -j[son] | -p[retty] |
                  -f[amily] { inet | inet6 | mpls | bridge | link } |
                  -4 | -6 | -M | -B | -0 |
                  -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                  -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
                  |
                  -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                  -c[olor]}
```

Paso 1: Ver ip

```
[root@localhost-live /]# ip addr show
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 08:00:27:0d:c2:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 80257sec preferred_lft 80257sec
    inet6 fe80::1539:1a7f:69a5:38c1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Paso 2: identificar interfaz de red y la mascara

```
2: enp0s3:
```

```
inet 10.0.2.15/24
```

Paso 3: cambio de id

```
[root@localhost-live /]# ip addr change 192.171.0.10/24 dev enp0s3
```

Paso 4: verificamos si funcionó

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0d:c2:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 80000sec preferred_lft 80000sec
    inet 192.171.0.10/24 scope global enp0s3
```

¿Cómo puedo verificar la conectividad de mi computador con otro equipo?

Para ello se puede utilizar el comando **ping**, el cual realiza un proceso de envío de paquetes llamados HELLO. Una vez que el otro dispositivo responde a través de otro paquete HELLO, entonces mi computador comprueba que hay conectividad.

#ping direccion_ip/nombre_dominio

La salida del comando ping es como sigue:

```
ping 192.168.0.1
```

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
```

```
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.08 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.871 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.850 ms
```

```
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=1.09 ms
```

```
^C
```

```
--- 192.168.0.1 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
```

```
rtt min/avg/max/mdev = 0.850/0.975/1.092/0.114 ms
```

Este resultado indica que la pila de protocolos TCP/IP está funcionando correctamente, que la dirección IP de prueba es correcta dado que alcanzada, que la máquina remota fue alcanzada, y que la máquina remota tiene la configuración para responder al comando.

Ejemplo:

#ping www.yahoo.com

#ping 192.168.18.2

Anote y analice los resultados. ¿Cuántos paquetes se enviaron? ¿Cuántos se recibieron? ¿Cuántos se perdieron? ¿Cuánto tiempo transcurrió? ¿Cuál fue el tiempo promedio de respuesta?

```
[root@localhost-live /]# ping www.instagram.com
PING z-p42-instagram.c10r.instagram.com (31.13.67.174) 56(84) bytes of data.
64 bytes from instagram-p42-shv-01-mia3.fbcdn.net (31.13.67.174): icmp_seq=1 ttl
=53 time=73.8 ms
64 bytes from instagram-p42-shv-01-mia3.fbcdn.net (31.13.67.174): icmp_seq=2 ttl
=53 time=68.6 ms
64 bytes from instagram-p42-shv-01-mia3.fbcdn.net (31.13.67.174): icmp_seq=3 ttl
=53 time=66.7 ms
64 bytes from instagram-p42-shv-01-mia3.fbcdn.net (31.13.67.174): icmp_seq=129 t
tl=53 time=66.5 ms
^C
--- z-p42-instagram.c10r.instagram.com ping statistics ---
129 packets transmitted, 129 received, 0% packet loss, time 128135ms
```

¿Para qué me sirve el comando ARP?

Revisar la conectividad Ethernet y la configuración IP.

#arp

La salida sería:

| Address | HWtype | HWaddress | Flags | Mask | Iface |
|---------|--------|-------------------|-------|------|-------|
| unknown | ether | 00:18:39:87:0e:60 | C | | wlan0 |

ARP significa Address Resolution Protocol o protocolo de resolución de dirección. Este comando muestra el tipo de interfaz (HWtype) en este caso Ethernet (ether), la dirección MAC o dirección Física (HWaddress),

banderas, la máscara y la identificación de la interfaz (Iface) que en este caso es una tarjeta inalámbrica (wlan0).

¿Cómo puedo ver el nombre de dominio y la información IP de un servidor?

Para ver el nombre de dominio se usa el comando **nslookup**. Este comando es útil cuando se realizan instalaciones o configuraciones de servidores y se requiere saber la dirección IP del servidor raíz o información de servidores remotos. También sirve para dar seguimiento a hosts que aparecen recurrentemente en nuestra red. La sintaxis del comando es:

#nslookup domain-name

Realice este ejemplo #nslookup www.utp.ac.pa Anote los resultados.

¿Puedo obtener más información sobre un dominio?

Se puede obtener la información de DNS de un dominio con el comando **dig**, así:

#dig dominio

Este mismo comando con la opción -x permite reservar un host, así:

#dig -x host

¿Cómo puedo recoger información estadística de red?

Para monitorear el comportamiento de una interfaz de red, podemos usar el comando **netstat -i**. Esto podría ayudar cuando se presentan problemas con alguna conexión de red. El resultado del comando despliega el nombre de la interfaz, el número máximo de caracteres que un paquete contiene (MTU), el número de paquetes de entrada recibidos sin error (RX-OK), el número de paquetes de entrada recibidos con error (RX-ERR), el número de paquetes descartados (RX-DRP), y el número de paquetes que no pudieron ser recibidos (RX-OVR). A continuación la salida del comando:

```
Kernel Interface table
```

Experiencia Práctica en Laboratorio No. 6

| Iface | MTU | Met | RX-OK | RX-ERR | RX-DRP | RX-OVR | TX-OK | TX-ERR | TX-DRP | TX-OVR | Flg |
|-------|-------|-----|--------|--------|--------|--------|-------|--------|--------|--------|------|
| eth0 | 1500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | BMU |
| lo | 16436 | 0 | 1173 | 0 | 0 | 0 | 1173 | 0 | 0 | 0 | LRU |
| wlan0 | 1500 | 0 | 182355 | 0 | 0 | 0 | 18173 | 0 | 0 | 0 | BMRU |

Este comando también me permite ver información de la tabla de enrutamiento, a través de la opción -r; así netstat -r; la salida sería como sigue:

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | MSS | Window | irtt | Iface |
|-------------|---------|---------------|-------|-----|--------|------|-------|
| 192.168.0.0 | * | 255.255.255.0 | U | 0 | 0 | 0 | wlan0 |
| loopback | * | 255.0.0.0 | U | 0 | 0 | 0 | lo |
| default | unknown | 0.0.0.0 | UG | 0 | 0 | 0 | wlan0 |

Las tablas de enrutamiento son actualizadas constantemente para reflejar conexiones con otras máquinas. La salida muestra la máquina destino, la dirección de la puerta de enlace (Gateway) a usar, una bandera que muestra si la ruta está activa (U) o si lleva a otra puerta de enlace (G) o a otro host (H), un contador de referencia (Refs) que especifica cuántas conexiones activas se pueden usar simultáneamente, el número de paquetes que pueden ser enviados sobre una ruta (Use) y el nombre de la interfaz (Iface).

¿Cómo puedo saber la ruta para llegar a un host o dominio?

Para conocer por dónde van los paquetes hasta llegar a un destino particular, use el comando **tracert**, por ejemplo:

#tracert www.cwpanama.net

La salida sería así:

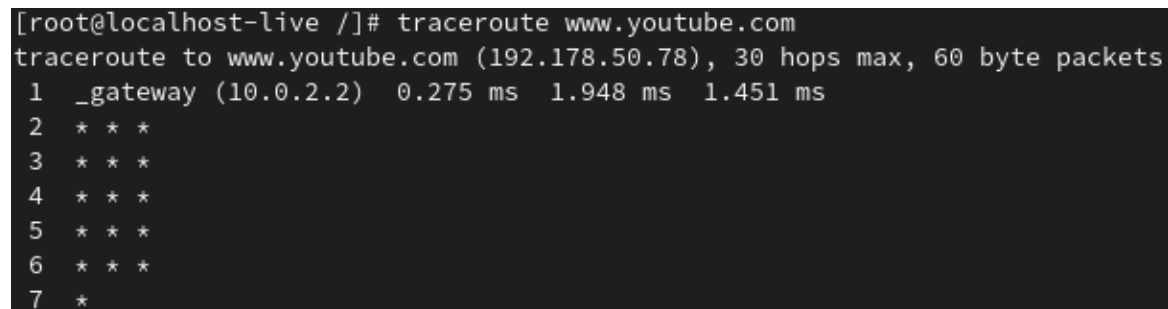
```
tracert www.cwpanama.net
```

```
tracert to www.cwpanama.net (201.224.58.205), 30 hops max, 40 byte packets using UDP
```

```
1  unknown (192.168.0.1)  1.330 ms  2.687 ms  0.829 ms

2  192.168.1.1 (192.168.1.1)  1.949 ms  1.738 ms  1.587 ms
```

Esto indica que se necesitaron dos saltos para llegar al destino, primero saliendo a través de la conexión del dispositivo 192.168.0.1 y luego a través del 192.168.1.1.



```
[root@localhost-live /]# tracert www.youtube.com
tracert to www.youtube.com (192.178.50.78), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.275 ms  1.948 ms  1.451 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *
```

Retroinformación.

1. Entregue cada una de las preguntas de ejercicio.
2. Busque los protocolos de red discutidos en esta experiencia. Describa su función y usos.
 - TCP/IP (Transmission Control Protocol/Internet Protocol): Es el conjunto de protocolos fundamentales utilizado en Internet y en la mayoría de las redes locales. TCP se encarga de garantizar la entrega ordenada y confiable de los datos, mientras que IP se encarga del enrutamiento y direccionamiento de los paquetes.
 - ICMP (Internet Control Message Protocol): Es un protocolo utilizado para enviar mensajes de control y diagnóstico dentro de una red. Se utiliza, por ejemplo, para enviar mensajes de error y mensajes de solicitud de eco utilizados en el comando "ping".

3. ¿En qué situaciones específicas considera que serían útiles los comandos utilizados?

- Obtener información de red: El comando `ip addr show` proporciona una visión general de la configuración de red de todas las interfaces disponibles. Esto puede ser útil para diagnosticar problemas de conectividad, verificar la configuración IP asignada a cada interfaz y obtener información sobre la dirección MAC y la dirección de broadcast.
- Cambiar la configuración de red: El comando `ip` permite modificar la configuración de las interfaces de red, como cambiar la dirección IP y la máscara de subred. Esto puede ser útil cuando se requiere una nueva configuración de red, como cambiar una dirección IP estática o ajustar la configuración de una interfaz para adaptarse a una red específica.
- Solucionar problemas de conectividad: Al utilizar los comandos mencionados, puedes verificar la configuración de red, comprobar si las interfaces están activas o inactivas, y ver detalles como la dirección IP y la dirección MAC. Estos comandos son útiles para diagnosticar problemas de conectividad, como la falta de respuesta de una interfaz de red o configuraciones incorrectas de IP o máscara de subred.
- Administrar y configurar rutas de red: El comando `ip` también permite administrar las rutas de red, incluyendo la adición, eliminación y modificación de rutas. Esto es útil cuando se necesita configurar rutas estáticas o ajustar el enrutamiento de red para optimizar el tráfico.
- Manipular políticas de red: El comando `ip` ofrece funcionalidades avanzadas para manipular políticas y marcas de paquetes. Esto puede ser útil para implementar reglas de filtrado de paquetes, redirecciones o cualquier otra configuración avanzada relacionada con la gestión del tráfico de red.

4. ¿Qué dificultades encontró durante el desarrollo del laboratorio?

Algunos comandos no me funcionaron por mas que lo intenté

5. ¿Qué mejoraría de esta experiencia de laboratorio?

Colocar algunas opciones extras en los comandos, pues en algunos casos no se utilizan los mismos, a veces depende de la versión del sistema operativo, varían o no los comandos.

Referencias:

1. Linux Network Configuration:

<http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworking.html>

2. Kernighan, B. y Pike, R. El Entorno de programación Unix. Prentice Hall.
3. Husain, Kamran y Parker, Timoty, et al. **Linux Unleashed**. Second Edition.