

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 00:18: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 #

```

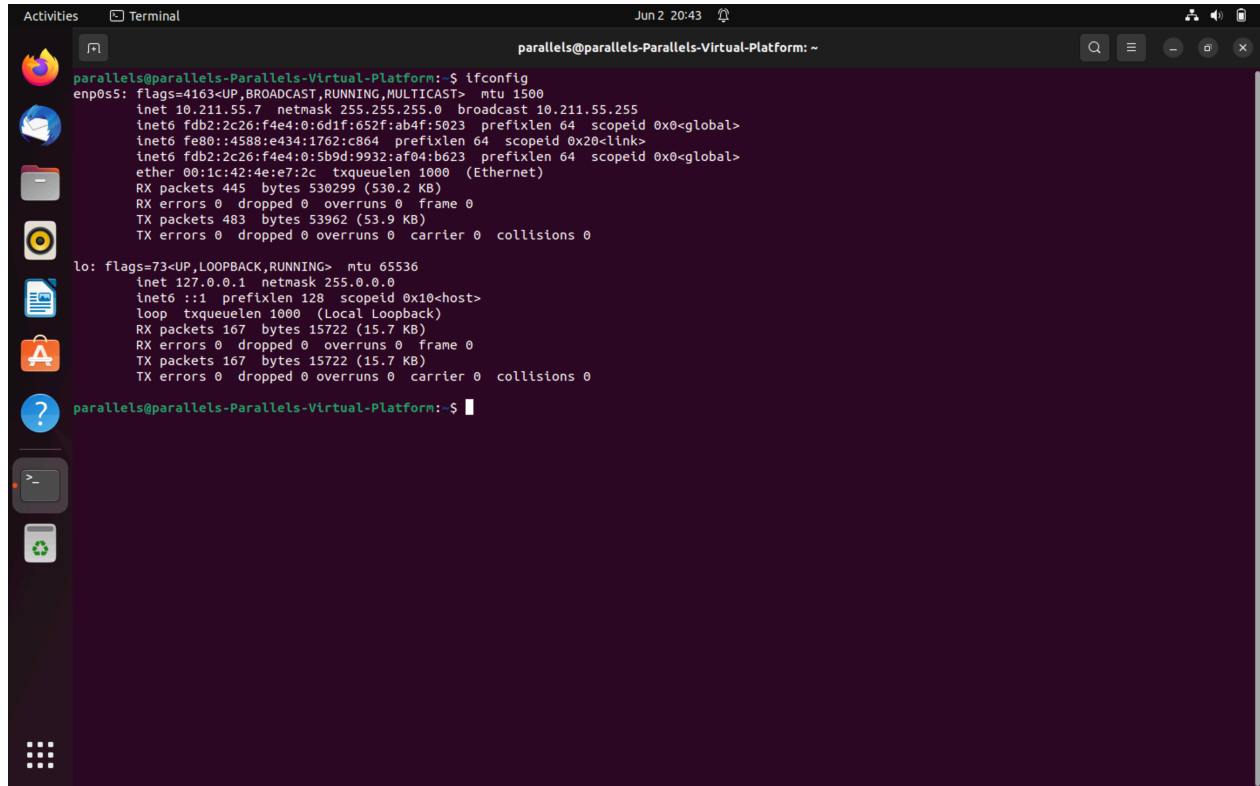
| | |
|--------------------|---|
| eth0 | es la tarjeta de red Ethernet del equipo |
| lo-loopback | se refiere a la pila de protocolos TCP/IP en el equipo. Si hubiese problemas en la pila, basta con ejecutar el comando ping a la dirección 127.0.0.1 para comprobar que la pila de protocolos está funcionando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



```
parallels@parallels-Parallels-Virtual-Platform: ~  
$ ifconfig  
enp0s5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.211.55.7 netmask 255.255.255.0 broadcast 10.211.55.255  
    inet6 fdb2:2c26:f4e4:0:6d1f:652f:ab4f:5023 prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::4588:e434:1762:c864 prefixlen 64 scopeid 0x20<link>  
    inet6 fdb2:2c26:f4e4:0:5b9d:9932:af04:b623 prefixlen 64 scopeid 0x0<global>  
    ether 00:1c:42:4e:e7:2c txqueuelen 1000 (Ethernet)  
    RX packets 445 bytes 530299 (530.2 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 483 bytes 53962 (53.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 167 bytes 15722 (15.7 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 167 bytes 15722 (15.7 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
parallels@parallels-Parallels-Virtual-Platform: $
```

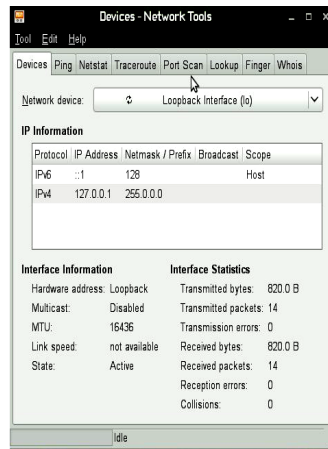
IP Address: 10.211.55.7

MAC Address: 00:1c:42:4e:e7:2c

Netmask: 255.255.255.0

Broadcast Address: 10.211.55.255

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.

```

link-local 169.254.0.0
parallels@parallels-Parallels-Virtual-Platform:~$ cat /etc/protocols
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers and other
# sources.
# New protocols will be added on request if they have been officially
# assigned by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.
ip 0 IP # Internet protocol, pseudo protocol number
hopopt 0 HOPOPT # IPv6 Hop-by-Hop Option [RFC1883]
icmp 1 ICMP # Internet control message protocol
igmp 2 IGMP # Internet Group Management
ggp 3 GGP # gateway-gateway protocol
ipencap 4 IP-ENCAP # IP encapsulated in IP (officially ``IP'')
st 5 ST # ST datagram mode
tcp 6 TCP # transmission control protocol
egp 8 EGP # exterior gateway protocol
igrp 9 IGRP # any private interior gateway (Cisco)
pup 12 PUP # PARC universal packet protocol
udp 17 UDP # user datagram protocol
hmp 20 HMP # host monitoring protocol
xns-ldp 22 XNS-IDP # Xerox NS IDP
rdp 27 RDP # "reliable datagram" protocol
iso-tp4 29 ISO-TP4 # ISO Transport Protocol class 4 [RFC905]
dccp 33 DCCP # Datagram Congestion Control Prot. [RFC4340]
xtp 36 XTP # Xpress Transfer Protocol
ddp 37 DDP # Datagram Delivery Protocol
idpr-cmtp 38 IDPR-CMTP # IDPR Control Message Transport
ipv6 41 IPv6 # Internet Protocol, version 6
ipv6-route 43 IPv6-Route # Routing Header for IPv6
ipv6-frag 44 IPv6-Frag # Fragment Header for IPv6
idrp 45 IDRP # Inter-Domain Routing Protocol
rsvp 46 RSVP # Reservation Protocol
gre 47 GRE # General Routing Encapsulation
esp 50 IPSEC-ESP # Encap Security Payload [RFC2406]
ah 51 IPSEC-AH # Authentication Header [RFC2402]
skip 57 SKIP # SKIP
ipv6-icmp 58 IPv6-ICMP # ICMP for IPv6
ipv6-nonxt 59 IPv6-Nonxt # No Next Header for IPv6
ipv6-opts 60 IPv6-Opts # Destination Options for IPv6
rsfp 73 RSFP CPHB # Radio Shortest Path First (officially CPHB)
vntp 81 VNTTP # Versatile Message Transport
efirdp 88 EFIRDP # Enhanced Interior Routing Protocol (Cisco)
  
```

1

```
parallels@parallels-Parallels-Virtual-Platform:~$ cat /etc/networks
```

symbolic names for networks, see networks(5) for more information

link-local 169.254.0.0. → **MUESTRA REDES A LA QUE SE CONECTA FRECUENTE, DEBIDO A LA MI CONFIGURACIÓN DE VM, LA VM SE CONECTA DIRECTAMENTE ES CON MI COMPUTADORA DONDE ESTA EL HYPERVISOR.**

2

Updated from <http://www.iana.org/assignments/protocol-numbers> and other

sources.

New protocols will be added on request if they have been officially

assigned by IANA and are not historical.

If you need a huge list of used numbers please install the nmap package.

ip 0 IP # internet protocol, pseudo protocol number

→ SE PUEDE VER EL PROTOCOLO IP EN etc/protocols, ESTE SIEMPRE SUELE ESTAR LISTADO DE PRIMERO

3

parallels@parallels-Parallels-Virtual-Platform:~\$ resolvectl status

Global

Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

resolv.conf mode: stub

Link 2 (enp0s5)

Current Scopes: DNS

Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Current DNS Server: 10.211.55.1

DNS Servers: 10.211.55.1

DNS Domain: localdomain

→ SE PUEDE APRECIAR LOS SERVIDORES DE DNS USADOS PARA EL SOLVE DE IPS EN MI VM.

4

parallels@parallels-Parallels-Virtual-Platform:~\$ cat /etc/services

Network services, Internet style

#

Updated from <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml> .

#

New ports will be added on request if they have been officially assigned

by IANA and used in the real-world or are needed by a debian package.

If you need a huge list of used numbers please install the nmap package.

```
tcpmux      1/tcp      # TCP port service multiplexer
```

→ SE PUEDE APRECIAR QUE EN CUANTO A SERVICIOS, EL MULTIPLEXOR PARA TRANSMISSION CONTROL PROTOCOL

5

```
# UNIX specific services
```

```
#
```

```
exec      512/tcp
biff      512/udp      comsat
login     513/tcp
who       513/udp      whod
shell     514/tcp      cmd syslog      # no passwords used
```

→ SE PUEDE APRECIAR QUE HAY UNA SECCIÓN DE SERVICES PROPIA PARA UNIX, DONDE SE ENCUENTRAN SERVICIOS COMO SHELL.

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

Se puede usar el comando **ip**.

Para cambiar la configuración TCP/IP de una interfaz de red manualmente en un sistema Ubuntu, puedes seguir estos pasos:

Abre una terminal en tu sistema Ubuntu.

Verifica el nombre de la interfaz de red para la cual deseas cambiar la configuración.

Puedes usar el comando **ifconfig** o **ip** para obtener una lista de las interfaces disponibles. Por ejemplo, supongamos que deseas cambiar la configuración de la interfaz **eth0**.

Desactiva la interfaz ejecutando el siguiente comando (reemplaza **eth0** con el nombre de tu interfaz):

sudo ifconfig eth0 down

Cambia la configuración TCP/IP ejecutando el siguiente comando (reemplaza los valores con los adecuados para tu red):

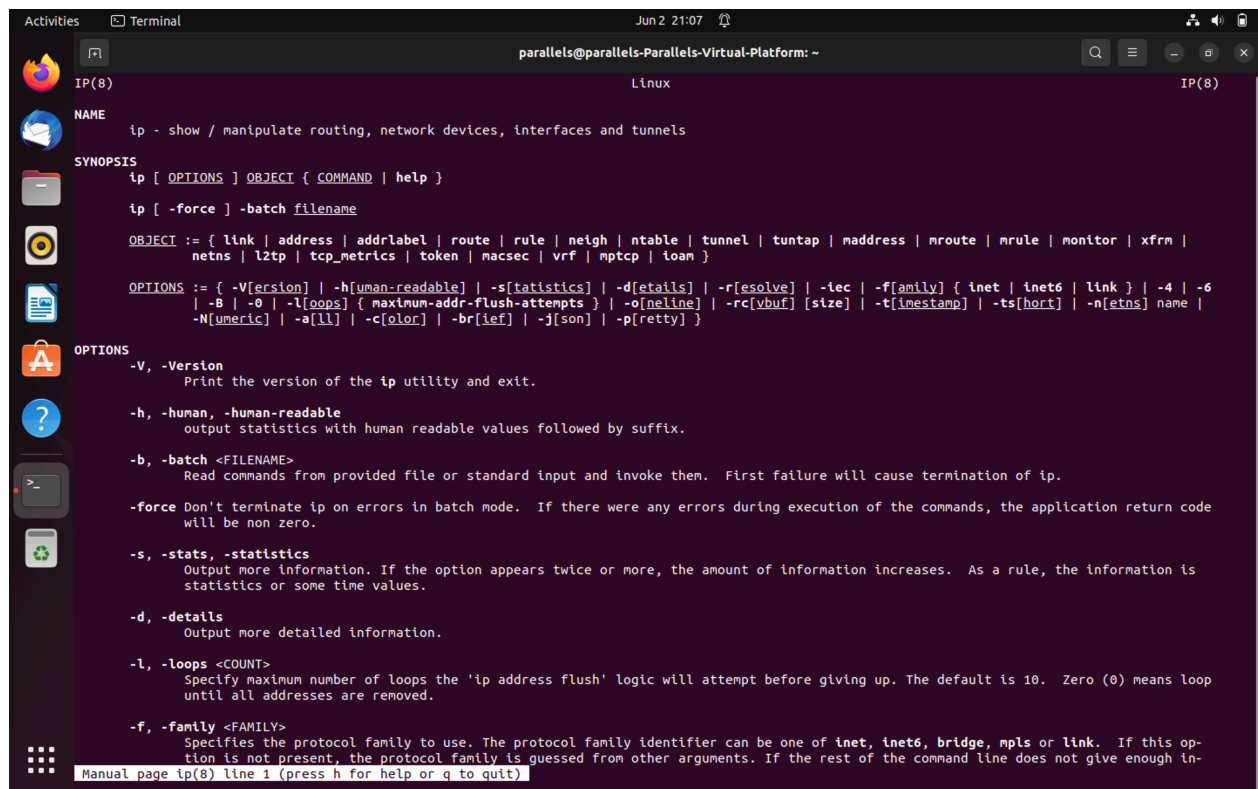
sudo ifconfig eth0 <nueva_dirección_IP> netmask <máscara_de_red>

Por ejemplo: **sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0**

Activa la interfaz nuevamente ejecutando el siguiente comando: **sudo ifconfig eth0 up**

Con estos pasos, has cambiado manualmente la configuración TCP/IP de la interfaz de red especificada en tu sistema Ubuntu. Recuerda reemplazar eth0 con el nombre correcto de tu interfaz y ajustar los valores de dirección IP y máscara de red según tus necesidades.

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?



```
parallels@parallels-Parallels-Virtual-Platform: ~
IP(8)
Linux
NAME
ip - show / manipulate routing, network devices, interfaces and tunnels

SYNOPSIS
ip [ OPTIONS ] OBJECT { COMMAND | help }
ip [ -force ] -batch filename

OBJECT := { link | address | addrlabel | route | rule | neigh | ntable | tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
netns | lztp | tcp_metrics | token | macsec | vrf | mptcp | toam }

OPTIONS := { -V[ersion] | -h[uman-readable] | -s[tatistics] | -d[etails] | -r[esolve] | -l[c] | -f[amily] { inet | inet6 | link } | -4 | -6
| -B | -0 | -l[oops] { maximum-addr-flush-attempts } | -o[neline] | -rc[vbuf] [size] | -t[imestamp] | -ts[hort] | -n[etns] name |
-N[umeric] | -a[ll] | -c[olor] | -br[ief] | -j[son] | -p[retty] }

OPTIONS
-V, -Version
Print the version of the ip utility and exit.

-h, -human, -human-readable
output statistics with human readable values followed by suffix.

-b, -batch <FILENAME>
Read commands from provided file or standard input and invoke them. First failure will cause termination of ip.

-force
Don't terminate ip on errors in batch mode. If there were any errors during execution of the commands, the application return code
will be non zero.

-s, -stats, -statistics
Output more information. If the option appears twice or more, the amount of information increases. As a rule, the information is
statistics or some time values.

-d, -details
Output more detailed information.

-l, -loops <COUNT>
Specify maximum number of loops the 'ip address flush' logic will attempt before giving up. The default is 10. Zero (0) means loop
until all addresses are removed.

-f, -family <FAMILY>
Specifies the protocol family to use. The protocol family identifier can be one of inet, inet6, bridge, mpls or link. If this op-
tion is not present, the protocol family is guessed from other arguments. If the rest of the command line does not give enough in-
Manual page ip(8) line 1 (press h for help or q to quit)
```

En cuanto al procedimiento para cambiar la dirección de una interfaz utilizando el comando ip, sigue estos pasos:

Abre una terminal en tu sistema Ubuntu.

Verifica el nombre de la interfaz de red para la cual deseas cambiar la dirección IP. Puedes usar el comando ip a para obtener una lista de las interfaces disponibles.

Desactiva la interfaz ejecutando el siguiente comando (reemplaza <nombre_interfaz> con el nombre de tu interfaz):

sudo ip link set <nombre_interfaz> down

Cambia la dirección IP de la interfaz ejecutando el siguiente comando (reemplaza <nueva_dirección_IP> con la dirección IP que deseas asignar):

```
sudo ip addr add <nueva_dirección_IP>/CIDR dev <nombre_interfaz>
```

Por ejemplo: **sudo ip addr add 192.168.1.100/24 dev eth0**

Asegúrate de reemplazar <nombre_interfaz> con el nombre correcto de tu interfaz y <nueva_dirección_IP> con la dirección IP que deseas asignar.

Activa la interfaz nuevamente ejecutando el siguiente comando:

```
sudo ip link set <nombre_interfaz> up
```

¿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
```

Experiencia Práctica en Laboratorio No. 6

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?

¿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 intefaz (Iface) que en este caso es una tarjeta inalámbrica (wlan0).

Experiencia Práctica en Laboratorio No. 6

```
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 | irrtt | 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 **traceroute**, por ejemplo:

#traceroute 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.

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.

IP (Internet Protocol): El Protocolo de Internet (IP) es el protocolo fundamental en Internet y proporciona la capacidad de interconectar redes y enrutar paquetes de datos entre ellas. IP es responsable de asignar direcciones IP únicas a los dispositivos en una red, fragmentar y reensamblar los paquetes de datos para su transporte y manejar el enrutamiento de los paquetes a través de la red.

- **Uso:** IP se utiliza para enviar paquetes de datos a través de Internet y redes locales. Es esencial para la comunicación entre dispositivos en una red IP y permite que los paquetes de datos lleguen a su destino correcto a través del enrutamiento.

TCP (Transmission Control Protocol): El Protocolo de Control de Transmisión (TCP) es un protocolo orientado a la conexión que proporciona una transmisión de datos confiable y ordenada. TCP segmenta los datos en paquetes, los envía a través de la red y garantiza que lleguen sin errores y en el orden correcto. También maneja el control de flujo y la congestión para evitar la pérdida de datos.

- **Uso:** TCP se utiliza en aplicaciones que requieren una entrega confiable de datos, como navegación web, correo electrónico, transferencia de archivos, streaming de video y muchas otras aplicaciones basadas en Internet.

UDP (User Datagram Protocol): El Protocolo de Datagramas de Usuario (UDP) es un protocolo sin conexión que proporciona una entrega no confiable de datos. A diferencia de TCP, UDP no garantiza la entrega ordenada ni la detección de errores. Es más rápido y eficiente que TCP, pero no ofrece la misma fiabilidad.

- **Uso:** UDP se utiliza en aplicaciones que requieren una transmisión rápida de datos, como videoconferencias, servicios de transmisión en tiempo real, juegos en línea y aplicaciones de voz sobre IP (VoIP).

HTTP (Hypertext Transfer Protocol): El Protocolo de Transferencia de Hipertexto (HTTP) es un protocolo de aplicación utilizado para la transferencia de datos en la web. HTTP define la estructura y el formato de las solicitudes y respuestas entre los clientes (navegadores web) y los servidores web.

- **Uso:** HTTP se utiliza para acceder y visualizar páginas web, cargar y descargar archivos, enviar formularios en línea y realizar solicitudes y respuestas entre clientes y servidores en aplicaciones web.

DNS (Domain Name System): El Sistema de Nombres de Dominio (DNS) es un protocolo utilizado para convertir los nombres de dominio legibles para los humanos en direcciones IP numéricas. DNS permite la resolución de nombres, lo que significa que traduce los nombres de dominio (como example.com) en direcciones IP (como 192.0.2.1) para que los dispositivos puedan encontrar los recursos de red correspondientes.

- **Uso:** DNS se utiliza en todos los aspectos de la comunicación en Internet, como la navegación web, el envío y recepción de correos electrónicos, la transferencia de archivos, la transmisión de contenido multimedia y cualquier otra actividad que involucre la identificación y localización de recursos basados en nombres de dominio.

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

ifconfig: El comando ifconfig se utiliza para configurar y mostrar información sobre las interfaces de red en un sistema. Algunas situaciones en las que puede ser útil son:

- Obtener información detallada sobre las direcciones IP asignadas a las interfaces de red.

- Verificar la configuración de red actual, incluyendo dirección IP, máscara de red y estado de la interfaz.
- Cambiar manualmente la configuración de red de una interfaz, como la dirección IP y la máscara de red.

ping: El comando ping se utiliza para verificar la conectividad y la latencia entre un dispositivo de origen y un dispositivo de destino en una red. Algunas situaciones en las que puede ser útil son:

- Verificar si un host remoto está accesible en la red.
- Comprobar la latencia (tiempo de ida y vuelta) entre el dispositivo local y un host remoto.
- Diagnosticar problemas de conectividad, como paquetes perdidos o altos tiempos de respuesta.

dig: El comando dig (Domain Information Groper) se utiliza para realizar consultas DNS y obtener información sobre los registros DNS de un dominio. Algunas situaciones en las que puede ser útil son:

- Obtener información detallada sobre los registros DNS de un dominio, como los registros A, CNAME, MX, NS, etc.
- Verificar la configuración DNS de un dominio y solucionar problemas relacionados con la resolución de nombres.
- Obtener direcciones IP asociadas con un nombre de dominio específico.

tracert: El comando tracert se utiliza para rastrear la ruta que siguen los paquetes desde el dispositivo local hasta un destino en una red. Algunas situaciones en las que puede ser útil son:

- Identificar los saltos (routers) que atraviesan los paquetes en la ruta hacia un destino.
- Determinar la latencia (tiempo de ida y vuelta) en cada salto de la ruta.
- Diagnosticar problemas de enrutamiento, como rutas incorrectas o paquetes que se pierden en el camino.

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

No encontré ninguna dificultad en el desarrollo del laboratorio.

5. ¿Qué mejoraría de esta experiencia de laboratorio?

Opino que este laboratorio sería perfecto para presentar nmap (Network Map), ya que a nivel profesional es muy usado ya que permite escaneo de puertos, descubrir hosts, identificar servicios/versiones y en general es una herramienta poderosa y común para SysAdmins como herramienta de chequeo de seguridad.

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.