



Apunte de comandos para TyR

Compendio de comandos necesarios para abordar las practicas de laboratorio de la asignatura Teleinformatica y Redes (10040).

Obtener acceso root

```
$ su -  
Contraseña: *****  
# <comando como root>
```

Comando ip

Comando general para manipulación y consulta de parametros de red, interfaces, etc...

Con la opción -6, el comando tiene efecto sobre el stack del protocolo ipv6

```
# ip <module> [<parametros>]  
# ip -6 <module> [<parametros>]  
$ man ip  
$ man ip-<module>
```

Comando ip link

Configura y Muestra información sobre interfaces de red.

```
$ ip link show  
$ ip link show INTERFAZ  
$ man ip-link
```

Activar interfaces disponibles:

```
# ip link set group default up # Todas las interfaces  
# ip link set dev INTERFAZ up # La interfaz de nombre INTERFAZ
```

Comando ip address

Administra y muestra los parametros de red

```
# ip addr add dev INTERFAZ DIRECCIÓN_IP/PREFIJO_MÁSCARA  
$ ip addr show  
# ip -6 addr add dev INTERFAZ DIRECCIÓN_IP/PREFIJO_MÁSCARA  
$ ip -6 addr show  
$ man ip-address
```

Comando ip maddress

Administra y muestra los parametros de direcciones multicast

```
$ ip maddr show  
$ ip -6 maddr show  
$ man ip-maddress
```



Comando ip route

Administra y muestra la tabla de rutas

```
$ ip route show
# ip route add DIRECCION_RED/PREFIJO_MASCARA via IP_GATEWAY dev INTERFAZ
# ip route add default via DEFAULT_GATEWAY
$ ip -6 route show
# ip -6 route add DIRECCION_RED/PREFIJO_MASCARA via IP_GATEWAY dev INTERFAZ
# ip -6 route add default via DEFAULT_GATEWAY
$ man ip-route
```

Comando ping

Herramienta de diagnostico de red. Permite verificar si la configuración de red (hasta capa 3) funciona adecuadamente.

```
$ ping DIRECCIÓN_IP
$ man ping
```

Comando hostname

Permite consultar y editar el nombre del host

```
$ hostname
# hostname NOMBRE_EQUIPO
```

(Esta edicion es efimera, al reiniciar el equipo se pierde)

Comando tcpdump

Permite crear capturas de red y volcarlas a un archivo para su posterior analisis.

Ejemplos de captura:

```
# tcpdump -n -p -w NOMBRE_ARCHIVO.PCAP 'icmp && host DIRECCION_IP'
# tcpdump -n -p -w NOMBRE_ARCHIVO.PCAP 'tcp && host DIRECCION_IP'
$ man tcpdump
```

- El primer comando captura todo el trafico de protocolo ICMP dirigido a la IP DIRECCION_IP.
- El segundo comando, permite capturar todo el trafico que en capa 4 utilice el protocolo TCP y dirigido a la ip DIRECCION_IP.
- El ultimo comando nos permite acceder al manual de ayuda del comando.

Comando tshark

Permite realizar o analizar capturas.

Ejemplos para analizar capturas:

```
tshark -r NOMBRE_ARCHIVO.PCAP
tshark -r NOMBRE_ARCHIVO.PCAP -nV
tshark -r NOMBRE_ARCHIVO.PCAP -O tcp
tshark -r NOMBRE_ARCHIVO.PCAP -nqz follow,tcp,hex,0
```



Comando `nc` : NetCat

Es un comando multipropósito que permite enviar datos desde teclado a través de una conexión con un servidor TCP, o bien operar como un servidor TCP en espera de conexiones y mostrar en pantalla los datos que recibe. Con el parámetro `-u` opera sobre transporte UDP, pudiendo tanto enviar como recibir mensajes UDP en un puerto arbitrario.

Para iniciar un proceso de tipo Servidor:

```
nc -l -p <NRO_DE_PUERTO>
```

Para realizar una conexión como cliente:

```
nc <IP_HOST_SERVIDOR> <NRO_DE_PUERTO_SERVIDOR>
```

Una vez establecida la conexión, la entrada estándar del proceso `nc` se reenviará al otro extremo de la conexión, donde la instancia par de `nc` la copiará en su salida estándar. Ahora pruebe escribir mensajes en su consola, recordando que la comunicación es bidireccional. Una vez realizado el intercambio de mensajes en ambos sentidos, puede finalizar la conexión enviando EOF (Ctrl+D) o deteniendo el proceso `nc` (Ctrl+C) desde cualquiera de los hosts.

Comando `telnet`

El cliente y servidor de telnet no suele venir instalado por defecto. En sistemas Debian o similares se lo suele instalar con el gestor de paquetes:

```
apt-get install telnet telnetd
```

Para iniciar una sesión telnet hacia un equipo servidor:

```
telnet IP_HOST_SERVIDOR
```

Una sesión telnet se finaliza tecleando `exit`.

Comando `ss`

Permite verificar el estado de las conexiones de red de un dispositivo

Ejemplo

```
ss -ltnp
```

El comando anterior muestra las conexiones que estén en estado *listening* (opción `l`), que sean conexiones TCP (opción `t`), mostar el ID de proceso (opción `p`) y no resuelve puertos ni ips (opción `n`).

Una alternativa en desuso es el comando `netstat`.

Comando `ps`

Permite obtener un listado de procesos del sistema. Se puede ejecutar sin parámetros.

```
ps
```



Archivos relevantes del sistema

En todos los casos puede utilizar el editor `nano` para editar los archivos.

- `/etc/hostname` permite modificar el nombre del host.
- `/etc/hosts` permite la gestión manual de la resolución de nombres.

Generales

Documentacion de un comando

`$ man comando`

Prompt

Son los primeros caracteres a la izquierda de la terminal:

`usuario@host:~$`

Indican que la consola esta lista para recibir comandos. En caso de administrador (root) se ve asi:

`root@host:~#`

Habitualmente se usan los caracteres `$` y `#` para indicar si un comando debe ejecutarse como usuario normal (sin privilegios) o como administrador (root), respectivamente.