

Universidad Politécnica de Quintana Roo



UNIVERSIDAD
POLITÉCNICA
DE QUINTANA ROO

Formando Triunfadores

Ingeniería en software 27 Av

Alumno: Canche Ucan Yoshua
Leonardo

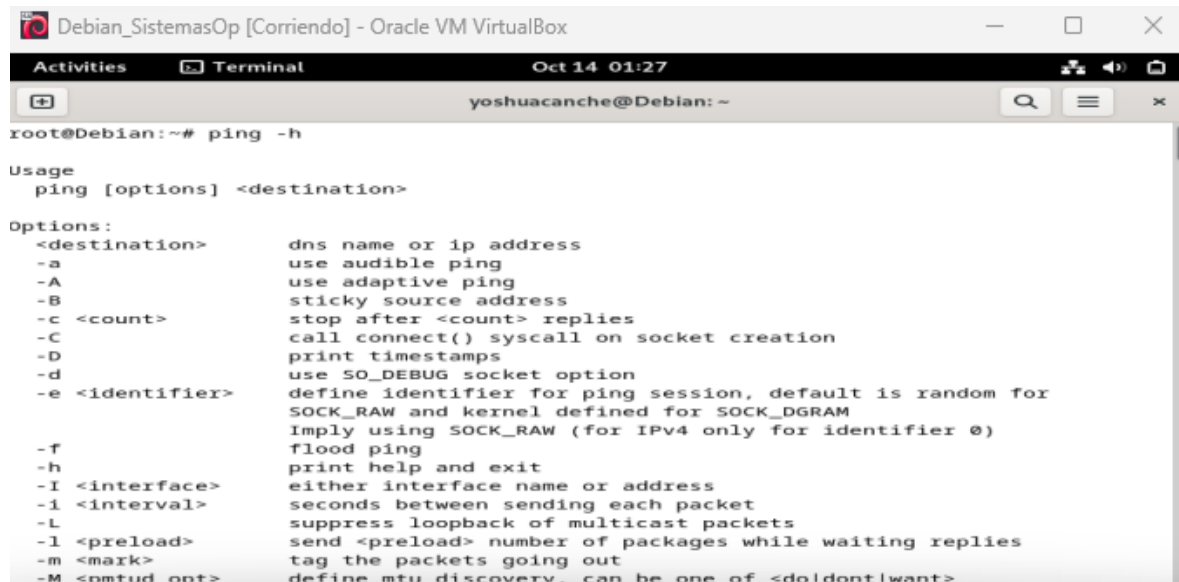
Materia : Sistema Operativos

Fecha:12-10-2023

Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola de Ms:

DOS

1-Obtener la ayuda del comando ping

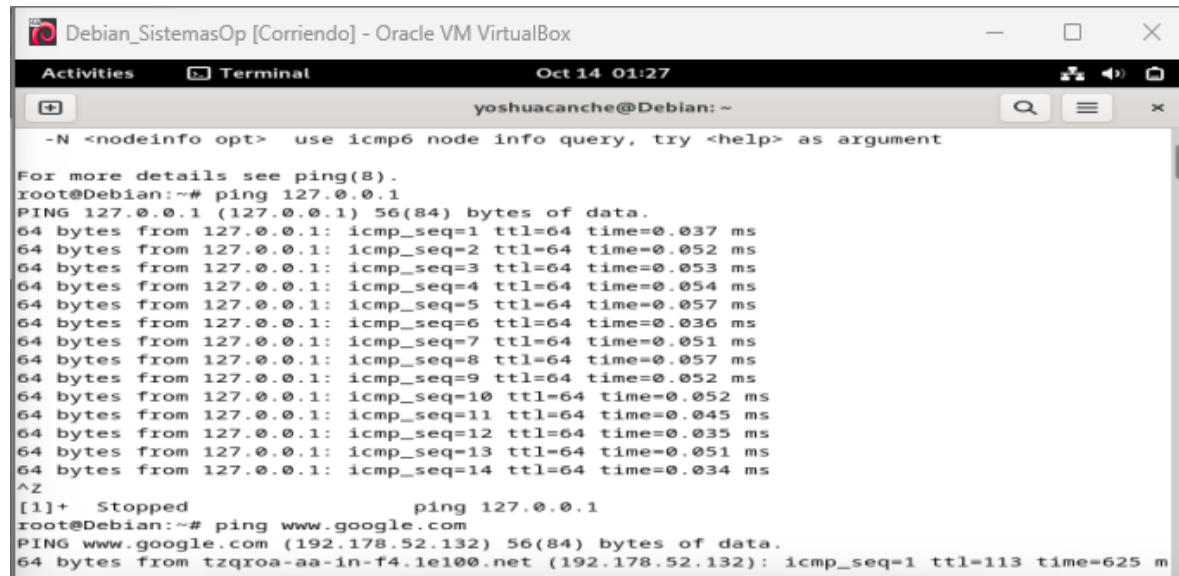


```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 01:27
yoshuacanche@Debian: ~
root@Debian:~# ping -h

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
  -C                 call connect() syscall on socket creation
  -D                 print timestamps
  -d                 use SO_DEBUG socket option
  -e <identifier>    define identifier for ping session, default is random for
                     SOCK_RAW and kernel defined for SOCK_DGRAM
                     (for IPv4 only for identifier 0)
  -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 <mtuopt>         define mtu discovery, can be one of <dodontwant>
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro



```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 01:27
yoshuacanche@Debian: ~
-N <nodeinfo opt> use icmp6 node info query, try <help> as argument

For more details see ping(8).
root@Debian:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.053 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.052 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.034 ms
^Z
[1]+  Stopped                  ping 127.0.0.1
root@Debian:~# ping www.google.com
PING www.google.com (192.178.52.132) 56(84) bytes of data.
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=1 ttl=113 time=625 m
```

3.- Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones

```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 01:28
yoshuacanche@Debian: ~
root@Debian:~# ping www.google.com
PING www.google.com (192.178.52.132) 56(84) bytes of data.
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=1 ttl=113 time=625 m
s
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=2 ttl=113 time=114 m
s
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=3 ttl=113 time=76.0
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=4 ttl=113 time=74.8
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=5 ttl=113 time=77.2
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=6 ttl=113 time=75.0
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=7 ttl=113 time=73.9
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=8 ttl=113 time=74.1
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=9 ttl=113 time=74.6
ms
64 bytes from tzqroa-aa-in-f4.1e100.net (192.178.52.132): icmp_seq=10 ttl=113 time=75.0
ms
^C
--- www.google.com ping statistics ---
```

Si hay conectividad por que los paquetes son enviados

4-Obtener la ayuda del comando nslookup

```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 00:57
yoshuacanche@Debian: ~
NSLOOKUP(1) BIND 9 NSLOOKUP(1)
NAME
    nslookup - query Internet name servers interactively
SYNOPSIS
    nslookup [-option] [name | -] [server]
DESCRIPTION
    nslookup is a program to query Internet domain name servers. nslookup has
    two modes: interactive and non-interactive. Interactive mode allows the user
    to query name servers for information about various hosts and domains or to
    print a list of hosts in a domain. Non-interactive mode prints just the name
    and requested information for a host or domain.
ARGUMENTS
    Interactive mode is entered in the following cases:
    a. when no arguments are given (the default name server is used);
    b. when the first argument is a hyphen (-) and the second argument is the
        host name or Internet address of a name server.
Manual page nslookup(1) line 1 (press h for help or q to quit)
```

5-Resolver la direccion ip de https://upqroo.edu.mx/ usando nslookup

```
root@Debian:~# man nslookup
root@Debian:~# nslookup upqroo.edu.mx
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
Name:   upqroo.edu.mx
```

6-Hacer ping a la ip obtenida en el paso anterior, anotar conclusiones

```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 01:29
yoshuacanche@Debian: ~
root@Debian:~# ping 77.68.126.20
PING 77.68.126.20 (77.68.126.20) 56(84) bytes of data.
64 bytes from 77.68.126.20: icmp_seq=1 ttl=49 time=882 ms
64 bytes from 77.68.126.20: icmp_seq=2 ttl=49 time=252 ms
64 bytes from 77.68.126.20: icmp_seq=3 ttl=49 time=171 ms
64 bytes from 77.68.126.20: icmp_seq=4 ttl=49 time=227 ms
64 bytes from 77.68.126.20: icmp_seq=5 ttl=49 time=217 ms
64 bytes from 77.68.126.20: icmp_seq=6 ttl=49 time=241 ms
64 bytes from 77.68.126.20: icmp_seq=7 ttl=49 time=264 ms
64 bytes from 77.68.126.20: icmp_seq=8 ttl=49 time=183 ms
64 bytes from 77.68.126.20: icmp_seq=9 ttl=49 time=207 ms
64 bytes from 77.68.126.20: icmp_seq=10 ttl=49 time=229 ms
64 bytes from 77.68.126.20: icmp_seq=11 ttl=49 time=251 ms
64 bytes from 77.68.126.20: icmp_seq=12 ttl=49 time=125 ms
64 bytes from 77.68.126.20: icmp_seq=13 ttl=49 time=193 ms
64 bytes from 77.68.126.20: icmp_seq=14 ttl=49 time=124 ms
64 bytes from 77.68.126.20: icmp_seq=15 ttl=49 time=127 ms
64 bytes from 77.68.126.20: icmp_seq=16 ttl=49 time=126 ms
64 bytes from 77.68.126.20: icmp_seq=17 ttl=49 time=126 ms
64 bytes from 77.68.126.20: icmp_seq=18 ttl=49 time=129 ms
64 bytes from 77.68.126.20: icmp_seq=19 ttl=49 time=124 ms
64 bytes from 77.68.126.20: icmp_seq=20 ttl=49 time=126 ms
64 bytes from 77.68.126.20: icmp_seq=21 ttl=49 time=127 ms
64 bytes from 77.68.126.20: icmp_seq=22 ttl=49 time=126 ms
64 bytes from 77.68.126.20: icmp_seq=23 ttl=49 time=125 ms
```

Si se pudo conectar

7-Obtener la ayuda del comando netstat

```
Debian_SistemasOp [Corriendo] - Oracle VM VirtualBox
Activities Terminal Oct 14 01:30
yoshuacanche@Debian: ~
rtt min/avg/max/mdev = 123.347/145.551/881.576/78.945 ms
root@Debian:~# ss -h
Usage: ss [ OPTIONS ]
       ss [ OPTIONS ] [ FILTER ]
-h, --help          this message
-V, --version       output version information
-n, --numeric       don't resolve service names
-r, --resolve       resolve host names
-a, --all           display all sockets
-l, --listening     display listening sockets
-o, --options       show timer information
-e, --extended      show detailed socket information
-m, --memory        show socket memory usage
-p, --processes     show process using socket
-T, --threads       show thread using socket
-i, --info          show internal TCP information
-t, --tipcinfo      show internal tipc socket information
-s, --summary       show socket usage summary
--tos              show tos and priority information
--cgroup           show cgroup information
-b, --bpf          show bpf filter socket information
-E, --events        continually display sockets as they are destroyed
-Z, --context       display task SELinux security contexts
-z, --contexts      display task and socket SELinux security contexts
-N, --net           switch to the specified network namespace name
```

8-Mostrar todas las conexiones y puertos de escucha

```
root@Debian:~# ss -ltn
LISTENING|CLOSING|
root@Debian:~# lsof -i -n
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
avahi-daemon 461 avahi 12u IPv4 14890 0t0 UDP *:mdns
avahi-daemon 461 avahi 13u IPv6 14891 0t0 UDP *:mdns
avahi-daemon 461 avahi 14u IPv4 14892 0t0 UDP *:43530
avahi-daemon 461 avahi 15u IPv6 14893 0t0 UDP *:39274
NetworkManager 514 root 26u IPv4 16485 0t0 UDP 10.0.2.15:bootpc->10.0.2.2:bootps
cupsd 552 root 6u IPv6 15564 0t0 TCP [::]:ipp (LISTEN)
cupsd 552 root 7u IPv4 15565 0t0 TCP 127.0.0.1:ipp (LISTEN)
cups-brow 594 root 7u IPv4 15732 0t0 UDP *:631
```

9- Ejecutar netstat sin resolver nombres de dominio o puertos

```

root@Debian:~# ss -n
Netid State Recv-Q Send-Q
Peer Address:Port
Local Address:Port
Process
u_str ESTAB 0 0 * 18473 * 17946
u_str ESTAB 0 0 * 19124 /run/user/1000/bus 19125
u_str ESTAB 0 0 * 18364 * 18363
u_str ESTAB 0 0 * 18686 * 18685
u_str ESTAB 0 0 * 15453 * 15448
u_str ESTAB 0 0 * 19611 * 19607
u_str ESTAB 0 0 * 19848 * 19847
u_str ESTAB 0 0 * 19829 * 19120

```

10-Mostrar las conexiones TCP

```

root@Debian:~# ss -tn
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

```

11-Mostrar las conexiones UDP

```

root@Debian:~# ss -un
Recv-Q Send-Q Local Address:Port Peer Address:Port Process
0 0 10.0.2.15:enp0s3:68 10.0.2.2:67

```

12-Utilizar el comando tasklist

```

root@Debian:~# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.6 102344 12332 ?        Ss   00:36   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S    00:36   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   00:36   0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I<   00:36   0:00 [rcu_par_gp]
root         5  0.0  0.0      0     0 ?        I<   00:36   0:00 [slub_flushwq]
root         6  0.0  0.0      0     0 ?        I<   00:36   0:00 [netns]
root        10  0.0  0.0      0     0 ?        I<   00:36   0:00 [mm_percpu_wq]
root        11  0.0  0.0      0     0 ?        I    00:36   0:00 [rcu_tasks_kthread]
root        12  0.0  0.0      0     0 ?        I    00:36   0:00 [rcu_tasks_rude_kthr]
root        13  0.0  0.0      0     0 ?        I    00:36   0:00 [rcu_tasks_trace_kth]
root        14  0.0  0.0      0     0 ?        S    00:36   0:00 [ksoftirqd/0]
root        15  0.0  0.0      0     0 ?        I    00:36   0:01 [rcu_preempt]
root        16  0.0  0.0      0     0 ?        S    00:36   0:00 [migration/0]
root        18  0.0  0.0      0     0 ?        S    00:36   0:00 [cpuhp/0]
root        19  0.0  0.0      0     0 ?        S    00:36   0:00 [cpuhp/1]
root        20  0.0  0.0      0     0 ?        S    00:36   0:00 [migration/1]
root        21  0.1  0.0      0     0 ?        S    00:36   0:02 [ksoftirqd/1]

```

13-Utilizar el comando taskkill

```

root@Debian:~# kill 2000
bash: kill: (2000) - No such process
root@Debian:~# traceroute www.google.com

```

14-Utilizar el comando tracert

```

root@Debian:~# traceroute www.google.com
traceroute to www.google.com (192.178.52.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.882 ms  0.297 ms  0.337 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *^C

```

15-Utilizar el comando ARP

```

root@Debian:~# arp
Address HWtype HWaddress Flags Mask Iface
_gateway ether 52:54:00:12:35:02 C enp0s3
root@Debian:~#

```

B) Contesta con tus propias palabras las siguientes preguntas:

1. Confirma la comunicación entre tu dispositivo y otros equipos en una red. Envía paquetes y evalúa la respuesta para verificar la disponibilidad de un servidor y medir el rendimiento de la red.
2. Se emplea para buscar y obtener datos sobre nombres de dominio, como la conversión de direcciones IP a partir de nombres de dominio y los detalles de servidores.
3. La orden netstat exhibe detalles sobre conexiones en la red, puertos abiertos y estadísticas. Su función es supervisar y solucionar problemas de red, identificar conexiones activas y puertos en modo escucha.
4. La instrucción ps proporciona información acerca de los procesos en sistemas Unix y Linux. Permite visualizar un listado de tareas en ejecución, incluyendo datos como el ID de proceso (PID) y los recursos utilizados.
5. La orden kill se emplea para terminar procesos en sistemas Unix y Linux. Permite detener aplicaciones en funcionamiento enviando señales específicas, como SIGTERM o SIGKILL, para cerrarlas de manera controlada o forzada.
6. El comando traceroute rastrea el trayecto de un paquete de datos. Esta herramienta es utilizada para diagnosticar problemas de red y comprender la ruta de los datos.
7. El comando Ping verifica la conectividad, Nslookup resuelve nombres de dominio, y Netstat exhibe conexiones. Estas herramientas ayudan a diagnosticar inconvenientes en la red, tales como problemas de conectividad, resolución de nombres de dominio y análisis de tráfico.

C) Investigar los siguientes comandos y anotar ejemplos prácticos:

1. El comando "atmadm" permite rastrear las conexiones y direcciones gestionadas por el Administrador de Llamadas en una red de Modo de Transferencia Asíncrona (ATM). Usando "atmadm," puedes acceder a estadísticas detalladas de las llamadas entrantes y salientes en adaptadores ATM. Al ejecutarlo sin parámetros, te proporciona estadísticas para supervisar el estado de las conexiones ATM activas.

Atmadm /c

2. "bitsadmin" es una utilidad de línea de comandos en sistemas Windows que facilita la gestión de trabajos de transferencia de archivos en segundo plano. "BITS" corresponde a "Servicio de Transferencia Inteligente en Segundo Plano". BITSAdmin posibilita la creación, modificación, consulta y administración de tareas de transferencia de archivos en el servicio BITS.

```
bitsadmin /transfer myDownloadJob /download /priority normal http://example
```

3. "cmstp" es una herramienta de línea de comandos empleada en sistemas Windows para instalar y administrar perfiles de conexión de red en un sistema. "CMSTP" representa "Instalador de Perfiles de Conexión de Administrador". Este comando automatiza la instalación de perfiles de conexión de red, que pueden englobar configuraciones de acceso a Internet o redes VPN.

```
cmstp /s mi_conexion.inf
```

4. El Protocolo de Transferencia de Archivos (FTP) es un protocolo de red utilizado para mover archivos entre un cliente y un servidor a través de una red, como Internet. FTP posibilita la copia eficiente de archivos y se utiliza extensamente para cargar y descargar archivos en servidores web, administrar sitios web y transferir datos entre sistemas.

```
ftp nombre_del_servidor_ftp
```

5. El comando "getmac" en Windows se emplea para obtener la dirección MAC (Control de Acceso a Medios) de una interfaz de red en un sistema Windows. La dirección MAC es un identificador único asociado a una tarjeta de red o adaptador en una computadora.

```

C:\Users\leona>getmac

Dirección física      Nombre de transporte
=====
20-2B-20-A9-F9-49     \Device\Tcpip_{707E7B70-65CC
-4337-B78F-5A1CC08BD082}
N/A                   Medios desconectados
00-FF-AF-3F-A3-03     Medios desconectados
20-2B-20-A9-F9-4A     Medios desconectados
0A-00-27-00-00-0D     \Device\Tcpip_{84FE7F43-CB2F
-4B7B-843E-73628BD20F85}

```

6. "hostname" es una orden que visualiza o permite la configuración del nombre de host de una computadora en sistemas Unix, Linux o Windows. El nombre de host es una etiqueta alfanumérica utilizada para identificar de forma única una computadora en una red.

```

C:\Users\leona>hostname
Yoshua_Canche

C:\Users\leona>|

```

7. "nbtstat" es una herramienta de línea de comandos en sistemas Windows que proporciona datos vinculados al protocolo NetBIOS (Sistema de Entrada y Salida Básica de Red). NetBIOS es un conjunto de protocolos que facilita la comunicación entre computadoras en una red local. "nbtstat" ofrece detalles sobre la resolución de nombres NetBIOS y el estado de NetBIOS en un sistema Windows.

```

C:\Users\leona>nbtstat -c

Ethernet 3:
Dirección IP del nodo: [192.168.56.1] Id. de ámbito : []

    No hay nombres en la caché

Conexión de área local:
Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

    No hay nombres en la caché

Ethernet 2:
Dirección IP del nodo: [0.0.0.0] Id. de ámbito : []

```

8. El comando "net" es una utilidad de línea de comandos en sistemas Windows que brinda una variedad de funciones relacionadas con la administración de redes y sistemas. Se utiliza para realizar tareas vinculadas a la gestión de usuarios, recursos compartidos, servicios, entre otras.


```
C:\Users\leona>net localgroup
Alias para \\YOSHUA_CANCHE
-----
*Administradores
*docker-users
*Hyper-V Administrators
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Propietarios del dispositivo
*SQLServer2005SQLBrowserUser$YOSHUA_CANCHE
*System Managed Accounts Group
*Usuarios
```

9. "net use" es un comando en sistemas Windows que posibilita la conexión o desconexión de unidades de red. Puedes utilizar esta orden para asignar una letra de unidad a una ubicación compartida en red, como una carpeta o recurso en otro equipo.

```
net use Z: \\servidor\compartir
```

10. "netsh" es una herramienta de línea de comandos en sistemas Windows que permite la configuración y administración de diversos componentes de red. Es útil para tareas como configurar la red, modificar parámetros de red, resolver problemas de conectividad y administrar servicios relacionados con la red.

```
netsh interface ipv4 show interfaces
```

11. "pathping" es una utilidad de diagnóstico de red en sistemas Windows que combina las funciones de "ping" y "tracert" (traceroute). Proporciona un seguimiento minucioso de la ruta de los paquetes en la red y ofrece estadísticas acerca de la calidad de la conexión en cada salto.

```
C:\Users\leona>pathping www.google.com

Seguimiento de ruta a www.google.com [142.250.189.132]
sobre un máximo de 30 saltos:
 0  Yoshua_Canche [192.168.1.199]
 1  192.168.1.254
 2  |
```

12. "rcp" (Protocolo de Copia Remota) es un protocolo que se utiliza para copiar archivos entre sistemas Unix y Linux. Facilita la copia de archivos desde una máquina local a una remota o viceversa, de forma similar al comando "cp" en sistemas Unix.

```
scp archivo.txt usuario@servidor:/ruta/destino/
```

13. El comando "rexec" (Ejecución Remota) permite ejecutar comandos en un sistema remoto desde una computadora local. Es utilizado en sistemas Unix y Linux y forma parte de las herramientas estándar de red en sistemas UNIX. A través de "rexec," es posible iniciar procesos o ejecutar comandos en un sistema remoto con el permiso del usuario remoto.

```
>rexec host -l usuario -p puerto comando
```

14. El comando "route" se emplea en sistemas Unix, Linux y Windows para mostrar y administrar la tabla de enrutamiento, la cual enumera las rutas por las cuales los paquetes de datos se dirigen en una red.

```
C:\Users\leona>route -n

Manipula tablas de enrutamiento de red.

ROUTE [-f] [-p] [-4|-6] comando [destino] [MASK máscara_red] [puerta_enlace]
[METRIC métrica] [IF interfaz]

    -f                Borra las tablas de enrutamiento de todas las entradas
                        de puerta de enlace. Si se usa junto con uno de los
```

15. "rpcping" es una herramienta de diagnóstico utilizada para verificar la conectividad entre un cliente y un servidor que emplean el Protocolo de Llamada a Procedimiento Remoto (RPC). RPC es un protocolo empleado para la comunicación entre aplicaciones distribuidas en sistemas Windows y otros sistemas operativos. "rpcping" permite confirmar si un servidor RPC es accesible desde un cliente y si los procedimientos remotos están disponibles.

```
rpcping -s servidor_rpc
```

16. "rsh" (Shell Remoto) es un protocolo y conjunto de comandos que posibilitan la ejecución de comandos en un sistema remoto desde una máquina local en una red. El protocolo rsh forma parte de las herramientas de comunicación de red en sistemas Unix y Linux, aunque carece de cifrado de datos, lo que lo hace inseguro en redes no confiables o públicas.

```
>rsh servidor-remoto -l usuario-remoto ls -l
```

17. "tcmsetup" se utiliza para configurar o deshabilitar el cliente TAPI (Interfaz de Programación de Aplicaciones de Telefonía). Es esencial para el funcionamiento correcto de TAPI, ya que permite especificar los servidores remotos utilizados por los clientes TAPI.

18. Telnet es un protocolo y herramienta de línea de comandos utilizados para establecer conexiones de terminal con sistemas remotos a través de una red, como Internet. Facilita el acceso a una computadora o dispositivo remoto y la ejecución de comandos en ese dispositivo, como si estuvieras físicamente presente en el lugar. Telnet se utiliza comúnmente en entornos de administración de sistemas y redes.

```
telnet servidor.com
```

19. El Protocolo de Transferencia de Archivos Trivial (TFTP) es un protocolo ligero utilizado para transferir archivos en una red, especialmente en entornos de arranque de dispositivos y sistemas integrados. A diferencia de protocolos de transferencia de archivos más complejos como FTP, TFTP es minimalista y carece de autenticación y características de seguridad avanzadas, lo que lo hace adecuado para tareas específicas y sencillas.

```
tftp -g -r archivo_remoto -l archivo_local dirección_servidor
```