



UNIVERSIDAD POLITÉCNICA DE QUINTANA ROO



Sistemas Operativos

Lopez Diaz Brandon

27 AV

Tema:
tarea #987

Cancún Quintana Roo

12/10/2023

A) Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola.

1.- Obtener la ayuda del comando ping.

```
Escritorio — -zsh — 80x24

IMac_13_Invitado@iMac-13 desktop % ping
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize]
          [-g sweepminsize] [-h sweepincrsize] [-i wait]
          [-l preload] [-M mask | time] [-m ttl] [-p pattern]
          [-S src_addr] [-s packetsize] [-t timeout] [-W waittime]
          [-z tos] host
      ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait]
          [-l preload] [-M mask | time] [-m ttl] [-p pattern] [-S src_addr]
          [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
          [-z tos] mcast-group
Apple specific options (to be specified before mcast-group or host like all options)
      -b boundif          # bind the socket to the interface
      -k traffic_class    # set traffic class socket option
      -K net_service_type # set traffic class socket options
      --apple-connect     # call connect(2) in the socket
      --apple-time        # display current time
IMac_13_Invitado@iMac-13 desktop %
```

2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro.

```
Escritorio — -zsh — 80x24

IMac_13_Invitado@iMac-13 desktop % ping -c 5 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.084 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.152 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.168 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.149 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.151 ms

--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.084/0.141/0.168/0.029 ms
IMac_13_Invitado@iMac-13 desktop %
```



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

```
IMac_13_Invitado@iMac-13 desktop % ping google.com
PING google.com (142.250.217.238): 56 data bytes
64 bytes from 142.250.217.238: icmp_seq=0 ttl=118 time=27.043 ms
64 bytes from 142.250.217.238: icmp_seq=1 ttl=118 time=24.659 ms
64 bytes from 142.250.217.238: icmp_seq=2 ttl=118 time=28.249 ms
64 bytes from 142.250.217.238: icmp_seq=3 ttl=118 time=26.905 ms
64 bytes from 142.250.217.238: icmp_seq=4 ttl=118 time=26.699 ms
64 bytes from 142.250.217.238: icmp_seq=5 ttl=118 time=25.031 ms
64 bytes from 142.250.217.238: icmp_seq=6 ttl=118 time=24.421 ms
64 bytes from 142.250.217.238: icmp_seq=7 ttl=118 time=22.049 ms
64 bytes from 142.250.217.238: icmp_seq=8 ttl=118 time=26.550 ms
64 bytes from 142.250.217.238: icmp_seq=9 ttl=118 time=29.432 ms
64 bytes from 142.250.217.238: icmp_seq=10 ttl=118 time=26.625 ms
64 bytes from 142.250.217.238: icmp_seq=11 ttl=118 time=26.789 ms
64 bytes from 142.250.217.238: icmp_seq=12 ttl=118 time=26.574 ms
64 bytes from 142.250.217.238: icmp_seq=13 ttl=118 time=28.133 ms
64 bytes from 142.250.217.238: icmp_seq=14 ttl=118 time=26.780 ms
64 bytes from 142.250.217.238: icmp_seq=15 ttl=118 time=26.858 ms
64 bytes from 142.250.217.238: icmp_seq=16 ttl=118 time=26.926 ms
64 bytes from 142.250.217.238: icmp_seq=17 ttl=118 time=26.331 ms
64 bytes from 142.250.217.238: icmp_seq=18 ttl=118 time=31.821 ms
64 bytes from 142.250.217.238: icmp_seq=19 ttl=118 time=26.300 ms
64 bytes from 142.250.217.238: icmp_seq=20 ttl=118 time=20.493 ms
64 bytes from 142.250.217.238: icmp_seq=21 ttl=118 time=27.109 ms
64 bytes from 142.250.217.238: icmp_seq=22 ttl=118 time=23.906 ms
64 bytes from 142.250.217.238: icmp_seq=23 ttl=118 time=26.556 ms
64 bytes from 142.250.217.238: icmp_seq=24 ttl=118 time=26.673 ms
64 bytes from 142.250.217.238: icmp_seq=25 ttl=118 time=28.013 ms
64 bytes from 142.250.217.238: icmp_seq=26 ttl=118 time=26.173 ms
64 bytes from 142.250.217.238: icmp_seq=27 ttl=118 time=26.939 ms
64 bytes from 142.250.217.238: icmp_seq=28 ttl=118 time=28.020 ms
64 bytes from 142.250.217.238: icmp_seq=29 ttl=118 time=26.333 ms
64 bytes from 142.250.217.238: icmp_seq=30 ttl=118 time=26.609 ms
```

Permite evaluar la conectividad de tu equipo con un server o dominó

4.-Obtener la ayuda del comando nslookup.

```
Escritorio — less · man nslookup — 123x34
NSLOOKUP(1)                                BIND9                                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 is used to print just the name and requested information for a host or domain.

ARGUMENTS
    Interactive mode is entered in the following cases:

    1. when no arguments are given (the default name server will be used)

    2. when the first argument is a hyphen (-) and the second argument is the host name or Internet address of a name server.

    Non-interactive mode is used when the name or Internet address of the host to be looked up is given as the first argument. The optional second argument specifies the host name or address of a name server.

    Options can also be specified on the command line if they precede the arguments and are prefixed with a hyphen. For example, to change the default query type to host information, and the initial timeout to 10 seconds, type:

        nslookup -query=hinfo -timeout=10

    The -version option causes nslookup to print the version number and immediately exits.

INTERACTIVE COMMANDS
:
```



5.- Resolver la dirección ip de <https://upqroo.edu.mx/> usando nslookup.

```
Escritorio — -zsh — 123x34
IMac_13_Invitado@iMac-13 desktop % man nslookup
Unknown locale, assuming C
IMac_13_Invitado@iMac-13 desktop % nslookup https://upqroo.edu.mx/
Server:      8.8.8.8
Address:     8.8.8.8#53

** server can't find https://upqroo.edu.mx/: NXDOMAIN

IMac_13_Invitado@iMac-13 desktop %
```

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

```
IMac_13_Invitado@iMac-13 desktop % ping 77.68.128.20
PING 77.68.128.20 (77.68.128.20): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
Request timeout for icmp_seq 15
Request timeout for icmp_seq 16
Request timeout for icmp_seq 17
Request timeout for icmp_seq 18
Request timeout for icmp_seq 19
Request timeout for icmp_seq 20
Request timeout for icmp_seq 21
Request timeout for icmp_seq 22
Request timeout for icmp_seq 23
Request timeout for icmp_seq 24
^C
--- 77.68.128.20 ping statistics ---
26 packets transmitted, 0 packets received, 100.0% packet loss
IMac_13_Invitado@iMac-13 desktop %
```

Permitió saber la conectividad de un servidor específico.



7.-Obtener la ayuda del comando netstat.

```
Escritorio — less « man netstat — 123x34

NETSTAT(1)                                     General Commands Manual                                     NETSTAT(1)

NAME
    netstat — show network status

SYNOPSIS
    netstat [-AaInW] [-f address_family | -p protocol]
    netstat [-gilns] [-v] [-f address_family] [-I interface]
    netstat -i | -I interface [-w wait] [-c queue] [-abdgqRtS]
    netstat -s [-s] [-f address_family | -p protocol] [-w wait]
    netstat -i | -I interface -s [-f address_family | -p protocol]
    netstat -m [-m]
    netstat -r [-Aaln] [-f address_family]
    netstat -rs [-s]
    netstat -B [-I interface]

DESCRIPTION
    The netstat command symbolically displays the contents of various network-related data structures. There are a number of output formats, depending on the options for the information presented. The first form of the command displays a list of active sockets for each protocol. The second form presents the contents of one of the other network data structures according to the option selected. Using the third form, with a wait interval specified, netstat will continuously display the information regarding packet traffic on the configured network interfaces. The fourth form displays statistics for the specified protocol or address family. If a wait interval is specified, the protocol information over the last interval seconds will be displayed. The fifth form displays per-interface statistics for the specified protocol or address family. The sixth form displays mbuf(9) statistics. The seventh form displays routing table for the specified address family. The eighth form displays routing statistics.

    The options have the following meaning:

    -A    With the default display, show the address of any protocol control blocks associated with sockets and the flow hash; used for debugging.

    -a    With the default display, show the state of all sockets; normally sockets used by server processes are not
```

8.-Mostrar todas las conexiones y puertos de escucha.

[illegible]

9.-ejecutar netstat sin resolver nombres de dominio o puertos.

```
Escritorio — zsh — 123x70

IMac_13_Invitado@iMac-13 desktop % netstat -n -p
netstat: option requires an argument -- p
Usage: netstat [-AaInW] [-f address_family | -p protocol]
       netstat [-gilns] [-f address_family]
       netstat -i | -I interface [-w wait] [-abdgRtS]
       netstat -s [-s] [-f address_family | -p protocol] [-w wait]
       netstat -i | -I interface -s [-f address_family | -p protocol]
       netstat -m [-m]
       netstat -r [-Aaln] [-f address_family]
       netstat -rs [-s]

IMac_13_Invitado@iMac-13 desktop %
```

10.-Mostrar las conexiones TCP.

```
Escritorio — less — 123x70

tcp4      0      0 172.16.128.11.54105    23.46.160.23.443      ESTABLISHED
tcp4      0      0 172.16.128.11.54088    172.217.3.67.443      ESTABLISHED
tcp4      0      0 172.16.128.11.53998    162.159.135.234.443   ESTABLISHED
tcp4      0      0 172.16.128.11.53974    192.178.50.78.443     ESTABLISHED
tcp4      0      0 172.16.128.11.53972    8.8.4.4.443           ESTABLISHED
tcp4      0      0 172.16.128.11.53969    192.178.50.46.443     ESTABLISHED
tcp4      0      0 172.16.128.11.53255    17.57.144.149.5223    ESTABLISHED
~
~
~
1          5          0      8192    32768 com.apple.network.tcp_ccdebug
```

11.-Mostrar las conexiones UDP.

[illegible]

12.-Utilizar el comando tasklist.

```
IMac_13_Invitado@iMac-13 desktop % ps
  PID TTY          TIME CMD
 2128 ttys000    0:00.17 -zsh
IMac_13_Invitado@iMac-13 desktop %
```

13.-Utilizar el comando taskkill.

```
[liveuser@localhost-live ~]$ killl 1548
[liveuser@localhost-live ~]$
```

14.-Utilizar el comando tracer.

```
[liveuser@localhost-live ~]$ traceroute google.com
traceroute to google.com (142.250.217.174), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.152 ms  0.191 ms  0.235 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
```

15.-Utilizar el comando ARP.

```
+ liveuser@localhost-live:~
[liveuser@localhost-live ~]$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
[liveuser@localhost-live ~]$
```



b)Contesta con tus propias palabras las siguientes preguntas:

1.-¿Para qué sirve el comando ping?

El comando ping se utiliza para verificar la conectividad entre el host local y un host remoto, enviando paquetes ICMP de solicitud de eco al host remoto y esperando una respuesta.

2.-¿Para qué sirve el comando nslookup?

El comando nslookup se utiliza para obtener información de DNS, como la dirección IP de un dominio o el nombre de dominio correspondiente a una dirección IP.

3.-¿Para qué sirve el comando netstat?

El comando netstat muestra estadísticas de la red, como conexiones de red activas, tablas de enrutamiento, estadísticas de interfaces de red y mucho más.

4.-¿Para qué sirve el comando tasklist?

El comando ps se utiliza para mostrar información sobre los procesos en ejecución en el sistema, incluidos los identificadores de proceso (PID), el consumo de recursos y el estado.

5.-¿Para qué sirve el comando taskkill?

El comando kill se utiliza para enviar señales a procesos específicos, permitiendo así terminar o detener un proceso en ejecución.

6.-¿Para qué sirve el comando tracert?

El comando traceroute se utiliza para rastrear la ruta que toman los paquetes de red desde el host local hasta un host remoto, mostrando los saltos (routers) entre ellos.

7.-¿Cómo ayudan los primeros tres comandos para detectar problemas en la red?

Estos comandos ayudan a detectar problemas en la red al permitirte verificar la conectividad con otros hosts (ping), realizar consultas DNS (nslookup) y examinar el estado de las conexiones de red y los procesos activos (netstat). Al proporcionar información detallada sobre el estado de la red y los procesos en ejecución, estos comandos pueden identificar problemas como la conectividad deficiente, la resolución de DNS incorrecta, la congestión de red y procesos problemáticos que consumen recursos.



C) Investiga los siguientes comandos y anotar ejemplos prácticos: atmadm, bitsadmin, cmstp, ftp, getmac, hostname, nbtsat, net, net use, netsh, pathping, rcp, rexec, route, rpcping, rsh, tcmsetup, telnet, tftp

atmadm

El comando se utiliza para administrar conexiones de red de modo asincrónico (ATM). Normalmente, su uso se limita a la administración técnica de redes ATM y no se emplea en situaciones cotidianas.

[atmadm -c consulta](#)

bitsadmin

Este comando permite administrar tareas de transferencia de archivos en segundo plano, conocido como Background Intelligent Transfer Service (BITS). Un ejemplo de su uso sería descargar archivos grandes de manera silenciosa en segundo plano.

[bitsadmin /transfer mi_descarga /download /priority normal](#)
[http://ejemplo.com/archivo.zip C:\carpeta\archivo.zip](#)

cmstp

Este comando se utiliza para instalar o desinstalar perfiles de conexión de red. Principalmente, resulta útil en entornos corporativos para implementar configuraciones de red específicas.

[cmstp /s archivo_de_configuracion.inf](#)

ftp

El comando FTP se utiliza para transferir archivos entre sistemas a través del Protocolo de Transferencia de Archivos. Permite la conexión a un servidor FTP para facilitar la transferencia de archivos.

[ftp ejemplo.com](#)

[get archivo_remoto.txt](#)

getmac



Este comando muestra la dirección MAC (Media Access Control) de una interfaz de red. Puedes utilizarlo para obtener la dirección MAC de tu tarjeta de red, lo que resulta útil para la resolución de problemas de red.

[getmac](#)

hostname

Este comando muestra el nombre del host o computadora local. Puede resultar útil para averiguar el nombre de tu propia computadora.

[hostname](#)

nbstat

El comando proporciona información sobre la resolución de nombres de NetBIOS en una red. Se utiliza específicamente para diagnosticar problemas de resolución de nombres NetBIOS.

[nbstat -A 192.168.1.1](#)

net

Este comando se utiliza para administrar diversas configuraciones y recursos de red. Por ejemplo, puedes emplear `net user` para gestionar cuentas de usuario y `'net share'` para administrar recursos compartidos.

[net nombre_usuario contraseña /add](#)

net use

Este comando permite conectar o desconectar recursos compartidos de red en tu computadora. Por ejemplo, puedes utilizarlo para mapear una unidad de red.

[net user nombre_usuario contraseña /add](#)



netsh

Netsh es una herramienta de configuración de red versátil que permite modificar la configuración de red, firewall, VPN y más. Por ejemplo, puedes utilizar netsh para configurar un servidor proxy.

[netsh interface ipv4 show interfaces](#)

pathping

Este comando combina la funcionalidad de ping y tracert. Proporciona información detallada sobre la ruta y la latencia en una red.

[pathping www.google.com](#)

rcp

Se utiliza para copiar archivos de y hacia sistemas remotos en una red.

[rcp archivo.txt usuario@servidor:/ruta/destino/](#)

rexec

Permite ejecutar comandos en un sistema remoto, lo que facilita la ejecución de programas o scripts si se cuenta con los permisos adecuados. Sin embargo, su uso ha disminuido debido a preocupaciones de seguridad relacionadas con posibles vulnerabilidades.

[rexec servidor comando](#)

route

Se utiliza para visualizar y modificar la tabla de enrutamiento en sistemas Windows. Puedes emplearlo para agregar, eliminar o modificar rutas de red, como por ejemplo, para añadir una ruta predeterminada a través de una puerta de enlace específica.

[route add 0.0.0.0 mask 0.0.0.0 192.168.1.1](#)



rpcping

Este comando se utiliza para realizar pruebas de ping a servicios RPC (Remote Procedure Call). Es útil para verificar la conectividad y la disponibilidad de dichos servicios en sistemas remotos.

`rpcping -s servidor`



rsh

Similar a rexec, el comando rsh (Remote Shell) permite la ejecución de comandos en sistemas remotos. No obstante, su uso ha disminuido debido a preocupaciones de seguridad. Requiere permisos adecuados para ejecutar comandos en un sistema remoto.

rsh servidor comando

tcmsetup

El comando se utiliza para configurar la autenticación de Trusted Platform Module (TPM) en sistemas Windows. Se trata de una herramienta técnica que se emplea para establecer la seguridad de hardware en sistemas compatibles con TPM.

tcmsetup -v -f -b 123456

telnet

El comando telnet se utiliza para establecer una conexión a otros dispositivos o servidores mediante una sesión de terminal. Facilita el acceso a sistemas remotos para administrarlos o llevar a cabo pruebas.

telnet servidor

tftp

El Protocolo de Transferencia de Archivos Trivial (TFTP) se utiliza para transferir archivos de forma sencilla entre sistemas remotos. Representa una manera simple de copiar archivos en sistemas conectados en red.

tftp -i servidor GET archivo.txt