



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Lab 1: Topología de Pruebas

Estudiante:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuertes Diaz

19 de junio de 2024

1. Objetivos de Aprendizaje

1. Comprender el funcionamiento de las redes Windows
2. Aprender los comandos básicos de conectividad de Windows
3. Identificar los elementos o componentes que interactúan

2. Marco Teórico

2.1. Historia de Windows

En 1975 Bill Gates y Paul Allen fundaron la compañía Microsoft en Estados Unidos, con el objetivo de desarrollar y comercializar programas para ejecutar el Altair 8800, un microordenador diseñado en 1974.



Figura 1: Bill Gates

La primera versión de Microsoft Windows, fue presentada en diciembre de 1985 y compitió con el sistema operativo de la compañía Apple, no tenía muchas funcionalidades y no era un software de sistema completo, por lo que careció de popularidad y aceptación.

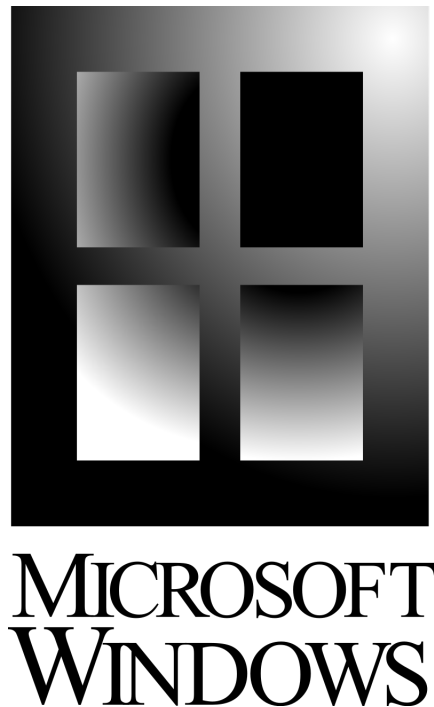


Figura 2: Windows 3.0

En 1990 Microsoft lanzó Windows 3.0, una nueva versión del sistema operativo. A medida que desarrolló versiones mejoradas, modificó el correspondiente número del nombre. Sin embargo, en 1995 lanzó el Windows 95 que ofrecía una interfaz completamente nueva con un explorador de archivos mejorado, un menú de inicio de acceso rápido y una mejor compatibilidad de hardware, entre otras ventajas.



Figura 3: Windows 95

A partir de 2012 se lanzó el sistema operativo Windows 8 con un nuevo diseño de imagen que resultó más interactivo y que permitió ser ejecutado a través de las pantallas táctiles. Fue una versión del software pensada para ser ejecutada desde otros dispositivos, como los teléfonos móviles o tabletas, y para convivir con el auge de Internet y las redes sociales.



Figura 4: Windows 8

2.2. Kernel

Kernel es el núcleo de un sistema operativo, es decir es la interfaz que existe entre el software y el hardware por lo que se usa constantemente. Sin embargo no es únicamente el núcleo del sistema, sino también un programa que controla y administra los accesos a la memoria y al procesador, responsable de los drivers.

Un kernel siempre tiene la misma estructura basada en capas:

1. **La capa más baja** es la interfaz con el hardware (procesadores, memoria y dispositivos). Esta capa realiza tareas como la de controlador de red o controlador PCI Express. Sobre ella se encuentra la gestión de la memoria, que distribuye la memoria RAM y la memoria virtual.
2. **Scheduler:** contiene el gestor de procesos que se encarga de la gestión del tiempo y permite el multitasking.
3. **Device Management.**
4. **La capa más alta** es el sistema de archivos. Allí, se le asigna un espacio en la memoria principal (caché, RAM, etc) o secundaria (disco duro, USB, etc) a los procesos.

2.3. Arquitectura de Windows

Los sistemas operativos Microsoft Windows usan una arquitectura de red basada en el modelo de redes de siete capas desarrollado por la Organización Internacional de Normalización (ISO) en 1978. El modelo de referencia de interconexión de sistemas abiertos ISO (OSI) describe las redes como una serie de capas de protocolo con un conjunto específico de funciones asignadas a cada capa. Cada capa ofrece servicios específicos a capas superiores al blindar estas capas a partir de los detalles de cómo se

implementan los servicios. Una interfaz bien definida entre cada par de capas adyacentes define los servicios ofrecidos por la capa inferior a la superior y cómo se accede a esos servicios”. La capa de vínculo de datos envía fotogramas entre direcciones físicas y es responsable de la detección y recuperación de errores que se producen en la capa física.

2.3.1. MAC

La subcapa MAC se encarga de regular el acceso a la capa física, verificar los errores en los fotogramas y gestionar el reconocimiento de direcciones de los fotogramas recibidos. En la arquitectura de red de Windows, la subcapa MAC se incorpora en la NIC (tarjeta de interfaz de red). Esta NIC es controlada por un controlador de dispositivo de software conocido como controlador de minipuerto. Windows ofrece soporte para diferentes tipos de controladores de minipuerto, que incluyen los controladores de miniporte WDM, los administradores de llamadas de miniporte (MCM) y los controladores intermedios de minipuerto.

2.3.2. LLC

La subcapa LLC se encarga de asegurar la transferencia de tramas de datos entre nodos sin errores. Esta subcapa establece y finaliza conexiones lógicas, gestiona el flujo de tramas, ordena las tramas, confirma su recepción y retransmite aquellas que no fueron reconocidas. Utiliza técnicas como la confirmación y retransmisión de tramas para garantizar una transmisión prácticamente libre de errores en el enlace con las capas superiores.

En el entorno de Windows, la implementación de la subcapa LLC se realiza mediante un controlador de software denominado controlador de protocolo.

2.3.3. Capa de Red

La función principal de la capa de red es supervisar el desempeño de la subred. Esta capa se encarga de determinar la ruta física que los datos deben seguir, considerando diversos factores como las condiciones de la red, la prioridad del servicio y otros elementos como el enrutamiento, el control de tráfico, la fragmentación y reensamblaje de tramas, la asignación de direcciones lógicas a físicas y el registro de uso de recursos.

En sistemas operativos como Windows, la implementación de la capa de red se realiza a través de un controlador de protocolo.

3. Desarrollo

Comandos básicos de Windows:

3.1. ipconfig

ipconfig/all
ipconfig/release
ipconfig/renew

```
C:\Users\ednan>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . :
    Dirección IPv6 . . . . . : 2800:440:9838:e400::1
    Dirección IPv6 . . . . . : 2800:440:9838:e400:d36a:5a73:fc88:758a
    Dirección IPv6 temporal. . . . . : 2800:440:9838:e400:a50e:fcfc:fc43:4dfe
    Vínculo: dirección IPv6 local. . . : fe80::3740:2bc8:d8f3:a54b%11
    Dirección IPv4. . . . . : 192.168.100.36
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::1%11
                                                192.168.100.1

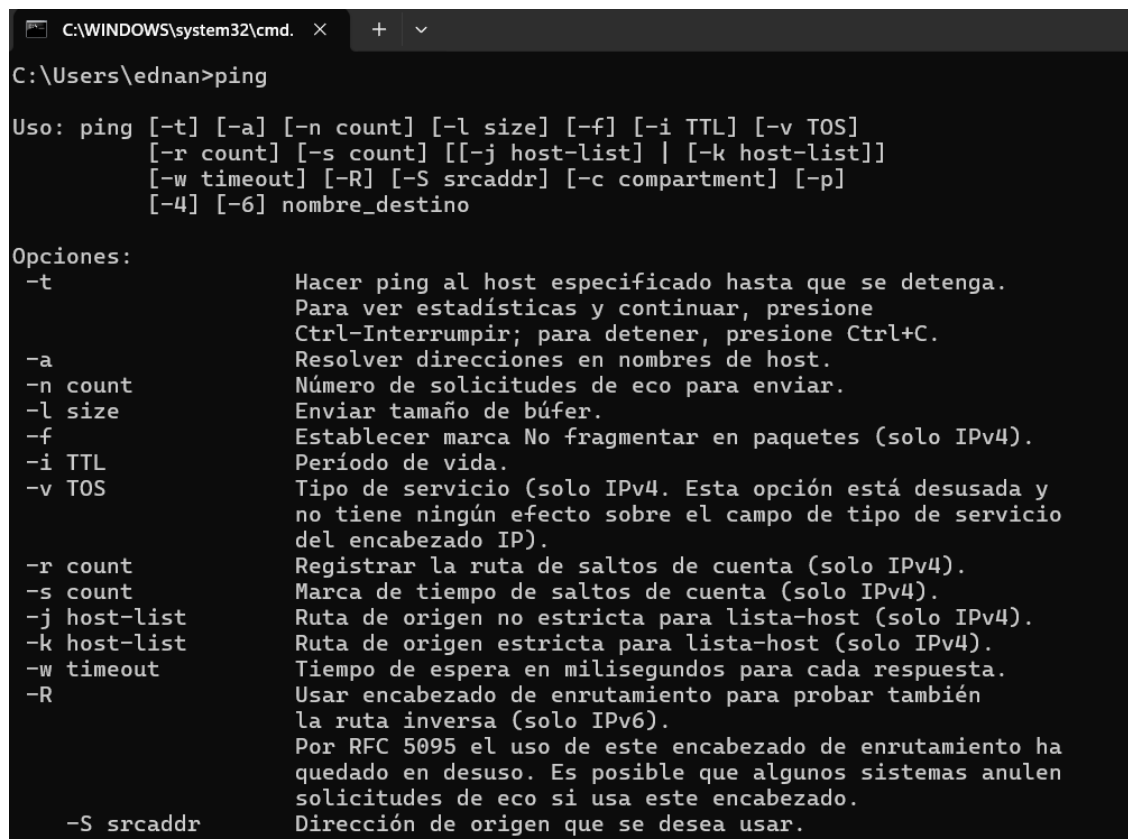
Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
```

Figura 5: ipconfig

Muestra todos los valores de configuración de red TCP/IP actuales y actualiza la configuración del Protocolo de configuración dinámica de host (DHCP) y del Sistema de nombres de dominio (DNS). Si se usa sin parámetros, ipconfig muestra la versión 4 (IPv4) del protocolo de Internet y las direcciones IPv6, la máscara de subred y la puerta de enlace predeterminada para todos los adaptadores.

3.2. ping



```
C:\WINDOWS\system32\cmd. x + v
C:\Users\ednan>ping

Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] | [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
        [-4] [-6] nombre_destino

Opciones:
-t          Hacer ping al host especificado hasta que se detenga.
            Para ver estadísticas y continuar, presione
            Ctrl-Interrumpir; para detener, presione Ctrl+C.
-a          Resolver direcciones en nombres de host.
-n count    Número de solicitudes de eco para enviar.
-l size     Enviar tamaño de búfer.
-f          Establecer marca No fragmentar en paquetes (solo IPv4).
-i TTL      Período de vida.
-v TOS      Tipo de servicio (solo IPv4. Esta opción está desusada y
            no tiene ningún efecto sobre el campo de tipo de servicio
            del encabezado IP).
-r count    Registrar la ruta de saltos de cuenta (solo IPv4).
-s count    Marca de tiempo de saltos de cuenta (solo IPv4).
-j host-list Ruta de origen no estricta para lista-host (solo IPv4).
-k host-list Ruta de origen estricta para lista-host (solo IPv4).
-w timeout  Tiempo de espera en milisegundos para cada respuesta.
-R          Usar encabezado de enrutamiento para probar también
            la ruta inversa (solo IPv6).
            Por RFC 5095 el uso de este encabezado de enrutamiento ha
            quedado en desuso. Es posible que algunos sistemas anulen
            solicitudes de eco si usa este encabezado.
-S srcaddr  Dirección de origen que se desea usar.
```

Figura 6: ping

Comprueba la conectividad a nivel de IP con otro equipo TCP/IP mediante el envío de mensajes de solicitud de eco del protocolo de mensajes de control de Internet (ICMP). Se muestra la recepción de los mensajes de respuesta de eco correspondientes, junto con los tiempos de ida y vuelta. ping es el comando TCP/IP principal que se usa para solucionar problemas de conectividad, disponibilidad y resolución de nombres.

3.3. nslookup

```
C:\Users\ednan>nslookup
DNS request timed out.
    timeout was 2 seconds.
Servidor predeterminado: UnKnown
Address: 2800:440:1:24ec:ae82:5dd4:13ac:1c5
```

Figura 7: nslookup

Muestra información que puede usar para diagnosticar la infraestructura del Sistema de nombres de dominio (DNS).

3.4. netstat

```
C:\Users\ednan>netstat

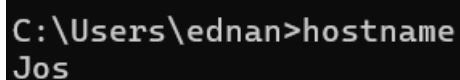
Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    127.0.0.1:49775       Jos:49776             ESTABLISHED
TCP    127.0.0.1:49776       Jos:49775             ESTABLISHED
TCP    127.0.0.1:49777       Jos:49778             ESTABLISHED
TCP    127.0.0.1:49778       Jos:49777             ESTABLISHED
TCP    127.0.0.1:49787       Jos:49788             ESTABLISHED
TCP    127.0.0.1:49788       Jos:49787             ESTABLISHED
TCP    127.0.0.1:49815       Jos:49816             ESTABLISHED
TCP    127.0.0.1:49816       Jos:49815             ESTABLISHED
TCP    192.168.100.36:49676  52.226.139.180:https  ESTABLISHED
TCP    192.168.100.36:49755  192.168.100.61:8009   ESTABLISHED
TCP    192.168.100.36:49768  162.159.135.234:https ESTABLISHED
TCP    192.168.100.36:49800  17.32.194.34:https    CLOSE_WAIT
TCP    192.168.100.36:49801  17.32.194.34:https    CLOSE_WAIT
TCP    192.168.100.36:49808  ec2-3-212-174-19:https CLOSE_WAIT
TCP    192.168.100.36:49810  17.32.194.22:https    CLOSE_WAIT
TCP    192.168.100.36:49813  a184-31-186-229:https  CLOSE_WAIT
TCP    192.168.100.36:49824  17.57.144.39:5223     ESTABLISHED
TCP    192.168.100.36:49844  ec2-54-175-141-61:https CLOSE_WAIT
TCP    192.168.100.36:49995  20.127.250.238:https  ESTABLISHED
TCP    192.168.100.36:49996  192.168.100.61:8008   ESTABLISHED
TCP    192.168.100.36:50068  64:https              ESTABLISHED
TCP    192.168.100.36:50076  64:https              ESTABLISHED
TCP    192.168.100.36:50091  ec2-35-174-127-31:https ESTABLISHED
TCP    192.168.100.36:50106  52.182.143.211:https  ESTABLISHED
TCP    192.168.100.36:50116  server-13-226-52-74:https ESTABLISHED
TCP    192.168.100.36:50118  ec2-52-30-201-170:https ESTABLISHED
TCP    192.168.100.36:50120  a92-122-157-146:https CLOSE_WAIT
TCP    192.168.100.36:50135  20.110.205.119:https  ESTABLISHED
TCP    [2800:440:9838:e400:c85:947:8123:7686]:49761 [2603:1030:210:f::2]:https ESTABLISHED
TCP    [2800:440:9838:e400:c85:947:8123:7686]:49773 [2600:1901:1:292::]:https ESTABLISHED
TCP    [2800:440:9838:e400:c85:947:8123:7686]:49779 [2620:149:a41:580::2:5]:https CLOSE_WAIT
TCP    [2800:440:9838:e400:c85:947:8123:7686]:49780 [2620:149:a41:580::2:5]:https CLOSE_WAIT
TCP    [2800:440:9838:e400:c85:947:8123:7686]:49781 [2620:149:a41:580::2:5]:https CLOSE_WAIT
```

Figura 8: netstat

Muestra las conexiones TCP activas, los puertos en los que escucha el equipo, las estadísticas de Ethernet, la tabla de enrutamiento IP, las estadísticas IPv4 (para los protocolos IP, ICMP, TCP y UDP) y las estadísticas de IPv6 (para los protocolos IPv6, ICMPv6, TCP a través de IPv6 y UDP a través de IPv6). Se usa sin parámetros; este comando muestra conexiones TCP activas.

3.5. hostname

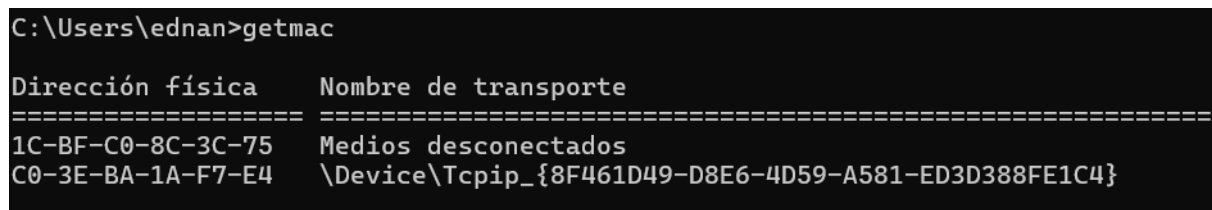


```
C:\Users\ednan>hostname
Jos
```

Figura 9: hostname

Muestra la parte del nombre de host del nombre del equipo completo del equipo.

3.6. getmac



```
C:\Users\ednan>getmac

Dirección física      Nombre de transporte
=====
1C-BF-C0-8C-3C-75     Medios desconectados
C0-3E-BA-1A-F7-E4     \Device\Tcpip_{8F461D49-D8E6-4D59-A581-ED3D388FE1C4}
```

Figura 10: getmac

Devuelve la dirección del control de acceso multimedia (MAC) y la lista de protocolos de red asociados a cada dirección para todas las tarjetas de red de cada equipo, ya sea localmente o a través de una red.

3.7. arp-a

```
C:\Users\ednan>arp -a

Interfaz: 192.168.100.36 --- 0xb
  Dirección de Internet      Dirección física      Tipo
  192.168.100.1              88-89-2f-26-03-ef    dinámico
  192.168.100.13             ac-ae-19-bd-32-e5    dinámico
  192.168.100.61             38-8b-59-34-1e-84    dinámico
  192.168.100.255            ff-ff-ff-ff-ff-ff    estático
  224.0.0.22                 01-00-5e-00-00-16    estático
  224.0.0.251                01-00-5e-00-00-fb    estático
  224.0.0.252                01-00-5e-00-00-fc    estático
  239.255.255.250            01-00-5e-7f-ff-fa    estático
  239.255.255.253            01-00-5e-7f-ff-fd    estático
  255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

Figura 11: arp -a

Se puede ver las direcciones IP y las direcciones MAC asociadas a los dispositivos con los que el equipo ha interactuado recientemente.

3.8. tracert

```
C:\Users\ednan>tracert

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
           [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
  -d          No convierte direcciones en nombres de hosts.
  -h saltos_máximos  Máxima cantidad de saltos en la búsqueda del objetivo.
  -j lista-host  Enrutamiento relajado de origen a lo largo de la
                  lista de hosts (solo IPv4).
  -w tiempo_espera  Tiempo de espera en milisegundos para esperar cada
                    respuesta.
  -R          Seguir la ruta de retorno (solo IPv6).
  -S srcaddr  Dirección de origen para utilizar (solo IPv6).
  -4          Forzar usando IPv4.
  -6          Forzar usando IPv6.
```

Figura 12: tracert

Determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino. En estos paquetes, TRACERT usa valores de período de vida (TTL) IP variables

3.9. route print

```
C:\Users\ednan>route print
=====
ILista de interfaces
 3...1c bf c0 8c 3c 75 .....Qualcomm QCA9377 802.11ac Wireless Adapter
 5...1e bf c0 8c 3c 75 .....Microsoft Wi-Fi Direct Virtual Adapter
10...2e bf c0 8c 3c 75 .....Microsoft Wi-Fi Direct Virtual Adapter #2
11...c0 3e ba 1a f7 e4 .....Realtek PCIe FE Family Controller
 1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
 0.0.0.0            0.0.0.0            192.168.100.1        192.168.100.36      35
 127.0.0.0          255.0.0.0          En vínculo           127.0.0.1          331
 127.0.0.1          255.255.255.255    En vínculo           127.0.0.1          331
127.255.255.255     255.255.255.255    En vínculo           127.0.0.1          331
192.168.100.0        255.255.255.0      En vínculo           192.168.100.36      291
192.168.100.36       255.255.255.255    En vínculo           192.168.100.36      291
192.168.100.255      255.255.255.255    En vínculo           192.168.100.36      291
 224.0.0.0          240.0.0.0          En vínculo           127.0.0.1          331
 224.0.0.0          240.0.0.0          En vínculo           192.168.100.36      291
255.255.255.255      255.255.255.255    En vínculo           127.0.0.1          331
255.255.255.255      255.255.255.255    En vínculo           192.168.100.36      291
=====
Rutas persistentes:
 Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
11  291 ::/0                          fe80::1
 1  331 ::1/128                        En vínculo
11  291 2800:440:9838:e400::/64      En vínculo
11  291 2800:440:9838:e400::1/128
                                     En vínculo
11  291 2800:440:9838:e400:c85:947:8123:7686/128
                                     En vínculo
```

Figura 13: route print

Muestra y modifica las entradas de la tabla de enrutamiento de IP local.

3.10. wget

```

Download:
-t, --tries=NUMBER          set number of retries to NUMBER (0 unlimited).
                             retry even if connection is refused.
--retry-connrefused          write documents to FILE.
-o, --output-document=FILE  skip downloads that would download to
                             existing files.
-nc, --no-clobber            resume getting a partially-downloaded file.
                             select progress gauge type.
-c, --continue              don't re-retrieve files unless newer than
                             local.
--progress=TYPE              print server response.
                             don't download anything.
-N, --timestamping          set all timeout values to SECONDS.
                             set the DNS lookup timeout to SECS.
-S, --server-response       set the connect timeout to SECS.
                             set the read timeout to SECS.
--spider                    wait SECONDS between retrievals.
-T, --timeout=SECONDS       wait 1..SECONDS between retries of a retrieval.
                             wait from 0..2*WAIT secs between retrievals.
--dns-timeout=SECS          explicitly turn off proxy.
--connect-timeout=SECS      set retrieval quota to NUMBER.
--read-timeout=SECS         bind to ADDRESS (hostname or IP) on local host.
                             limit download rate to RATE.
-w, --wait=SECONDS          disable caching DNS lookups.
                             restrict chars in file names to ones OS allows.
--waitretry=SECONDS        ignore case when matching files/directories.
                             connect only to IPv4 addresses.
--random-wait               connect only to IPv6 addresses.
                             connect first to addresses of specified family,
                             one of IPv6, IPv4, or none.
--no-proxy                  set both ftp and http user to USER.
-Q, --quota=NUMBER         set both ftp and http password to PASS.
--bind-address=ADDRESS
--limit-rate=RATE
--no-dns-cache
--restrict-file-names=OS
--ignore-case
-4, --inet4-only
-6, --inet6-only
--prefer-family=FAMILY
--user=USER
--password=PASS

```

Figura 14: wget

Es útil para descargar archivos de forma automatizada, reanudar descargas interrumpidas y realizar descargas recursivas de sitios web enteros. Es una herramienta esencial para la administración de servidores y la automatización de tareas de descarga en entornos de línea de comandos.

4. Conclusiones

Durante el desarrollo del laboratorio se lograron alcanzar con éxito los objetivos establecidos, comprendiendo el funcionamiento de las redes Windows. Asimismo, se practicaron los comandos básicos de conectividad de Windows, como ipconfig, ping, y tracert,

proporcionando herramientas esenciales para diagnosticar problemas de red. Además, se identificaron y comprendieron los diferentes elementos y componentes que interactúan en una red Windows, desde dispositivos físicos hasta servicios y protocolos de red, lo que contribuye significativamente a la gestión efectiva y el diagnóstico preciso de problemas de red en entornos Windows

5. Referencias Bibliográficas

- Equipo editorial, Etecé. (2023, 21 septiembre). Windows: historia, evolución y características. Enciclopedia Humanidades. <https://humanidades.com/sistema-operativo-windows/>
- Equipo editorial de IONOS. (2021, 5 julio). Kernel - El núcleo del sistema operativo. IONOS Digital Guide. <https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-kernel/>
- Aviviano. (2023, 16 diciembre). Arquitectura de red de Windows y el modelo OSI - Windows drivers. Microsoft Learn. <https://learn.microsoft.com/es-es/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model>
- JasonGerend. (2023, 15 septiembre). ping. Microsoft Learn. <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/ping>
- Cyberstream. (2024, 18 febrero). Guía completa para visualizar ARP en CMD: Todo lo que necesitas saber. Byron Vargas ®. <https://www.byronvargas.com/web/como-ver-arp-en-cmd>
- JasonGerend. (2023b, abril 14). netstat. Microsoft Learn. <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/netstat>
- Cómo usar TRACERT para solucionar problemas de TCP/IP en Windows - Soporte técnico de Microsoft. (s. f.). <https://support.microsoft.com>