



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Lab 2: Software de Gestión de Redes

Estudiantes:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuentes Diaz

19 de junio de 2024

1. Objetivos de Aprendizaje

Al finalizar esta práctica el estudiante aprenderá a utilizar software de gestión de redes lo que le permitirá:

1. Conocer la dirección IP y de hardware de cualquier red
2. Conocer el dns de cualquier red
3. Transformar direcciones IP a binario o viceversa
4. Conocer en tiempo real los ataques ciberneticos en la web
5. Conocer la capacidad de descarga y de subida

2. Marco Teórico

2.1. ¿Qué es la WWW?

Son las siglas de World Wide Web, es una red de alcance mundial, que consiste en un sistema de hipertextos e hipermedio interconectados entre sí, a los que se puede acceder mediante una conexión a internet.

Se desarrolló entre 1989 y 1990, por científicos de CERN en Suiza, se publicó en 1993, desde entonces se ha multiplicado y crecido hasta convertirse en el principal medio de consulta de información digital y de telecomunicaciones.

Los tres pasos son:

- **Traducción:** La dirección URL (la que se introduce en el navegador) se vincula a una dirección IP a través de una gran base de datos distribuida de Internet (llamada DNS). Una vez obtenida la dirección IP, se establece la comunicación entre el usuario y el servidor web, e inicia la transmisión de datos.
- **Petición HTML:** El navegador entonces solicita el recurso y obtiene las partes de la página web a partir de los recursos solicitados para los gráficos, el texto, etc.
- **Renderización:** El navegador entonces sigue las instrucciones del código html o css para ensamblar la página web de manera correcta, poniendo cada gráfico en su sitio y cada texto como debe lucir. El usuario entonces puede verla en pantalla y podrá, a su deseo, saltar a otras similares.

2.2. ¿Qué es el internet?

Es la red de computadoras interconectadas entre sí a nivel mundial, para hacer común información de acceso público. Internet se vale de protocolos, recursos y servicios para operar a través de diferentes medios de conexión a la red, ya sea por medio de una línea telefónica, un cable o medios más modernos como conexión: 4G (LTE) y 5G, fibra óptica o ADSL.

2.2.1. Características del Internet

- Ofrece información las 24 horas del día, y se puede acceder a ella siempre y cuando la conexión sea posible.
- Es de carácter público.
- No pertenece a ningún ente, es de orden universal y descentralizado, por lo que no hay puntos de control a nivel jerárquico.
- Es colaborativo, es decir, toda persona puede compartir información en Internet.
- Es de crecimiento ilimitado y colaborativo, permitiendo nuevas conexiones a la red de forma compartida.
- Genera rastro a partir de cada interacción que realizan los usuarios, de manera que se puede ofrecer una experiencia personalizada adaptada a sus intereses y preferencias. No obstante, es una red anónima que no exige que los usuarios se identifiquen para su uso.
- Puede consultarse desde cualquier dispositivo de forma inmediata, y los mensajes se transmiten de forma instantánea.
- Sus usos pueden ir desde la búsqueda de información, pasando por la investigación, contacto social, comunicación inmediata, educación hasta llegar a operaciones financieras.

2.3. ¿Qué es una WAN?

Una red de área amplia (WAN) es una gran red de ordenadores que conecta grupos de ordenadores a grandes distancias. Las grandes empresas suelen utilizar WAN para conectar sus redes de oficinas; cada oficina suele tener su propia red de área local, o LAN, y estas LAN se conectan a través mediante WAN. Estas largas conexiones pueden formarse de diferentes maneras, incluyendo líneas alquiladas, VPN, o túneles IP (ver a continuación).

La definición de lo que constituye una WAN es bastante amplia. Técnicamente, cualquier red grande que se extienda por una zona geográfica amplia es una WAN. La propia Internet se considera una WAN.

2.4. ¿Qué es el Software de Gestión de Redes?

Un software de gestión de redes es una herramienta o conjunto de herramientas diseñadas para facilitar la administración, monitoreo y optimización de una red de computadoras. Este tipo de software ayuda a los administradores de redes a mantener la red funcionando de manera eficiente y segura.

2.4.1. Características:

- **Monitoreo de Red:** Permite observar el estado de los dispositivos y el tráfico en tiempo real. Esto incluye el monitoreo de routers, switches, servidores y otros dispositivos conectados a la red.
- **Configuración y Gestión de Dispositivos:** Facilita la configuración de dispositivos de red, como routers y switches, y permite realizar cambios en la configuración de manera remota.
- **Detección de Fallos:** Identifica y alerta sobre problemas o fallos en la red, permitiendo una respuesta rápida para minimizar el tiempo de inactividad.
- **Gestión del Rendimiento:** Monitorea y optimiza el rendimiento de la red para asegurar que se esté utilizando de manera eficiente y que no haya cuellos de botella.
- **Seguridad de la Red:** Incluye funciones para detectar intrusiones, gestionar políticas de seguridad y proteger la red contra amenazas y ataques.
- **Inventario de Red:** Mantiene un registro de todos los dispositivos y recursos de la red, incluyendo información sobre hardware y software.
- **Generación de Informes:** Proporciona informes detallados sobre el estado y el rendimiento de la red, así como sobre incidentes y eventos importantes.
- **Automatización de Tareas:** Permite la automatización de tareas repetitivas, como actualizaciones de software, copias de seguridad y monitoreo rutinario.

2.4.2. Ejemplos

- **SolarWinds Network Performance Monitor:** Una herramienta potente para monitoreo y gestión de redes, conocida por su capacidad para detectar problemas de rendimiento y proporcionar una visión detallada de la red.

- **Nagios:** Una opción de código abierto muy popular que ofrece monitoreo de red y alertas para servidores, switches, aplicaciones y servicios.
- **PRTG Network Monitor:** Proporciona monitoreo en tiempo real y ofrece un amplio rango de sensores que pueden ser utilizados para diversas funciones de la red.
- **Cisco Prime:** Una suite de herramientas de Cisco para la gestión y monitoreo de redes, ideal para entornos que utilizan equipos de Cisco.

3. Desarrollo

3.1. IPAdvanced Scanner

El programa escanea todos los dispositivos de red, le da acceso a las carpetas compartidas y a los servidores FTP, le proporciona control remoto de las computadoras (mediante RDP y Radmin) e incluso puede apagar las computadoras de manera remota. Es fácil de usar y se ejecuta como una edición portable.

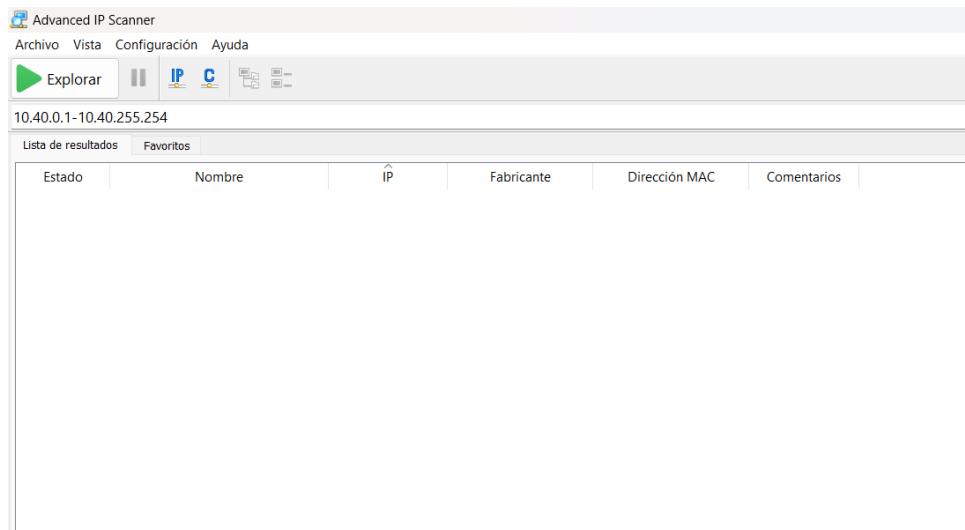
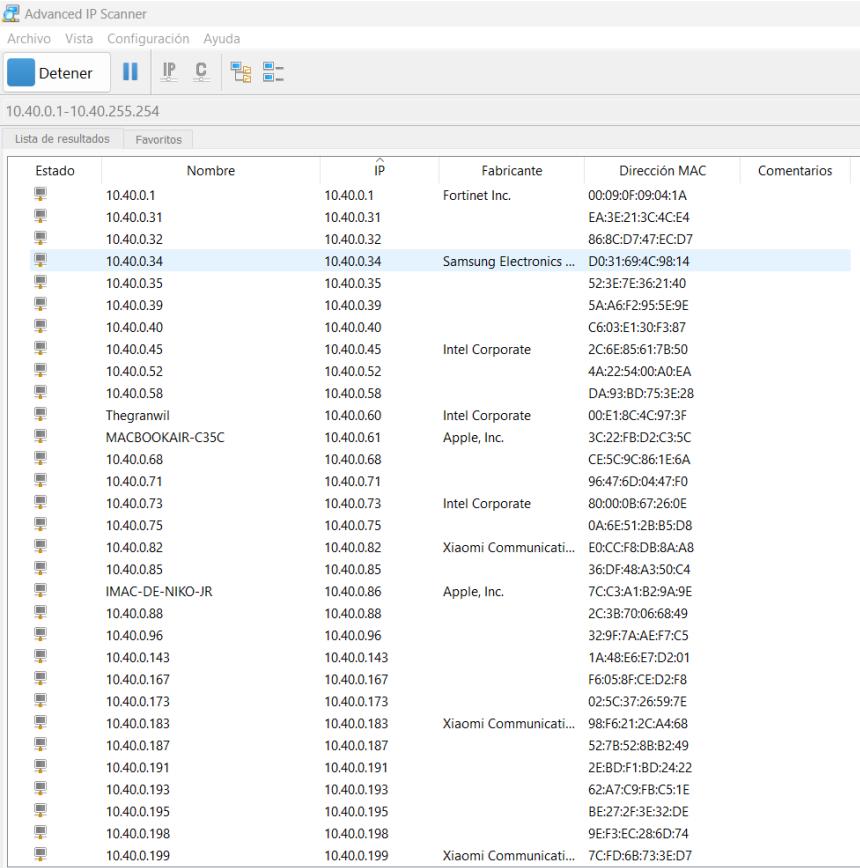


Figura 1: Advanced IP Scanner

Lab 2: Software de Gestión de Redes



The screenshot shows the Advanced IP Scanner interface. At the top, there's a menu bar with Archivo, Vista, Configuración, Ayuda, and several icons for stopping, pausing, and filtering results. Below the menu is a search bar with the text "10.40.0.1-10.40.255.254". Underneath the search bar, there are two tabs: "Lista de resultados" (selected) and "Favoritos". The main area is a table with the following columns: Estado, Nombre, IP, Fabricante, Dirección MAC, and Comentarios. The table lists numerous IP addresses from 10.40.0.1 to 10.40.0.199, along with their manufacturer names and MAC addresses. One row, "10.40.0.34", is highlighted with a blue background.

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
■	10.40.0.1	10.40.0.1	Fortinet Inc.	00:09:0F:09:04:1A	
■	10.40.0.31	10.40.0.31		EA:3E:21:3C:4C:E4	
■	10.40.0.32	10.40.0.32		86:8C:D7:47:EC:D7	
■	10.40.0.34	10.40.0.34	Samsung Electronics ...	D0:31:69:4C:98:14	
■	10.40.0.35	10.40.0.35		52:3E:7E:36:21:40	
■	10.40.0.39	10.40.0.39		5A:46:F2:95:5E:9E	
■	10.40.0.40	10.40.0.40		C6:03:E1:30:F3:87	
■	10.40.0.45	10.40.0.45	Intel Corporate	2C:6E:85:61:7B:50	
■	10.40.0.52	10.40.0.52		4A:22:54:00:A0:EA	
■	10.40.0.58	10.40.0.58		DA:93:BD:75:3E:28	
■	Thegranwil	10.40.0.60	Intel Corporate	00:E1:8C:4C:97:3F	
■	MACBOOKAIR-C35C	10.40.0.61	Apple, Inc.	3C:22:FB:D2:C3:5C	
■	10.40.0.68	10.40.0.68		CE:5C:9C:86:1E:6A	
■	10.40.0.71	10.40.0.71		96:47:6D:04:47:F0	
■	10.40.0.73	10.40.0.73	Intel Corporate	80:00:08:67:26:0E	
■	10.40.0.75	10.40.0.75		0A:6E:51:2B:B5:D8	
■	10.40.0.82	10.40.0.82	Xiaomi Communicati...	E0:CC:F8:DB:8A:A8	
■	10.40.0.85	10.40.0.85		36:DF:48:A3:50:C4	
■	IMAC-DE-NIKO-JR	10.40.0.86	Apple, Inc.	7C:C3:A1:B2:9A:9E	
■	10.40.0.88	10.40.0.88		2C:3B:70:06:68:49	
■	10.40.0.96	10.40.0.96		32:9F:7AA:EE:F7:C5	
■	10.40.0.143	10.40.0.143		1A:48:E6:E7:D2:01	
■	10.40.0.167	10.40.0.167		F6:05:8F:CE:D2:F8	
■	10.40.0.173	10.40.0.173		02:5C:37:26:59:7E	
■	10.40.0.183	10.40.0.183	Xiaomi Communicati...	98:F6:21:2CA:4:68	
■	10.40.0.187	10.40.0.187		52:7B:52:8B:82:49	
■	10.40.0.191	10.40.0.191		2E:BD:F1:BD:24:22	
■	10.40.0.193	10.40.0.193		62:A7:C9:FB:C5:1E	
■	10.40.0.195	10.40.0.195		BE:27:25:3E:32:DE	
■	10.40.0.198	10.40.0.198		9EF:3:EC:28:6D:74	
■	10.40.0.199	10.40.0.199	Xiaomi Communicati...	7CFD:6B:73:3E:D7	

Figura 2: Advanced IP Scanner 2

3.2. Speed Test

Es la forma de probar el rendimiento y la calidad de una conexión a Internet. Optimizado para medir incluso las conexiones modernas más avanzadas, proporciona información transparente sobre los factores que más impactan las experiencias conectadas, incluido el ancho de banda, la latencia, la cobertura, las métricas de video y más.

Lab 2: Software de Gestión de Redes



Figura 3: SpeedTest

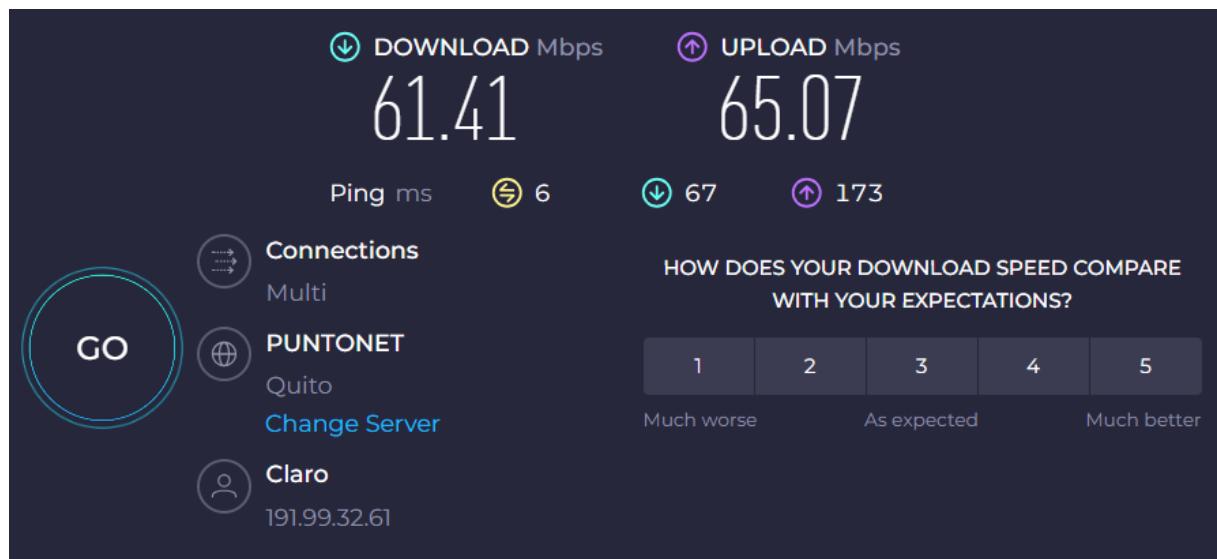


Figura 4: SpeedTest

3.3. whois.domaintools.com

WHOIS es la herramienta utilizada para buscar detalles del registro de nombre de dominios. Estos detalles contienen información sobre la fecha en que se registró el dominio, su fecha de vencimiento, la información del registrante, los nameservers y

Lab 2: Software de Gestión de Redes

el registrador del dominio. Cuando se registra un dominio, ICANN requiere que esta información se incluya en una base de datos pública que pueda ser vista por cualquiera que use el protocolo WHOIS.

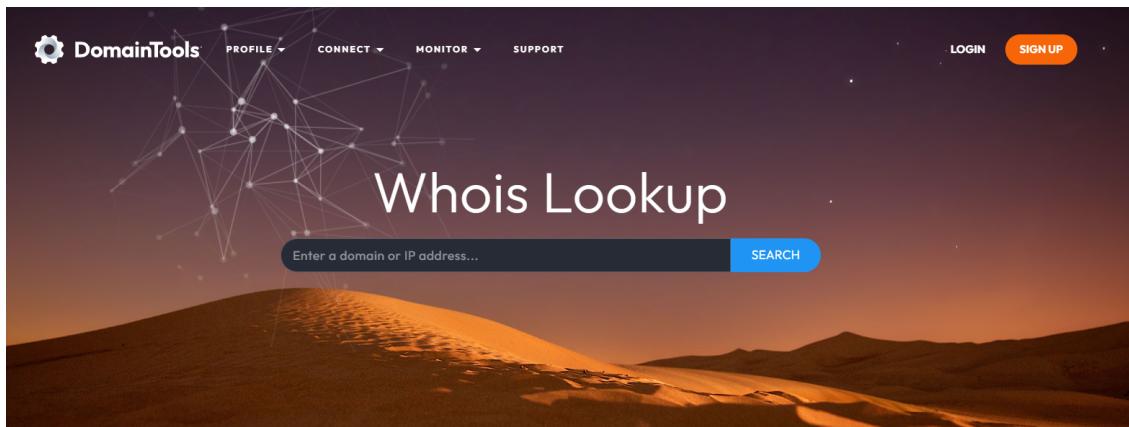


Figura 5: Who Is Domain Tools

Whois Record for ElComercio.com

Domain Profile	
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	10,351 days old Created on 1996-01-17 Expires on 2031-01-18 Updated on 2021-01-18
Name Servers	NS1.ELCOMERCIO.COM (has 1 domains) NS2.ELCOMERCIO.COM (has 1 domains)
IP Address	3.163.24.16 - 7,126 other sites hosted on this server
IP Location	 - Oregon - Portland - Amazon.com Inc.
ASN	 AS16509 AMAZON-02, US (registered May 04, 2000)
IP History	88 changes on 88 unique IP addresses over 19 years
Registrar History	2 registrars with 2 drops
Hosting History	7 changes on 6 unique name servers over 18 years

[Whois Record](#) (last updated on 2024-05-20)

Figura 6: Who Is Domain Tools

3.4. Visual Route

Ofrece una amplia variedad de herramientas de red que ayudan a los usuarios a mantenerse un paso por delante de los problemas de red, como cuellos de botella y problemas de latencia/pérdida de paquetes.

Lab 2: Software de Gestión de Redes

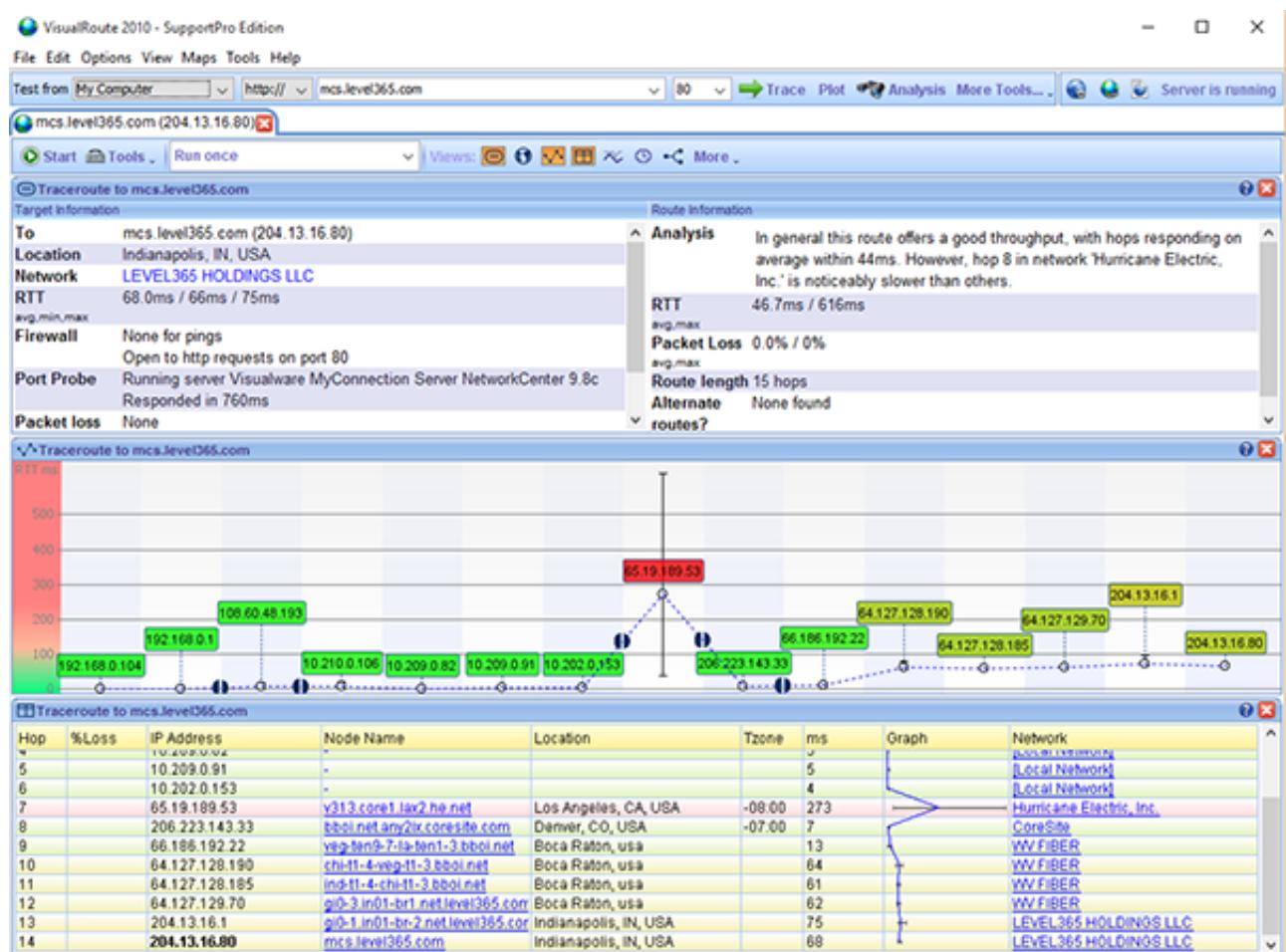


Figura 7: Visual Route

3.5. subnetonline.com

Con el creciente conjunto de herramientas IPv6, ofrece un medio para probar dispositivos habilitados para IPv6 y conectados a Internet. La página web tiene conversor de IPv4 a IPv6, calculadora de subred IPv6 y herramientas como Ping6, Traceroute6 y Tracepath6. Y recientemente agregó un escáner de puertos en línea habilitado para IPv6 para probar la conectividad de los servicios en servidores habilitados para IPv6.

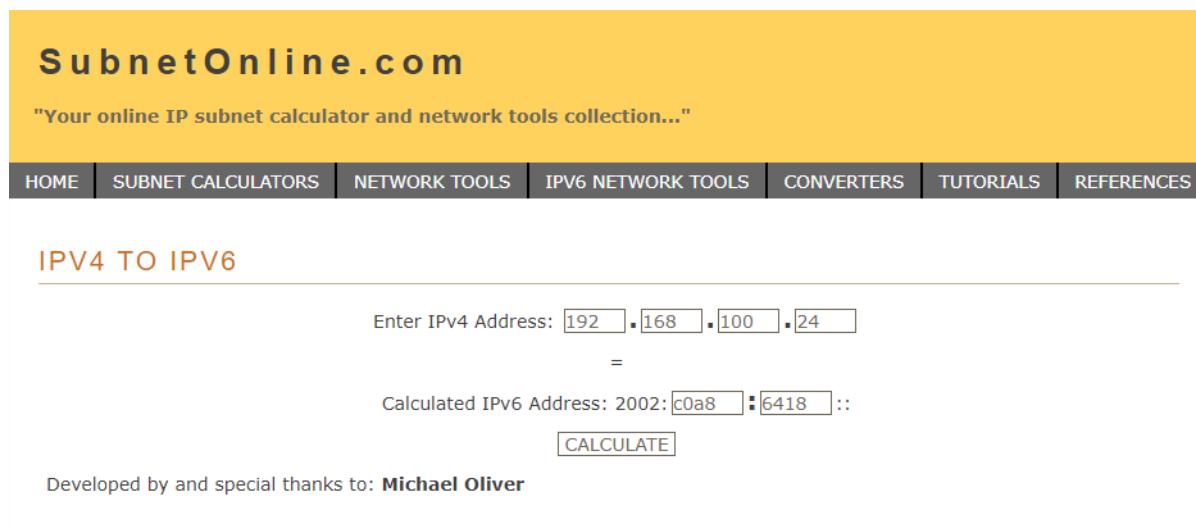


Figura 8: subnetonline.com

3.6. Live Cyber Threats

ES una herramienta que permite ver en tiempo real los ataques realizados por hackers, terroristas, espías, etc. Entre las amenazas se encuentran: virus, pérdida y robo de datos, ciberataques, phishing, malware, spyware, etc.

También se puede ver los países con mayor cantidad de ataques al día, entre los que destacan: Rusia, Estados Unidos y China



Figura 9: Live Cyber Threat Map

3.7. Kaspersky

Es una herramienta interactiva que muestra en tiempo real las ciberamenazas detectadas a nivel mundial. Este mapa incluye datos sobre ataques de malware, spam, intentos de phishing, ataques web y otras formas de ciberataques que Kaspersky ha identificado a través de su red global de sensores.

El mapa permite ver detalles específicos de las amenazas, como su tipo, origen y destino, y proporciona una visión global del panorama de seguridad cibernética actual. Es una herramienta muy útil para entender mejor cómo se distribuyen las amenazas cibernéticas en el mundo y cómo varían con el tiempo.

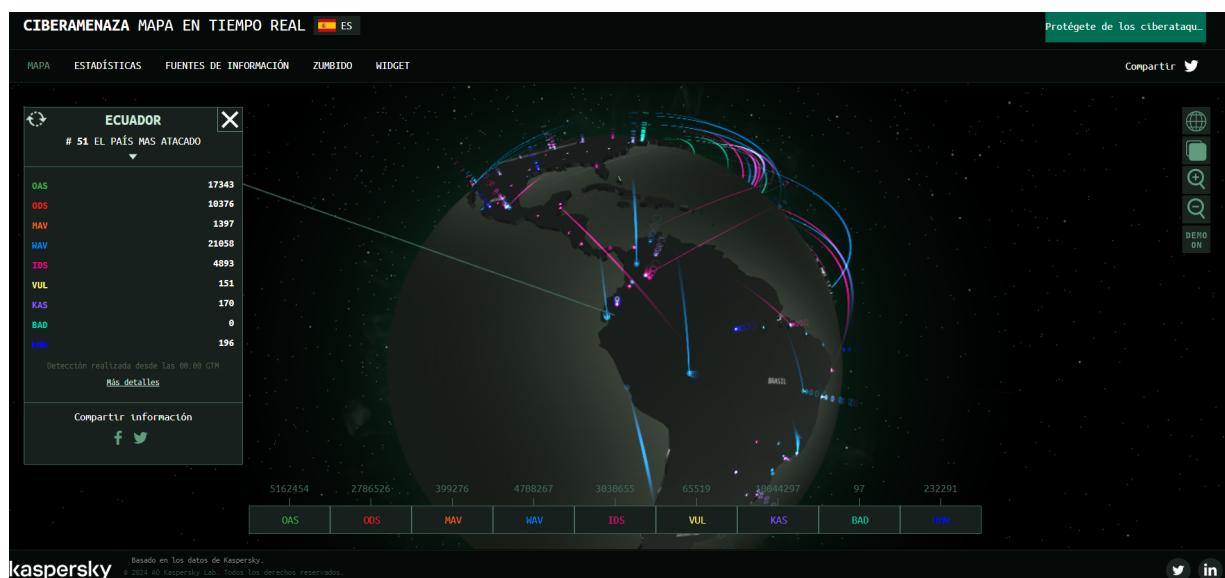


Figura 10: Karpersky

4. Conclusiones

Al finalizar esta práctica, se han adquirido competencias fundamentales en el uso de software de gestión de redes. Se es capaz de identificar y gestionar direcciones IP y MAC de dispositivos conectados a la red, facilitando la administración y el monitoreo efectivo de los recursos. Se ha aprendido a convertir direcciones IP entre formatos decimal y binario, fortaleciendo la comprensión de la estructura de direcciones IP y su aplicación en diversas configuraciones y diagnósticos de red. También se puede monitorear y detectar actividades maliciosas en tiempo real, utilizando herramientas de gestión de redes para identificar y responder a ciberataques de manera rápida y eficaz, mejorando la seguridad de la red. Finalmente, se tiene la habilidad de medir y analizar el ancho de banda disponible, así como la velocidad de descarga y subida de la red, optimizando el rendimiento y asegurando una distribución adecuada de los recursos de red.

5. Referencias Bibliográficas

- Advanced IP Scanner – Explorador de redes de descarga gratuita. (s.f.). <https://www.advanced-ip-scanner.com/es/>
- About Speedtest. (s. f.). <https://www.speedtest.net/about>

- Dreamhost. (2024, 26 febrero). Dreamhost. <https://help.dreamhost.com/hc/es/articles/216458220-Generalidades-de-WHOIS>
- VisualRoute Overview. (s. f.). <http://www.visualroute.com/overview.html>
- MAPA — Mapa en tiempo real de amenazas ciberneticas Kaspersky. (s. f.). MAPA — Mapa En Tiempo Real de Amenazas Ciberneticas Kaspersky. <https://cybermap.kaspersky.com/>
- Equipo editorial, Etecé. (2023b, noviembre 19). ¿Qué es la World Wide Web? -Concepto, importancia y más. Concepto. <https://concepto.de/www/>
- Internet: qué es, qué tipos de conexión existen - Ferrovial. (2022, 25 octubre). Ferrovial. <https://www.ferrovial.com/es/stem/internet/:text=El%20t%C3%A9rmino%20Internet>
- Internet: qué es, qué tipos de conexión existen - Ferrovial. (2022, 25 octubre). Ferrovial. <https://www.ferrovial.com/es/stem/internet/:text=El%20t%C3%A9rmino%20Internet>
- What is a wan? (2021). Cloudflare. <https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-wan/>



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Lab 3: Visita UTIC

Estudiantes:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuertes Diaz

19 de junio de 2024

1. Objetivos de Aprendizaje

1. Descripción de la Infraestructura Tecnológica, detallar el tipo de equipos y tecnologías utilizadas en el cuarto de servidores. Explicar la configuración y el propósito de los distintos servidores y dispositivos de red presentes en la instalación.
2. Evaluación de las Medidas de Seguridad, analizar las políticas de seguridad física y lógica implementadas en el cuarto de servidores. Describir los sistemas de protección contra incendios, fallos eléctricos y accesos no autorizados.

2. Desarrollo

Desde el año 2005 la ESPE cuenta con un Data Center que fue remodelado en el año 2012 – 2013 Concentra todos los servicios de comunicaciones, servicios de aplicaciones, redes de comunicación e Internet de la Universidad para dar Servicios como:

- Correo Electrónico
- Portal de Servicios MiESPE
- Acceso vía Wireless y LAN.
- Consolidación de enlaces WAN – Sedes y Extensiones.
- Monitoreo de los Servicios.

Lab 3: Visita UTIC

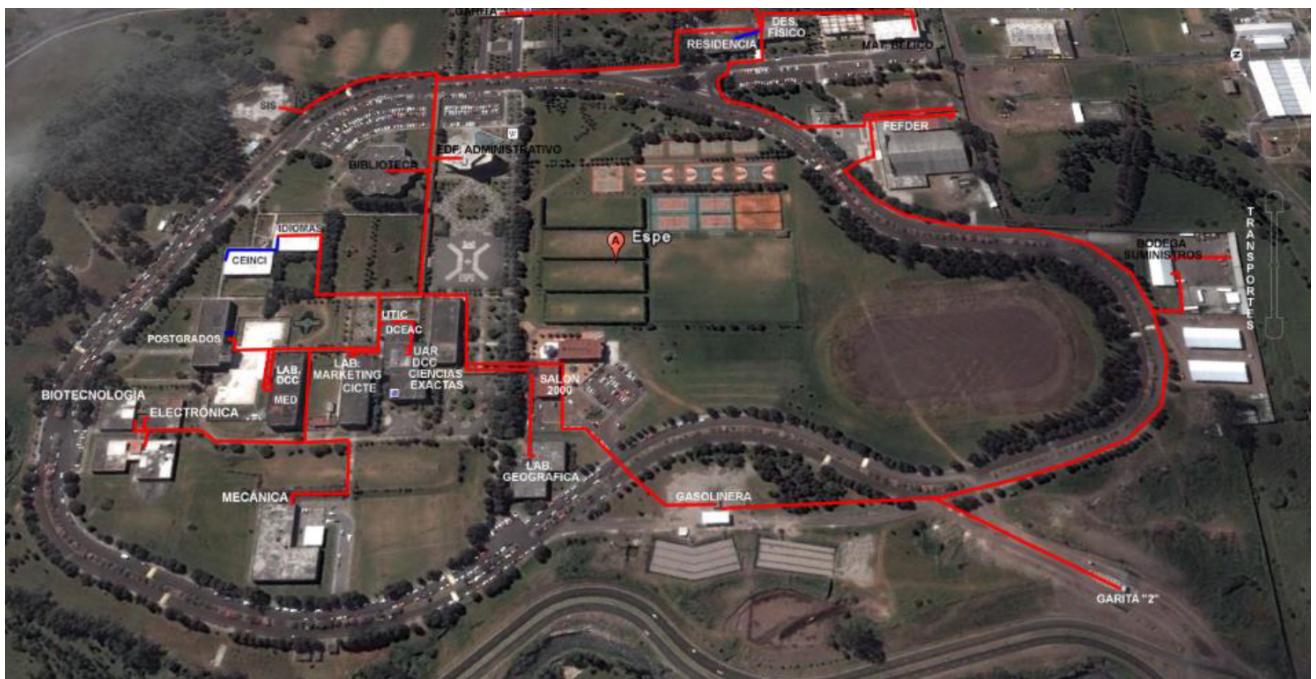


Figura 1: Redes

Infraestructura. monitoreo, óptima y ofrecer servicios. PRTG: Analiza los servidores y equipos a través de una dirección IP para verificar la conectividad. El internet de la ESPE lo proporciona CEDIA, para la matriz principal y para todas sus sedes.

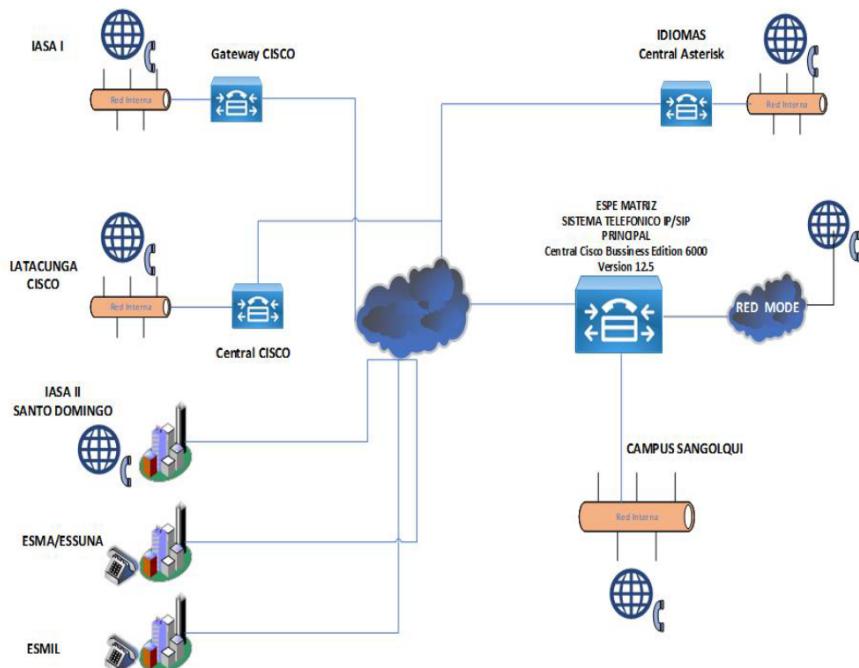


Figura 2: Redes

2.1. Componentes Básicos

- Parte Eléctrica.
- Aire Acondicionados.
- Sistema Contra Incendios.
- Acceso Biométrico.

El Data center está siempre a 21-22 grados, 50 % de humedad, bien diseñado, humedad y temperatura. Cuenta con dos cuartos fríos y un cuarto caliente.

Lab 3: Visita UTIC



Figura 3: Data Center

La Arquitectura está detallada a continuación:



Figura 4: Arquitectura Data Center

Para la prevención de incendios, el datacenter cuenta con un extintor, cuyo material para apagar el fuego es uno que no dañaría los dispositivos eléctricos. La puerta de entrada al datacenter es gruesa y pesada, para que en caso de un accidente o un incendio las llamas no se esparzcan de forma fácil al resto del edificio. La ESPE cuenta con su propio generador eléctrico, adicional a ello el datacenter cuenta con su propio generador eléctrico.



Figura 5: Generador Eléctrico

3. Conclusiones

Durante la visita al cuarto de servidores de la UTIC, se observó una infraestructura tecnológica robusta y bien organizada. Los equipos presentes incluyen servidores de última generación, dispositivos de almacenamiento, y sistemas de red avanzados. Cada componente cumple un propósito específico dentro de la red de la universidad, desde la gestión de datos hasta el soporte de aplicaciones críticas. La configuración de estos dispositivos está diseñada para maximizar la eficiencia y la disponibilidad, asegurando un rendimiento óptimo y minimizando el tiempo de inactividad.

Las medidas de seguridad implementadas en el cuarto de servidores son exhaustivas y abarcan tanto aspectos físicos como lógicos. Se cuenta con sistemas de protección contra incendios, tales como detectores de humo y sistemas de supresión. Adicionalmente, se han instalado dispositivos de alimentación ininterrumpida (UPS) y generadores de respaldo para prevenir fallos eléctricos. En cuanto a la seguridad lógica, se utilizan cortafuegos, sistemas de detección de intrusos y protocolos de autenticación estrictos para proteger la integridad y confidencialidad de los datos. El acceso al cuarto de servidores está restringido a personal autorizado, y se llevan registros detallados de todas las entradas y salidas.

4. Referencias Bibliográficas

- Universidad de las Fuerzas Armadas, ESPE. (2023, 1 junio). UTIC — ESPE. ESPE. <https://www.espe.edu.ec/utic/>



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 interactuan

2. Marco Teórico

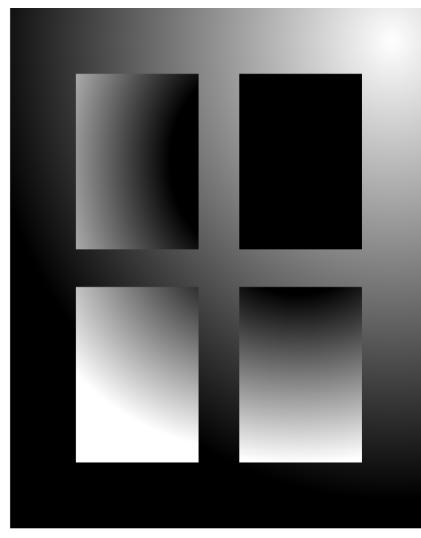
2.1. Historia de Windows

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.



MICROSOFT
WINDOWS

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 miniorte WDM, los administradores de llamadas de miniorte (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. . . :

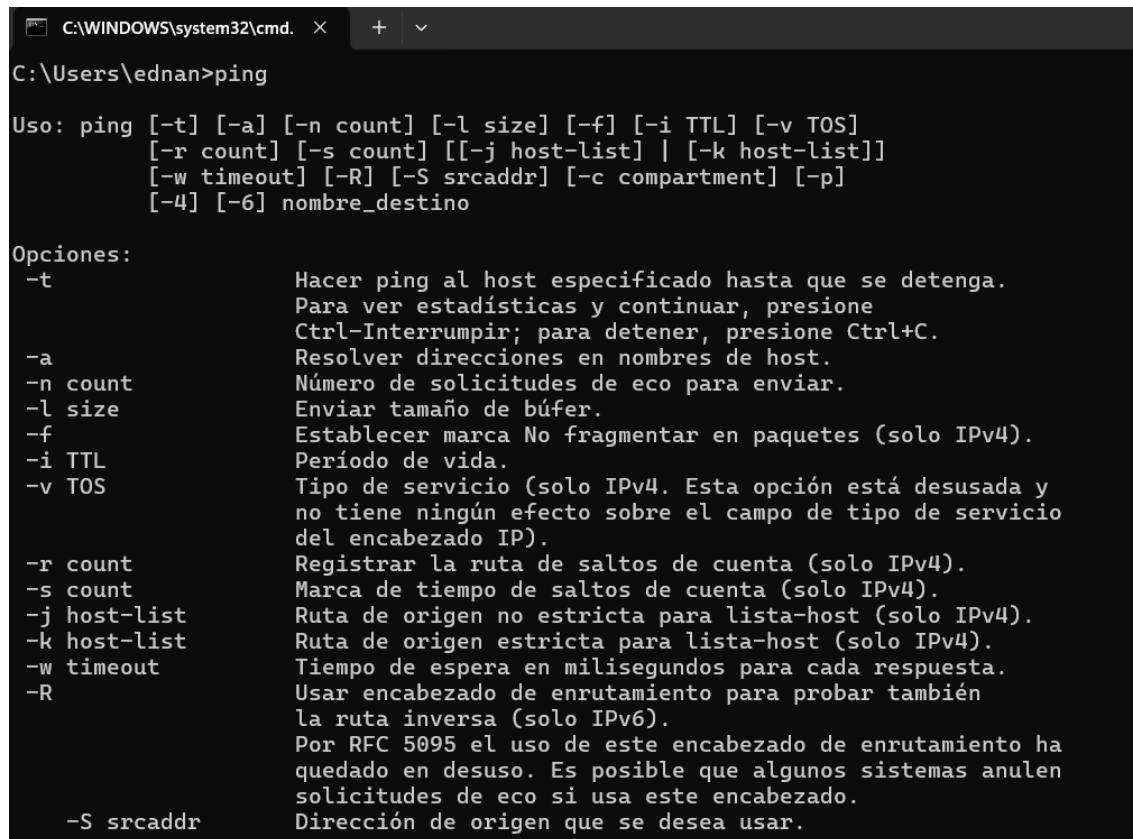
Adaptador de Ethernet Ethernet:
  Sufijo DNS específico para la conexión. . . :
  Dirección IPv6 . . . . . : 2800:440:9838:e400::1
  Dirección IPv6 . . . . . : 2800:440:9838:e400:d36a:5a73:fc88:758a
  Dirección IPv6 temporal. . . . . : 2800:440:9838:e400:a50e:fcfc:fc43:4dfe
  Vínculo: dirección IPv6 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. × + ▾
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

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