

Protocolos de Capa de Aplicación y Estándares de Capa Física en Infraestructuras de Red

Santiago Botero García

Laura Natalia Perilla Quintero

Escuela Colombiana de Ingeniería Julio Garavito

AYSR-1L: Arquitectura y Servicios de Red

Ing. Jhon Alexander Pachón Pinzón

Octubre 05, 2025

Resumen

El desarrollo de infraestructuras de red modernas requiere la integración eficiente de protocolos de capa de aplicación junto con la implementación adecuada de la capa física. Este trabajo se centra en la configuración, monitoreo y análisis de protocolos como DNS, HTTP, FTP y correo electrónico en entornos simulados y reales, utilizando herramientas como Cisco Packet Tracer y Wireshark. Asimismo, se aborda la importancia de los servicios de sincronización temporal mediante NTP, esenciales para garantizar la coherencia en sistemas distribuidos. En el ámbito físico, se incluyen prácticas de construcción de cables UTP con conectores RJ-45, pruebas de crimpado en patch panels y la observación de estándares de cableado estructurado en entornos académicos. El objetivo principal es fortalecer las competencias técnicas en el diseño, configuración y verificación de redes, fomentando la comprensión del flujo de información en la capa de aplicación y la correcta gestión de los elementos físicos. De esta manera, se promueve un aprendizaje integral que vincula el análisis lógico de protocolos con la manipulación práctica de componentes de infraestructura, asegurando un enfoque completo en la formación de ingenieros en sistemas y telecomunicaciones.

Palabras clave. Protocolos de Red, Capa de Aplicación, Capa Física, DNS, HTTP, FTP, Correo Electrónico, NTP, Cableado Estructurado, Packet Tracer, Wireshark.

	Contenido
Resumen.....	2
Metodología	4
Caso Santiago: Desarrollo de Red en Packet Tracer	4
<i>Configuración Inicial</i>	4
<i>Configuración de red</i>	9
<i>Configuración de servicios</i>	12
Caso Natalia: Desarrollo de Red en Packet Tracer.....	37
En la Red Real.....	45
Wireshark	45
Prueba del servicio DNS.....	60
Servidor NTP.....	74
<i>Team 01 – NTP Server en Solaris con clientes multiplataforma</i>	74
<i>Team 02 – NTP Server en Slackware con clientes Solaris y Windows</i>	79
Cableado estructurado y construcción de cables	82
<i>Implementación de Santiago: Cable Directo T568A y Cable Cruzado T568A/T568B</i>	85
<i>Implementación de Natalia: Cable Directo T568B y Cable Cruzado T568A/T568B.....</i>	88
<i>Ponchado con Patch Panel y Conexión de Máquinas.....</i>	91
Conocimiento del Cableado Estructurado de la Universidad.....	95
Conclusiones	96
Bibliografía	97

Metodología

Caso Santiago: Desarrollo de Red en Packet Tracer

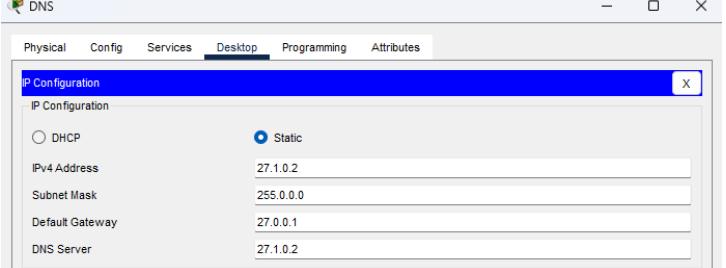
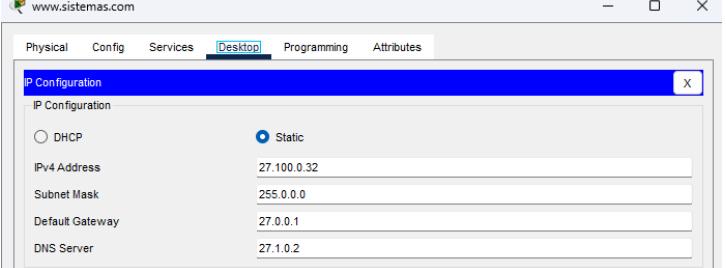
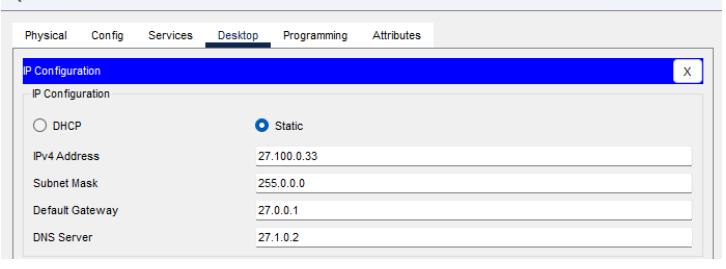
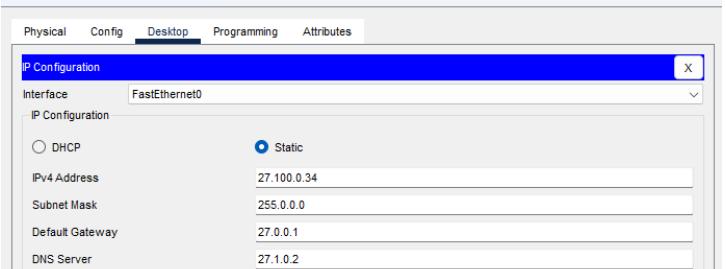
Como parte del desarrollo individual del proyecto de simulación de redes, esta sección presenta la implementación realizada por Santiago en el entorno de Packet Tracer. El objetivo principal fue diseñar y configurar una red académica que integrara los programas de Sistemas, Civil y Eléctrica, asegurando conectividad, resolución de nombres y servicios básicos como correo electrónico y web. Para ello, se incorporaron dispositivos clave como servidores, PCs y switches, y se establecieron parámetros de red específicos que permiten la comunicación fluida entre los distintos nodos. Esta implementación completa se encuentra documentada y disponible en el archivo campus-network-santiago-implementation.pkt, el cual contiene toda la topología funcional y las configuraciones desarrolladas. A continuación, se detallan las acciones realizadas durante la configuración inicial y el despliegue de la topología física.

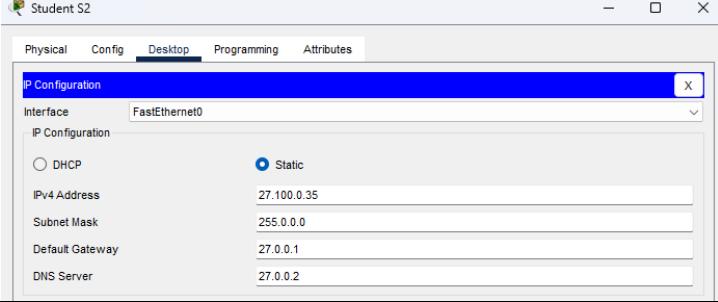
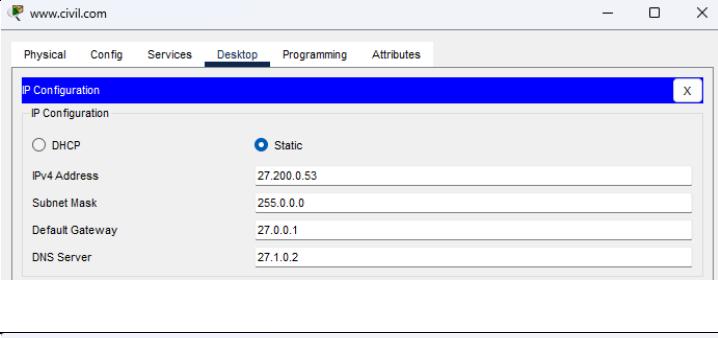
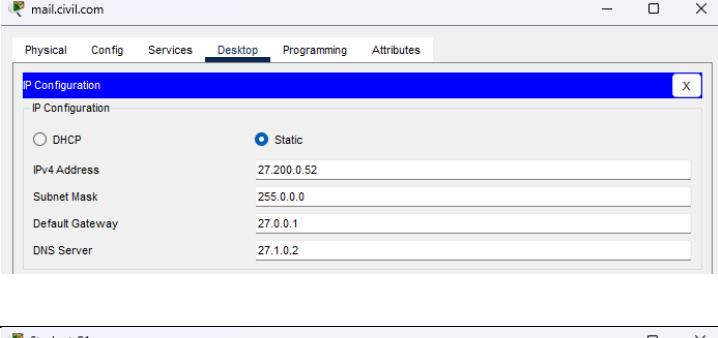
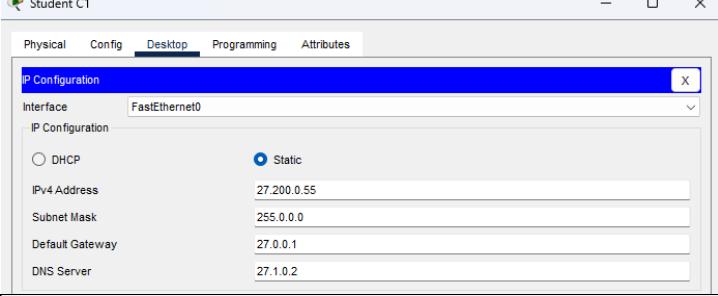
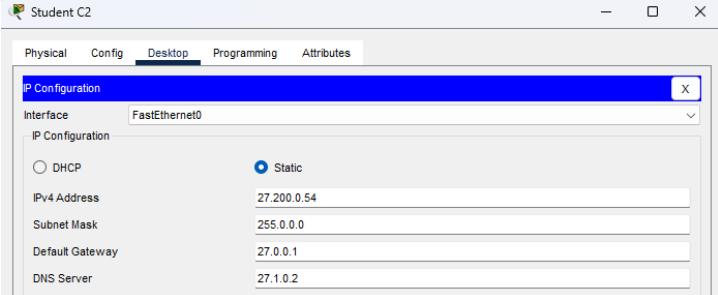
Configuración Inicial

Para la configuración inicial de la red, se deben agregar los siguientes dispositivos en el entorno de Packet Tracer: 6 servidores (Server-PT), 6 PCs (PC-PT) y 3 switches del modelo 2950-24. En cada PC y servidor (accediendo a la pestaña **Desktop > IP Configuration**), se debe configurar la siguiente información:

- **IP Address:** Por ejemplo, 27.100.0.34 para el PC "Student S1".
- **Subnet Mask:** 255.0.0.0
- **Default Gateway:** 27.0.0.1
- **DNS Server:** 27.1.0.2 (la IP del servidor DNS).

Este proceso establece la conectividad básica entre los dispositivos de la red antes de continuar con configuraciones más avanzadas.

Actividad/Acción/Tarea	Detalles relevantes
Se configuró un servidor DNS de tipo Server-PT con la dirección IPv4 27.1.0.2, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2	
Se configuró un servidor Server-PT con la dirección IPv4 27.100.0.32, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2, estableciendo dicho servidor como el encargado de gestionar las solicitudes del dominio www.sistemas.com	
Se configuró un servidor Server-PT con la dirección IPv4 27.100.0.33, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2; este equipo será el encargado de gestionar los servicios de correo electrónico y atender las solicitudes asociadas al dominio mail.sistemas.com	
Se configuró una PC-PT correspondiente al estudiante 1 del programa de Sistemas con la dirección IPv4 27.100.0.34, máscara de subred 255.0.0.0, puerta de enlace predeterminada 27.0.0.1 y servidor DNS 27.1.0.2	

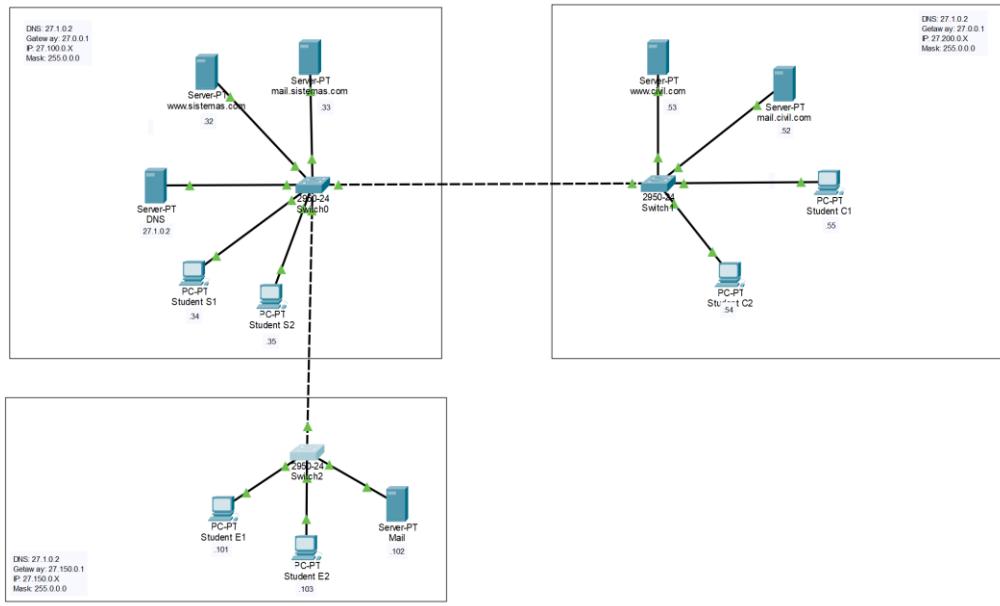
<p>Se configuró una PC-PT correspondiente al estudiante 2 del programa de Sistemas con la dirección IPv4 27.100.0.35, máscara de subred 255.0.0.0, puerta de enlace predeterminada 27.0.0.1 y servidor DNS 27.1.0.2</p>	 <p>IP Configuration</p> <p>Interface: FastEthernet0</p> <p>IP Configuration</p> <p><input type="radio"/> DHCP <input checked="" type="radio"/> Static</p> <p>IPv4 Address: 27.100.0.35</p> <p>Subnet Mask: 255.0.0.0</p> <p>Default Gateway: 27.0.0.1</p> <p>DNS Server: 27.0.0.2</p>
<p>Se configuró un servidor Server-PT con la dirección IPv4 27.200.0.53, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2, estableciendo dicho servidor como el encargado de recibir y gestionar las solicitudes asociadas al dominio www.civil.com.</p>	 <p>IP Configuration</p> <p>IP Configuration</p> <p><input type="radio"/> DHCP <input checked="" type="radio"/> Static</p> <p>IPv4 Address: 27.200.0.53</p> <p>Subnet Mask: 255.0.0.0</p> <p>Default Gateway: 27.0.0.1</p> <p>DNS Server: 27.1.0.2</p>
<p>Se configuró un servidor Server-PT con la dirección IPv4 27.200.0.52, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2. Este equipo será el encargado de gestionar los servicios de correo electrónico y atender las solicitudes relacionadas con el dominio mail.civil.com</p>	 <p>IP Configuration</p> <p>IP Configuration</p> <p><input type="radio"/> DHCP <input checked="" type="radio"/> Static</p> <p>IPv4 Address: 27.200.0.52</p> <p>Subnet Mask: 255.0.0.0</p> <p>Default Gateway: 27.0.0.1</p> <p>DNS Server: 27.1.0.2</p>
<p>Se configuró una PC-PT correspondiente al estudiante 1 del programa de Civil con la dirección IP 27.200.0.55, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2</p>	 <p>IP Configuration</p> <p>Interface: FastEthernet0</p> <p>IP Configuration</p> <p><input type="radio"/> DHCP <input checked="" type="radio"/> Static</p> <p>IPv4 Address: 27.200.0.55</p> <p>Subnet Mask: 255.0.0.0</p> <p>Default Gateway: 27.0.0.1</p> <p>DNS Server: 27.1.0.2</p>
<p>Se configuró una PC-PT correspondiente al estudiante 2 del programa de Civil con la dirección IP 27.200.0.54, máscara de subred 255.0.0.0, puerta de enlace 27.0.0.1 y servidor DNS 27.1.0.2</p>	 <p>IP Configuration</p> <p>Interface: FastEthernet0</p> <p>IP Configuration</p> <p><input type="radio"/> DHCP <input checked="" type="radio"/> Static</p> <p>IPv4 Address: 27.200.0.54</p> <p>Subnet Mask: 255.0.0.0</p> <p>Default Gateway: 27.0.0.1</p> <p>DNS Server: 27.1.0.2</p>

<p>Se activó el servicio DNS en el servidor configurado con la dirección IP 27.1.0.2, accediendo a la pestaña Services > DNS, donde se habilitó dicha funcionalidad. Posteriormente, se añadieron los siguientes registros de dominio: www.sistemas.com apuntando a 27.100.0.32, mail.sistemas.com a 27.100.0.33, www.civil.com a 27.200.0.53 y mail.civil.com a 27.200.0.52, permitiendo la correcta resolución de nombres dentro de la red.</p>	<table border="1"> <thead> <tr> <th>No.</th> <th>Name</th> <th>Type</th> <th>Detail</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>mail.civil.com</td> <td>A Record</td> <td>27.200.0.52</td> </tr> <tr> <td>1</td> <td>mail.sistemas.com</td> <td>A Record</td> <td>27.100.0.33</td> </tr> <tr> <td>2</td> <td>www.civil.com</td> <td>A Record</td> <td>27.200.0.53</td> </tr> <tr> <td>3</td> <td>www.sistemas.com</td> <td>A Record</td> <td>27.100.0.32</td> </tr> </tbody> </table>	No.	Name	Type	Detail	0	mail.civil.com	A Record	27.200.0.52	1	mail.sistemas.com	A Record	27.100.0.33	2	www.civil.com	A Record	27.200.0.53	3	www.sistemas.com	A Record	27.100.0.32
No.	Name	Type	Detail																		
0	mail.civil.com	A Record	27.200.0.52																		
1	mail.sistemas.com	A Record	27.100.0.33																		
2	www.civil.com	A Record	27.200.0.53																		
3	www.sistemas.com	A Record	27.100.0.32																		
<p>Se configuró una PC-PT correspondiente al estudiante 1 del programa de Eléctrica con la dirección IP 27.150.0.101, máscara de subred 255.0.0.0, puerta de enlace 27.150.0.1 y servidor DNS 27.1.0.2</p>	<table border="1"> <tr> <td>Interface</td> <td>FastEthernet0</td> </tr> <tr> <td>IP Configuration</td> <td> <input type="radio"/> DHCP <input checked="" type="radio"/> Static </td> </tr> <tr> <td>IPv4 Address</td> <td>27.150.0.101</td> </tr> <tr> <td>Subnet Mask</td> <td>255.0.0.0</td> </tr> <tr> <td>Default Gateway</td> <td>27.150.0.1</td> </tr> <tr> <td>DNS Server</td> <td>27.1.0.2</td> </tr> </table>	Interface	FastEthernet0	IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	IPv4 Address	27.150.0.101	Subnet Mask	255.0.0.0	Default Gateway	27.150.0.1	DNS Server	27.1.0.2								
Interface	FastEthernet0																				
IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static																				
IPv4 Address	27.150.0.101																				
Subnet Mask	255.0.0.0																				
Default Gateway	27.150.0.1																				
DNS Server	27.1.0.2																				
<p>Se configuró una PC-PT correspondiente al estudiante 2 del programa de Eléctrica con la dirección IP 27.150.0.103, máscara de subred 255.0.0.0, puerta de enlace 27.150.0.1 y servidor DNS 27.1.0.2</p>	<table border="1"> <tr> <td>Interface</td> <td>FastEthernet0</td> </tr> <tr> <td>IP Configuration</td> <td> <input type="radio"/> DHCP <input checked="" type="radio"/> Static </td> </tr> <tr> <td>IPv4 Address</td> <td>27.150.0.103</td> </tr> <tr> <td>Subnet Mask</td> <td>255.0.0.0</td> </tr> <tr> <td>Default Gateway</td> <td>27.150.0.1</td> </tr> <tr> <td>DNS Server</td> <td>27.1.0.2</td> </tr> </table>	Interface	FastEthernet0	IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	IPv4 Address	27.150.0.103	Subnet Mask	255.0.0.0	Default Gateway	27.150.0.1	DNS Server	27.1.0.2								
Interface	FastEthernet0																				
IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static																				
IPv4 Address	27.150.0.103																				
Subnet Mask	255.0.0.0																				
Default Gateway	27.150.0.1																				
DNS Server	27.1.0.2																				
<p>Se configuró un servidor Server-PT con la dirección IP 27.150.0.105, máscara de subred 255.0.0.0, puerta de enlace 27.150.0.1 y servidor DNS 27.1.0.2; este equipo tiene como propósito gestionar los servicios de correo electrónico del programa de Eléctrica, asegurando su operatividad y disponibilidad dentro de la red.</p>	<table border="1"> <tr> <td>IP Configuration</td> <td> <input type="radio"/> DHCP <input checked="" type="radio"/> Static </td> </tr> <tr> <td>IPv4 Address</td> <td>27.150.0.102</td> </tr> <tr> <td>Subnet Mask</td> <td>255.0.0.0</td> </tr> <tr> <td>Default Gateway</td> <td>27.150.0.1</td> </tr> <tr> <td>DNS Server</td> <td>27.1.0.2</td> </tr> </table>	IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	IPv4 Address	27.150.0.102	Subnet Mask	255.0.0.0	Default Gateway	27.150.0.1	DNS Server	27.1.0.2										
IP Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static																				
IPv4 Address	27.150.0.102																				
Subnet Mask	255.0.0.0																				
Default Gateway	27.150.0.1																				
DNS Server	27.1.0.2																				

De esta manera, utilizando cables Copper Straight-Through, se conectaron los servidores Server-PT correspondientes a www.sistemas.com, mail.sistemas.com y el servidor DNS al Switch 0, junto con las PC-PT de los estudiantes del programa de Sistemas. De forma similar, se conectaron los servidores www.civil.com y mail.civil.com, así como las PC-PT de los estudiantes de Civil, al Switch 1. Posteriormente, también mediante cables Copper Straight-Through, se conectaron las PC-PT de los estudiantes de Eléctrica y el servidor de correo correspondiente al programa al Switch 2. Finalmente, se establecieron las interconexiones entre switches utilizando cables Copper Cross-Over, conectando el Switch 2 con el Switch 0, y el Switch 0 con el Switch 1, permitiendo la comunicación entre las distintas redes locales.

Figura 1

Topología de Red Física del Proyecto

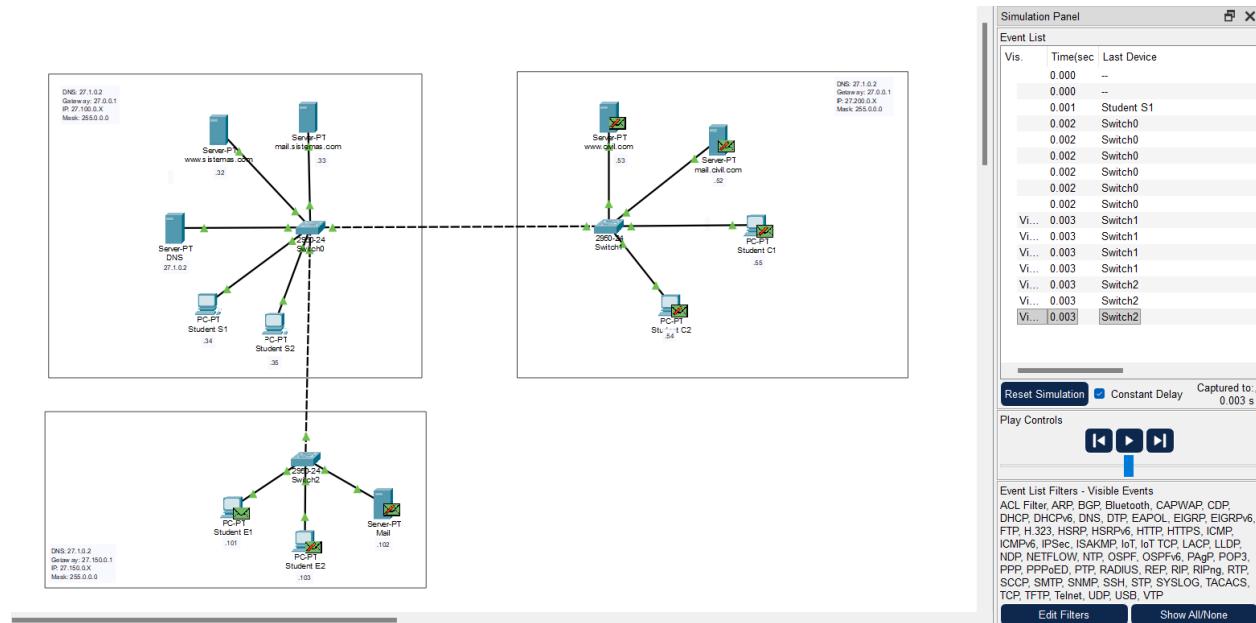


Nota. Se observa la conexión de los servidores y PC-PT de los programas de Sistemas, Civil y Eléctrica a sus respectivos switches, así como la interconexión entre los switches mediante cables Copper Cross-Over, reflejando la estructura completa de la red.

Configuración de red

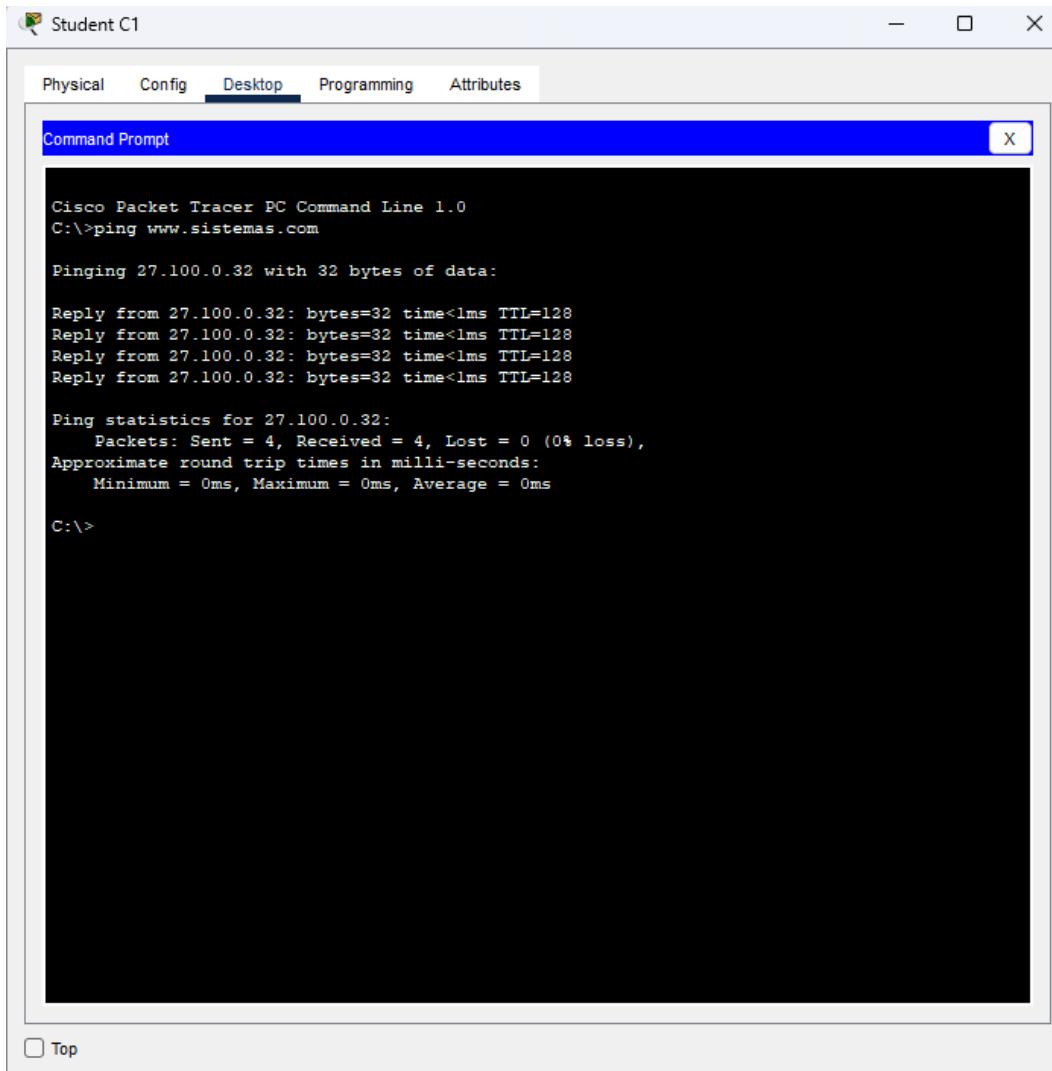
Una vez establecidas todas las conexiones físicas entre los dispositivos, se procedió a verificar que los equipos estuvieran encendidos y con las interfaces de red activas. Para ello, se observó que los indicadores visuales en ambos extremos de cada cable fueran de color verde, lo cual confirma el funcionamiento correcto del enlace. En caso de señales naranjas o rojas, se revisaron tanto las conexiones como la configuración IP de los dispositivos involucrados.

A continuación, se realizaron pruebas de conectividad lógica utilizando la herramienta "Add Simple PDU" en Cisco Packet Tracer. Esta permite enviar mensajes de prueba entre distintos dispositivos. Se seleccionó un origen y un destino, y se verificó que la comunicación fuera exitosa mediante la aparición de un check verde en la barra inferior del simulador. Una de estas pruebas se realizó desde el dispositivo PC-PT Student S1 hasta PC-PT Student E1, observando que el mensaje llegó correctamente al destinatario, mientras que los demás dispositivos de la red ignoraron el paquete, como es esperado en una comunicación unicast.

Figura 2*Prueba de Conectividad con PDU Simple*

Nota. Se muestra el resultado de la prueba de conectividad utilizando la herramienta Add Simple PDU, en la cual se generaron un total de 14 eventos. La imagen evidencia que el mensaje fue entregado exitosamente al dispositivo de destino, mientras los demás dispositivos descartaron el paquete, confirmando el correcto direccionamiento del mensaje.

Posteriormente, se utilizó el comando ping para comprobar la conectividad real entre dispositivos. Desde la interfaz Command Prompt en PC-PT Student C1, se ejecutó un ping hacia el servidor asignado al dominio www.sistemas.com, recibiendo una respuesta exitosa con mensajes del tipo Reply from..., lo que confirma que la red está correctamente configurada y los nodos pueden comunicarse entre sí sin inconvenientes.

Figura 3*Verificación de Conectividad mediante Comando PING*

The screenshot shows a window titled "Student C1" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside, a Command Prompt window is open with the title "Command Prompt". The command entered is "C:\>ping www.sistemas.com". The output shows four successful replies from the IP 27.100.0.32, each with bytes=32, time<1ms, and TTL=128. It also displays ping statistics: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), and approximate round trip times (Minimum = 0ms, Maximum = 0ms, Average = 0ms). The prompt "C:\>" is visible at the bottom.

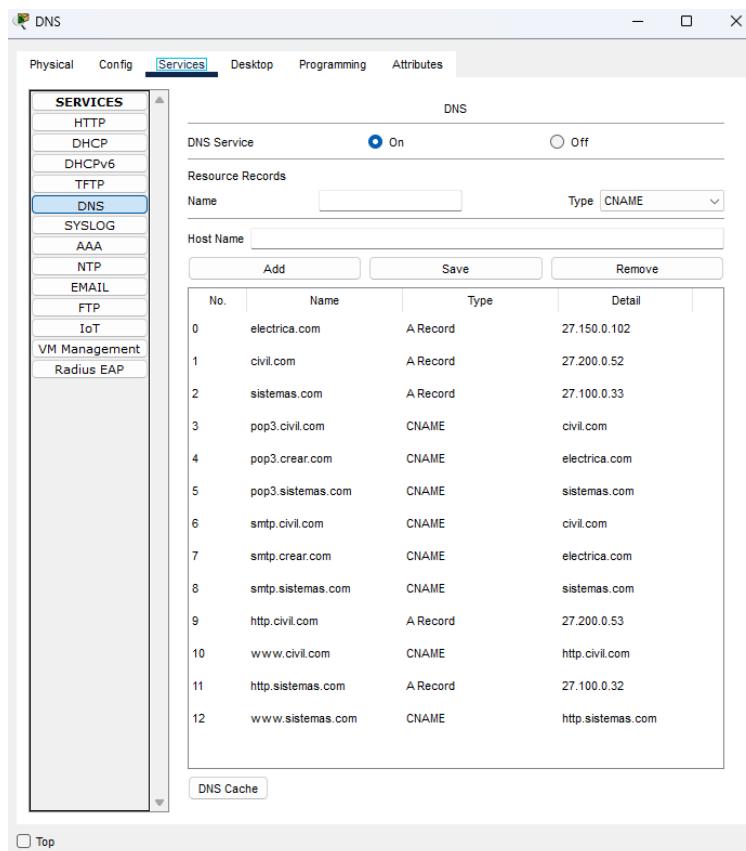
Nota. La imagen muestra la ejecución exitosa del comando ping desde el dispositivo PC-PT Student C1 hacia el dominio www.sistemas.com (IP 27.100.0.32). Se observan 4 respuestas recibidas con un tiempo de respuesta menor a 1 ms y sin pérdida de paquetes (0% loss), lo que confirma la correcta resolución de nombres a través del DNS y una comunicación eficiente entre los dispositivos en la red.

Configuración de servicios

Para cumplir con los requisitos del ejercicio, se configuró el servidor DNS con dirección IP 27.1.0.2, incorporando todas las entradas solicitadas para los dominios sistemas.com, civil.com, y electrica.com. Se añadieron registros principales y alias correspondientes para los servicios de correo (pop3, smtp) y web (http, www) de cada dominio. Esta configuración garantiza que cualquier dispositivo en la red pueda resolver correctamente los nombres de dominio hacia sus respectivas direcciones IP. Una vez finalizada la configuración, se verificó la correcta asociación de cada entrada mediante pruebas de resolución.

Figura 4

Configuración del servidor DNS en Cisco Packet Tracer



Nota. En esta imagen se muestra la tabla de registros DNS con todos los dominios y alias configurados según los requerimientos del ejercicio.

Con la configuración del servidor DNS completada, se procedió a realizar las pruebas de conectividad desde una estación de trabajo simulada. Para ello, se seleccionó aleatoriamente el dispositivo PC-PT Student S1, desde el cual se ejecutaron comandos ping hacia los distintos dominios configurados. Las pruebas incluyeron tanto los nombres principales como sus alias, y los resultados obtenidos se documentaron en una tabla que incluye descripciones detalladas y capturas de pantalla de cada caso.

Descripción del Ping	Captura de Pantalla
<p>Servidor de correo de sistemas.com (27.100.0.33):</p> <p>Se realizó ping exitosamente a tres dominios: sistemas.com, pop3.sistemas.com y smtp.sistemas.com, todos resolviendo correctamente a la IP del servidor de correo. El tiempo de respuesta fue consistentemente menor a 1 ms, lo que generó un promedio de 0 ms. Esto indica una conexión directa y sin latencia perceptible dentro de la red simulada.</p>	<pre>Cisco Packet Tracer PC Command Line 1.0 C:\>ping sistemas.com Pinging 27.100.0.33 with 32 bytes of data: Reply from 27.100.0.33: bytes=32 time<1ms TTL=128 Ping statistics for 27.100.0.33: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping pop3.sistemas.com Pinging 27.100.0.33 with 32 bytes of data: Reply from 27.100.0.33: bytes=32 time<1ms TTL=128 Ping statistics for 27.100.0.33: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping smtp.sistemas.com Pinging 27.100.0.33 with 32 bytes of data: Reply from 27.100.0.33: bytes=32 time<1ms TTL=128 Reply from 27.100.0.33: bytes=32 time<1ms TTL=128 Reply from 27.100.0.33: bytes=32 time=5ms TTL=128 Reply from 27.100.0.33: bytes=32 time<1ms TTL=128 Ping statistics for 27.100.0.33: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 5ms, Average = 1ms C:\></pre>

Servidor web de sistemas.com (27.100.0.32):

El dominio http.sistemas.com y su alias www.sistemas.com resolvieron correctamente a la IP del servidor web. El tiempo de respuesta fue menor a 1 ms, reflejando una conexión rápida y estable.

```
C:\>ping http.sistemas.com
Pinging 27.100.0.32 with 32 bytes of data:
Reply from 27.100.0.32: bytes=32 time<1ms TTL=128

Ping statistics for 27.100.0.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping www.sistemas.com
Pinging 27.100.0.32 with 32 bytes of data:
Reply from 27.100.0.32: bytes=32 time<1ms TTL=128

Ping statistics for 27.100.0.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Servidor de correo de civil.com (27.200.0.52):

Los dominios civil.com, pop3.civil.com y smtp.civil.com fueron probados con éxito. El tiempo promedio de respuesta fue de 2 ms, ligeramente superior pero aún dentro de parámetros óptimos para una red local simulada.

```
C:\>ping civil.com
Pinging 27.200.0.52 with 32 bytes of data:
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128
Reply from 27.200.0.52: bytes=32 time=6ms TTL=128
Reply from 27.200.0.52: bytes=32 time=6ms TTL=128

Ping statistics for 27.200.0.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 3ms

C:\>ping pop3.civil.com
Pinging 27.200.0.52 with 32 bytes of data:
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128

Ping statistics for 27.200.0.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping smtp.civil.com
Pinging 27.200.0.52 with 32 bytes of data:
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128
Reply from 27.200.0.52: bytes=32 time=2ms TTL=128
Reply from 27.200.0.52: bytes=32 time=5ms TTL=128
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128

Ping statistics for 27.200.0.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>
```

Servidor web de civil.com (27.200.0.53):

Se verificó conectividad con http.civil.com y www.civil.com, ambos resolviendo correctamente a la IP del servidor web. El tiempo de respuesta fue menor a 1 ms, lo que indica una conexión eficiente.

```
C:\>ping http.civil.com
Pinging 27.200.0.53 with 32 bytes of data:
Reply from 27.200.0.53: bytes=32 time<1ms TTL=128

Ping statistics for 27.200.0.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping www.civil.com
Pinging 27.200.0.53 with 32 bytes of data:
Reply from 27.200.0.53: bytes=32 time<1ms TTL=128

Ping statistics for 27.200.0.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Servidor de correo de electrica.com (27.150.0.102):

Se realizó ping a electrica.com, pop3.crear.com y smtp.crear.com, todos configurados como alias del servidor de correo. La resolución DNS fue correcta y el tiempo promedio de respuesta fue menor a 1 ms, demostrando una conectividad óptima.

```
C:\>ping electrica.com
Pinging 27.150.0.102 with 32 bytes of data:
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128
Reply from 27.150.0.102: bytes=32 time=6ms TTL=128
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128

Ping statistics for 27.150.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>ping pop3.crear.com
Pinging 27.150.0.102 with 32 bytes of data:
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128

Ping statistics for 27.150.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping smtp.crear.com
Pinging 27.150.0.102 with 32 bytes of data:
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128

Ping statistics for 27.150.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

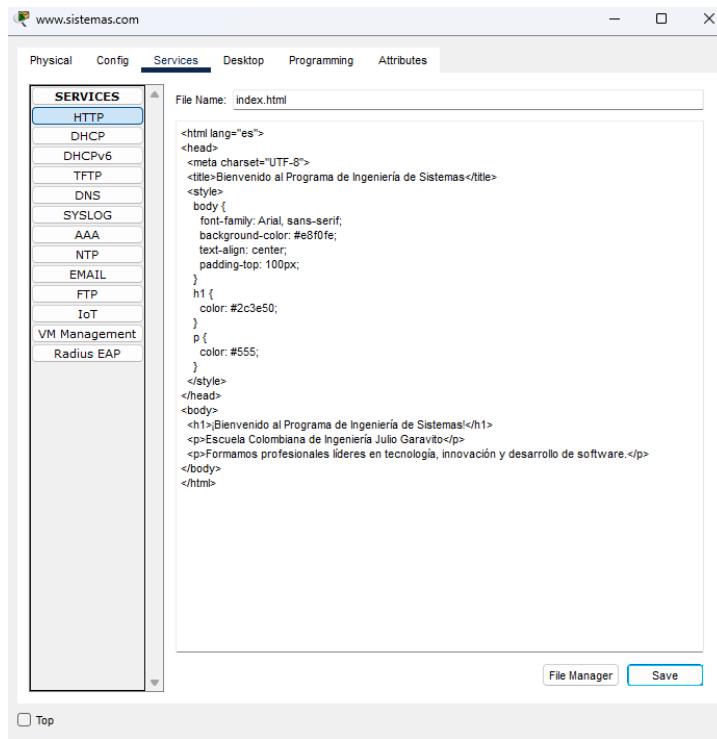
C:\>
```

Se procedió a la configuración del servicio HTTP en los servidores web asignados a los dominios www.sistemas.com y www.civil.com dentro del entorno de simulación Packet Tracer. Para ello, en cada servidor previamente configurado con su respectiva dirección IP, se accedió a la pestaña Services > HTTP, donde se activó el servicio correspondiente.

En la pestaña File System del mismo módulo, se editó el archivo index.html con el objetivo de personalizar la página principal de cada servidor. Por ejemplo, en el caso de www.sistemas.com, se incluyó un mensaje de bienvenida. Una vez realizados los cambios, se guardaron y se verificó que el servicio HTTP estuviera correctamente activo.

Figura 5

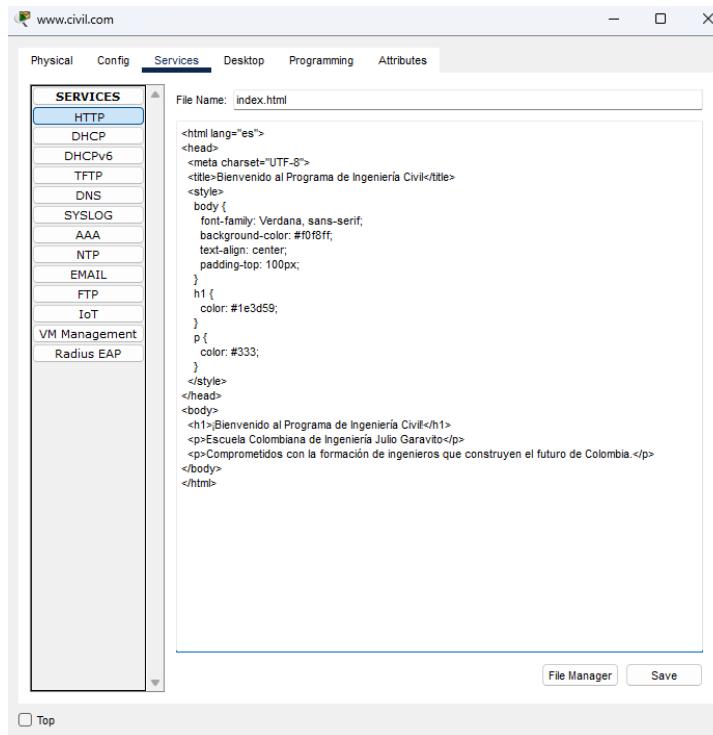
Configuración del Servicio HTTP en www.sistemas.com



Nota. Se muestra la habilitación del servicio HTTP en el servidor correspondiente a www.sistemas.com, así como la edición del archivo index.html en la pestaña File System, donde se personalizó la página principal con un mensaje de bienvenida.

Figura 6

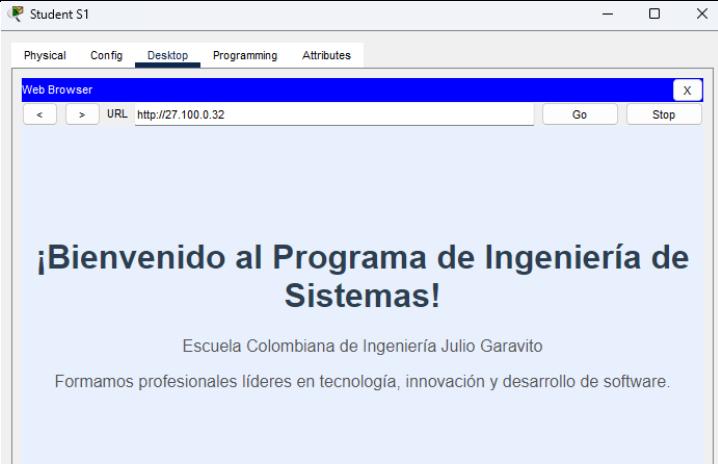
Configuración del Servicio HTTP en www.civil.com



Nota. En esta imagen se evidencia la activación del servicio HTTP en el servidor de www.civil.com, junto con la modificación del archivo index.html para mostrar contenido personalizado, simulando una página web institucional.

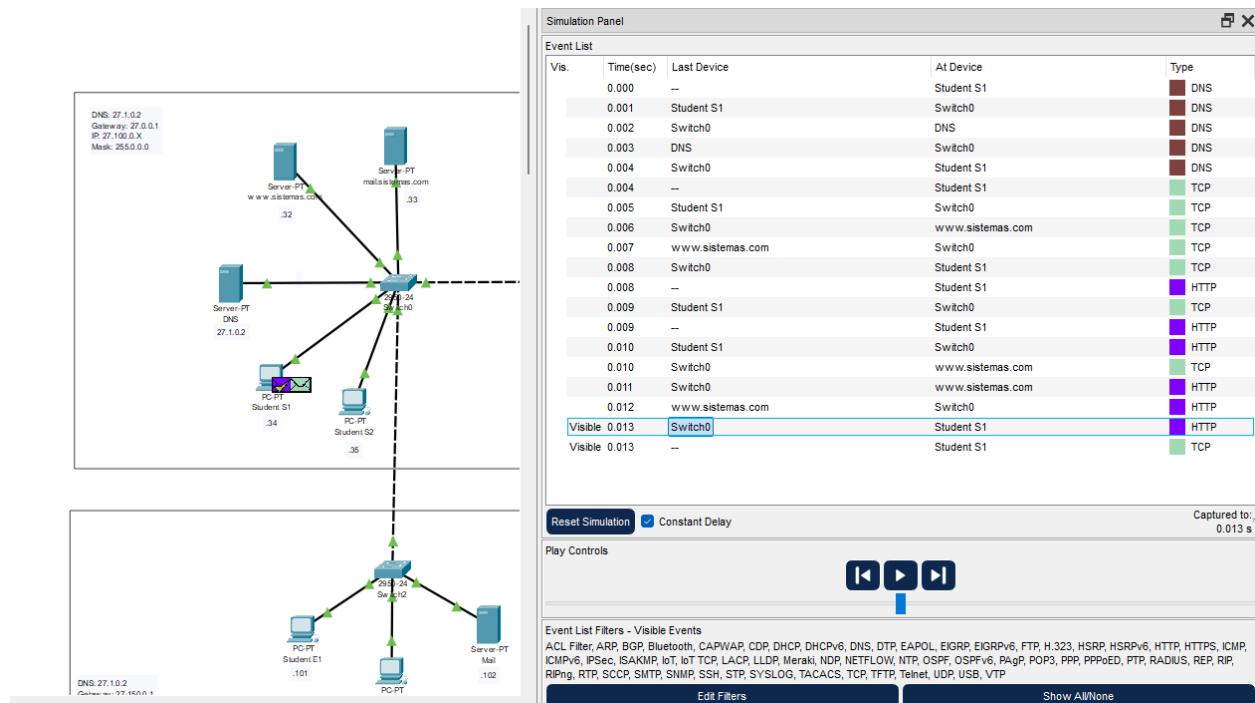
Desde una estación de trabajo (PC-PT), se utilizó el navegador web integrado en Packet Tracer para realizar pruebas de acceso a los sitios web configurados. Primero, se ingresó la dirección IP del servidor web (por ejemplo, http://27.100.0.32 para www.sistemas.com) y se verificó que el navegador cargara correctamente la página personalizada. Posteriormente, se probó el acceso usando el nombre de dominio configurado en el servidor DNS (por ejemplo, http://www.sistemas.com), confirmando que el servicio de resolución de nombres funcionaba correctamente.

Estas pruebas se repitieron con el servidor correspondiente al dominio www.civil.com, obteniendo resultados exitosos tanto por IP como por nombre de dominio.

Acción Realizada	Captura de Pantalla
<p>Acceso al Sitio Web www.sistemas.com mediante Dirección IP:</p> <p>Desde un cliente se accede al servidor web de www.sistemas.com escribiendo su dirección IP directamente en el navegador, confirmando que el servicio HTTP está activo y entregando correctamente la página personalizada.</p>	
<p>Acceso al Sitio Web www.sistemas.com mediante Nombre de Dominio:</p> <p>Se prueba el acceso al servidor web de www.sistemas.com mediante la URL configurada en el servicio DNS. El navegador resuelve el nombre correctamente y muestra la página web, validando la funcionalidad del DNS.</p>	

<p>Acceso al Sitio Web www.civil.com mediante Dirección IP:</p> <p>El navegador accede exitosamente al servidor web de www.civil.com usando su dirección IP, mostrando la página personalizada y comprobando la operatividad del servicio HTTP en dicho servidor.</p>	
<p>Acceso al Sitio Web www.civil.com mediante Nombre de Dominio:</p> <p>Se accede al sitio web de www.civil.com mediante su nombre de dominio, demostrando que la resolución DNS y el servicio HTTP funcionan correctamente al mostrar la página configurada.</p>	

Como parte de la verificación lógica, se realizó una prueba de simulación utilizando la herramienta Add Simple PDU, enviando una solicitud desde el servidor www.sistemas.com hacia el dispositivo PC-PT Student S1. La simulación generó un total de 19 eventos, lo que indica el flujo completo de la comunicación en las distintas capas del modelo OSI.

Figura 7*Simulación de Comunicación HTTP mediante PDU*

Nota. Se realiza una prueba de conectividad lógica desde el servidor www.sistemas.com hacia el dispositivo PC-PT Student S1 utilizando un PDU. La simulación registra un total de 19 eventos, indicando la secuencia completa del intercambio de datos en la red.

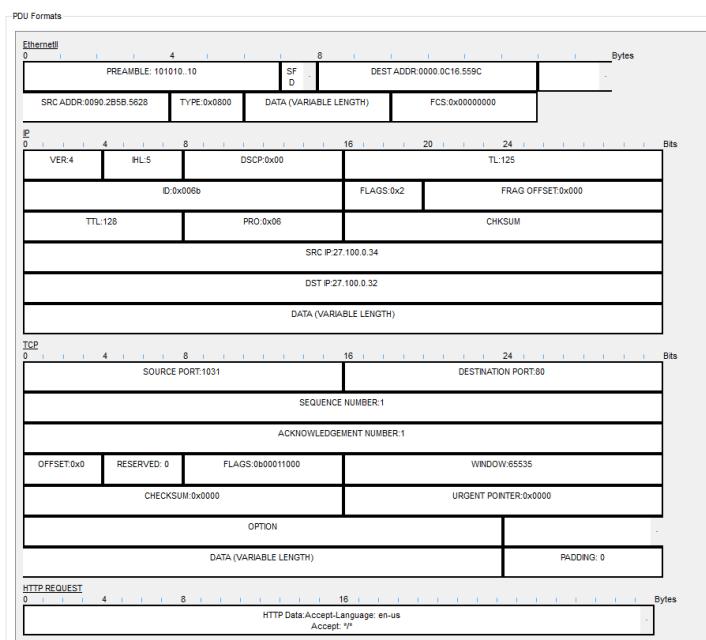
Se analizó uno de los eventos clasificados como tipo HTTP, confirmando que la comunicación se realizó en la Capa 7 (Aplicación) del modelo OSI. Al revisar el contenido del PDU, tanto en las secciones Inbound como Outbound, se identificó correctamente la estructura de la solicitud HTTP enviada desde el cliente, con campos como:

```
HTTP Data:
Accept-Language: en-US
Accept: */*
Connection: close
Host: www.sistemas.com
```

Esto evidencia que la red fue correctamente configurada no solo a nivel físico y lógico, sino también a nivel de servicios, permitiendo una comunicación completa entre cliente y servidor a través del protocolo HTTP, con soporte de resolución DNS y comportamiento conforme al modelo OSI.

Figura 8

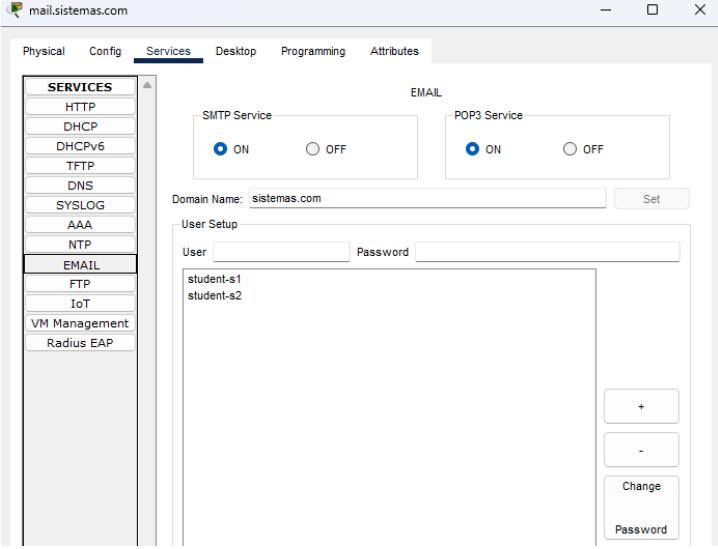
Formato de PDU HTTP: Inbound y Outbound



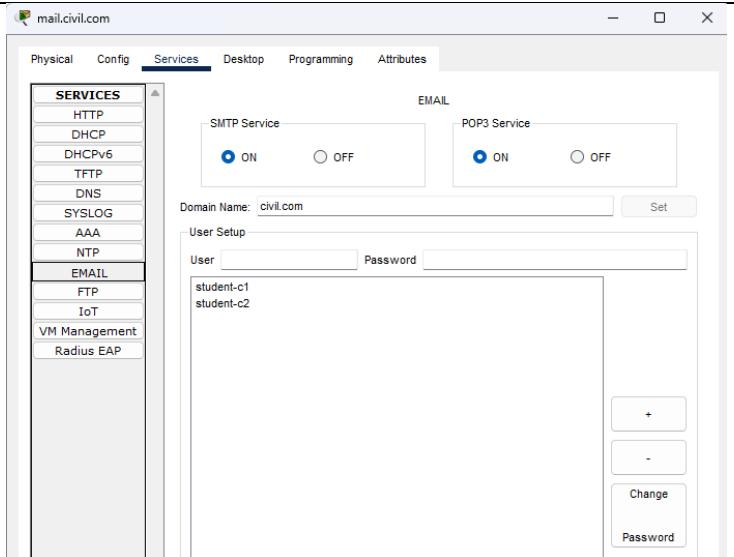
Nota. Se muestra el formato del PDU en sus secciones Inbound y Outbound, donde se detalla el contenido de la solicitud HTTP, incluyendo encabezados como Accept, Connection y Host, evidenciando el correcto funcionamiento de la comunicación web.

En esta sección, se configura el servicio de correo electrónico en el archivo de Packet Tracer. El objetivo es permitir el envío y recepción de correos entre PCs de distintas áreas (Sistemas, Civil y Eléctrica), simulando un entorno real dentro de las limitaciones del simulador.

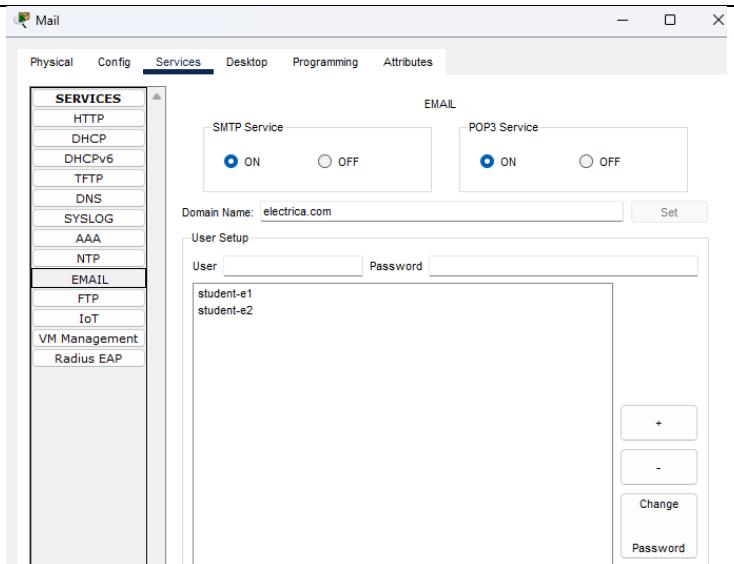
Packet Tracer no permite el reenvío de mensajes entre servidores de correo como en el mundo real. Por esta razón, la entrega de correos entre dominios se simula usando entradas DNS tipo A, no MX. Es fundamental que el nombre de dominio del destinatario coincida con el registrado en el servidor DNS, permitiendo que la PC emisora contacte directamente al servidor correcto.

Acción Realizada	Captura de Pantalla
<p>En el servidor de correo del área de sistemas se accedió a Services > Email, donde se encendieron los servicios de correo SMTP y POP3. Luego, se crearon dos cuentas de correo: student-s1@sistemas.com y student-s2@sistemas.com, utilizando los nombres de las PCs como nombre de usuario. Ambas cuentas se configuraron con la contraseña "abc123".</p>	

En el servidor de correo del área de civil se accedió a Services > Email, donde se encendieron los servicios de correo SMTP y POP3. Luego, se crearon dos cuentas de correo: student-c1@sistemas.com y student-c2@sistemas.com, utilizando los nombres de las PCs como nombre de usuario. Ambas cuentas se configuraron con la contraseña "abc123".

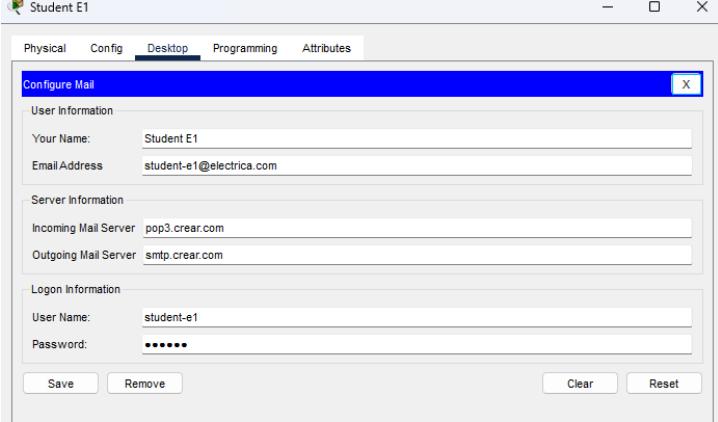
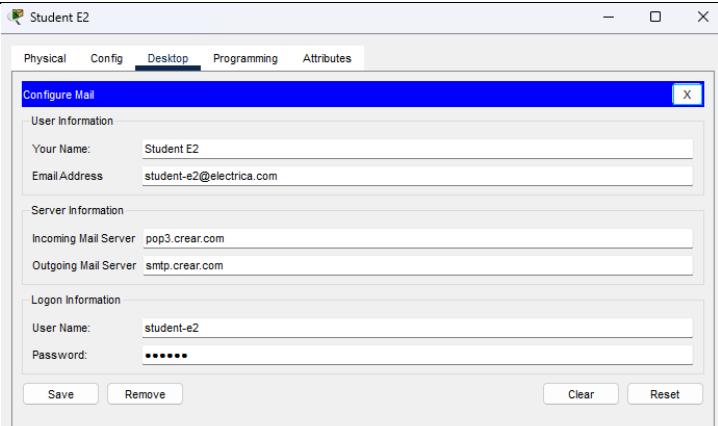


En el servidor de correo del área de electrica se accedió a Services > Email, donde se encendieron los servicios de correo SMTP y POP3. Luego, se crearon dos cuentas de correo: student-e1@sistemas.com y student-e2@sistemas.com, utilizando los nombres de las PCs como nombre de usuario. Ambas cuentas se configuraron con la contraseña "abc123".

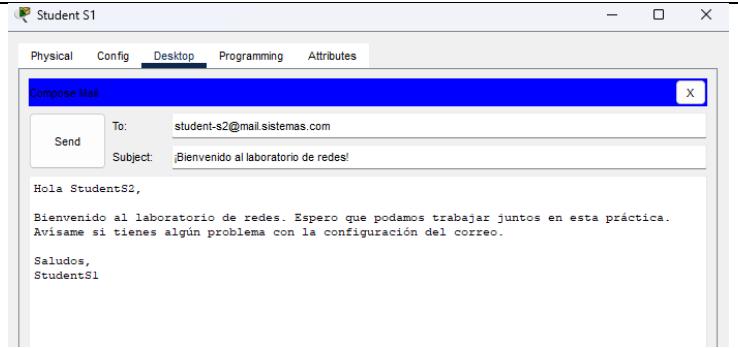


<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student S1, Email Address: student-s1@sistemas.com , Incoming Mail Server (POP3): pop3.sistemas.com, Outgoing Mail Server (SMTP): smtp.sistemas.com, Username: student-s1, y Password: abc123.</p>	
<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student S2 Email Address: student-s2@sistemas.com , Incoming Mail Server (POP3): pop3.sistemas.com, Outgoing Mail Server (SMTP): smtp.sistemas.com, Username: student-s2, y Password: abc123.</p>	

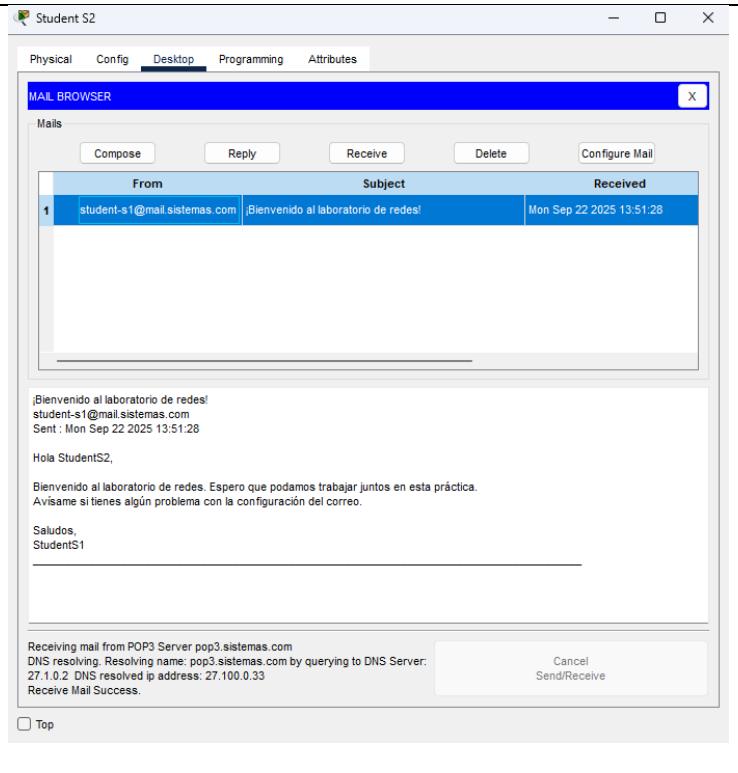
<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student C1, Email Address: student-c1@civil.com , Incoming Mail Server (POP3): pop3.civil.com, Outgoing Mail Server (SMTP): smtp.civil.com, Username: student-c1, y Password: abc123.</p>	
<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student C2, Email Address: student-c2@civil.com , Incoming Mail Server (POP3): pop3.civil.com, Outgoing Mail Server (SMTP): smtp.civil.com, Username: student-c2, y Password: abc123.</p>	

<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student E1, Email Address: student-e1@electrica.com , Incoming Mail Server (POP3): pop3.crear.com, Outgoing Mail Server (SMTP): smtp.crear.com, Username: student-e1, y Password: abc123.</p>	
<p>En el cliente PC se accedió a Desktop > Email y se configuró la cuenta de correo correspondiente.</p> <p>Se ingresaron los siguientes datos:</p> <p>Display Name: Student E2, Email Address: student-e2@electrica.com , Incoming Mail Server (POP3): pop3.crear.com, Outgoing Mail Server (SMTP): smtp.crear.com, Username: student-e2, y Password: abc123.</p>	

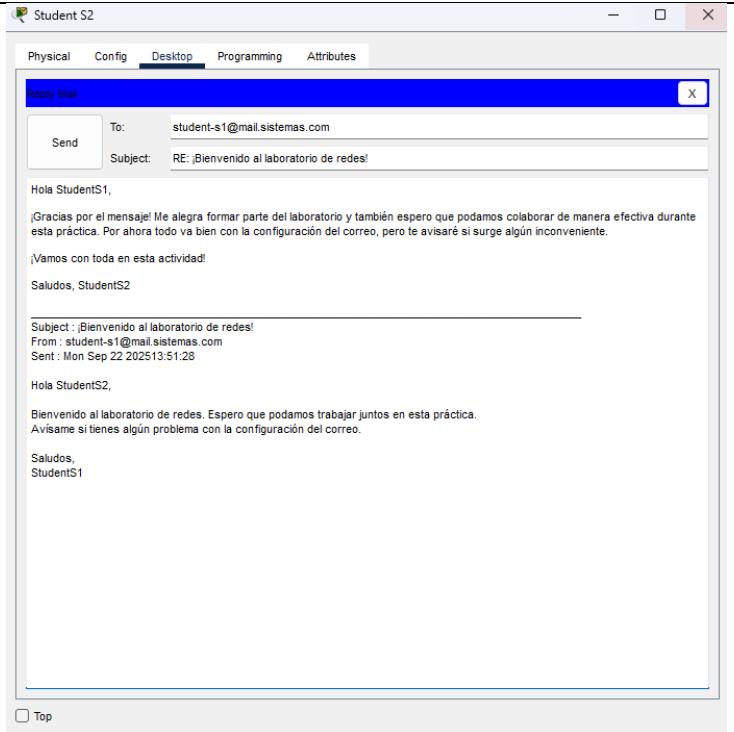
Desde la PC Student S1, se abrió el cliente de correo electrónico y se redactó un mensaje dirigido a student-s2@sistemas.com, perteneciente a la misma red local.



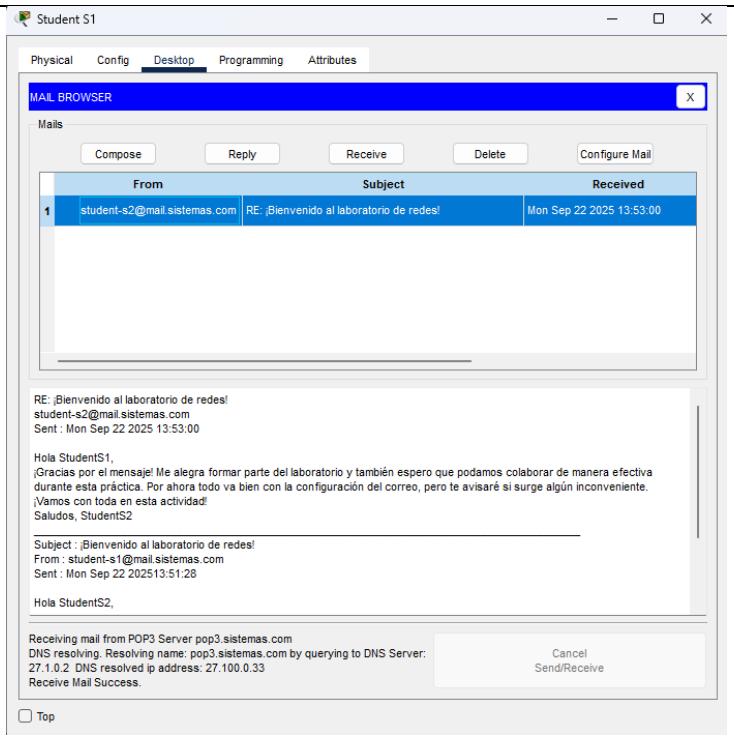
En la PC Student S2, se abrió el cliente de correo y se verificó la recepción del mensaje enviado por Student S1.



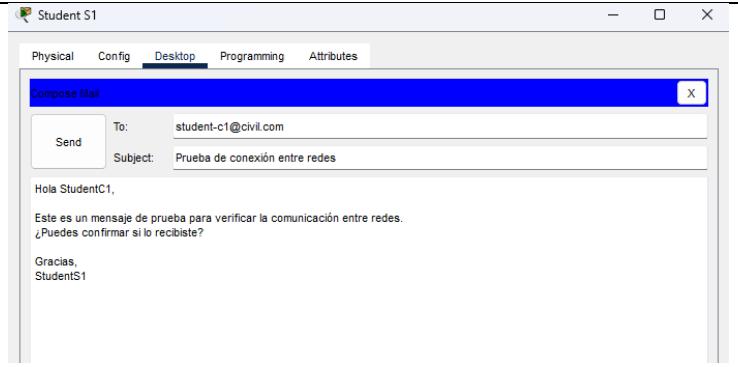
Luego, desde la PC Student S2, se redactó y envió una respuesta al correo original de Student S1.



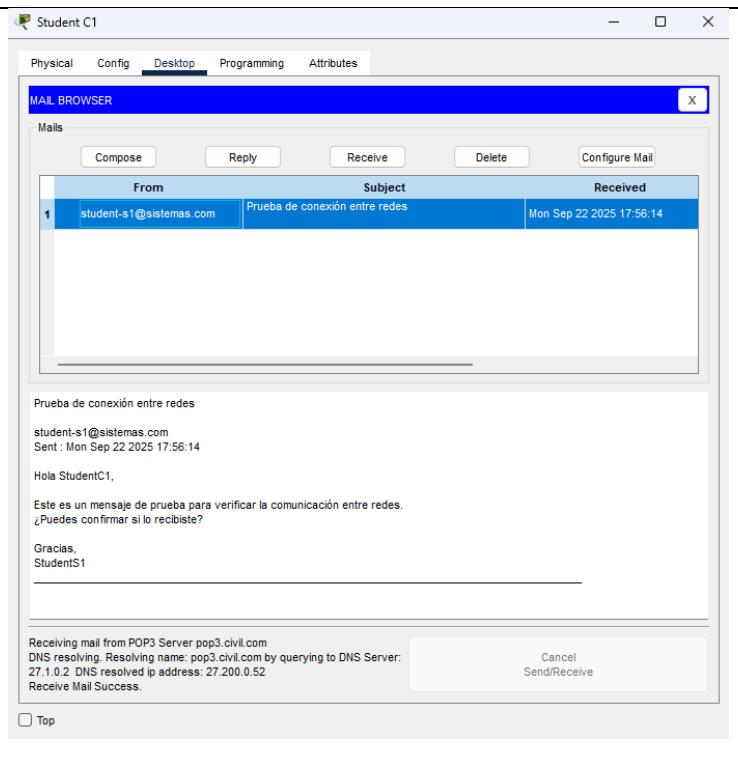
Finalmente, en la PC Student S1, se verificó que el mensaje de respuesta fue recibido correctamente, confirmando el correcto funcionamiento del servicio de correo en ambos sentidos.



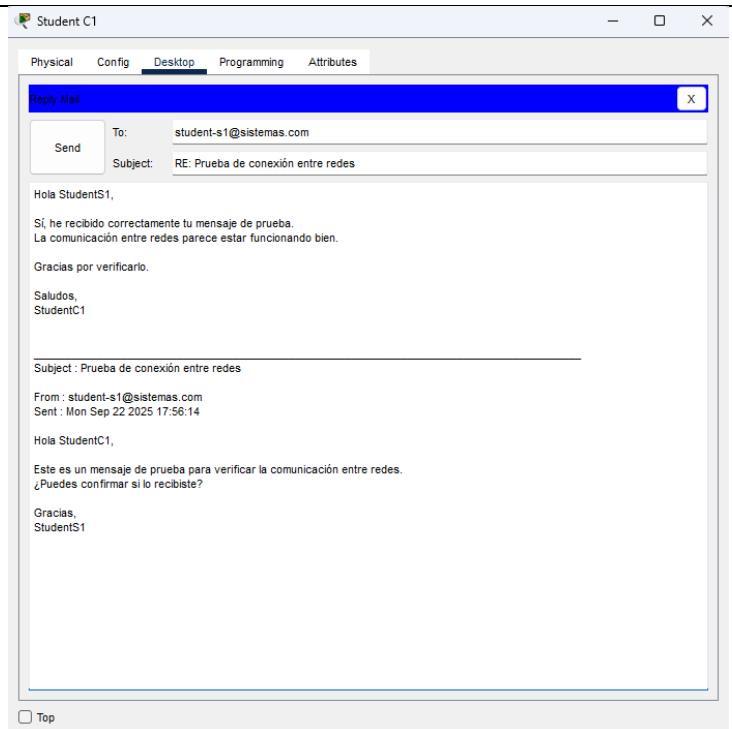
Desde la PC Student S1, perteneciente a la red del área de Sistemas, se abrió el cliente de correo electrónico y se redactó un mensaje dirigido a student-c1@civil.com , un usuario alojado en el servidor de correo de la red de Civil.



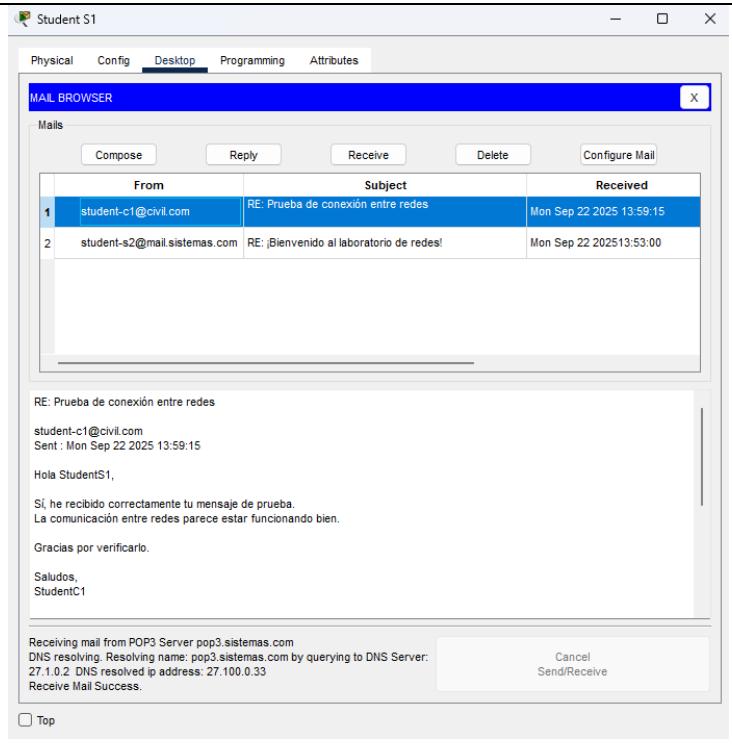
En la PC Student C1, de la red de Civil, se comprobó que el mensaje fue recibido correctamente, demostrando que la entrega directa entre redes es posible cuando se configura adecuadamente el dominio y el DNS.



Luego, desde Student C1, se respondió al mensaje dirigido a student-s1@civil.com, utilizando como servidor saliente el SMTP correspondiente y asegurándose de que el dominio coincida con el servidor DNS de destino.



Finalmente, se verificó que la respuesta fue recibida correctamente en Student S1, completando la comunicación entre dos redes distintas. Esto valida que, aunque Packet Tracer no permite reenvío real entre servidores, es posible simular correctamente la entrega interdominios si se respetan las restricciones del simulador.

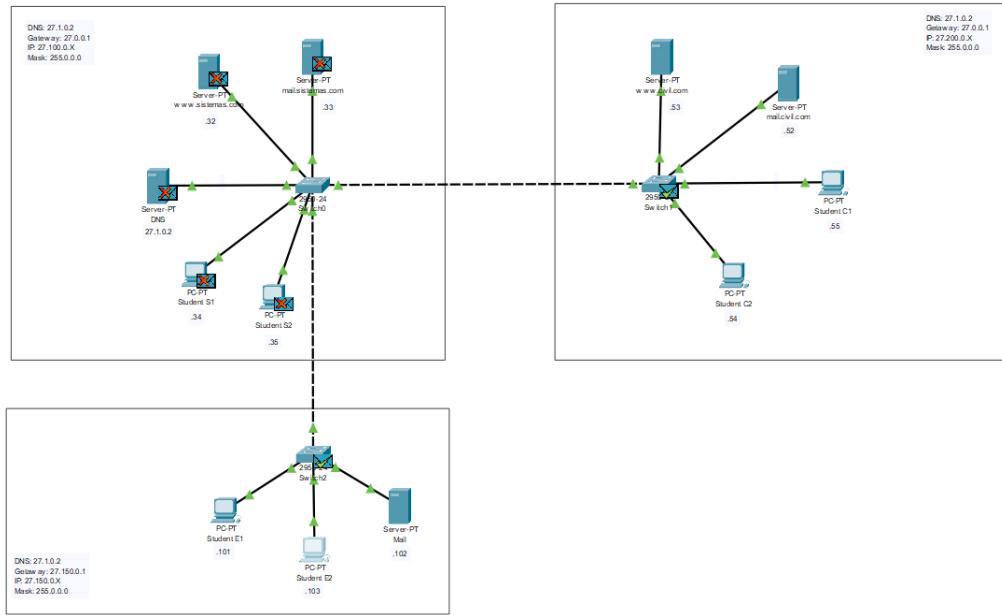


Aunque el modo Simulation de Packet Tracer permite observar el recorrido de los paquetes a través de la red, es importante aclarar que no representa todos los procesos reales que ocurren en una red durante una sesión de correo electrónico. En particular, el envío de correos involucra múltiples capas del modelo OSI, intercambio de mensajes entre servidores (SMTP, POP3), resolución DNS, y gestión de sesiones TCP, muchos de los cuales no se muestran con fidelidad en esta herramienta.

Por ello, en esta sección solo se presentan dos screenshots clave que evidencian el recorrido básico del paquete, destacando que la simulación es limitada y más conceptual que técnica.

Figura 9

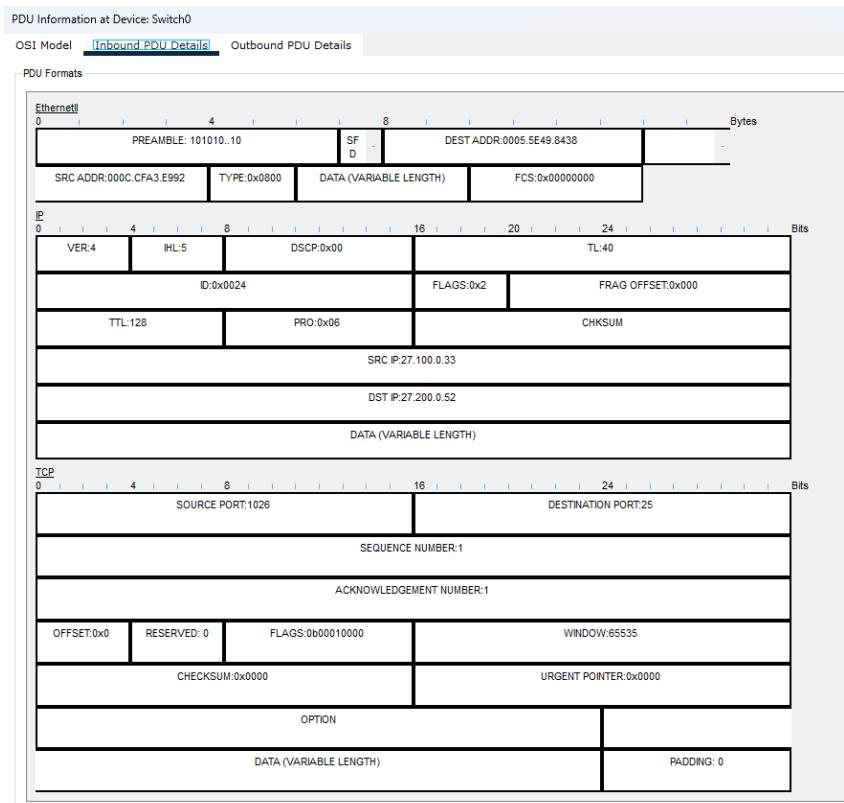
Paquete exitosamente entregado al switch de la red Eléctrica



Nota. Este paquete representa un mensaje de correo electrónico saliente, encapsulado y dirigido correctamente al destino correspondiente.

Figura 10

Detalles de la PDU entrante – Formato TCP/IP

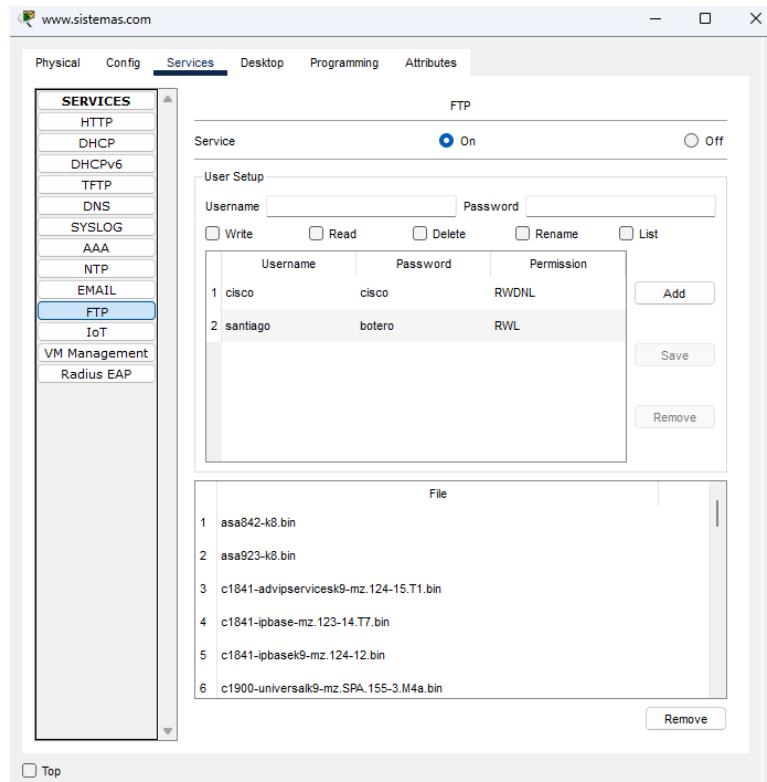


Nota. Esta vista técnica del paquete permite confirmar que la información viaja encapsulada de acuerdo con los protocolos TCP/IP y que el proceso de envío de correo fue iniciado correctamente, aunque la herramienta no visualice el intercambio completo de mensajes entre cliente y servidor.

Se realizó la configuración del servicio FTP en el servidor web www.sistemas.com, perteneciente a la red de Sistemas. Para ello, se habilitó la opción correspondiente en la pestaña Services > FTP y se creó un usuario denominado "santiago" con la contraseña "botero". A este usuario se le asignaron los permisos Read, Write y List (RWL), con el objetivo de permitirle descargar archivos, cargar nuevos contenidos y visualizar el listado de archivos disponibles en el servidor FTP desde una estación cliente.

Figura 11

Creación de usuario FTP en el servidor web www.sistemas.com



Nota. Se activó el servicio FTP y se creó el usuario santiago con permisos RWL (Read, Write, List).

Desde una estación cliente, se accedió al símbolo del sistema (Command Prompt) para establecer una conexión con el servidor FTP www.sistemas.com mediante el comando `ftp www.sistemas.com`. Tras ingresar las credenciales del usuario "santiago" con la contraseña "botero", se ejecutó el comando `dir` para visualizar los archivos disponibles en el servidor, identificando el archivo `asa842-k8.bin` como apto para descarga. A continuación, se utilizó el comando `get asa842-k8.bin` para transferir el archivo al equipo local. El procedimiento concluyó exitosamente y se verificó la presencia del archivo en el sistema de archivos de la PC cliente.

Figura 12

Comandos utilizados para conectarse al servidor FTP y descargar archivo

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp www.sistemas.com
Trying to connect...www.sistemas.com
Connected to www.sistemas.com
220- Welcome to FT Ftp server
Username:santiago
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from www.sistemas.com:
0 : asa842-k8.bin                               5571584
1 : asa923-k8.bin                               30468096
2 : c1841-advpiservicesk9-mz.124-15.T1.bin   33591768
3 : c1841-ipbasek9-mz.123-14.T7.bin          13832032
4 : c1841-ipbasek9-mz.124-12.bin              16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin    33591768
6 : c2600-advpiservicesk9-mz.124-15.T1.bin   33591768
7 : c2600-i-mz.122-28.bin                      5571584
8 : c2600-ipbasek9-mz.124-8.bin                13169700
9 : c2800nm-advpiservicesk9-mz.124-15.T1.bin  50938004
10 : c2800nm-advpiservicesk9-mz.151-4.M4.bin   33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin          5571584
12 : c2800nm-ipbasek9-mz.124-8.bin            15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin    33591768
14 : c2950-16q412-mz.121-22.EA4.bin           3058048
15 : c2950-16q412-mz.121-22.EA8.bin           3117390
16 : c2960-lanbase-mz.122-25.FX.bin           4414921
17 : c2960-lanbase-mz.122-25.SEEL.bin         4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin         4670455
19 : c3560-advpiservicesk9-mz.122-37.SE1.bin  8662192
20 : c3560-advpiservicesk9-mz.122-46.SE.bin   10713275
21 : c800-universalk9-mz.SPA.152-4.M4.bin     33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin    83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin   505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG      159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG      184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968069
27 : ir800-universalk9-mz.SPA.155-3.M        61750062
28 : ir800-universalk9-mz.SPA.156-3.M        63753767
29 : ir800_yocto-1.7.2.tar                   2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar     6912000
31 : pt1000-i-mz.122-28.bin                  5571584
32 : pt3000-16q412-mz.121-22.EA4.bin         3117390
ftp>get asa842-k8.bin

Reading file asa842-k8.bin from www.sistemas.com:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 12.358 secs (103302 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

12/31/1969  19:0 PM           5571584  asa842-k8.bin
12/31/1969  19:0 PM               26  sampleFile.txt
                           5571610 bytes      2 File(s)

C:\>
```

Nota. Se observa la secuencia de comandos ftp, dir, y get, junto con los mensajes de conexión y transferencia exitosa del archivo asa842-k8.bin.

En una tercera prueba realizada desde la misma estación cliente, se procedió a cargar el archivo de texto denominado sampleFile.txt al servidor FTP. Tras iniciar sesión con el usuario "santiago", se ejecutó el comando put sampleFile.txt, lo que permitió transferir el archivo al

servidor de manera exitosa. El cliente mostró una confirmación de la operación, verificando que el archivo fue subido correctamente.

Figura 13

Comando para subir un archivo .txt al servidor FTP

```
Cisco Packet Tracer PC Command Line 1.0
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

12/31/1969  19:0 PM           5571584  asa842-k8.bin
12/31/1969  19:0 PM                26  sampleFile.txt
                           5571610 bytes      2 File(s)

C:\>ftp www.sistemas.com
Trying to connect...www.sistemas.com
Connected to www.sistemas.com
220- Welcome to PT Ftp server
Username:santiago
331- Username ok, need password
Password:
230- Logged in
( passive mode On)
ftp>put sampleFile.txt

Writing file sampleFile.txt to www.sistemas.com:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.017 secs (1529 bytes/sec)
ftp>dir

Listing /ftp directory from www.sistemas.com:
0 : asa842-k8.bin                               5571584
1 : asa923-k8.bin                               30468096
2 : c1841-adviservicesk9-mz.124-15.T1.bin    33591768
3 : c1841-ipbasek9-mz.123-14.T7.bin          13832032
4 : c1841-ipbasek9-mz.124-12.bin              16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin   33591768
6 : c2600-adviservicesk9-mz.124-15.T1.bin    33591768
7 : c2600-i-mz.122-28.bin                      5571584
8 : c2600-ipbasek9-mz.124-8.bin               13169700
9 : c2800nm-adviservicesk9-mz.124-15.T1.bin   50938004
10 : c2800nm-adviservicesk9-mz.151-4.M4.bin   33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin          5571584
12 : c2800nm-ipbasek9-mz.124-8.bin            15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin   33591768
14 : c2950-16q12-mz.121-22.EA4.bin            3058048
15 : c2950-16q12-mz.121-22.EA8.bin            3117390
16 : c2960-lanbase-mz.122-25.FX.bin          4414921
17 : c2960-lanbase-mz.122-25.SE1.bin         4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin        4670455
19 : c3560-adviservicesk9-mz.122-37.SE1.bin   8662192
20 : c3560-adviservicesk9-mz.122-46.SE.bin    10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin    33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin   83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin  505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG     159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG     184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M         61750062
28 : ir800-universalk9-mz.SPA.156-3.M         63753767
29 : ir800_yocto-1.7.2.tar                   2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar       6912000
31 : pt1000-i-mz.122-28.bin                  5571584
32 : pt3000-1eq4l2-mz.121-22.EA4.bin        3117390
33 : sampleFile.txt                           26

ftp>
```

Nota. Se muestra el uso del comando put sampleFile.txt para subir el archivo desde la estación cliente al servidor remoto.

En la cuarta prueba, se activó el modo de simulación (Simulation Mode) con el propósito de monitorear el tráfico generado durante la transferencia FTP. Se capturó un paquete de salida (Outbound PDU) y se procedió a analizar la información correspondiente a la capa de aplicación

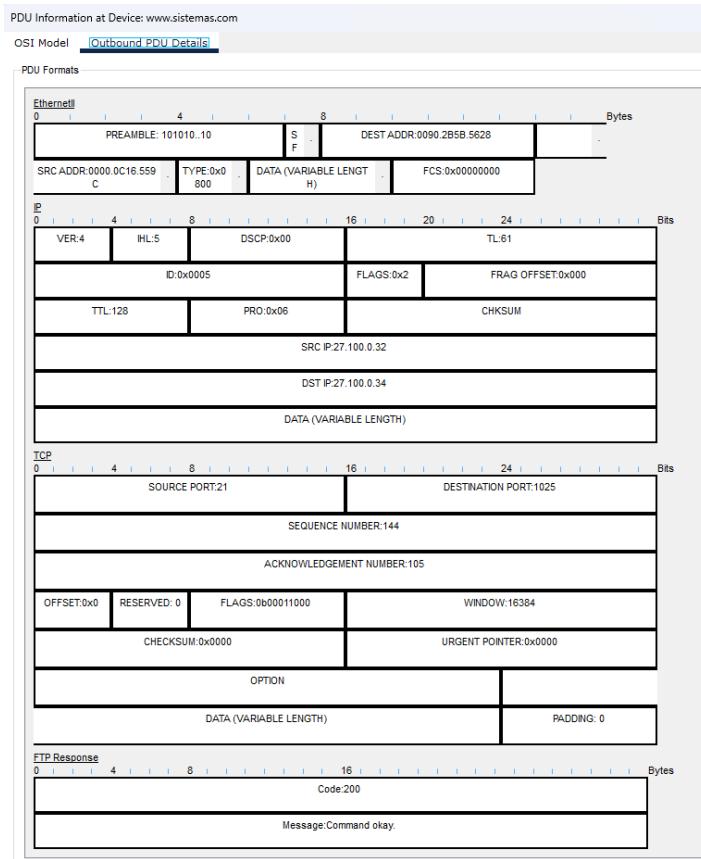
(Layer 7) del modelo OSI. En dicho paquete, se identificó una respuesta emitida por el servidor FTP, la cual reflejaba el estado de la comunicación y confirmaba la interacción entre el cliente y el servidor en el contexto de la transferencia de archivos.

Code: 200
Message: Command Okay.

Esto indica que el comando fue recibido, interpretado y aceptado por el servidor, validando el correcto funcionamiento del proceso de transferencia.

Figura 14

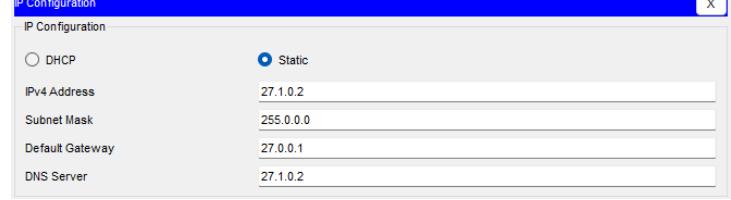
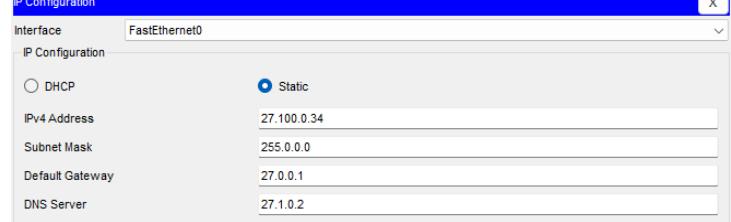
Outbound PDU Details con encabezado de aplicación (Layer 7)



Nota. Se observa la respuesta 200 Command Okay del servidor FTP en el encabezado de la capa de aplicación, confirmando que la orden fue aceptada correctamente.

Caso Natalia: Desarrollo de Red en Packet Tracer

Se realizará la implementación de los servicios DNS, HTTP, FTP y correo electrónico en los servidores correspondientes. Además, documentaré todo el proceso, desde la configuración inicial hasta las pruebas de conectividad y funcionamiento de los servicios, asegurando que cada protocolo de la capa de aplicación esté correctamente implementado y operativo.

Actividad/Acción/Tarea	Detalles Relevantes
Se configuró manualmente una IP estática en Cisco Packet Tracer: 27.1.0.2 con una máscara 255.0.0.0, puerta de enlace 27.0.0.1 y DNS 27.1.0.2. Esto permite al dispositivo comunicarse en la red, acceder a otras redes y resolver nombres de dominio, útil para probar servicios como HTTP y FTP.	
En la imagen, se muestra la configuración de una estación cliente en Cisco Packet Tracer con IP estática 27.100.0.34, máscara 255.0.0.0 y puerta de enlace 27.0.0.1. Se configuró también el servidor DNS 27.1.0.2 para resolver dominios como mail.sistemas.com y www.sistemas.com.	

Se configuró el servicio DNS en el servidor 27.1.0.2, agregando registros "A" para dominios como mail.sistemas.com y www.sistemas.com. Esto permite que los clientes resuelvan nombres de dominio de manera más práctica que usando direcciones IP.

No.	Name	Type	Detail
0	civil.com	CNAME	27.200.0.52
1	electrica.com	CNAME	27.150.0.102
2	http.civil.com	CNAME	27.200.0.53
3	http.sistemas.com	CNAME	27.100.0.32
4	mail.civil.com	A Record	27.200.0.52
5	mail.sistemas.com	A Record	27.100.0.33
6	pop3.civil.com	CNAME	civil.com
7	pop3.crear.com	CNAME	electrica.com
8	pop3.sistemas.com	CNAME	sistemas.com
9	sistemas.com	CNAME	27.100.0.33
10	smtp.civil.com	CNAME	civil.com

Tras configurar el DNS, se verificó su funcionamiento desde una estación cliente, utilizando el comando ping. El dominio www.sistemas.com se resolvió correctamente a 27.100.0.32, lo que confirma que el DNS está funcionando bien.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.sistemas.com

Pinging 27.100.0.32 with 32 bytes of data:
Reply from 27.100.0.32: bytes=32 time<lms TTL=128

Ping statistics for 27.100.0.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping http.sistemas.com

Pinging 27.100.0.32 with 32 bytes of data:
Reply from 27.100.0.32: bytes=32 time=lms TTL=128
Reply from 27.100.0.32: bytes=32 time<lms TTL=128
Reply from 27.100.0.32: bytes=32 time<lms TTL=128
Reply from 27.100.0.32: bytes=32 time<lms TTL=128

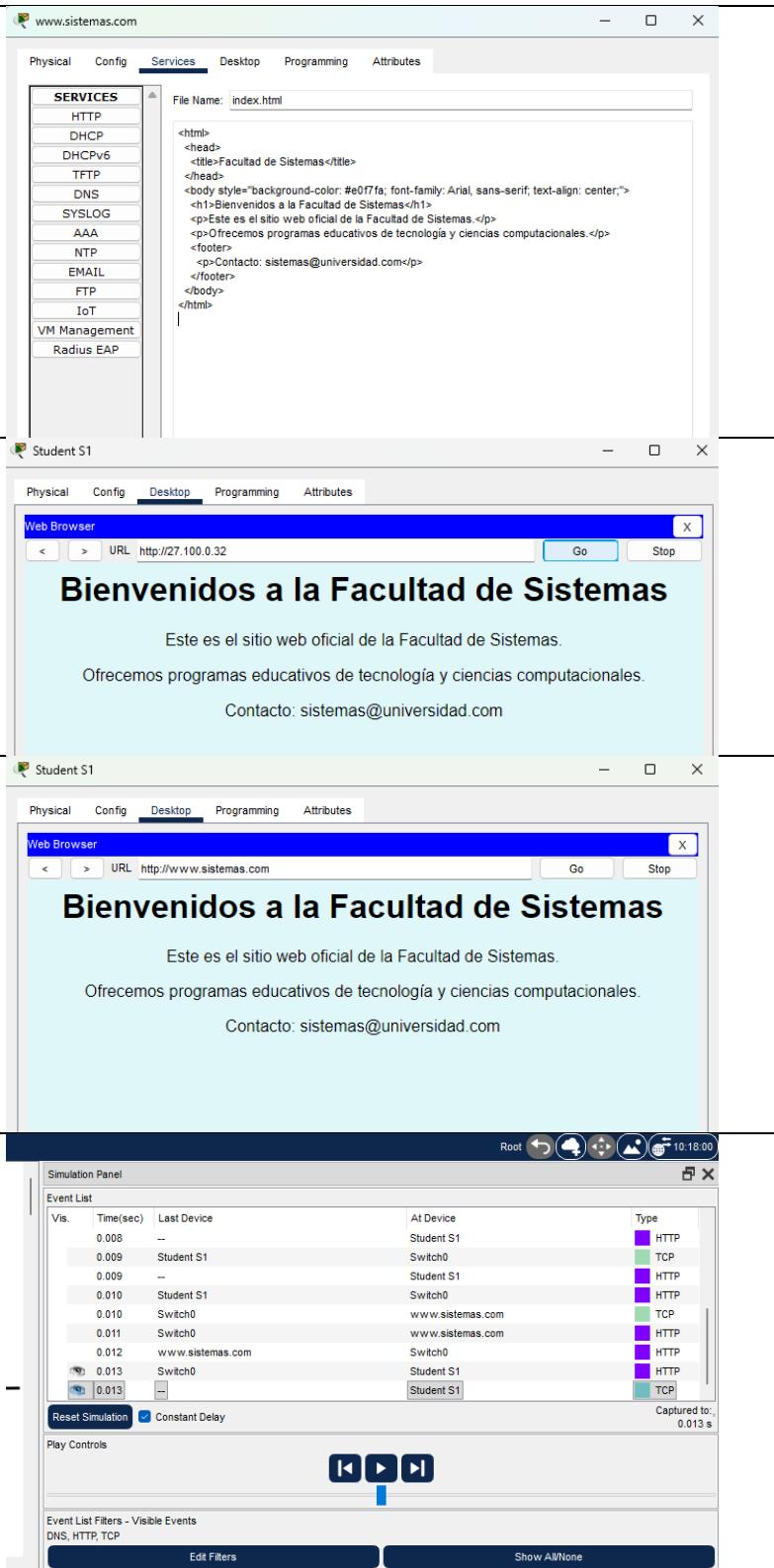
Ping statistics for 27.100.0.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms
```

Se configuró el servicio HTTP en el servidor web de la Facultad de Sistemas, activando el servicio en Cisco Packet Tracer y personalizando la página index.html con información sobre programas educativos y contacto.

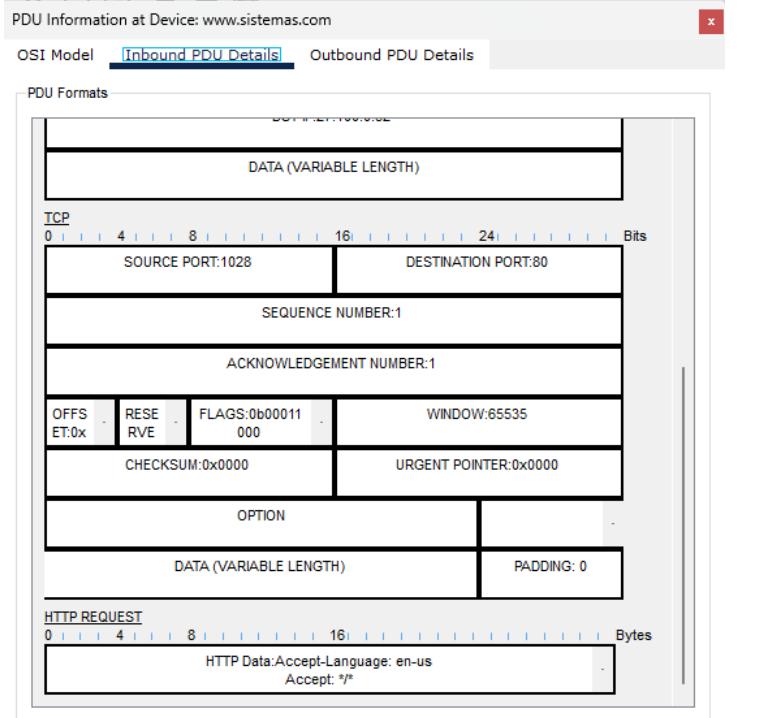
Se verificó el servicio HTTP accediendo a la página del servidor web desde un cliente. El contenido configurado en index.html se mostró correctamente, confirmando que el servicio web está funcionando.

Se probó el servicio HTTP usando el nombre de dominio www.sistemas.com en lugar de la IP. La página se cargó correctamente, lo que confirma que el DNS y el HTTP funcionan juntos.

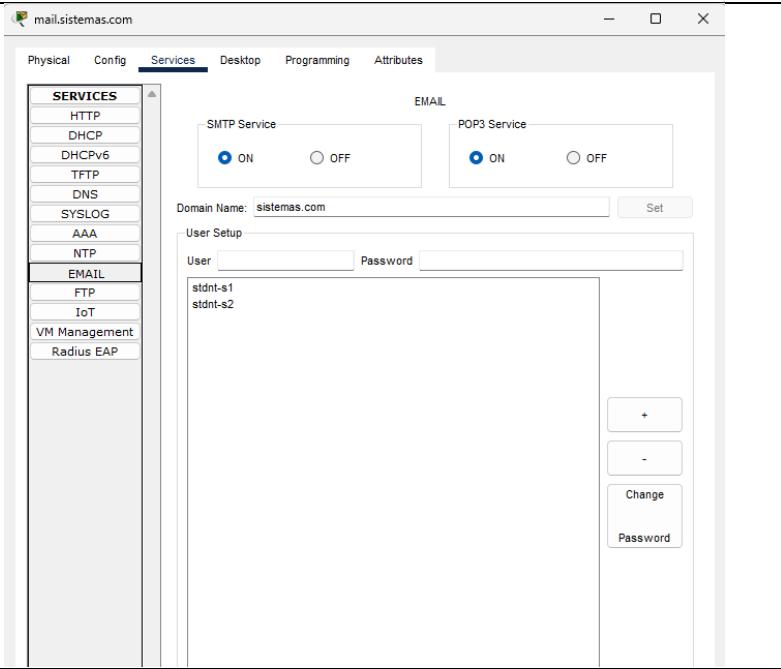
En modo simulación de Cisco Packet Tracer, se observó la solicitud HTTP desde un cliente, pasando por el switch y router. Se registraron los eventos y protocolos como HTTP y TCP, ayudando a entender el flujo de comunicación.



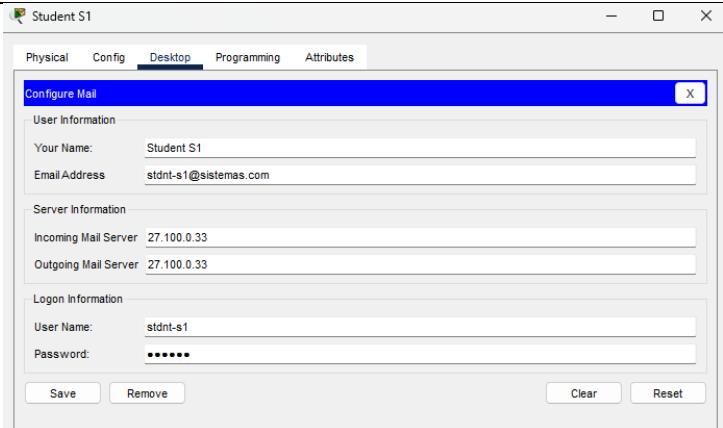
Se detalló el segmento TCP de una solicitud HTTP, mostrando puertos de origen y destino, así como los encabezados HTTP que indican preferencias del cliente como idioma y tipo de contenido.



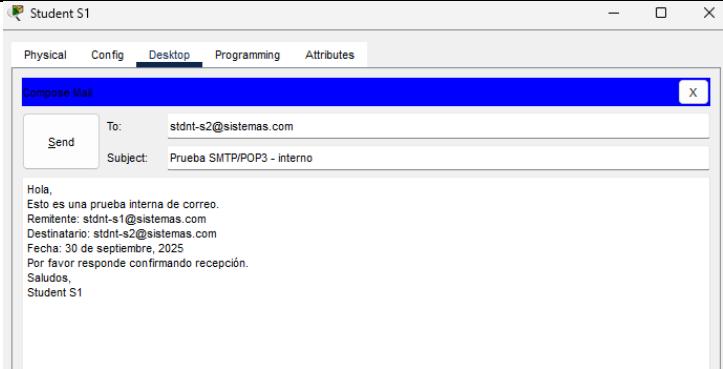
Se configuró el servicio de correo electrónico en el servidor de la Facultad de Sistemas, activando SMTP y POP3 para envío y recepción de correos. Se crearon cuentas de correo para los usuarios, permitiendo la comunicación dentro del dominio sistemas.com.



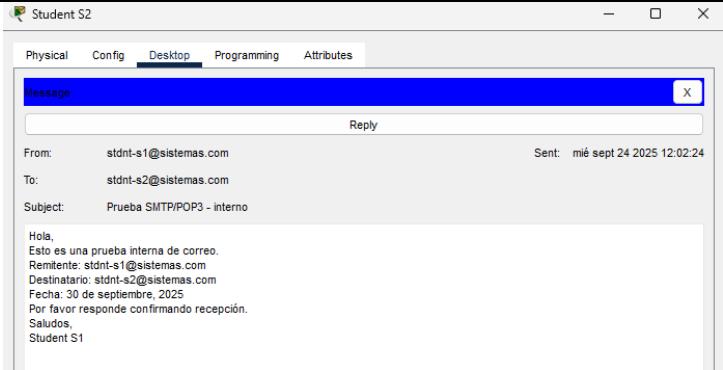
En la estación cliente Student S1, se configuró el cliente de correo con dirección stdnt-s1@sistemas.com, servidor SMTP/POP3 en 27.100.0.33 y las credenciales correspondientes, permitiendo enviar y recibir mensajes.



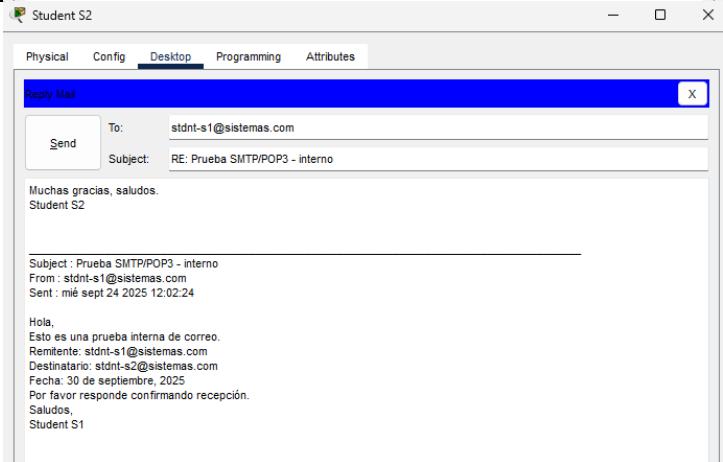
Se realizó una prueba de correo electrónico entre Student S1 y S2 dentro del dominio sistemas.com. El mensaje se envió y recibió correctamente, validando el funcionamiento de SMTP y POP3 dentro del dominio.



Se verificó la recepción del correo en Student S2, confirmando que POP3 está funcionando adecuadamente y que el correo fue recibido sin problemas.



Student S2 respondió al correo enviado por Student S1, confirmando que el servicio de correo electrónico está funcionando correctamente en ambas direcciones dentro del dominio sistemas.com.



Se verificó la recepción del mensaje de respuesta en Student S1, confirmando que la comunicación bidireccional por correo electrónico está funcionando dentro del dominio sistemas.com.

The image displays three windows from the 'Student' software, illustrating the bidirectional email communication between two students, S1 and C1, across different domains.

Student S1 (Top Window):

- MAIL BROWSER:** Shows an incoming message from 'stdnt-s2@sistemas.com' with subject 'RE: Prueba SMTP/POP3 - interno'. The message was received on 'jue sept 25 2025 12:17:54'.
- Message Content:**

```
Subject : Prueba SMTP/POP3 - interno
From : stdnt-s1@sistemas.com
Sent : mié sept 24 2025 12:02:24

Hola,
Esto es una prueba interna de correo.
Remitente: stdnt-s1@sistemas.com
Destinatario: stdnt-s2@sistemas.com
Fecha: 30 de septiembre, 2025
Por favor responde confirmando recepción.
Saludos,
Student S1
```
- Status Bar:** Shows 'Receiving mail from POP3 Server 27.100.0.33' and 'Receive Mail Success.'
- Buttons:** Includes 'Compose', 'Reply', 'Receive', 'Delete', and 'Configure Mail'.

Student C1 (Middle Window):

- Message:** Shows an outgoing message to 'stdnt-c1@civil.com' with subject 'Prueba interdominio: sistemas → civil'.
- Message Content:**

```
From: stdnt-s1@sistemas.com
To: stdnt-c1@civil.com
Subject: Prueba interdominio: sistemas → civil

Hola,
Envío este mensaje para verificar envío entre dominios.
Remitente: stdnt-s1@sistemas.com
Destinatario: stdnt-c1@civil.com
Por favor confirma y responde.
```

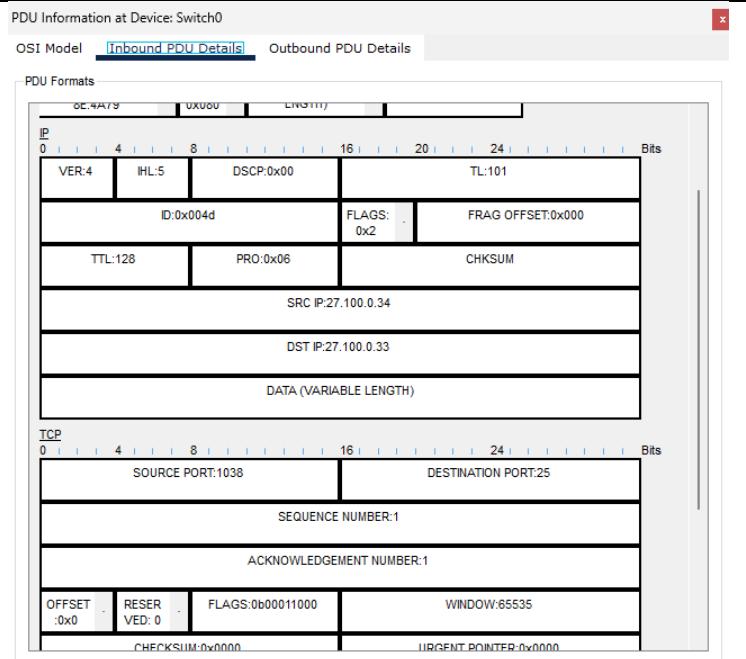
Student S1 (Bottom Window):

- Message:** Shows a response message from 'stdnt-c1@civil.com' with subject 'RE: Prueba interdominio: sistemas → civil'.
- Message Content:**

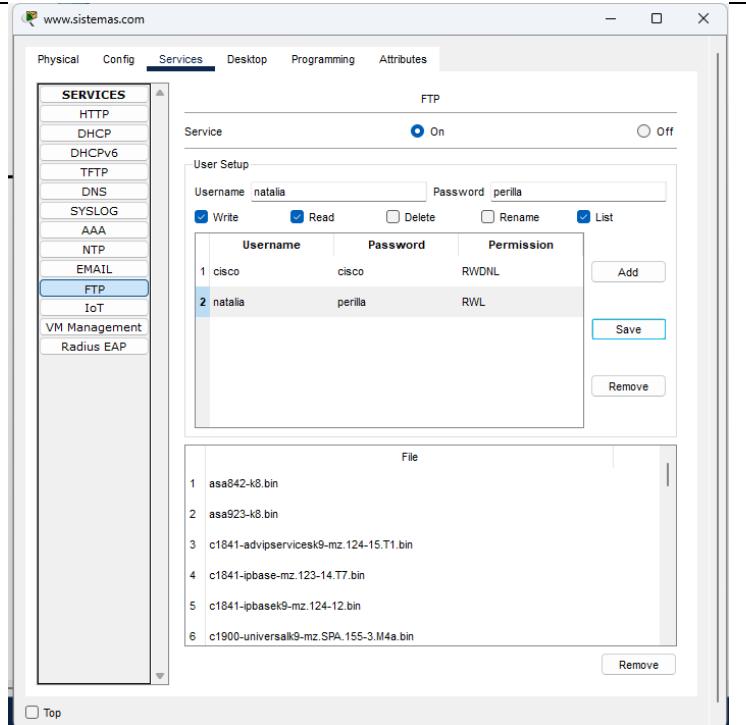
```
From: stdnt-c1@civil.com
To: stdnt-s1@sistemas.com
Subject: RE: Prueba interdominio: sistemas → civil

Muchas gracias, saludos.
Student C1.
```
- Message Footer:** Shows the original message content sent by Student C1.

Usando la simulación de Cisco Packet Tracer, se analizó el PDU durante el envío de correo electrónico. Se observó el paquete con las capas IP y TCP, verificando que los datos se transmiten correctamente al servidor SMTP.



En la imagen se muestra la configuración FTP en el servidor web de sistemas.com, con un usuario creado para permitir acceso remoto y permisos para transferir archivos, lo cual habilita la transferencia de archivos entre cliente y servidor.



Un usuario accedió al servidor FTP, descargó un archivo binario (asa842-k8.bin) y verificó su presencia en el directorio local, confirmando que el servicio FTP está funcionando correctamente.

```
ftp>get asa842-k8.bin
Reading file asa842-k8.bin from www.sistemas.com:
File transfer in progress...
[Transfer complete - 5571584 bytes]
5571584 bytes copied in 12.918 secs (98824 bytes/sec)
ftp>quit
221- Service closing control connection.
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

12/31/1969  19:0 PM           5571584   asa842-k8.bin
12/31/1969  19:0 PM             26   sampleFile.txt
                           5571610 bytes   2 File(s)
C:\>|
```

Se estableció conexión FTP, subiendo un archivo (sampleFile.txt) al servidor con el comando "put". La transferencia fue exitosa, lo que confirma que el servicio FTP está correctamente configurado.

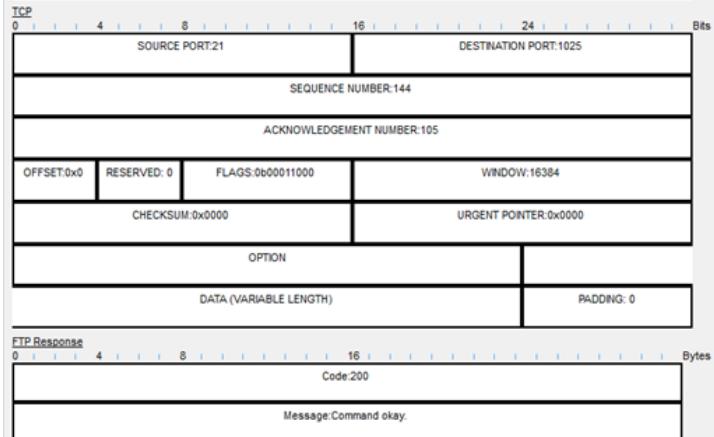
```
C:\>ftp www.sistemas.com
Trying to connect...www.sistemas.com
Connected to www.sistemas.com
220- Welcome to PT Ftp server
Username:natalia
331- Username ok, need password
Password:
230- Logged in|
(passive mode On)
ftp>put sampleFile.txt

Writing file sampleFile.txt to www.sistemas.com:
File transfer in progress...

[Transfer complete - 26 bytes]

26 bytes copied in 0.037 secs (702 bytes/sec)
```

Se analizaron los encabezados de las capas OSI en una simulación FTP, destacando el código de respuesta 200 en la capa de aplicación, que confirma que la operación FTP se completó correctamente.



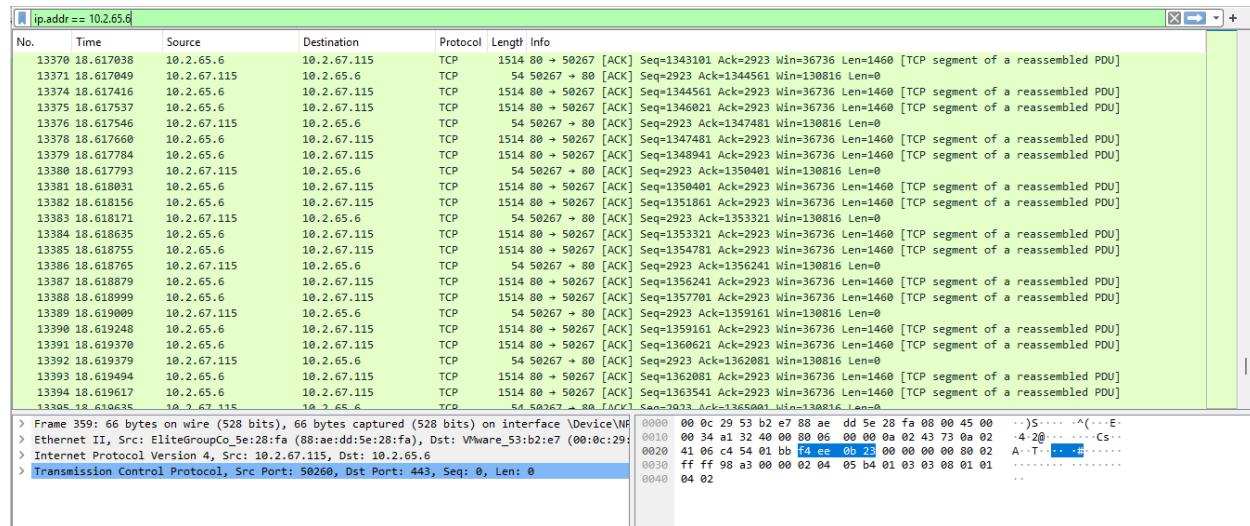
En la Red Real

Wireshark

En esta parte del laboratorio se utiliza la herramienta Wireshark para capturar y analizar el tráfico de red generado por distintos protocolos de la capa de aplicación. El objetivo principal es observar cómo se comportan los protocolos HTTP, DHCP y Telnet en una red real, y cómo se encapsulan sus mensajes en las capas superiores del modelo OSI.

Figura 15

Análisis de tráfico TCP mediante Wireshark: Consulta web y captura de protocolos de aplicación



Nota. La imagen muestra una captura de tráfico realizada con Wireshark, se observa la comunicación entre el host 10.2.65.6 y el servidor 10.2.67.115 utilizando el protocolo TCP. El puerto de destino identificado es el 443, que corresponde al servicio HTTPS, lo que indica que la consulta web al sitio del laboratorio se realizó de forma segura. El puerto de origen (50260) es dinámico y fue asignado por el cliente para establecer la conexión. La información de la capa de transporte y de aplicación confirma que el protocolo activo en la consulta web es HTTPS.

Los paquetes filtrados en la captura muestran tráfico TCP, en el que se pueden observar las interacciones entre ambos sistemas, como los segmentos TCP, secuencias de números, y la confirmación de la recepción de los datos (ACK). El uso del puerto 80 indica que el protocolo

activo en la capa de aplicación es HTTP, utilizado para la transferencia de páginas web. En la capa de transporte, se identifica el puerto 50267 como puerto dinámico del cliente, mientras que el servidor responde desde el puerto estándar 80. Esta evidencia confirma que se está realizando una comunicación web y permite analizar los encabezados y el flujo de datos entre ambos dispositivos.

Figura 16

Evidencia de liberación y renovación de dirección IP mediante comandos DHCP en Windows

```
C:\Users\Redes>ipconfig /release
Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Wi-Fi:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . .

Wireless LAN adapter Local Area Connection* 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . .

Wireless LAN adapter Local Area Connection* 10:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . .

Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::3a95:e4d3:bd21:6d1a%9
  IPv4 Address . . . . . : 192.168.132.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::49c1:6f4:822c:d0a5%23
  IPv4 Address . . . . . : 192.168.47.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter Ethernet 5:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::15da:dd74:cb33:63d2%4
  Default Gateway . . . . .

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

C:\Users\Redes>ipconfig /renew
Windows IP Configuration

No operation can be performed on Wi-Fi while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Wi-Fi:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Wireless LAN adapter Local Area Connection* 10:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::3a95:e4d3:bd21:6d1a%9
  IPv4 Address . . . . . : 192.168.132.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::49c1:6f4:822c:d0a5%23
  IPv4 Address . . . . . : 192.168.47.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . .

Ethernet adapter Ethernet 5:
  Connection-specific DNS Suffix . . . : is.escuelaing.edu.co
  Link-local IPv6 Address . . . . . : fe80::15da:dd74:cb33:63d2%4
  IPv4 Address . . . . . : 10.2.67.115
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.2.65.1
  . . . . .

Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

C:\Users\Redes>
```

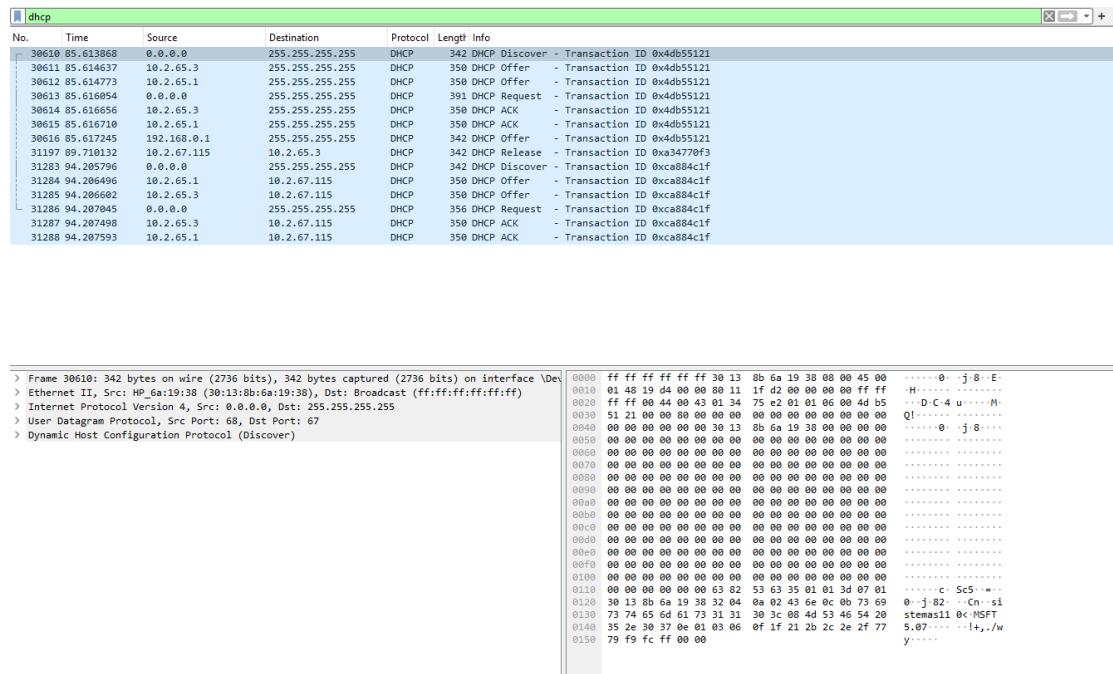
Nota. En la imagen se observa el proceso de liberación (ipconfig /release) y posterior renovación (ipconfig /renew) de la dirección IP en un sistema Windows. Inicialmente, las interfaces de red muestran estado Media disconnected o direcciones locales de VMware. Tras ejecutar el comando de renovación, la interfaz Ethernet 5 obtiene una dirección IPv4 (10.2.67.115) asignada

dinámicamente por el servidor DHCP, junto con máscara de subred (255.255.0.0) y puerta de enlace predeterminada (10.2.65.1).

Durante el proceso, los adaptadores de red con estado "Media disconnected" no pueden realizar operaciones DHCP. Sin embargo, se observa que el adaptador Ethernet adapter Ethernet 5 logra renovar su configuración, recibiendo una dirección IP (10.2.65.3), una máscara de subred (255.255.0.0) y una puerta de enlace predeterminada (10.2.65.1), además de un sufijo DNS específico (is.escuelaing.edu.co). Este proceso refleja el flujo típico de mensajes DHCP: Discover, Offer, Request y Acknowledge

Figura 17

Captura de tráfico DHCP con Wireshark durante el proceso de asignación de dirección IP



Nota. En la captura de Wireshark se visualiza el proceso de asignación de direcciones IP mediante DHCP. Se distinguen los paquetes de la secuencia DHCP Discover → Offer → Request → ACK, que representan la negociación entre el cliente y los servidores que ofrecen direcciones.

Este proceso comienza con un paquete DHCP Discover enviado por el cliente (IP 0.0.0.0) como difusión a toda la red (255.255.255.255), solicitando un servidor DHCP disponible. A

continuación, varios servidores (como 10.2.65.1 y 10.2.67.115) responden con DHCP Offer, ofreciendo direcciones IP. El cliente selecciona una oferta y responde con un DHCP Request, solicitando formalmente esa dirección. Finalmente, el servidor confirma la asignación con un DHCP ACK. También se puede ver un paquete DHCP Release, donde el cliente libera una IP previamente asignada. En la capa de aplicación, se identifican claramente estos mensajes como parte del protocolo DHCP. En la capa de transporte, se utiliza UDP, con el puerto 67 para el servidor y 68 para el cliente. Esta secuencia es fundamental para la configuración automática de red en dispositivos conectados a redes locales.

```
pkgmgr /iu:"TelnetClient"
```

Se utiliza para instalar el cliente Telnet en Windows desde la línea de comandos. Este cliente permite establecer conexiones remotas a otros equipos usando el protocolo Telnet.

Figura 18

Respuesta HTTP obtenida mediante TELNET al solicitar index.html

```
HTTP/1.1 200 OK
Date: Fri, 26 Sep 2025 03:09:15 GMT
Server: Apache/2.4.53 (Unix) PHP/8.1.4
Last-Modified: Wed, 08 Jul 2020 03:46:48 GMT
ETag: "f2-5a9e5f515ba00"
Accept-Ranges: bytes
Content-Length: 242
Connection: close
Content-Type: text/html

<html>
    <head>
        <title>Claudia Santiago</title>
    </head>
    <body>
        <h1> Espacio de prueba del Laboratorio de RECO </h
1>
        <p>Esta es un archivo de prueba para revisar el funcionamiento del protocolo HTTP y TCP</p>
    </body>
</html>
```

Nota. La imagen muestra la consola TELNET mostrando la respuesta del servidor web al comando GET /~csantiago/RECO/index.html HTTP/1.0. La respuesta incluye encabezados HTTP como el código de estado 200 OK, tipo de contenido text/html, longitud del contenido, y metadatos del servidor Apache. También se muestra el contenido HTML del archivo solicitado.

La capa de aplicación está representada por el protocolo HTTP, que responde con una versión HTTP/1.1 y un código de estado 200 OK, indicando que la solicitud fue procesada correctamente. Los encabezados HTTP proporcionan información adicional como la fecha del servidor (Date), el tipo de servidor (Apache/2.4.53 con soporte para PHP), el tipo de contenido (text/html), y la longitud del contenido (Content-Length: 242). Además, se incluye el contenido HTML del archivo solicitado, que contiene un título y un mensaje de prueba del laboratorio de RECO. Esta respuesta demuestra cómo HTTP transmite tanto metadatos como contenido estructurado en texto plano.

Figura 19

Captura de paquetes en Wireshark durante la solicitud HTTP vía TELNET

45 9.855077	192.168.0.211	45.239.88.86	HTTP	56 GET /~csantiago/RECO/index.html HTTP/1.0
46 9.878307	45.239.88.86	192.168.0.211	TCP	56 80 → 53167 [ACK] Seq=1 Ack=84 Win=64256 Len=0
47 9.879105	45.239.88.86	192.168.0.211	HTTP	551 HTTP/1.1 200 OK (text/html)

Nota. La imagen muestra la captura de paquetes en Wireshark correspondiente a la ejecución de una solicitud HTTP mediante TELNET. Se muestran tres paquetes: la solicitud GET, una confirmación TCP (ACK) y la respuesta HTTP con código 200 OK.

En la capa de transporte se utiliza el protocolo TCP, que garantiza la entrega confiable de los datos. El primer paquete contiene la solicitud HTTP enviada desde la dirección IP del cliente (192.168.0.211) al servidor (45.239.88.86) usando el puerto 80, que es el puerto estándar para servicios HTTP. El segundo paquete es un ACK, que confirma la recepción de datos por parte del cliente, mostrando los números de secuencia y ventana TCP. Finalmente, el tercer paquete contiene la respuesta HTTP con el código 200 OK, junto con los encabezados y el contenido HTML. Esta secuencia de paquetes ilustra cómo TELNET puede ser utilizado para enviar solicitudes HTTP manuales, y cómo TCP maneja el control de flujo y la confiabilidad de la conexión.

Figura 20

Solicitud HTTP de archivo PDF mediante TELNET

Nota. La imagen muestra la consola TELNET tras ejecutar el comando GET /~csantiago/RECO/prueba.pdf HTTP/1.0. La imagen muestra una respuesta incompleta o mal renderizada, posiblemente debido a la naturaleza binaria del archivo PDF, que no puede visualizarse correctamente en una terminal de texto plano.

Se intentó acceder a un archivo PDF utilizando TELNET, lo cual genera una respuesta HTTP que incluye datos binarios. Como TELNET no interpreta ni renderiza contenido binario, el resultado aparece como texto corrupto o ilegible. A nivel de capa de aplicación, se utilizó el protocolo HTTP para solicitar el recurso, y el servidor respondió con el tipo de contenido application/pdf. Sin embargo, debido a las limitaciones de TELNET, no se puede visualizar el archivo correctamente, lo que demuestra que este método no es adecuado para descargar archivos binarios como documentos PDF o imágenes.

Figura 21

Captura de paquetes en Wireshark durante la solicitud de prueba.pdf vía TELNET

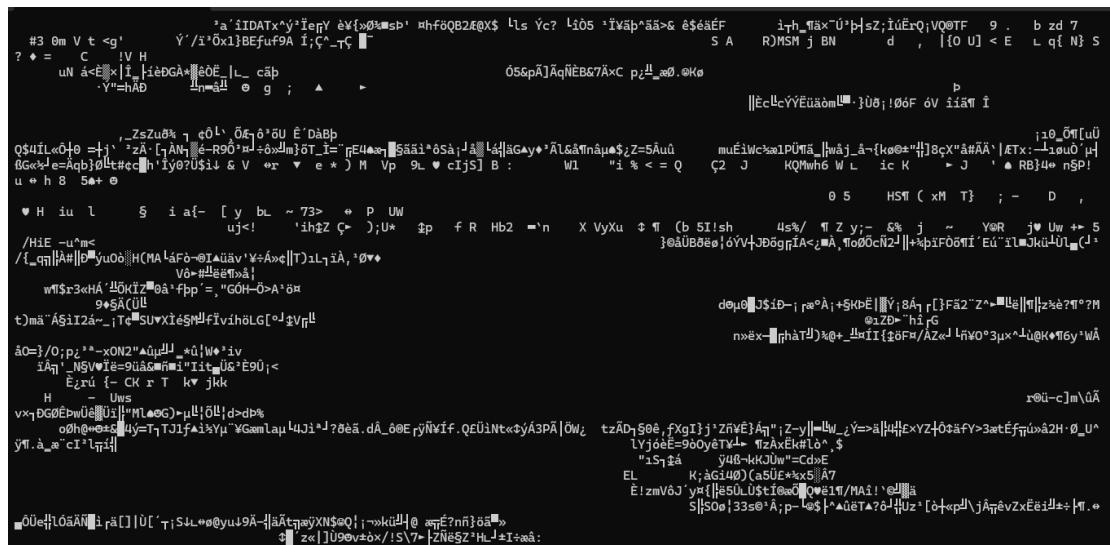
331 29.350602	192.168.0.211	45.239.88.86	TCP	54 53168 → 80 [ACK] Seq=84 Ack=144541 Win=54784 Len=0
332 29.351496	45.239.88.86	192.168.0.211	HTTP	1463 HTTP/1.1 200 OK (application/pdf)
333 29.351580	192.168.0.211	45.239.88.86	TCP	54 53168 → 80 [ACK] Seq=84 Ack=145951 Win=53504 Len=0

Nota. Captura de paquetes en Wireshark correspondiente a la solicitud del archivo prueba.pdf mediante TELNET. Se muestran un paquete con una respuesta HTTP con código 200 OK y tipo de contenido application/pdf.

En la capa de transporte se observa el uso del protocolo TCP, con el puerto de destino 80, correspondiente al servicio HTTP, y un puerto de origen dinámico (53168) asignado por el sistema operativo del cliente. El paquete contiene la respuesta HTTP con el código 200 OK, indicando que el archivo fue encontrado y enviado correctamente. El encabezado Content-Type: application/pdf especifica que el contenido es un archivo PDF. Esta captura evidencia cómo HTTP transmite archivos binarios sobre TCP, y cómo TELNET puede iniciar la solicitud, pero no manejar adecuadamente la visualización del contenido.

Figura 22

Solicitud HTTP de imagen PNG mediante TELNET



Nota. La imagen muestra la consola TELNET tras ejecutar el comando GET /~csantiago/RECO/network.png HTTP/1.0. La imagen muestra una respuesta ilegible o corrompida, lo cual es común al intentar visualizar archivos binarios como imágenes en una terminal de texto plano.

A nivel de capa de aplicación, se utilizó el protocolo HTTP para enviar la solicitud, y el servidor respondió con un encabezado que indica el tipo de contenido image/png. Sin embargo, TELNET no está diseñado para manejar ni visualizar archivos binarios, lo que limita su utilidad

en este tipo de operaciones. Esta situación evidencia cómo TELNET puede ser útil para probar solicitudes HTTP, pero no para consumir contenido multimedia.

Figura 23

Captura de paquetes en Wireshark durante la solicitud de network.png vía TELNET

167 6.236140	192.168.0.211	45.239.88.86	TCP	54 53203 → 80 [ACK] Seq=88 Ack=61321 Win=130816 Len=0
168 6.236725	45.239.88.86	192.168.0.211	HTTP	403 HTTP/1.1 200 OK (PNG)
169 6.236761	192.168.0.211	45.239.88.86	TCP	54 53203 → 80 [ACK] Seq=88 Ack=61671 Win=130560 Len=0

Nota. La imagen muestra la captura de paquetes en Wireshark correspondiente a la solicitud del archivo network.png mediante TELNET. Se muestra un paquete con una respuesta HTTP con código 200 OK y tipo de contenido image/png.

En la capa de transporte se utiliza el protocolo TCP, con puerto de destino 80 (HTTP) y un puerto de origen dinámico (53203) asignado por el sistema operativo del cliente. El primer paquete es un ACK que confirma la recepción de datos. El segundo paquete contiene la respuesta HTTP con el código 200 OK, lo que indica que el archivo fue encontrado y enviado correctamente. El encabezado Content-Type: image/png especifica que el contenido es una imagen en formato PNG. Finalmente, el tercer paquete es otro ACK que confirma la recepción de la respuesta. Esta captura demuestra cómo HTTP transmite archivos binarios sobre TCP, y cómo TELNET puede iniciar la solicitud, pero no manejar adecuadamente la visualización del contenido.

Figura 24

Captura de tráfico HTTP en Wireshark al acceder a una página web desde el navegador



Espacio de prueba del Laboratorio de RECO

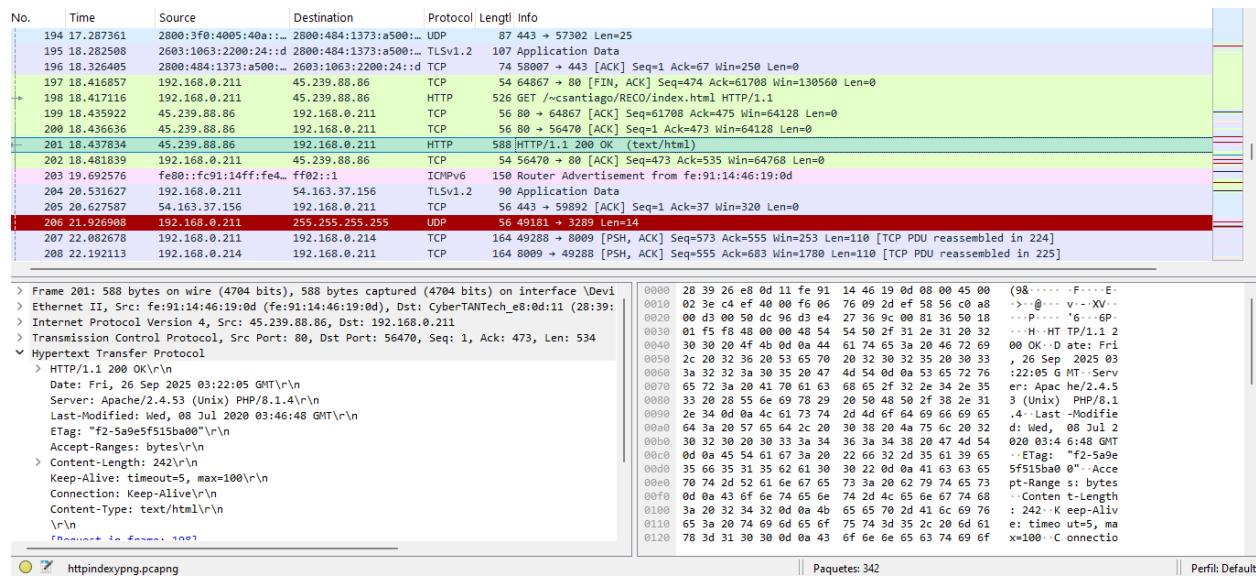
Esta es un archivo de prueba para revisar el funcionamiento del protocolo HTTP y TCP

Nota. Se muestra el navegador web mostrando el archivo index.html alojado en el servidor profesores.is.escuelaing.edu.co.

El navegador interpreta correctamente el contenido HTML del archivo index.html. A través del protocolo HTTP, el navegador realiza una solicitud GET al servidor, que responde con un código 200 OK y el contenido del archivo. En la capa de aplicación, se observa el uso de HTTP/1.1, y el tipo de contenido especificado es text/html. El navegador procesa este contenido y lo presenta de forma estructurada y visual, lo que permite al usuario interactuar con la información de manera más intuitiva que con TELNET.

Figura 25

Captura de paquetes en Wireshark durante acceso HTTP a index.html vía navegador



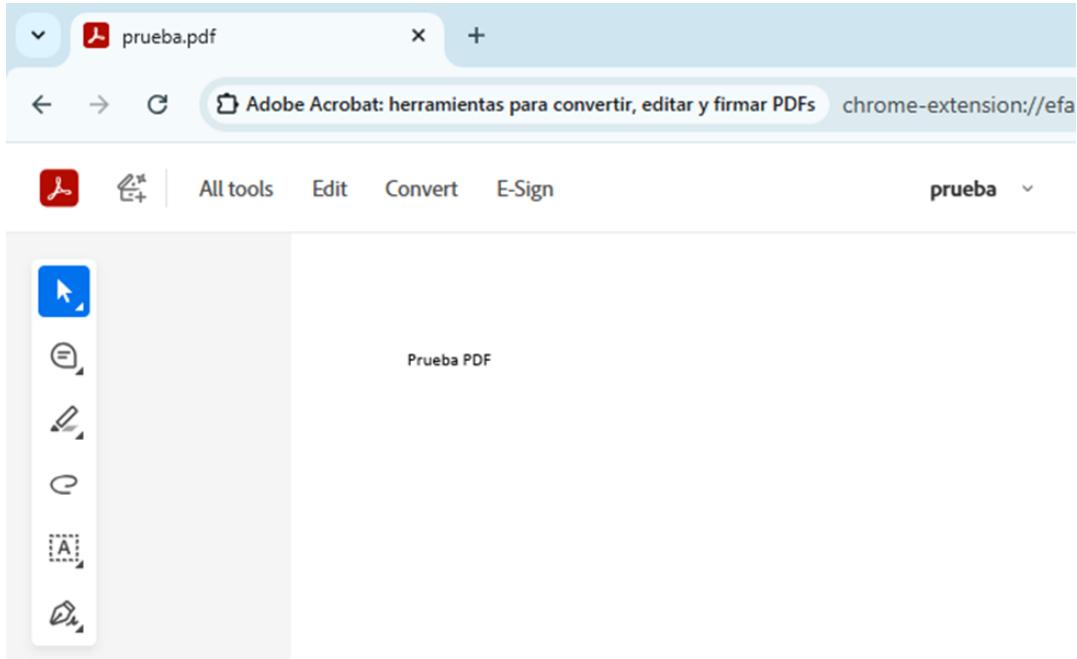
Nota. Captura de paquetes en Wireshark correspondiente al acceso al archivo index.html mediante navegador web. Se observan paquetes TCP y HTTP, incluyendo la solicitud GET, encabezados de respuesta, y confirmaciones de recepción.

En la capa de transporte se utiliza TCP, con puerto de destino 80 (HTTP) y un puerto de origen dinámico (56470). Se observa el establecimiento de la conexión mediante el handshake TCP (SYN, SYN-ACK, ACK), seguido por la solicitud HTTP GET. El servidor responde con un

código 200 OK y encabezados que indican el tipo de contenido text/html, longitud del archivo (2427 bytes), fecha de modificación, entre otros.

Figura 26

Visualización del archivo prueba.pdf en navegador mediante Adobe Acrobat

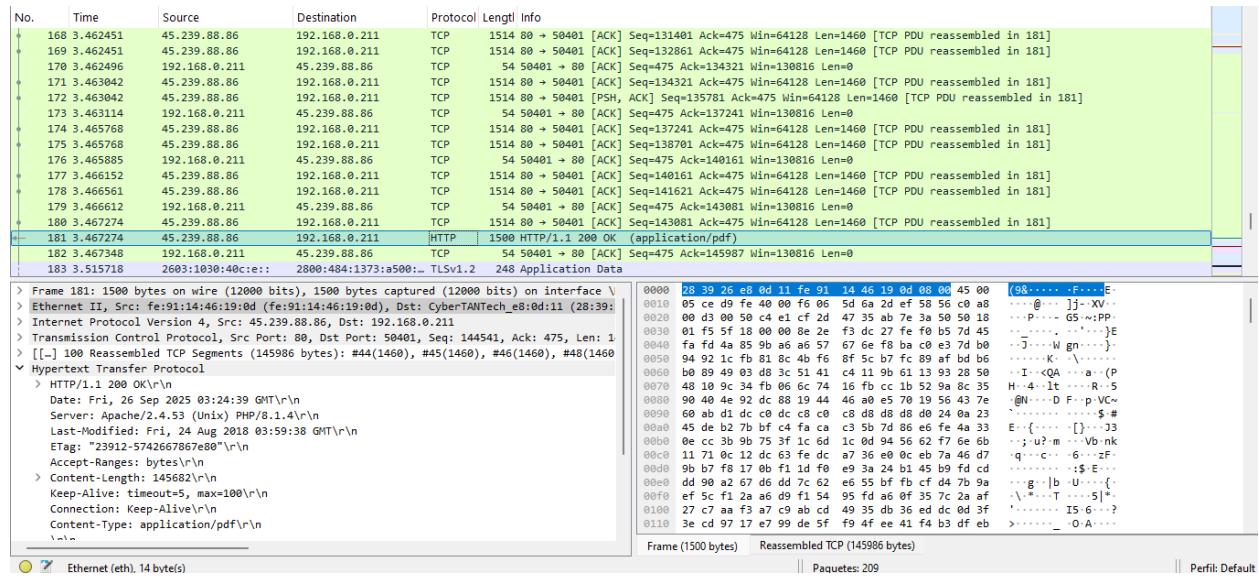


Nota. Captura de pantalla del archivo prueba.pdf abierto en Adobe Acrobat tras ser descargado desde el servidor profesores.is.escuelaing.edu.co mediante navegador web.

El navegador pudo descargar correctamente el archivo PDF solicitado mediante el protocolo HTTP. Una vez descargado, el archivo se abre en Adobe Acrobat, lo que indica que el navegador interpretó correctamente los encabezados HTTP, identificó el tipo de contenido como application/pdf, y gestionó la descarga sin errores.

Figura 27

Captura de tráfico HTTP en Wireshark durante la descarga de un archivo desde el navegador



Nota. Captura de paquetes en Wireshark correspondiente a la descarga del archivo prueba.pdf mediante navegador web. Se observa una respuesta HTTP con código 200 OK, encabezados detallados, y contenido binario transmitido desde el servidor.

En la capa de transporte se utiliza TCP, con puerto de destino 80 (HTTP) y un puerto de origen dinámico asignado por el cliente. El paquete destacado contiene una respuesta HTTP con código 200 OK, lo que indica que el archivo fue encontrado y enviado correctamente. Los encabezados HTTP incluyen información como el tipo de servidor (Apache/2.4.29), fecha de modificación, longitud del contenido (Content-Length: 145621), y tipo de contenido (application/pdf).

Figura 28

Visualización de imagen descargada vía navegador

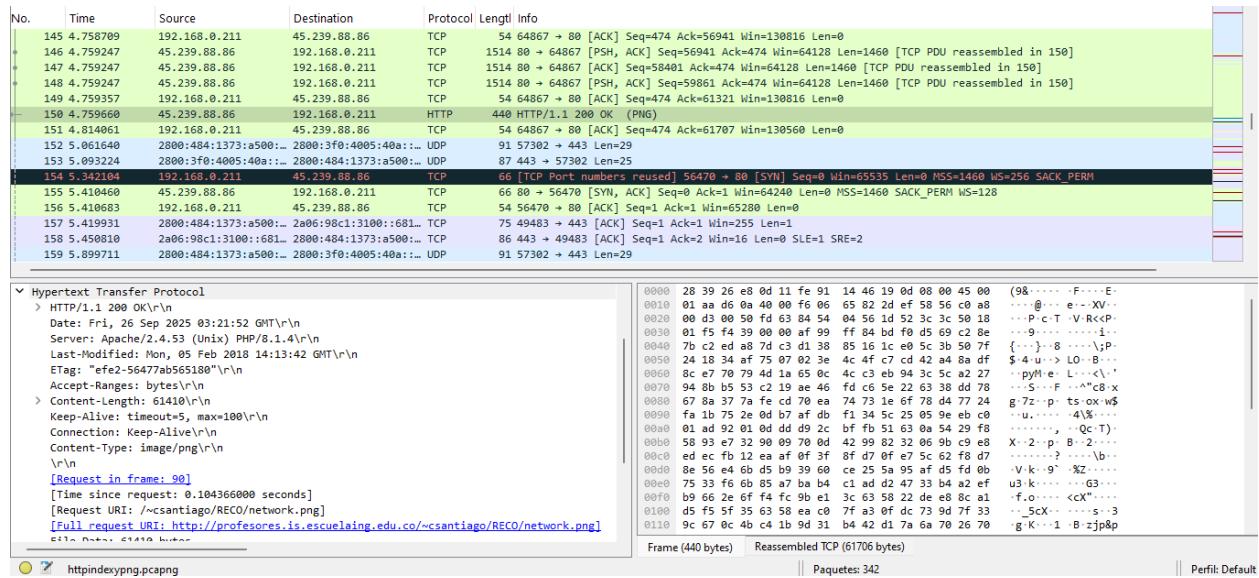


Nota. Captura de pantalla de la imagen network.png descargada desde el servidor profesores.is.escuelaing.edu.co mediante navegador web.

El navegador pudo descargar y visualizar correctamente el archivo network.png, que es una imagen en formato binario. A través del protocolo HTTP, el navegador interpreta los encabezados de respuesta que indican el tipo de contenido (image/png) y renderiza la imagen sin errores.

Figura 29

Captura de paquetes en Wireshark durante descarga de network.png vía navegador



Nota. Captura de paquetes en Wireshark correspondiente a la descarga del archivo network.png mediante navegador web. Se observa una solicitud HTTP GET y una respuesta con código 200 OK, encabezados detallados, y transmisión de datos binarios.

En la capa de transporte se utiliza TCP, con puerto de destino 80 (HTTP) y un puerto de origen dinámico asignado por el cliente. El paquete destacado contiene una solicitud HTTP GET para el recurso /~csantiago/RECO/network.png, y la respuesta del servidor incluye el código 200 OK, junto con encabezados que especifican el tipo de contenido como image/png. También se observa la transmisión de datos binarios correspondientes a la imagen.

¿Qué diferencia se encuentra entre los archivos descargados vía TELNET y vía el navegador?

La diferencia principal radica en la manera en que se procesan y presentan los datos. Al usar TELNET, el usuario debe escribir manualmente la petición HTTP y la respuesta del servidor se recibe en formato crudo, mostrando tanto las cabeceras como el contenido binario del archivo en la consola, el cual aparece como caracteres ilegibles y requiere ser redirigido y guardado

manualmente para poder utilizarse. En cambio, cuando se utiliza un navegador, este genera automáticamente las peticiones HTTP, interpreta las cabeceras de la respuesta y gestiona el contenido recibido de acuerdo con el campo Content-Type, descargando el archivo en su formato correcto y mostrándolo directamente si es compatible (por ejemplo, visualizar una imagen o abrir un PDF). De esta forma, TELNET expone los detalles internos del protocolo, mientras que el navegador simplifica el proceso y garantiza la usabilidad de los archivos descargados.

Prueba del servicio DNS

En esta sección se llevará a cabo un conjunto de pruebas DNS con el propósito de analizar la configuración, la infraestructura y los datos de registro de diferentes dominios de Internet. El objetivo principal de esta actividad es identificar información técnica relevante asociada a cada dominio, como la cantidad de servidores de nombre (Name Servers), los detalles del registro WHOIS, y la asignación de direcciones IP, entre otros aspectos. Este tipo de análisis permite comprender cómo están estructurados los dominios en términos de resolución de nombres, así como verificar la vigencia y validez de los registros asociados a ellos.

Para la realización de estas pruebas se utilizará la plataforma en línea [CentralOps.net](#), una herramienta que permite consultar registros DNS, acceder a información WHOIS, realizar pruebas de resolución de nombres de dominio, y verificar parámetros de red relacionados. A través de esta herramienta se analizarán los siguientes dominios: escuelaing.edu.co, jbb.gov.co, google.com, y un dominio adicional perteneciente a una organización no estadounidense, el cual será elegido específicamente para diversificar el análisis en función del origen del dominio.

Para el análisis del dominio escuelaing.edu.co se utilizaron las herramientas de CentralOps.net, las cuales permiten consultar registros DNS, información de WHOIS y datos de red relevantes para evaluar la infraestructura digital asociada.

Figura 30

Análisis del dominio: escuelaing.edu.co

The screenshot shows the CentralOps.net interface with the 'Domain Dossier' tool selected. The main search bar contains 'escuelaing.edu.co'. Under 'Domain Whois record', it shows the domain was queried from whois.nic.co with the IP '45.239.88.68'. The WHOIS details are heavily redacted, but the creation date is listed as 1998-06-02T00:00:00Z and the expiration date as 2038-12-31T23:59:59Z. The 'Address lookup' section shows the canonical name 'escuelaing.edu.co.', aliases, and the IP address '45.239.88.68'.

Nota. Captura de pantalla de los resultados obtenidos a través de CentralOps.net para el dominio escuelaing.edu.co, incluyendo registros DNS, información WHOIS y detalles sobre la asignación de dirección IP.

Desde el punto de vista de resolución de nombres, el dominio cuenta con una dirección IP asociada: 45.239.88.68, la cual pertenece al rango 45.239.88.0/22, asignado por la organización LACNIC (Latin American and Caribbean Internet Addresses Registry). Este bloque de direcciones está registrado a nombre de la misma institución educativa, evidenciando que la Escuela administra directamente su infraestructura de red pública.

En cuanto a los registros DNS, el dominio dispone de dos servidores de nombre configurados: ns1.escuelaing.edu.co y ns2.escuelaing.edu.co. Ambos se encuentran activos y registrados con tiempos de vida (TTL) de 300 segundos, lo que indica una política de

actualización relativamente frecuente. Aunque solo se presentan dos servidores en los registros, en la pregunta se menciona un total de cuatro, lo cual podría deberse a servidores internos o secundarios no visibles en esta consulta directa.

El dominio fue originalmente creado el 2 de junio de 1998, lo que indica que lleva más de 27 años en funcionamiento. Este hecho resalta la antigüedad y estabilidad de la entidad en el entorno digital. La última actualización del registro fue realizada el 19 de julio de 2025, y el dominio se encuentra registrado con vigencia hasta el 31 de diciembre de 2028, lo cual garantiza su validez por al menos tres años más.

El registrador oficial del dominio es .CO Internet S.A.S., entidad que administra los dominios con extensión “.co” en Colombia. Esta organización cuenta con el ID de registrador IANA 111111. La entidad registrante, según los datos disponibles, es la misma Escuela Colombiana de Ingeniería, identificada en el sistema de LACNIC con el ID CO-ECIN2-LACNIC. Aunque la mayoría de los datos personales del registrante han sido ocultados por razones de privacidad, se observa como contacto técnico a Julián García, cuyo correo y datos de contacto están registrados para el manejo técnico de la red institucional.

Finalmente, los registros TXT del dominio revelan una configuración avanzada de seguridad y verificación de servicios, incluyendo validaciones de propiedad con Google, Facebook, Microsoft y otros proveedores. Además, se encuentra configurado un registro SPF (Sender Policy Framework), lo cual indica la implementación de medidas de protección contra el correo no deseado (spam).

Pregunta	Respuesta
¿Cuántos servidores de dominio tiene?	Tiene 2 servidores listados públicamente (ns1 y ns2), aunque en el planteamiento inicial se menciona un total de 4 servidores.
¿Hace cuánto fue asignado este dominio?	El dominio fue creado el 2 de junio de 1998, es decir, hace 27 años (en 2025).
¿Con quién está registrado?	Está registrado con la entidad .CO Internet S.A.S.
¿Cuál es el ID de la entidad registrante?	CO-ECIN2-LACNIC
¿Cuándo fue la última actualización del registro?	El 19 de julio de 2025.
¿Cuál es la validez del registro?	El dominio es válido hasta el 31 de diciembre de 2028.
¿Cuál es el rango de IP asignado y qué entidad lo asignó?	El rango asignado es 45.239.88.0/22, asignado por LACNIC.
¿A qué empresa fue asignado?	A la Escuela Colombiana de Ingeniería Julio Garavito.

El dominio jbb.gov.co pertenece al Jardín Botánico José Celestino Mutis, una entidad del orden distrital en Bogotá, Colombia. A través de la plataforma CentralOps.net se ha recopilado información referente a sus registros DNS, datos WHOIS y asignación de direcciones IP, lo que permite analizar la infraestructura técnica que soporta este dominio.

Figura 31

Análisis del dominio: *jbb.gov.co*

The screenshot shows the CentralOps.net interface. In the 'Domain Dossier' section, the domain *jbb.gov.co* is entered. Under 'Domain Whois record', it shows the following details:

- Domain Name: *jbb.gov.co*
- Registrant Name: REDACTED FOR PRIVACY
- Registrar URL: www.cointernet.com.co
- Creation Date: 2000-01-20T00:00:00Z
- Registration Expiry Date: 2026-01-20T23:59:59Z
- Registrant Organization: Jardin Botanico Jose Celestino Mutis
- Registrant Street: REDACTED FOR PRIVACY
- Registrant City: REDACTED FOR PRIVACY
- Registrant State/Province: Bogota
- Registrant Postal Code: REDACTED FOR PRIVACY

Nota. Captura de pantalla de los resultados obtenidos desde la herramienta CentralOps.net para el dominio *jbb.gov.co*, que incluye registros DNS, detalles del WHOIS y asignación de direcciones IP.

En cuanto a su resolución de nombres, el dominio presenta dos direcciones IPv4:

20.94.123.146 y 20.119.228.39, así como una dirección IPv6: 2603:1030:403:3::a2, lo cual evidencia compatibilidad con la nueva generación de direcciones IP. Estas direcciones están asignadas a través de Microsoft Azure, lo que sugiere que el sitio está alojado en la nube de Microsoft Corporation. Esto se confirma con los registros ARIN, donde se indica que el rango IP utilizado (20.33.0.0 - 20.128.255.255) fue asignado directamente a Microsoft Corporation, organización con sede en Redmond, Washington (EE.UU.).

El dominio cuenta con dos servidores de nombre públicos: ns31.domaincontrol.com y ns32.domaincontrol.com, gestionados por GoDaddy. A pesar de que la consulta DNS muestra solo dos, se hace referencia a servidores adicionales en los registros inversos y de IPv6, específicamente servidores de Azure (ns1-07.azure-dns.com, ns4-07.azure-dns.info, entre otros), lo cual indica que Microsoft también participa en la resolución inversa de IPs y posiblemente en la redundancia del servicio.

Este dominio fue creado el 20 de enero del año 2000, por lo tanto, ha estado activo por más de 25 años. La última actualización de su registro fue el 14 de mayo de 2021, y su validez está garantizada hasta el 20 de enero de 2026, lo que indica que aún se encuentra vigente por más de un año. La entidad registradora responsable es también .CO Internet S.A.S., al igual que en otros dominios ".co", y posee el ID IANA 111111.

Aunque gran parte de la información sobre el registrante ha sido redactada por motivos de privacidad, se puede confirmar que el dominio está registrado a nombre del Jardín Botánico José Celestino Mutis, como lo indica el campo “Registrant Organization”. Este hecho, junto con el uso de servicios en la nube de Microsoft, evidencia un enfoque moderno en la gestión de infraestructura digital por parte de esta entidad gubernamental.

Los registros DNS reflejan una configuración técnica adecuada, con tiempos de vida (TTL) que oscilan entre los 5 minutos y 1 hora, lo cual es razonable para entornos donde se requiere cierta flexibilidad para cambios de configuración. Adicionalmente, la existencia de registros de tipo HINFO muestra una intención de documentar información adicional sobre la plataforma técnica, aunque los campos de CPU y sistema operativo aparecen vacíos.

Pregunta	Respuesta
¿Cuántos servidores de dominio tiene?	Tiene 2 servidores principales listados (ns31.domaincontrol.com y ns32.domaincontrol.com). Adicionalmente, existen servidores auxiliares relacionados con Azure para resolución inversa, por lo que puede estimarse una infraestructura de hasta 6 servidores DNS en total.
¿Hace cuánto fue asignado este dominio?	Fue creado el 20 de enero del año 2000, hace 25 años (en 2025).
¿Con quién está registrado?	Con la entidad .CO Internet S.A.S.
¿Cuál es el ID de la entidad registrante?	Aunque el WHOIS lo oculta por privacidad, el ID de la organización propietaria de las direcciones IP es: MSFT (Microsoft Corporation), y el dominio pertenece al Jardín Botánico José Celestino Mutis.
¿Cuándo fue la última actualización del registro?	El 14 de mayo de 2021.
¿Cuál es la validez del registro?	Hasta el 20 de enero de 2026.
¿Cuál es el rango de IP asignado y qué entidad lo asignó?	Las IPs fueron asignadas a Microsoft Corporation, pero el dominio pertenece al Jardín Botánico José Celestino Mutis, entidad gubernamental de Colombia.

¿A qué empresa fue asignado?	A Google LLC, con sede en California, Estados Unidos.
-------------------------------------	---

El dominio google.com pertenece a Google LLC, una de las empresas tecnológicas más grandes del mundo. Este dominio es parte fundamental de la infraestructura global de servicios de Google, incluyendo su motor de búsqueda, correo electrónico, plataformas de publicidad, almacenamiento en la nube, entre muchos otros.

Figura 32

Análisis del dominio: google.com

The screenshot shows the CentralOps.net interface. In the top navigation bar, there's a link to 'https://centralops.net/co/'. The main content area has a blue header 'Central Ops .net Advanced online Internet utilities'. On the left, a sidebar titled 'Utilities' lists various tools: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup / Dig. The main panel is titled 'Domain Dossier' with the sub-instruction 'Investigate domains and IP addresses'. A search bar contains 'google.com'. Below it, there are several checkboxes: 'domain whois record' (checked), 'DNS records' (checked), 'traceroute' (unchecked), 'network whois record' (checked), and 'service scan' (unchecked). There are also user-related fields: 'user: anonymous [152.201.106.226]', 'balance: 47 units', and buttons for 'log in | account info' and 'CentralOps.net'. A note at the bottom says 'To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]'. The 'Address lookup' section shows canonical name 'google.com.' and a list of IP addresses: 173.194.208.139, 173.194.208.101, 173.194.208.138, 173.194.208.113, 173.194.208.100, 173.194.208.102, 2607:fbb0:4023:1000::64, 2607:fbb0:4023:1000::66, 2607:fbb0:4023:1000::8b, 2607:fbb0:4023:1000::65. The 'Domain Whois record' section shows the following details:

```

Domain Name: GOOGLE.COM
Registrar Domain ID: 2119814 DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registration Expiry Date: 2020-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086517580
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

```

Nota. Captura de pantalla generada desde CentralOps.net mostrando los registros DNS, WHOIS y asignación de IP para el dominio google.com.

A nivel técnico, el dominio está respaldado por una robusta infraestructura de resolución de nombres. Se identifican cuatro servidores de nombres (NS): ns1.google.com, ns2.google.com, ns3.google.com y ns4.google.com, lo cual proporciona una alta disponibilidad y redundancia. Estos servidores están distribuidos globalmente y pertenecen a Google LLC.

En cuanto a sus registros A y AAAA, Google emplea una estrategia de balanceo de carga por IP, ya que múltiples direcciones IPv4 están asociadas al dominio, como 173.194.208.139, 173.194.208.100, entre otras. Además, también utiliza varias direcciones IPv6, como 2607:f8b0:4023:1000::64 y ::66, lo cual garantiza compatibilidad con ambas versiones del protocolo IP y un rendimiento óptimo a nivel global.

El registro WHOIS muestra que el dominio fue creado el 15 de septiembre de 1997, siendo uno de los dominios más antiguos en funcionamiento dentro del ecosistema de empresas tecnológicas. La última actualización de su información fue el 2 de agosto de 2024, y su validez se extiende hasta el 13 de septiembre de 2028, mostrando una gestión activa y preventiva para evitar expiraciones accidentales.

El dominio está registrado a través de MarkMonitor Inc., un registrador especializado en la protección de marcas globales, lo cual es coherente con el perfil de una empresa como Google. Además, su información de contacto se mantiene protegida mediante formularios internos del registrador, cumpliendo con buenas prácticas de privacidad y protección de datos.

Los registros DNS adicionales, como TXT, MX, SOA y CAA, demuestran una configuración avanzada. Existen registros de verificación para múltiples plataformas (como Facebook, Apple, Cisco, y DocuSign), lo que indica la participación de Google en múltiples ecosistemas y protocolos. También se observan políticas de correo saliente definidas mediante

registros SPF (v=spf1 include:_spf.google.com ~all), y políticas de autenticación y autorización reflejadas en registros CAA y múltiples google-site-verification.

En términos de asignación de IP, el rango 173.194.0.0 – 173.194.255.255 está registrado directamente a Google LLC, organización identificada en ARIN con el código GOGL. La empresa está ubicada en 1600 Amphitheatre Parkway, Mountain View, California, EE.UU., y mantiene registros de contacto técnico y de abuso actualizados y disponibles.

Pregunta	Respuesta
¿Cuántos servidores de dominio tiene?	Tiene cuatro servidores de nombre (NS): ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com.
¿Hace cuánto fue asignado este dominio?	Fue registrado el 15 de septiembre de 1997, por lo tanto tiene 28 años (en 2025).
¿Con quién está registrado?	Con la empresa MarkMonitor Inc.
¿Cuál es el ID de la entidad registrante?	El ID del registrador es 292 (IANA) y la organización propietaria es Google LLC, identificada en ARIN con el ID GOGL.
¿Cuándo fue la última actualización del registro?	El 2 de agosto de 2024.
¿Cuál es la validez del registro?	Hasta el 13 de septiembre de 2028.

¿Cuál es el rango de IP asignado y qué entidad lo asignó?	El rango 173.194.0.0/16 fue asignado por ARIN (American Registry for Internet Numbers) a Google LLC.
¿A qué empresa fue asignado?	A Google LLC, con sede en California, Estados Unidos.

El dominio lufthansa.com corresponde a Deutsche Lufthansa AG, una de las aerolíneas más grandes de Europa, con sede en Alemania. Este dominio representa su plataforma oficial en línea, utilizada para reservaciones de vuelos, servicios a pasajeros, comunicación institucional y comercio electrónico internacional.

Figura 33

Análisis del dominio: *lufthansa.com*

CentralOps.net Advanced online Internet utilities
a service of :Hexillion

Domain Dossier Investigate domains and IP addresses

domain or IP address: **lufthansa.com**

domain whois record DNS records traceroute

network whois record service scan

User: anonymous [152.201.106.226]
Balance: 46 units
log in | account info

To obtain Whois data redacted because of the **GDPR** or privacy services, try [ICANN's RDRS](#). [more information]

Address lookup
canonical name: **lufthansa.com**,
aliases:
addresses: **20.101.251.232**

Domain Whois record
Queried whois.internic.net with "dom lufthansa.com"...

Domain Name: LUFTHANSA.COM
Registry Domain ID: 6443374_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://csedb.cs
Updated Date: 2025-03-12T15:21:19Z
Creation Date: 1996-01-10T05:00:00Z
Registration Expiry Date: 2026-01-09T05:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1-888-902-7222
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: UDNNNS1.CLOUDNS.COM
Name Server: UDNNNS2.CLOUDNS.COM
DNSSEC signedDelegation
DNSSEC DS Data: 14242 13 1 98566EB062C699AA11230E337EEAF8244050A224
DNSSEC DS Data: 14242 13 2 493A0CDD768647DBE5F7F48BD070AC739056B62729A384BBA934320438280A0A
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of Whois database: 2025-09-27T22:57:54Z <<

Nota. Captura de pantalla generada desde CentralOps.net que presenta los registros WHOIS, DNS y red del dominio *lufthansa.com*, perteneciente a la aerolínea alemana Deutsche Lufthansa AG.

El dominio fue registrado el 10 de enero de 1996, posicionándose entre los más antiguos del sector aéreo en internet. A lo largo de casi tres décadas, Lufthansa ha mantenido una gestión sólida de este activo digital. La última actualización del dominio ocurrió el 12 de marzo de 2025, y su expiración está prevista para el 9 de enero de 2026, lo que refleja una renovación activa por parte de la organización.

El registrador actual es CSC Corporate Domains, Inc., identificado por el IANA con el código 299, una compañía especializada en la gestión de dominios corporativos para marcas globales. La organización titular es claramente identificada como Deutsche Lufthansa AG, con sede en Alemania (código de país DE), lo que confirma su carácter no estadounidense.

A nivel técnico, el dominio cuenta con dos servidores de nombres (NS): udns1.cscudns.com y udns2.cscudns.org. Ambos forman parte de la red de CSC, y se encargan de la resolución de nombres para el dominio. Además, el dominio tiene implementado DNSSEC (Domain Name System Security Extensions), una característica que mejora la seguridad de las consultas DNS mediante firmas digitales. Los registros RRSIG indican que el dominio está firmado criptográficamente, lo que protege contra manipulaciones como ataques de envenenamiento de caché DNS.

En cuanto a la dirección IP pública principal del dominio (20.101.251.232), esta se encuentra dentro del rango de direcciones propiedad de Microsoft Corporation, específicamente bajo el bloque 20.33.0.0 - 20.128.255.255, según los registros de ARIN. Esto indica que Lufthansa está utilizando infraestructura en la nube de Microsoft Azure, una práctica común entre empresas multinacionales que buscan alta disponibilidad, rendimiento global y cumplimiento normativo a través de servicios cloud.

Los servidores DNS inversos (in-addr.arpa) asociados a la IP apuntan a nombres dentro del sistema de Azure (ns1-04.azure-dns.com, etc.), lo que confirma la delegación de servicios de red a la plataforma de Microsoft. Este tipo de configuración es coherente con una organización de gran escala que busca tercerizar infraestructura técnica a proveedores especializados.

Pregunta	Respuesta
¿Cuántos servidores de dominio tiene?	Tiene dos servidores de nombre: udns1.cscudns.com y udns2.cscudns.org.
¿Hace cuánto fue asignado este dominio?	Fue registrado el 10 de enero de 1996, hace aproximadamente 29 años (en 2025).
¿Con quién está registrado?	Está registrado con CSC Corporate Domains, Inc.
¿Cuál es el ID de la entidad registrante?	IANA ID del registrador: 299 Organización registrante: Deutsche Lufthansa AG
¿Cuándo fue la última actualización del registro?	El 12 de marzo de 2025.
¿Cuál es la validez del registro?	Hasta el 9 de enero de 2026.
¿Cuál es el rango de IP asignado y qué entidad lo asignó?	IP 20.101.251.232 pertenece al rango 20.33.0.0 - 20.128.255.255, asignado por ARIN a Microsoft Corporation (MSFT).
¿A qué empresa fue asignado?	A Microsoft Corporation, pero utilizada por Lufthansa mediante servicios en la nube (Azure).

Servidor NTP

En esta práctica se implementa un servidor NTP (Network Time Protocol) con el objetivo de sincronizar la hora entre distintos sistemas operativos dentro de una infraestructura de red. La sincronización horaria es fundamental para el correcto funcionamiento de servicios distribuidos, registros de eventos, autenticación y tareas programadas. Utilizando una de las máquinas como servidor NTP, ya sea Solaris o Linux Slackware, según la asignación del equipo. Se configurarán el resto de los sistemas operativos (como Windows Server, CentOS, Android, entre otros) como clientes NTP, asegurando que todos obtengan la hora desde una fuente central confiable. Esta configuración se realizará en entornos virtualizados.

Team 01 – NTP Server en Solaris con clientes multiplataforma

En esta sección se documenta la implementación realizada por el Team 01, cuya responsabilidad consistió en configurar un servidor NTP sobre el sistema operativo Solaris y establecer la sincronización horaria con diversos clientes multiplataforma. El objetivo principal fue asegurar que todos los sistemas dentro del entorno virtualizado obtuvieran la hora de una fuente centralizada, fiable y consistente. Para ello, se configuraron clientes en sistemas operativos como Slackware Linux, Windows Server y Android, siguiendo procedimientos específicos para cada plataforma.

Acción Realizada	Captura de Pantalla
<p>Primero, inicia sesión como root, entra a /etc/inet y copia ntp.server a ntp.conf con cp ntp.server ntp.conf para configurar Solaris como servidor NTP confiable.</p>	<pre>root@solaris:~# ls /etc/inet datemsk.ndpd ipnodes ntp.server dhcpd.conf.example ipsecalgs protocols hosts ipsecinit.sample secret ike netmasks services inetd.conf networks wanboot.conf.sample ipaddrsel.conf ntp.client root@solaris:~# cd /etc/inet root@solaris:/etc/inet# cp ntp.server ntp.conf root@solaris:/etc/inet# ls datemsk.ndpd ipnodes ntp.conf dhcpd.conf.example ipsecalgs ntp.server hosts ipsecinit.sample protocols ike netmasks secret inetd.conf networks services ipaddrsel.conf ntp.client wanboot.conf.sample root@solaris:/etc/inet#</pre>
<p>Una vez copiado el archivo de plantilla ntp.server como ntp.conf, el siguiente paso consiste en editar este último para configurar adecuadamente la sincronización horaria. En esta etapa, se agregan las direcciones de los servidores públicos del pool de NTP.</p>	<pre># While all the current refclock drivers are configured and compiled, # not all the actual hardware can be supported on all systems. The # gpsvme driver can only be expected to work on systems with a VME # bus. The WWW audio driver can only be used on systems with audio # input. # # In general, refclock type 1, the LOCAL clock is not necessary and # should not be configured. It should only be used when either there # is some other process being used to synchronize the clock, such as # with hardware with vendor provided drivers, or when it is desired # that a server without access to a real NTP time source needs to # act as a multicast or broadcast server. The LOCAL clock should not # be configured as a "backup" to other external servers. # # Some of the devices have tuning parameters, called "fudge" factors, # that can be set on the server line. See the ntpd documentation. server 0.pool.ntp.org server 1.pool.ntp.org server 2.pool.ntp.org driftfile /var/ntp/ntp.drift root@solaris:/etc/inet#</pre>
<p>El archivo driftfile guarda la deriva del reloj y se inicia con echo "0.000" > /var/ntp/ntp.drift. Luego, se habilita NTP con svcadm enable ntp, se verifica con svcs ntp y se consulta la sincronización con ntpq -p.</p>	<pre>root@solaris:~# echo "0.000" > /var/ntp/ntp.drift root@solaris:~# svcadm enable ntp root@solaris:~# svcs ntp STATE STIME FMRI online 7:15:29 svc:/network/ntp:default root@solaris:~# ntpq -p ===== remote refid st t when poll reach delay offset jitter ===== ntp.telegu.clou 192.58.120.8 2 u 13 64 1 31.548 1803243 0.004 0.cl.ntp.edgeum 169.229.128.142 2 u 16 64 1 70.317 1803243 0.004 root@solaris:~#</pre>

Para configurar Slackware como cliente NTP, inicia sesión como root. Instala NTP con slackpkg install ntp o actualízalo con slackpkg upgrade ntp. Edita /etc/ntp.conf y reemplaza los servidores por la IP del servidor Solaris. Guarda los cambios para que el sistema sincronice con el servidor configurado.

```
GNU nano 6.0                               /etc/ntp.conf                                         Modified
#
# NTP server (list one or more) to synchronize with:
#server 0.pool.ntp.org iburst
#server 1.pool.ntp.org iburst
#server 2.pool.ntp.org iburst
#server 3.pool.ntp.org iburst
server 10.2.77.100 prefer

#
# Full path of a directory where statistics files should be created
#statsdir /var/lib/ntp/stats

#
# Location of an alternate log file to be used instead of the default system syslog(3) facility.
# This is not enabled by default, because ntpd has to be restarted when the logs are rotated
# which causes unnecessary network traffic as ntpd resynchronizes.
#
#logfile /var/log/ntp

#
# Drift file. Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then renameO'ing
# it to the file.
#
driftfile /var/lib/ntp/ntp.drift

#
# Location of PID file
#
pidfile /var/run/ntpd.pid

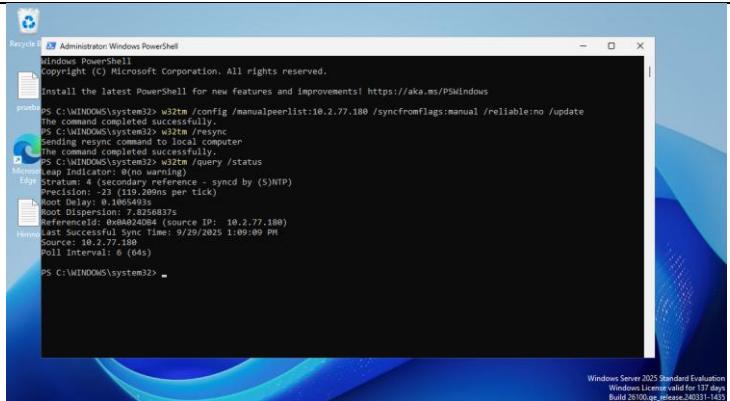
  Help   Write Out  Where Is   Cut   Execute   Location   Undo
  Exit   Read File Replace   Paste  Justify   Go To Line  Redo
```

Ejecuta ntpd -gq para sincronizar la hora. Instala libedit con slackpkg install libedit si es necesario. Luego, inicia NTP en segundo plano con ntpd -g y verifica el puerto 123 con netstat -ulnp | grep 123.

```
root@darkstar:~# ntpd -gq
29 Sep 12:59:30 ntpd[3535]: ntpd 4.2.8p10@1.4062-o Tue Jul 16 10:06:33 UTC 2024 (1): Starting
29 Sep 12:59:30 ntpd[3535]: Command line: ntpd -gq
29 Sep 12:59:30 ntpd[3535]:
29 Sep 12:59:30 ntpd[3535]: ntp-4 is maintained by Network Time Foundation,
29 Sep 12:59:30 ntpd[3535]: Inc. (NTP), a non-profit 501(c)(3) public-benefit
29 Sep 12:59:30 ntpd[3535]: corporation. Support and training for ntp-4 are
29 Sep 12:59:30 ntpd[3535]: available at https://www.ntptime.org/support
29 Sep 12:59:30 ntpd[3535]:
29 Sep 12:59:30 ntpd[3535]: DEBUG behavior is enabled - a violation of any diagnostic assertion will
cause ntpd to abort
29 Sep 12:59:30 ntpd[3535]: proto: precision = 0.050 uscc (-24)
29 Sep 12:59:30 ntpd[3535]: basetime set to 2024-07-04
29 Sep 12:59:30 ntpd[3535]: gps base set to 2024-07-07 (week 2322)
29 Sep 12:59:30 ntpd[3535]: Listen and drop on 0 us wildcard 1::1:123
29 Sep 12:59:30 ntpd[3535]: Listen and drop on 1 vWildcard 0.0.0.0:123
29 Sep 12:59:30 ntpd[3535]: Listen normally on 2 lo 127.0.0.1:123
29 Sep 12:59:30 ntpd[3535]: Listen normally on 3 eth0 10.2.77.102:123
29 Sep 12:59:30 ntpd[3535]: Listen normally on 4 lo 1::1:123
29 Sep 12:59:30 ntpd[3535]: Listen normally on 5 eth0 fe00::2ec:29ff:fe69:bfc1:21:123
29 Sep 12:59:30 ntpd[3535]: Listening on routing socket on fd #22 for interface updates
29 Sep 12:59:30 ntpd[3535]: ntpd: time slew +0.007006 s
ntp: time slew +0.007006s
root@darkstar:~# netstat -ulnp | grep 123
  udp        0      0 10.2.77.102:123          0.0.0.0:*          3539/ntpd
  udp        0      0 127.0.0.1:123          0.0.0.0:*          3539/ntpd
  udp        0      0 0.0.0.0:123          0.0.0.0:*          3539/ntpd
  udp6       0      0 fe00::2ec:29ff:fe69:123  ::*:*              3539/ntpd
  udp6       0      0 ::1:123                ::*:*              3539/ntpd
  udp6       0      0 ::::123               ::*:*              3539/ntpd
root@darkstar:~#
```

En Windows Server, ya sea con interfaz gráfica o en modo Core, configura la sincronización por línea de comandos con PowerShell.

Ejecuta w32tm /config /manualpeerlist:"10.2.77.180" /syncfromflags:manual /reliable:no /update. Luego, sincroniza con w32tm /resync. Verifica el estado con w32tm /query /status para confirmar origen y desviación del tiempo.



```

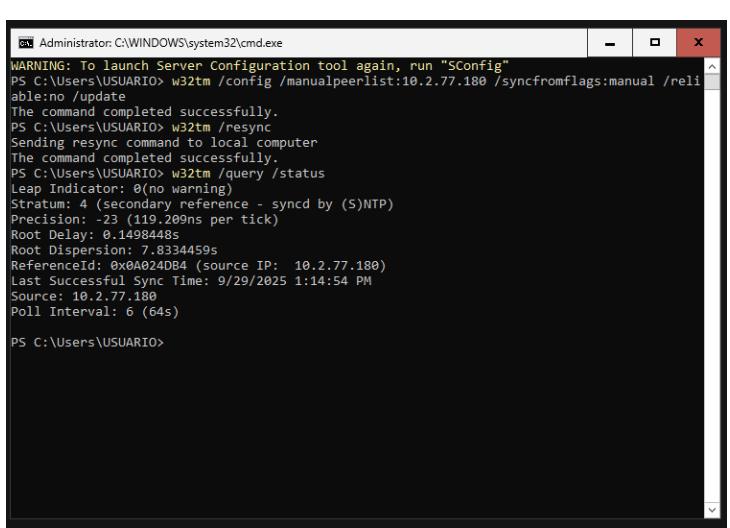
Administrator: PS C:\WINDOWS\system32> w32tm /config /manualpeerlist:10.2.77.180 /syncfromflags:manual /reliable:no /update
The command completed successfully.

Administrator: PS C:\WINDOWS\system32> w32tm /resync
Sending resync command to local computer
The command completed successfully.

Administrator: PS C:\WINDOWS\system32> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - synced by (S)NTP)
Precision: -23 (119.299ns per tick)
Root Delay: 0.16849s
Root Dispersion: 7.8256837s
ReferenceId: 0xA0A24D84 (source IP: 10.2.77.180)
Last Successful Sync Time: 9/29/2025 1:09:09 PM
Source: 10.2.77.180
Poll Interval: 6 (64s)

Administrator: PS C:\WINDOWS\system32>

```

```

Administrator: PS C:\WINDOWS\system32> w32tm /config /manualpeerlist:10.2.77.180 /syncfromflags:manual /reliable:no /update
The command completed successfully.

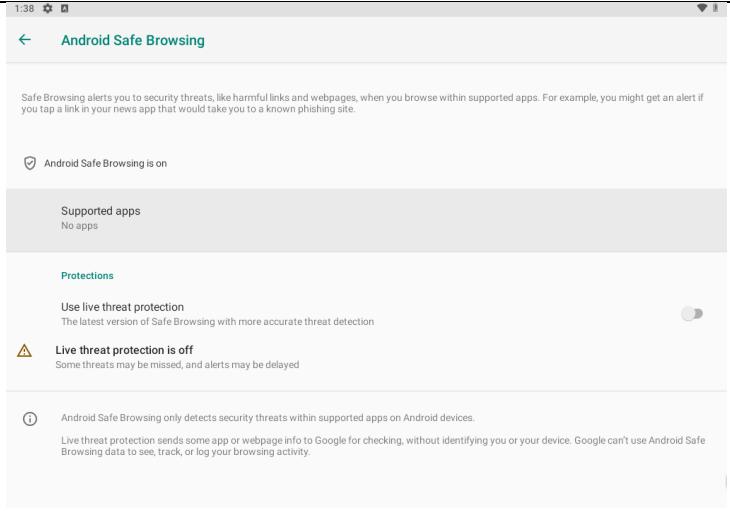
Administrator: PS C:\WINDOWS\system32> w32tm /resync
Sending resync command to local computer
The command completed successfully.

Administrator: PS C:\WINDOWS\system32> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.299ns per tick)
Root Delay: 0.1498448s
Root Dispersion: 7.8334459s
ReferenceId: 0xA0A24D84 (source IP: 10.2.77.180)
Last Successful Sync Time: 9/29/2025 1:14:54 PM
Source: 10.2.77.180
Poll Interval: 6 (64s)

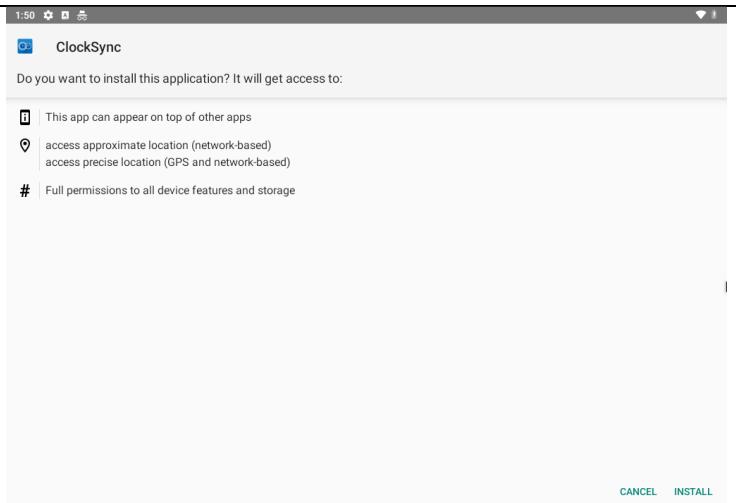
Administrator: PS C:\WINDOWS\system32>

```

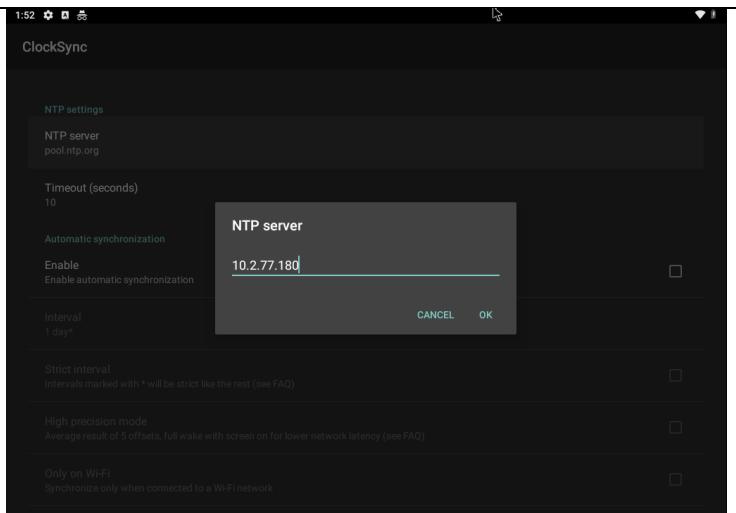
Desactiva la opción "Live Threat Protection" desde el menú de seguridad del sistema. Esto permite instalar ClockSync desde fuentes externas sin restricciones. Es necesario en dispositivos con acceso root para configuraciones avanzadas.



Descarga la aplicación ClockSync desde [Uptodown](#), ya que no siempre está en tiendas oficiales. Esta app permite modificar manualmente la fuente de sincronización horaria. Es útil en entornos donde se requiere control preciso del tiempo.



Abre ClockSync y configura la IP del servidor Solaris (10.2.77.180) como fuente NTP. Esto permite que el dispositivo se sincronice directamente con el servidor local. Así se garantiza mayor precisión y estabilidad en la hora del sistema.



Para validar la correcta configuración y el funcionamiento del servidor NTP en Solaris, así como la sincronización efectiva con los clientes multiplataforma, se ejecutó el comando:

```
ntpq -c mrulist
```

Este comando permite visualizar la lista de las direcciones IP de los clientes que han interactuado recientemente con el servidor NTP. La salida del comando confirmó exitosamente la

conexión de las cuatro máquinas configuradas como clientes: Slackware, Windows Server, Android y el propio servidor Solaris como referencia interna.

Figura

Verificación de clientes NTP conectados al servidor Solaris

```
root@solaris:~# ntpq -c mrulist
Ctrl-C will stop MRU retrieval and display partial results.
Retrieved 6 unique MRU entries and 0 updates.
lstant avgint rstr r m v count rport remote address
=====
 19    399    0 . 4 4      60    123 0.cl.ntp.edgeuno.com
 97      0    0 . 3 3      2 43137 10.2.77.181
 137   403    0 . 4 4      59    123 ntp.telecu.cloud
 2306    26    0 . 3 3      3    123 10.2.77.179
 2587    37    0 . 3 3      4    123 10.2.77.177
 3192    70    0 . 3 4      27    123 10.2.77.182
root@solaris:~#
```

Nota. En la imagen se muestra la salida del comando ntpq -c mrulist, donde se observan las direcciones IP de las cuatro máquinas clientes: 10.2.77.181, 10.2.77.179, 10.2.77.177 y 10.2.77.182. Esta información confirma que todos los sistemas configurados están estableciendo comunicación activa con el servidor NTP en Solaris (10.2.77.180), completando exitosamente la sincronización horaria en la red.

Team 02 – NTP Server en Slackware con clientes Solaris y Windows

Se configuró un servidor NTP en una máquina con Linux Slackware, y se establecieron como clientes NTP las máquinas con Solaris, Windows Server con GUI. Cada cliente fue configurado para sincronizar su hora con el servidor Slackware, asegurando que todos los sistemas compartieran una referencia temporal común. Esta práctica permite comprender cómo se distribuye el tiempo en una red y cómo verificar que la sincronización se realiza correctamente.

Acción Realizada	Captura de pantalla
Se ejecuta el comando ntpd --version en una terminal de Linux Slackware, lo que confirma que el servicio NTP está instalado.	<pre>root@aysr:~# ntpd --version ntpd 4.2.8p15@1.3728-o Fri May 21 19:24:13 UTC 2021 (1)</pre>

<p>Primero, se intenta localizar la biblioteca libedit mediante los comandos ls, find y ldconfig, confirmando su presencia en /usr/lib/libedit.so.0. Posteriormente, se ejecuta el comando ntpq -p, que muestra el estado de sincronización del servidor NTP. Se observa que el servidor está sincronizado con el host mrtg.wisp.net.e, con un estado óptimo de conexión (reach 377) y una desviación de tiempo aceptable. Esta salida confirma que el servidor NTP está funcionando correctamente y sincronizado con fuentes externas.</p>	<pre>root@aysr: # ls /usr/lib64/libedit.so* /bin/ls: cannot access '/usr/lib64/libedit.so*': No such file or directory root@aysr: # find /usr -name "libedit" root@aysr: # ldconfig -p grep libedit libedit.so.0 (libc6) => /usr/lib/libedit.so.0 root@aysr: # ntpq -p remote refid st t when poll reach delay offset jitter -----+ *LOCAL(0) .LOCL. 10 l 696 64 0 0.000 +0.000 0.000 *mrty.wisp.net.e 218.73.139.35 2 u 53 64 377 72.926 +12.649 14.599 +ntp.telecu.clou 192.58.120.8 2 u 68 64 377 25.199 +2.061 22.501 root@aysr: #</pre>
<p>En Solaris, se ejecuta el comando pkg list service/network/ntp, el resultado confirma que el paquete correspondiente al servicio NTP está instalado, con la versión 4.2.8.11.</p>	<pre>root@solaris:~# pkg list service/network/ntp NAME (PUBLISHER) VERSION IFO service/network/ntp 4.2.8.11-11.4.0.0.1.14.0 i--</pre>
<p>Utilizando nano, se modifica el contenido del archivo de configuración /etc/inet/ntp.conf en el sistema Solaris. Se ha especificado el servidor NTP con la dirección IP 10.2.77.185, correspondiente al servidor Slackware configurado previamente. El parámetro prefer indica que este servidor debe ser priorizado en la sincronización horaria. Esta configuración permite que Solaris actúe como cliente NTP, sincronizando su reloj con el servidor principal de la infraestructura.</p>	<p>server 10.2.77.185 prefer</p>
<p>Se ejecuto el comando ntpq -p en el sistema Solaris, ejecutado después de habilitar el servicio NTP con svcadm enable ntp. Esta verificación confirma que el cliente Solaris está sincronizando su reloj con el servidor Slackware como se requiere en el laboratorio.</p>	<pre>root@solaris:~# ntpq -p remote refid st t when poll reach delay offset jitter -----+ *10.2.77.185 179.60.247.252 3 u 66 64 37 0.311 -16.424 9.925 root@solaris:~#</pre>

En Windows Server para sincronizar con el servidor NTP ubicado en la dirección IP 10.2.77.185. Se utiliza el comando w32tm /config /manualpeerlist:"10.2.77.185" /syncfromflags:manual /reliable:YES /update para establecer el servidor NTP manualmente. Luego, se reinicia el servicio con net stop w32time y net start w32time, seguido de una sincronización forzada mediante w32tm /resync. Finalmente, el comando w32tm /query /status confirma que el sistema está sincronizado correctamente.

```
PS C:\Users\Administrator> w32tm /config /manualpeerlist:"10.2.77.185" /syncfromflags:manual /reliable:YES /update
date
The command completed successfully.
PS C:\Users\Administrator> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator> net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

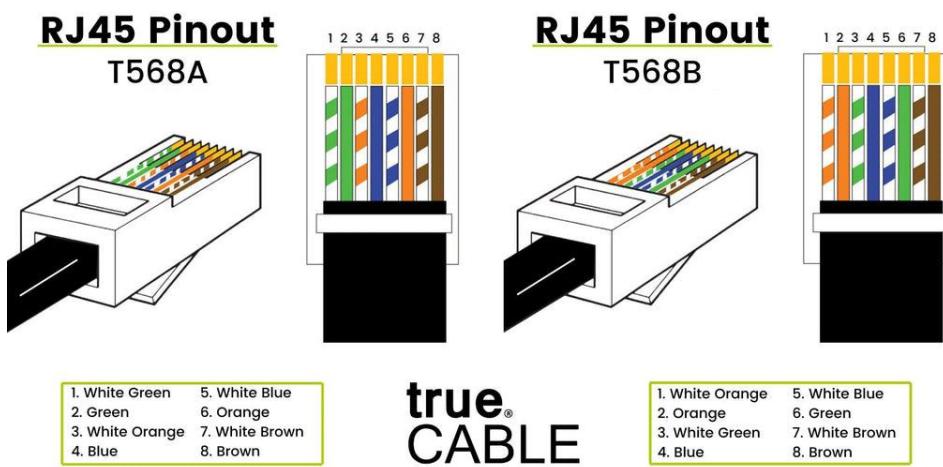
PS C:\Users\Administrator> w32tm /resync
Sending resync command to local computer
The command completed successfully.
PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.1377208s
Root Dispersion: 7.8342029s
ReferenceId: 0xA024DB9 (source IP: 10.2.77.185)
Last Successful Sync Time: 9/26/2025 11:33:03 AM
Source: 10.2.77.185
Poll Interval: 6 (64s)
```

Cableado estructurado y construcción de cables

En esta actividad, trabajaremos en conjunto para construir cables de red utilizando estándares de cableado estructurado. La tarea consiste en realizar la fabricación de cables tipo "directo" y "cruzado", cada uno con diferentes configuraciones de terminación, en los cuales tanto Santiago como Natalia participamos activamente. Santiago se encargó del ponchado de cables directos con los finales T568A, mientras que Natalia realizó los cables directos con terminaciones T568B. Además, ambos colaboramos en la creación de cables cruzados, utilizando una terminación T568A en un extremo y T568B en el otro. Posteriormente, realizamos pruebas para asegurarnos de que los cables estuvieran correctamente fabricados, utilizando un cable tester. Además, implementamos el panel de parcheo (patch panel) para establecer una conexión de red entre computadoras, probando la funcionalidad de la red a través de la herramienta ping.

Figura 34

T568A vs T568B. (trueCABLE, 2020). [Imagen]. Shopify.



Nota. Esta imagen ilustra las diferencias en la disposición de los cables según los estándares T568A y T568B, fundamentales para la correcta terminación de cables Ethernet.

En el proceso de fabricación de los cables, se utilizaron varias herramientas esenciales para asegurar la correcta crimpación y verificación de los cables de red. Entre las herramientas destacadas están los desforradores de cables, cortadores de cables, crimpadoras y testers de cables. Estas herramientas fueron necesarias tanto para el ponchado de los cables como para verificar la continuidad de las conexiones, asegurando que el cableado esté listo para su uso.

Figura 35

Materiales de Cableado



Nota. La fotografía se ven los cables UTP y los conectores RJ45, listos para ser utilizados en la fabricación de los cables.

Figura 36*Herramientas de Crimpado*

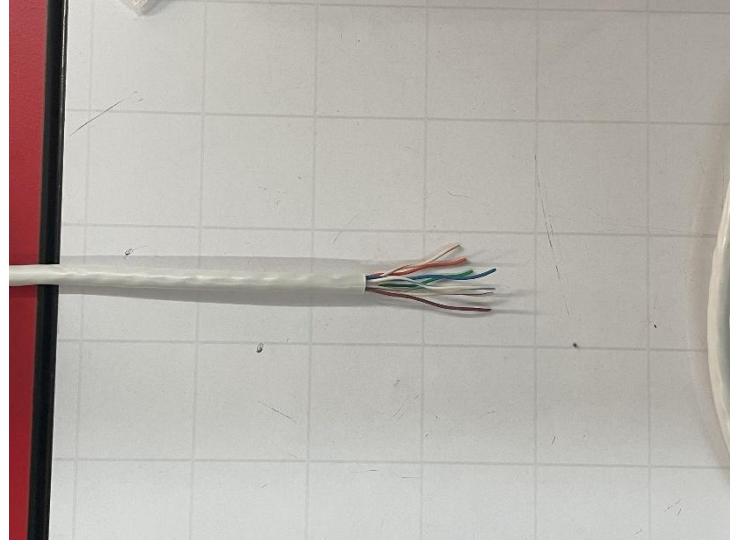
Nota. La fotografía muestra las herramientas necesarias para la fabricación de cables de red. De izquierda a derecha, vemos el desforrador de cables (para retirar el aislamiento de los cables), el cortador (para cortar los cables a la medida adecuada), la crimpadora (utilizada para insertar y asegurar los conectores RJ45 a los cables) y el tester de cables (para comprobar que la conexión de los cables sea correcta y que no haya fallos).

Figura 38*Patch Panel y Componentes de Cableado Adicionales*

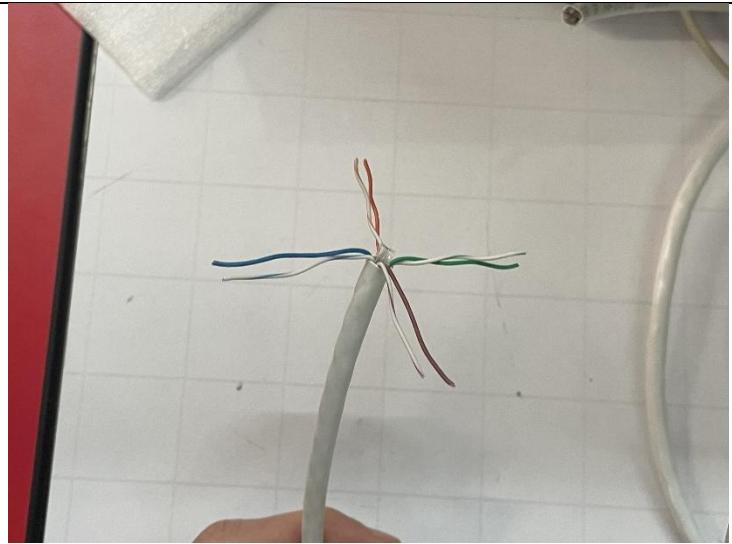
Nota. La imagen muestra un patch panel como parte de un sistema de cableado estructurado, utilizado para la organización y distribución de conexiones de red. Se observan bloques de ponchado con etiquetas de colores que siguen los estándares T568A y T568B, así como una tarjeta de circuito que indica integración electrónica. A la derecha, se incluyen conectores modulares tipo keystone, empleados para la terminación de cables UTP en instalaciones de red.

Implementación de Santiago: Cable Directo T568A y Cable Cruzado T568A/T568B

En esta sección, se detallará el proceso seguido por Santiago en la fabricación de los cables directos con terminación T568A y los cables cruzados con las terminaciones T568A/T568B. Santiago se encargó de realizar el ponchado de los cables siguiendo el estándar T568A para la terminación directa, asegurando la correcta disposición de los cables en el conector RJ45. También participó en la creación de los cables cruzados, donde se emparejaron las terminaciones T568A y T568B. Después de completar la crimpación, se verificó la continuidad de los cables utilizando un cable tester para asegurarse de que todo funcionara correctamente.

Descripción del Paso	Foto del Paso
1. Se utilizó el desfornecedor para retirar la capa exterior del cable UTP, dejando los hilos internos expuestos y listos para su manipulación. Este paso es esencial para poder trabajar con los cables de forma individual.	

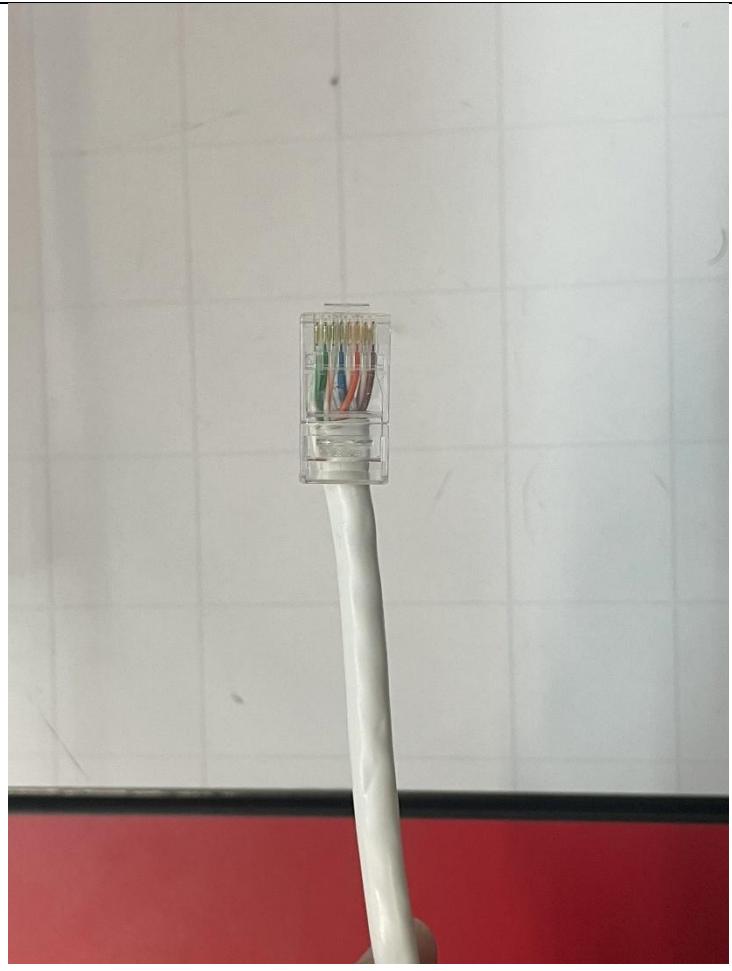
2. Se desamarraron los hilos internos del cable Cat6 y se cortó el divisor que separa los pares trenzados. Este divisor es utilizado para minimizar la interferencia y se eliminó para que los cables pudieran alinearse correctamente.



3. En este paso, los cables internos fueron alineados siguiendo el estándar T568A. Los cables fueron colocados en el orden correcto, de acuerdo con las posiciones específicas del conector RJ45, asegurando que cada uno de los cables estuviera en su lugar correcto. Luego, se utilizó un alicate para cortar los cables a la misma longitud, asegurando que todos los hilos fueran uniformes y estuvieran listos para ser insertados en el conector.



4. Una vez los cables fueron alineados y cortados, se procedió a ponchar ambos extremos de cada cable utilizando la crimpadora. Este proceso se repitió para todos los cables, tanto directos T568A y T568B, como cruzados T568A/T568B. Con todos los cables ponchados, se puede proceder con las pruebas de conectividad.



5. Se conectó el cable directo T568A al tester para verificar que cada uno de los hilos estuviera correctamente conectado. El tester mostró si las conexiones eran correctas y si el cable estaba listo para su uso en la red.

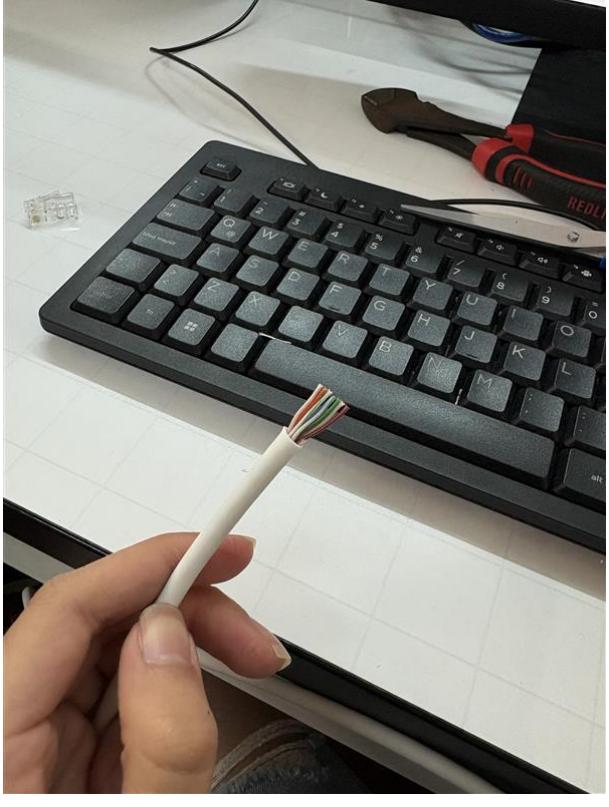


6. Se utilizó el tester para comprobar que el cable cruzado, con terminaciones T568A y T568B, estuviera correctamente crimpado. Esta prueba aseguró que el cable permitiera la comunicación adecuada entre dos dispositivos sin un hub o switch.

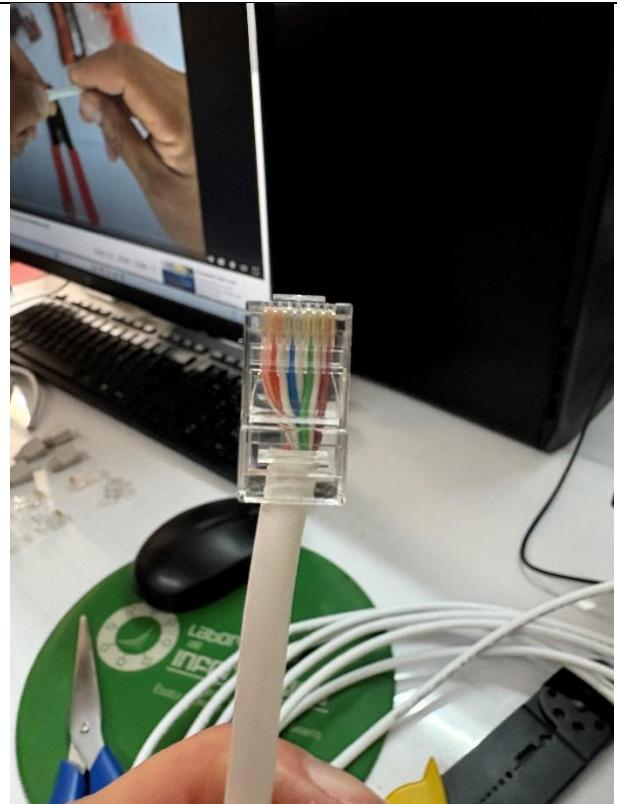


Implementación de Natalia: Cable Directo T568B y Cable Cruzado T568A/T568B

En este apartado, se describe el proceso realizado por Natalia para la fabricación de los cables directos con terminación T568B y los cables cruzados con terminaciones T568A/T568B. Natalia se encargó de realizar el ponchado de los cables directos siguiendo el estándar T568B en un extremo de los cables, y luego participó en la creación de los cables cruzados. En estos, la terminación T568B fue utilizada en un extremo y T568A en el otro, garantizando así la correcta disposición de los cables para la correcta comunicación entre dispositivos. Al igual que Santiago, Natalia utilizó un cable tester para comprobar la continuidad y asegurarse de que los cables estuvieran correctamente terminados.

Descripción del paso	Foto del paso
<p>Se organizaron los hilos internos del cable siguiendo el estándar T568B. Cada hilo fue colocado en el orden correcto según la disposición del conector RJ45, garantizando que estuvieran en la posición adecuada.</p> <p>Luego, se utilizó una herramienta de corte para igualar la longitud de los cables, asegurando que todos los hilos quedaran alineados y listos para ser insertados en el conector de manera uniforme.</p>	

Después de alinear y cortar los hilos del cable, se procedió a insertar y fijar ambos extremos en los conectores RJ45 utilizando la herramienta de crimpado. Este procedimiento se aplicó tanto a los cables rectos (siguiendo los estándares T568A y T568B) como a los cables cruzados (combinando T568A en un extremo y T568B en el otro). Una vez finalizado el crimpado de todos los cables, se realizaron pruebas de conectividad para verificar que la construcción fuera correcta y funcional.



Se conectó el cable directo con norma T568B al comprobador de cables para verificar que cada hilo estuviera correctamente posicionado. El dispositivo de prueba permitió confirmar si las conexiones internas eran adecuadas y si el cable estaba listo para funcionar correctamente dentro de la red.

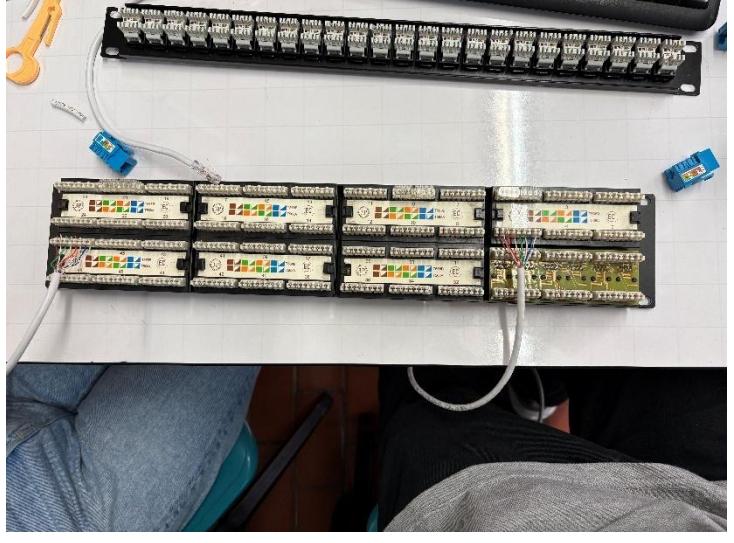


Se utilizó el comprobador de cables para verificar que el cable cruzado, con terminaciones T568A en un extremo y T568B en el otro, estuviera correctamente armado. Esta verificación permitió asegurar que el cable funcionara adecuadamente para establecer comunicación directa entre dos dispositivos sin necesidad de un switch o concentrador intermedio.



Ponchado con Patch Panel y Conexión de Máquinas

Usando el panel de parcheo y las caras de panel correspondientes, se configuró el sistema para realizar un ping entre las máquinas, verificando que la conectividad de la red estuviera funcionando correctamente. Este proceso permitió comprobar la funcionalidad de la red utilizando los cuatro cables previamente fabricados. Además, se utilizaron herramientas para asegurar que la conexión estuviera libre de fallas y con continuidad en la señal.

Descripción del paso	Foto del paso
<p>Se utilizó un patch panel como punto de distribución para el ponchado de los cables. En el lado izquierdo del panel se aplicó el estándar de cableado T568A, mientras que en el lado derecho se empleó el estándar T568B.</p>	
<p>Cada uno de los cables previamente ponchados en el patch panel fue terminado utilizando conectores modulares tipo keystone. Estos conectores fueron instalados para convertir las salidas del patch panel en conexiones directas</p>	

Se realizó una prueba de conectividad. Para ello, se conectó un cable directo entre los puertos frontales del patch panel, mientras que en la parte posterior de cada conector keystone se instalaron cables cruzados. Esta configuración fue diseñada para verificar la funcionalidad de las conexiones mediante el uso de un tester de red. El dispositivo mostró continuidad en todos los pares hasta el número 8.



Para probar el patch panel en un entorno real, se conectaron dos equipos mediante cables cruzados. A cada uno se le asignó una IP estática usando el comando netsh interface ip set address.

```
Microsoft Windows [Version 10.0.22631.5699]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>netsh interface ipv4 show interfaces
Idx Met MTU State Name
--- -- -- -- --
1 25 4294967295 connected Pseudo-Interface 1
16 25 1500 connected Ethernet 1
9 25 1500 connected Ethernet 2
11 35 1500 connected VMware Network Adapter VMnet1
17 35 1500 connected VMware Network Adapter VMnet8
7 5 1500 disconnected Ethernet 3

C:\Windows\System32>netsh interface ip set address name="Ethernet" static 10.2.77.100 255.255.0.0 10.2.65.1

C:\Windows\System32>
```

<p>Se asignó la IP 10.2.77.180 con máscara de subred 255.255.0.0 y puerta de enlace 10.2.65.1.</p>	<pre>Ethernet adapter Ethernet: Connection-specific DNS Suffix . : Description : Realtek PCIe GbE Family Controller Physical Address. : 18-60-24-DE-F2-A2 DHCP Enabled. : No Autoconfiguration Enabled : Yes Link-local IPv6 Address : fe80::9e65:8640:7990:64b1%16(PREFERRED) IPv4 Address. : 10.2.77.180(PREFERRED) Subnet Mask : 255.255.0.0 Default Gateway : 10.2.65.1 DHCPv6 IAID : 102260772 DHCPv6 Client DUID. : 00-01-00-01-2F-D4-C2-15-18-60-24-DE-F2-A2 DNS Servers : fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1 NetBIOS over Tcpip. : Enabled</pre>
<p>En la segunda máquina se asignó la IP 10.2.77.182, con máscara 255.255.0.0 y puerta de enlace 10.2.65.1.</p>	<pre>Ethernet adapter Ethernet 4: Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::ac59:4aa7:fd3e:ef85%18 IPv4 Address. : 10.2.77.182 Subnet Mask : 255.255.0.0 Default Gateway : 10.2.65.1</pre>
<p>Se realizó una prueba de conectividad desde la primera máquina hacia la segunda utilizando el comando ping con la dirección IP 10.2.77.182. La respuesta fue exitosa, con un tiempo promedio de 1 ms.</p>	<pre>C:\Windows\System32>ping 10.2.77.182 Pinging 10.2.77.182 with 32 bytes of data: Reply from 10.2.77.182: bytes=32 time=1ms TTL=128 Reply from 10.2.77.182: bytes=32 time=1ms TTL=128 Reply from 10.2.77.182: bytes=32 time=1ms TTL=128 Reply from 10.2.77.182: bytes=32 time=2ms TTL=128 Ping statistics for 10.2.77.182: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms C:\Windows\System32></pre>
<p>Desde la segunda máquina se realizó una prueba de conectividad hacia la primera utilizando el comando ping con la dirección IP 10.2.77.180. La respuesta fue exitosa, con un promedio de 1 ms.</p>	<pre>C:\Windows\System32>ping 10.2.77.180 Pinging 10.2.77.180 with 32 bytes of data: Reply from 10.2.77.180: bytes=32 time=1ms TTL=128 Ping statistics for 10.2.77.180: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms</pre>

Conocimiento del Cableado Estructurado de la Universidad

En el edificio I de la universidad se observa un gabinete de telecomunicaciones que alberga varios patch panels. Estos paneles permiten organizar y distribuir las conexiones de red mediante cables Ethernet, los cuales están conectados de forma ordenada y codificados por colores.

Figura 39

Estructuración del cableado en el edificio I de la Escuela



Nota. Gabinete mostrando el cableado estructurado en el edificio I de la Escuela. Los cables de colores, principalmente en tonos rojos y blancos, se organizan de manera ordenada dentro del armario, que parece ser parte de la infraestructura de red.

Conclusiones

Este laboratorio permitió comprobar de forma práctica que los protocolos de la capa de aplicación funcionan correctamente tanto en simulaciones como en redes reales. Se destacó la relevancia de servicios como DNS, HTTP, FTP, correo electrónico y NTP, fundamentales para mantener el flujo de información constante. También se evidenció que una buena configuración de parámetros IP, servidores de nombres y servicios de red requiere precisión para asegurar el funcionamiento estable de la red.

La combinación de Cisco Packet Tracer y Wireshark fue útil para validar que los servicios se comunican bien entre sí y que las capas del modelo OSI están alineadas. Las pruebas realizadas incluyeron resolución de nombres, envío y recepción de correos mediante SMTP y POP3, transferencia de archivos por FTP y sincronización horaria con NTP. Estas actividades ayudaron a comprender mejor cómo se monitorean y diagnostican redes distribuidas.

El análisis de tráfico con Wireshark permitió observar la encapsulación de datos y el comportamiento del protocolo TCP/IP, lo que aportó una visión más clara del flujo de información en redes actuales. Además, el armado físico de cables y el uso de paneles de conexión siguiendo las normas T568A y T568B ayudaron a garantizar una transmisión estable y a entender mejor la infraestructura física que sostiene los servicios de red.

En resumen, esta experiencia fortaleció conocimientos en la configuración de servicios lógicos, el análisis de tráfico de red y el montaje de infraestructura física.

Bibliografía

trueCABLE. (2020). T568A vs T568B [Imagen]. Shopify.

https://cdn.shopify.com/s/files/1/0014/6404/1539/files/T568A_vs_T568B_trueCABLE_1024x1024.jpg?v=1588882478