

Redes de Cómputo

Laboratorio No. 4 Protocolos, capa de aplicación y capa física

Integrantes:

Andrea Camila Torres González
Jorge Andrés Gamboa Sierra

Presentado a:
Fabian Eduardo Sierra Sánchez

Semestre 2024-2

Contenido

Resumen	8
Objetivos	8
Herramientas a utilizar	8
Introducción	8
Marco Teórico	9
Experimentos	12
1. Packet tracer.....	12
2. Configuración de red:	12
3. Configuración de serviciosDNS	21
4. Configuración de servicio HTTP	29
5. Configuración de servicio de Correo electrónico	38
6. Configuración de servicio FTP	52
En la red real	63
1. Wireshark	63
1.1. Captura web http://laboratorio.is.escuelaing.edu.co/	63
1.2. Captura tráfico DHCP	73
1.3. Captura tráfico TELNET y HTTP	78
2. Prueba con equipos servicio DNS	88
2.1. Escuelaing.edu.co.....	88
2.2. jbb.gov.co.....	91
2.3. google.com.....	95
2.4. Ikea.com.....	99
3. NTP Server.....	103
3.1. Configuración Servidor NTP en Linux Slackware	104
3.2. Configuración Cliente NTP en Solaris	106
3.3. Configuración Cliente NTP en Windows con GUI	107
3.4. Configuración Cliente NTP en Windows sin GUI	112
3.5. Configuración Cliente NTP en Android	115
4. Cableado estructurado y construcción de cables	120
4.1. Construcción de patch cord	121
4.1.1. Cable cruzado	122

4.1.2. Cable directo.....	127
4.2. Ponchado de patch panel.....	131
 4.2.1. Prueba de ponchado en patch panel y faceplate con cable directo	132
 4.2.2. Prueba de ponchado en patch panel con cable cruzado y faceplate con cable directo	137
 4.2.3. Pruebas de ponchado con cable directo en patch panel y cruzado en faceplate	138
 4.2.4. Prueba de ponchado en patch panel y faceplate con cable cruzado	139
4.3. Conocimiento el Cableado estructurado de la Escuela.....	140
Conclusiones.....	141
Bibliografía	142

Tabla de Imágenes

Imagen No. 1 Modelado del funcionamiento de una red	9
Imagen No. 2 Ejemplo de modelado de servidores y clientes en packet tracer	12
Ilustración 3 ejemplo de configuración de red realizado	13
Ilustración 4 configuración mail.sistemas.com	13
Ilustración 5 configuración www.sistemas.com	14
Ilustración 6 configuración servidor DNS	14
Ilustración 7 configuración cliente estudianteS1	14
Ilustración 8 configuración cliente estudianteS2	15
Ilustración 9 configuración www.civil.com	15
Ilustración 10 configuración correo.civil.com	16
Ilustración 11 configuración cliente EstudianteC1	16
Ilustración 12 configuración EstudianteC2	16
Ilustración 13 Configuración servidor Correo	17
Ilustración 14 configuración cliente EstudianteE1	17
Ilustración 15 configuración cliente EstudianteE2	17
Ilustración 16 prueba conexión 1	18
Ilustración 17 prueba conexión 2	19
Ilustración 18 prueba conexión 3	20
Ilustración 19 configuración DNS 1	21
Ilustración 20 configuración DNS 2	21
Ilustración 21 configuración DNS 3	21
Ilustración 22 configuración DNS 3	21
Ilustración 23 configuración DNS 4	22
Ilustración 24 configuración DNS 5	22
Ilustración 25 configuración DNS 6	22
Ilustración 26 configuración DNS 7	22
Ilustración 27 configuración DNS 8	22
Ilustración 28 configuración DNS 9	22
Ilustración 29 configuración DNS 10.....	22
Ilustración 30 configuración DNS 11.....	23

Ilustración 31 configuración DNS 12	23
Ilustración 32 configuración general parte 1	24
Ilustración 33 configuración general parte 2	24
Ilustración 34 activación servicio DNS	25
Ilustración 35 prueba DNS 1	26
Ilustración 36 prueba DNS 2	27
Ilustración 37 prueba DNS 3	28
Ilustración 38 configuración servidor web sistemas	29
Ilustración 39 personalización página web sistemas	30
Ilustración 40 configuración servidor web Civil	31
Ilustración 41 personalización página web Civil	32
Ilustración 42 consulta 1	33
Ilustración 43 consulta 2	33
Ilustración 44 consulta 3	34
Ilustración 45 consulta 4	34
Ilustración 46 PDU consulta HTTP	35
Ilustración 47 DPU cierre conexión HTTP	36
Ilustración 48 DPU consulta DNS	37
Ilustración 49 PDU resolución de consulta DNS	38
Ilustración 50 configuración usuarios y dominio sistemas	39
Ilustración 51 configuración usuarios y dominio civil	40
Ilustración 52 configuración usuarios y dominio eléctrica	40
Ilustración 53 configuración correo estudianteS1	41
Ilustración 54 configuración correo estudianteS2	41
Ilustración 55 configuración correo EstudianteC1	42
Ilustración 56 configuración correo EstudianteC2	42
Ilustración 57 configuración correo EstudianteE1	43
Ilustración 58 configuración correo EstudianteE2	43
Ilustración 59 envío correo 1	44
Ilustración 60 envío correo 2	44
Ilustración 61 envío correo 3	45
Ilustración 62 respuesta correo 1	45
Ilustración 63 respuesta correo 2	46
Ilustración 64 respuesta correo 3	46
Ilustración 65 envío correo otro dominio 1	47
Ilustración 66 envío correo otro dominio 2	47
Ilustración 67 envío correo otro dominio 3	48
Ilustración 68 envío correo otro dominio 1	48
Ilustración 69 respuesta envío correo otro dominio 2	49
Ilustración 70 respuesta envío correo otro dominio 3	49
Ilustración 71 PDU SMTP	50
Ilustración 72 PDU POP3	51
Ilustración 73 configuración FTP usuario y contraseña	52
Ilustración 74 inicio FTP	53
Ilustración 75 ingreso servidor FTP	53
Ilustración 76 revisión archivos del servidor	53

Ilustración 77 descarga de archivo servidor a cliente	54
Ilustración 78 cierre sesión	54
Ilustración 79 conexión y transferencia a servidor.....	55
Ilustración 80 verificación del archivo subido al servidor.....	55
Ilustración 81 finalización de sesión	56
Ilustración 82 solicitud conexión	56
Ilustración 83 validación contraseña correcta	57
Ilustración 84 validación correcta	58
Ilustración 85 proceso transferencia de documentos	59
Ilustración 86 transferencia de datos 1.....	59
Ilustración 87 transferencia de datos 2.....	59
Ilustración 88 transferencia de datos 3.....	60
Ilustración 89 transferencia de datos 4.....	60
Ilustración 90 transferencia de datos 5.....	60
Ilustración 91 transferencia de datos 6.....	60
Ilustración 92 transferencia de datos 7.....	60
Ilustración 93 transferencia de datos 8.....	61
Ilustración 94 proceso revisión documentos	61
Ilustración 95 traspaso de datos 1	61
Ilustración 96 traspaso de datos 2	61
Ilustración 97 traspaso de datos 3	62
Ilustración 98 traspaso de datos 4	62
Ilustración 99 traspaso de datos 5	62
Ilustración 100 traspaso de datos 6	62
Ilustración 101 traspaso de datos 7	62
Ilustración 102 cierre sesión 1	63
Ilustración 103 cierre sesión 2	63
Imagen No 104. Capturas DNS del dominio laboratorio.escuelaing.edu.co.....	64
Imagen No 105. Paquetes específicos del funcionamiento DNS	64
Imagen No 106. Paquete DNS cliente al servidor DNS laboratorio.is.escuelaing.edu.co	65
Imagen No. 107 Captura de la respuesta del servidor DNS	66
Imagen No. 108 Paquete de respuesta del servidor DNS al cliente	67
Imagen No. 109 Captura del tráfico del servidor web de laboratorio.is.escuelaing.edu.co	68
Imagen No. 110 Captura del tráfico del protocolo HTTP.....	68
Imagen No. 111 Paquete del primer GET del cliente al servidor web.....	69
Imagen No. 112 Paquete de respuesta 200 del servidor web al cliente	70
Imagen No. 113 Segundo GET del cliente al servidor web	71
Imagen No. 114 Paquete de respuesta 404 del servidor web al cliente	72
Imagen No. 115 Capturas del servidor web al interactuar con la página varias veces.....	73
Imagen No. 116 Desactivar la ip actual del computador	73
Imagen No. 117 Capturas del servicio DHCP	74
Imagen No. 118 Filtro del protocolo DHCP	74
Imagen No. 119 Paquete del mensaje Discover	75
Imagen No. 120 Paquete del mensaje Offer	76
Imagen No. 121 Paquete del mensaje Request	77
Imagen No. 122 Paquete del mensaje Acknowledge.....	78

Ilustración 123 configuración cliente Telnet.....	79
Ilustración 124 configuración ventana de ajustes.....	79
Ilustración 125 Selección programas y características	80
Ilustración 126 activación de características especiales de Windows.....	80
Ilustración 127 activación cliente telnet	80
Ilustración 128 inicio conexión mediante telnet.....	81
Ilustración 129 respuesta solicitud get index.html	81
Ilustración 130 captura paquetes.....	81
Ilustración 131 captura solicitud index.html	82
Ilustración 132 respuesta solicitud get prueba.pdf	82
Ilustración 133 captura de paquetes	83
Ilustración 134 captura solicitud get prueba.pdf	83
Ilustración 135 visualización solicitud network.png	84
Ilustración 136 consulta wireShark	84
Ilustración 137 visualización solicitud get network.png.....	85
Ilustración 138 visualización index.html	85
Ilustración 139 visualización prueba.pdf	85
Ilustración 140 visualización network.png	86
Ilustración 141 captura de telnet con wireShark.....	86
Imagen No. 142 Búsqueda del dominio escuelaing.edu.co.....	88
Imagen No. 143 Información general del servicio DNS de escuelaing.edu.co	89
Imagen No. 144 Información del propietario del servidor DNS de escuelaing.edu.co	89
Imagen No. 145 Registros de nombres de dominios del servidor DNS escuelaing.edu.co	90
Imagen No. 146 Búsqueda del dominio jbb.gov.co.....	91
Imagen No. 147 Información general del servicio DNS jbb.gov.co.....	92
Imagen No. 148 Información del propietario del servidor DNS jbb.gov.co	93
Imagen No. 149 Registros de los nombres de dominio del servidor DNS jbb.gov.co	93
Imagen No. 150 Búsqueda del dominio google.com.....	95
Imagen No. 151 Información general del servicio DNS de google.com	96
Imagen No. 152 Información del propietario del servidor DNS google.com	97
Imagen No. 153 Registro de los nombres de dominio del servidor DNS google.com	98
Imagen No. 154 Búsqueda del dominio ikea.com	100
Imagen No. 155 Información general del servicio DNS ikea.com.....	101
Imagen No. 156 Información del propietario del servidor DNS ikea.com	102
Imagen No. 157 Registros de los nombres de dominio de ikea.com	102
Imagen No. 158 Montaje del disco óptico	104
Imagen No. 159 Navegación entre las carpetas del disco óptico	104
Imagen No. 160 Instalación NTP	105
Imagen No. 161 Configuración NTP Server	105
Imagen No. 162 Configurar clientes en el servidor	106
Imagen No. 163 Iniciar servicio NTP.....	106
Imagen No. 164 Prueba del funcionamiento del servidor NTP	106
Imagen No. 165 Archivo de configuración NTP cliente en Solaris.....	107
Imagen No. 166 Prueba como cliente NTP en Solaris	107
Imagen No. 167 Panel de control de Windows.....	108
Imagen No. 168 Configuración NTP cliente en Windows	109

Imagen No. 169 Configuración del servidor NTP en Windows	110
Imagen No. 170 Configuración de la zona horario de Windows	111
Imagen No. 171 Sincronización con el servidor NTP en Windows	112
Imagen No. 172 Interfaz de configuración de Windows	113
Imagen No. 173 Zona horaria de Windows	114
Imagen No. 174 Sincronización con el servidor NTP en Windows sin GUI.....	115
Imagen No. 175 Instalación de la aplicación NTP en Android	116
Imagen No. 176 Interfaz de la aplicación NTP en Android	117
Imagen No. 177 Vinculo con el servidor NTP en Android.....	118
Imagen No. 178 Sincronización con el servidor NTP en Android	119
Imagen No. 179 Comprobación de la hora de Android con la hora del sistema.....	120
Imagen No. 180 Estandarización de la disposición de cables de red	121
Imagen No. 181 Materiales para la construcción de los cables de red	121
Imagen No. 182 Conductores internos del cable rj45.....	122
Imagen No. 183 Ordenamiento de los cables siguiendo el estándar.....	122
Imagen No. 184 Acomodación de los cables en el conector rj45	123
Imagen No. 185 Empalme del conector rj45 de un cable cruzado.....	124
Imagen No. 186 Resultado final de la construcción del cable cruzado.....	124
Imagen No. 187 Prueba 1 y 2 del cable cruzado.....	125
Imagen No. 188 Prueba 3 y 4 del cable cruzado.....	125
Imagen No. 189 Prueba 5 y 6 del cable cruzado.....	126
Imagen No. 190 Prueba 7 y 8 del cable cruzado.....	126
Imagen No. 191 Empalme del conector rj45 de un cable directo.....	127
Imagen No. 192 Resultado final de la construcción del cable directo	127
Imagen No. 193 Prueba 1 del cable directo.....	128
Imagen No. 194 Prueba 2 del cable directo.....	128
Imagen No. 195 Prueba 3 del cable directo.....	129
Imagen No. 196 Prueba 4 del cable directo.....	129
Imagen No. 197 Prueba 5 del cable directo.....	130
Imagen No. 198 Prueba 6 y 7 del cable directo	130
Imagen No. 199 Prueba 7 y 8 del cable directo	131

Resumen

Este informe presenta la configuración de servidores DNS, HTTP, MAIL y FTP en Packet Tracer, así como la captura de paquetes con Wireshark para analizar protocolos de la capa de aplicación. Se utiliza CentralOps para obtener información de un dominio y se configura NTP para sincronizar relojes en un servidor. También se construyen cables directos y cruzados, probándolos con un patch panel para entender su funcionamiento.

Palabras clave: Servidor, protocolo, red, estándar.

Objetivos

- Seguimiento a protocolos de la capa de aplicación
- Revisar el estándar de cableado estructurado y su aplicación.
- Realizar ponchado de cables con conectores RJ-45 y patch panel.

Herramientas a utilizar

- Elementos provistos por la Escuela
 - Computadores
 - Acceso a Internet
 - Patch panel y face plate
 - Ponchadoras (para patchcords y de golpe)
 - Pelacables y corta fríos
 - Probador de cables
- Elementos que deben traer los estudiantes
 - 4 a 6 metros de cable UTP/FTP cat. 6
 - 8 conectores RJ-45
 - Si tienen:
 - Pelacable o bisturí, corta fríos
 - ponchadora para patchcord
 - Probador de cables

Introducción

Seguimos trabajando sobre una infraestructura de una empresa, la cual normalmente cuenta con varios servicios de infraestructura TI. En ella se encuentran estaciones de usuario alámbricas e inalámbricos y servidores (físicos y virtualizados), todos estos conectados a través de switches (capa 2 y 3), equipos inalámbricos y routers que lo conectan a Internet. También es común contar con infraestructuras en la nube desde donde se provisionan recursos según las necesidades de la organización. Dentro de los servidores se pueden encontrar servicios web, DNS, correo, base de datos, almacenamiento y aplicaciones, entre otros. Recordemos la configuración que estamos usando de base:

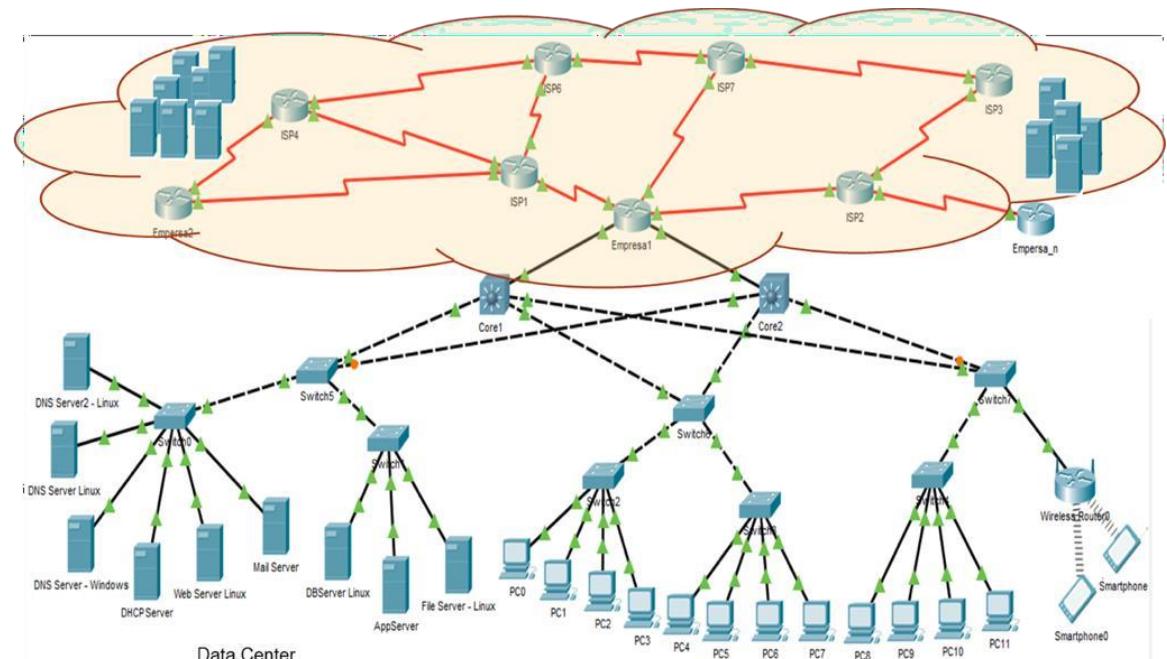


Imagen No. 1 Modelado del funcionamiento de una red

En este laboratorio nos enfocaremos en pruebas de protocolos de la capa de aplicación y realizaremos actividades de la capa física.

Marco Teórico

- **Cables UTP (Unshielded Twisted Pair):** Los cables UTP son un tipo de cable de par trenzado sin blindaje, ampliamente utilizados en redes de área local (LAN). Están compuestos por pares de conductores de cobre trenzados entre sí para reducir la interferencia electromagnética (EMI) y la diafonía. Los cables UTP son categorizados según su rendimiento, siendo las categorías más comunes CAT5e, CAT6 y CAT6a, que soportan diferentes velocidades de transmisión y frecuencias.
- **Cables FTP (Foiled Twisted Pair):** Los cables FTP, también conocidos como cables de par trenzado con blindaje de lámina, tienen una capa de blindaje de aluminio o lámina de poliéster que envuelve todos los pares de cables, proporcionando una protección adicional contra las interferencias externas. Este blindaje ayuda a mejorar la calidad de la señal y la integridad de la transmisión, especialmente en entornos con alta interferencia electromagnética.

- **Cable Directo:** El cable directo es un tipo de cable de red en el cual los pines de los conectores en ambos extremos siguen el mismo orden. Este tipo de cable se utiliza principalmente para conectar diferentes tipos de dispositivos, como un computador a un switch o un router. El estándar más comúnmente utilizado para el cableado directo es el T568B en ambos extremos.
- **Cable Cruzado:** El cable cruzado es un tipo de cable de red donde los pines de los conectores en cada extremo están invertidos, específicamente cruzando los pares de transmisión y recepción. Este tipo de cable se utiliza para conectar dispositivos similares entre sí, como dos computadores directamente o dos switches. Un extremo sigue el estándar T568A y el otro el T568B.
- **Servicio de NTP:** NTP es un protocolo utilizado para sincronizar los relojes de los dispositivos en una red. Asegura que todos los dispositivos tengan la misma hora, lo cual es crucial para aplicaciones que requieren una sincronización precisa de eventos y registros de tiempo, como la seguridad, la coordinación de eventos de red y la administración de sistemas. NTP funciona utilizando un algoritmo jerárquico que distribuye la hora desde servidores maestros hasta clientes.
- **DNS** Sistema de nomenclatura jerárquico y descentralizado utilizado para resolver nombres de dominio en direcciones IP. Actúa como una "agenda telefónica" de Internet, permitiendo a los usuarios acceder a sitios web mediante nombres de dominio legibles en lugar de memorizar direcciones IP numéricas. Los servidores DNS realizan consultas recursivas y iterativas para traducir un nombre de dominio a su correspondiente dirección IP, facilitando la navegación en la red.
- **HTTP** es el protocolo base de la World Wide Web, utilizado para la transferencia de recursos como documentos HTML, imágenes, videos y otros tipos de datos. Opera sobre una arquitectura cliente-servidor, donde el cliente envía solicitudes HTTP al servidor, que a su vez responde con los recursos solicitados. HTTP es un protocolo sin estado, lo que significa que cada solicitud es independiente y no mantiene información sobre solicitudes anteriores.
- **FTP** es un protocolo estándar de red utilizado para la transferencia de archivos entre un cliente y un servidor en una red TCP/IP. FTP permite a los usuarios cargar, descargar, eliminar y renombrar archivos en un servidor remoto. Existen dos modos de conexión: modo activo y modo pasivo, que determinan cómo se establecen las conexiones de datos y control entre el cliente y el servidor.

- **Servicio de Correo** El servicio de correo electrónico en redes se basa en varios protocolos para la transferencia y acceso a los mensajes. Los más comunes son:
 - **SMTP:** Utilizado para enviar correos desde un cliente a un servidor de correo o entre servidores de correo.
 - **POP3:** Permite a los usuarios descargar correos desde un servidor a su dispositivo local y luego eliminarlos del servidor.
 - **IMAP:** Permite a los usuarios acceder y gestionar sus correos directamente en el servidor, manteniendo una copia en el servidor y sincronizando las acciones realizadas en diferentes dispositivos.
- **Filtro en Wireshark:** Wireshark es una herramienta de análisis de protocolos de red que permite capturar y examinar el tráfico de la red en tiempo real. Los filtros en Wireshark son utilizados para aislar y analizar paquetes específicos entre una gran cantidad de datos capturados. Existen dos tipos principales de filtros:
 - **Filtros de captura:** Aplicados durante la captura de paquetes para limitar los datos almacenados.
 - **Filtros de visualización:** Utilizados después de la captura para mostrar únicamente los paquetes que cumplen con ciertos criterios, como direcciones IP específicas, puertos, protocolos, etc. Esto facilita el análisis detallado y la resolución de problemas en la red.

Experimentos

Entender la manera como circulan mensajes sobre la red y poder analizar los contenidos de ellos es importante para hacer revisiones y afinamientos de la red. En esta parte del Laboratorio vamos a revisar la información de los protocolos de la capa de aplicación y capa de transporte (solo los puertos) que hemos visto.

1. Packet tracer

Como parte de nuestra práctica en el uso de Cisco Packet Tracer, se nos asignó la tarea de configurar una red específica y documentar nuestra experiencia. A continuación, se detallan los pasos que seguí para completar esta actividad, incluyendo la configuración de los servicios de DNS, HTTP, FTP y correo electrónico en los servidores de la red.

2. Configuración de red:

- A continuación, se van a incluir todos los servidores y clientes presentados junto con sus respectivas conexiones, a cada equipo se le asignará un DNS, Gateway, Dirección IP y máscara según el siguiente esquema:

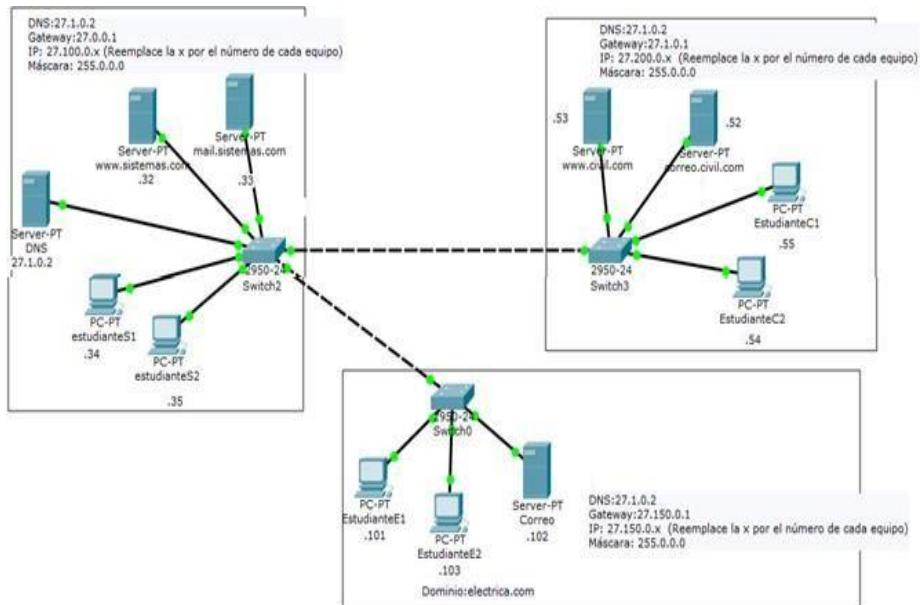


Imagen No. 2 Ejemplo de modelado de servidores y clientes en packet tracer

UNIVERSIDAD

Se crean los respectivos servidores y clientes, luego se asigna un cableado, cruzado para dispositivos similares y directo para dispositivos diferentes. También cambiamos el nombre de cada equipo

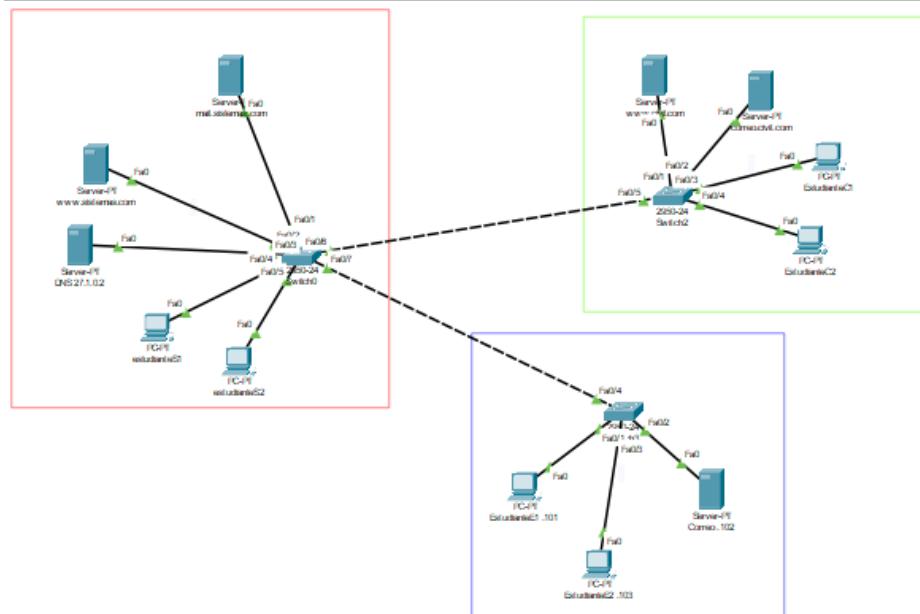


Ilustración 3 ejemplo de configuración de red realizado

Se configuran los diferentes dispositivos con su IP, servidor DNS, Gateway y máscara.

- Dominio Sistemas

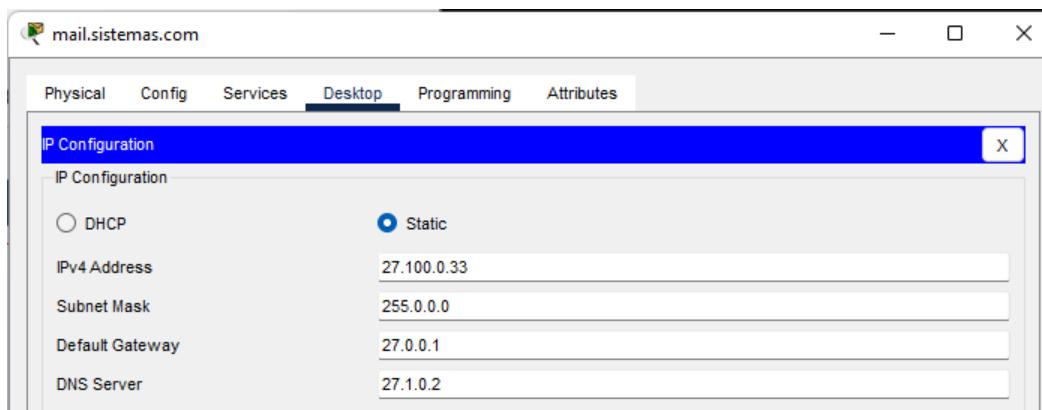


Ilustración 4 configuración mail.sistemas.com

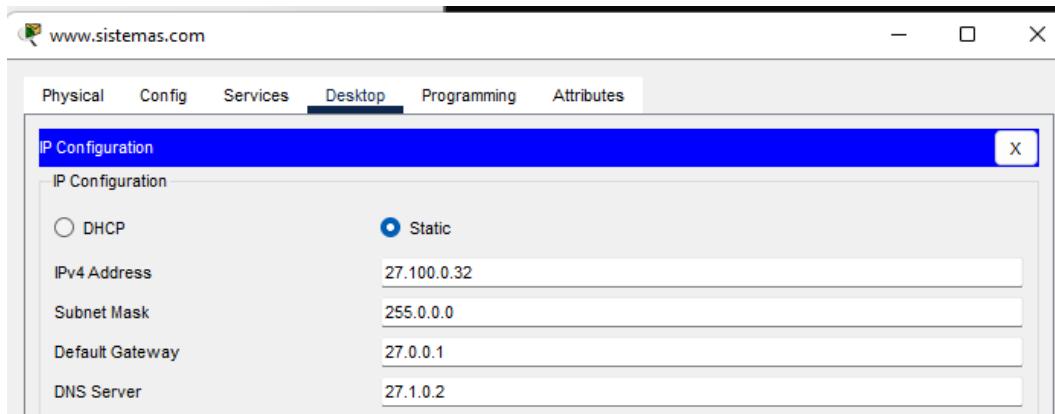


Ilustración 5 configuración www.sistemas.com

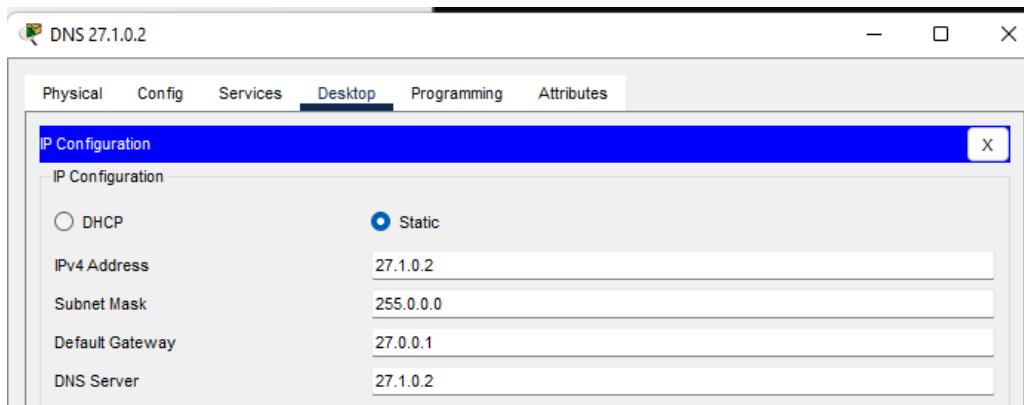


Ilustración 6 configuración servidor DNS

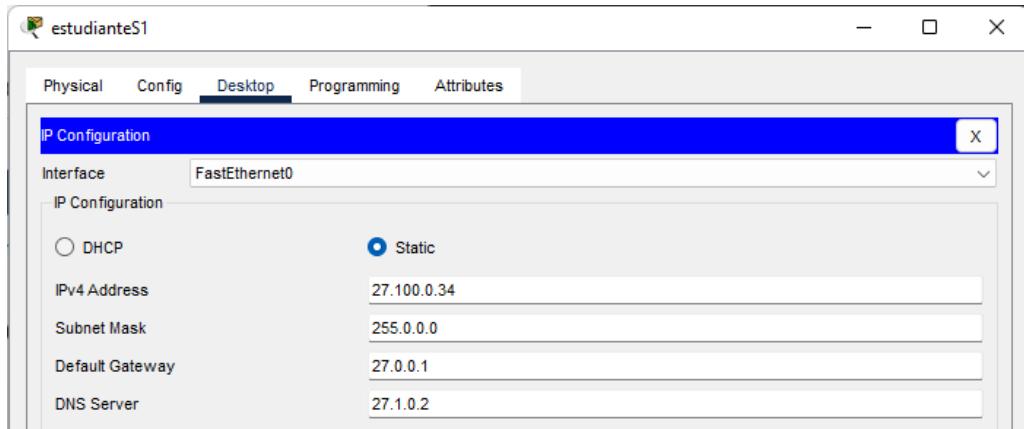


Ilustración 7 configuración cliente estudianteS1

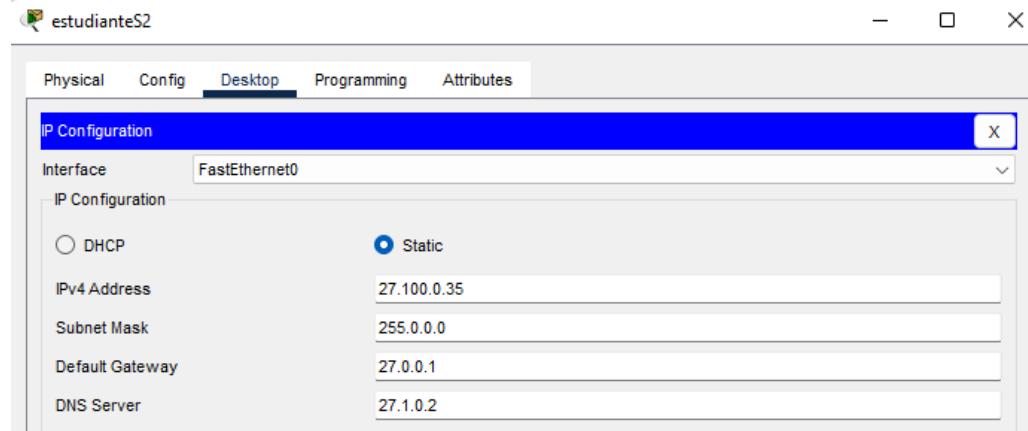


Ilustración 8 configuración cliente estudianteS2

- Dominio Civil

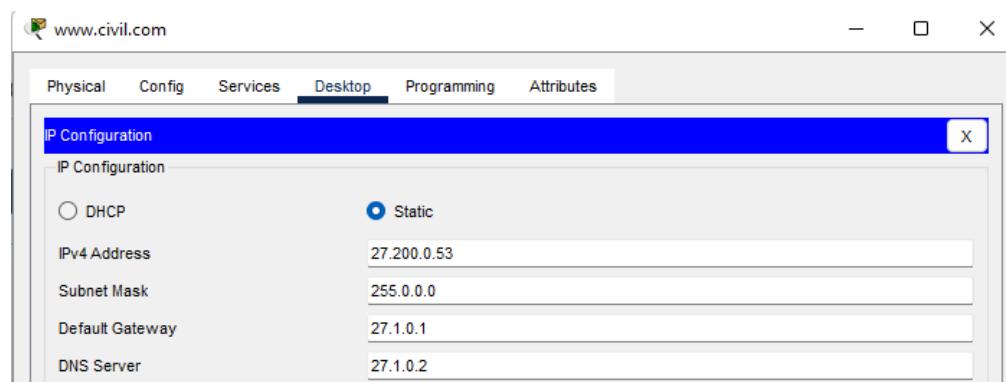


Ilustración 9 configuración www.civil.com

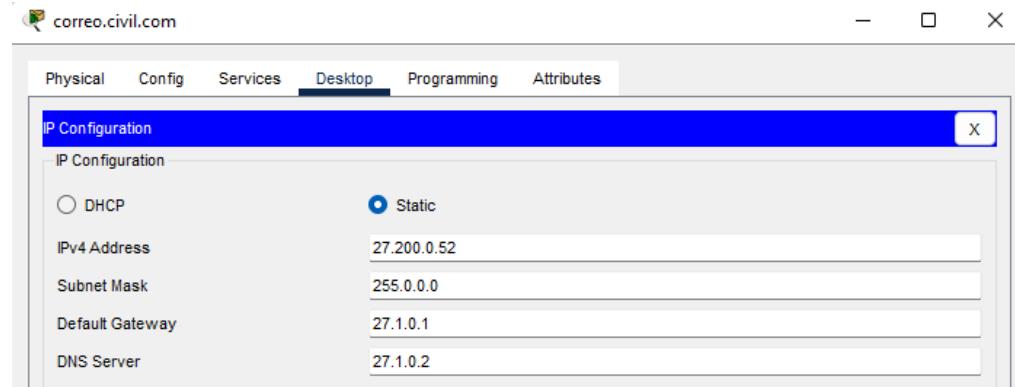


Ilustración 10 configuración correo.civil.com

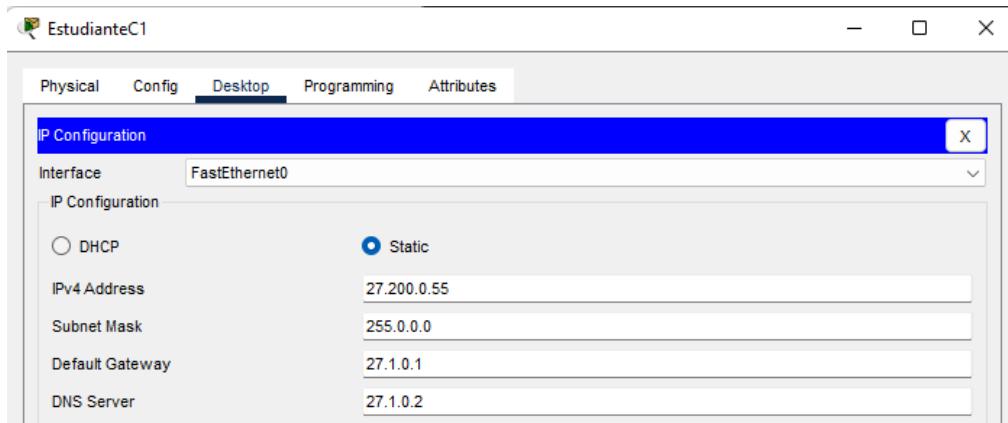


Ilustración 11 configuración cliente EstudianteC1

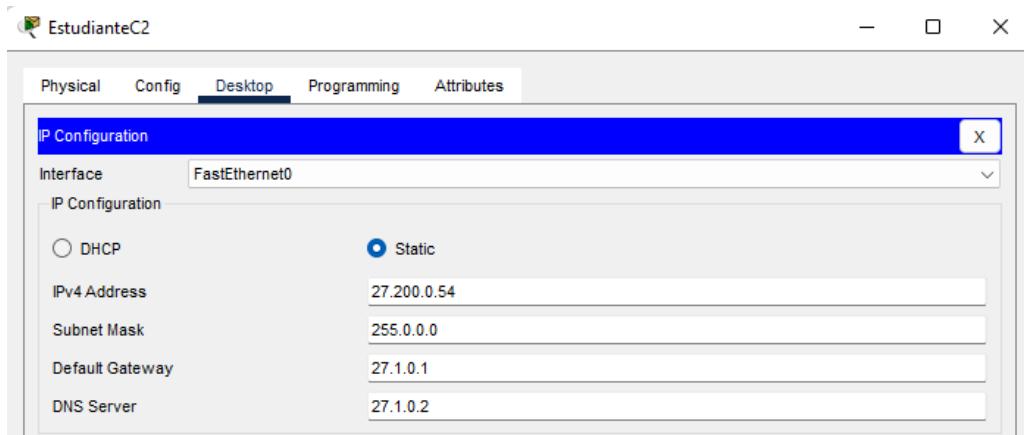


Ilustración 12 configuración EstudianteC2

- Dominio Eléctrica

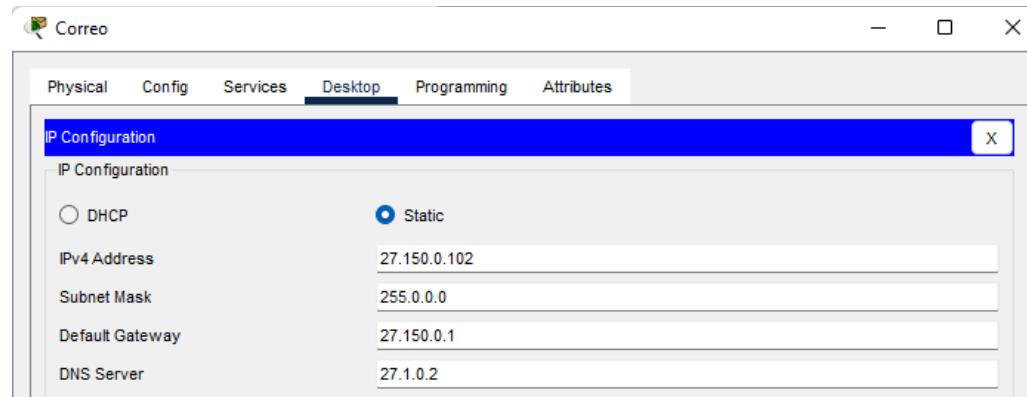


Ilustración 13 Configuración servidor Correo

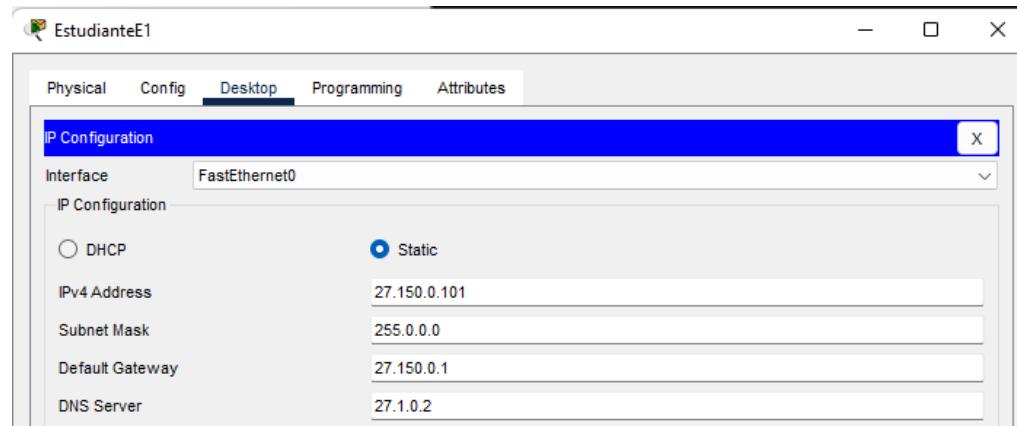


Ilustración 14 configuración cliente EstudianteE1

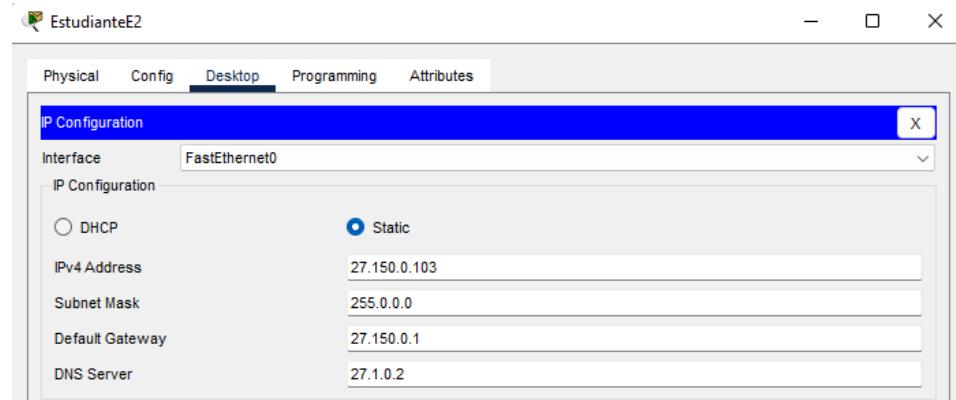
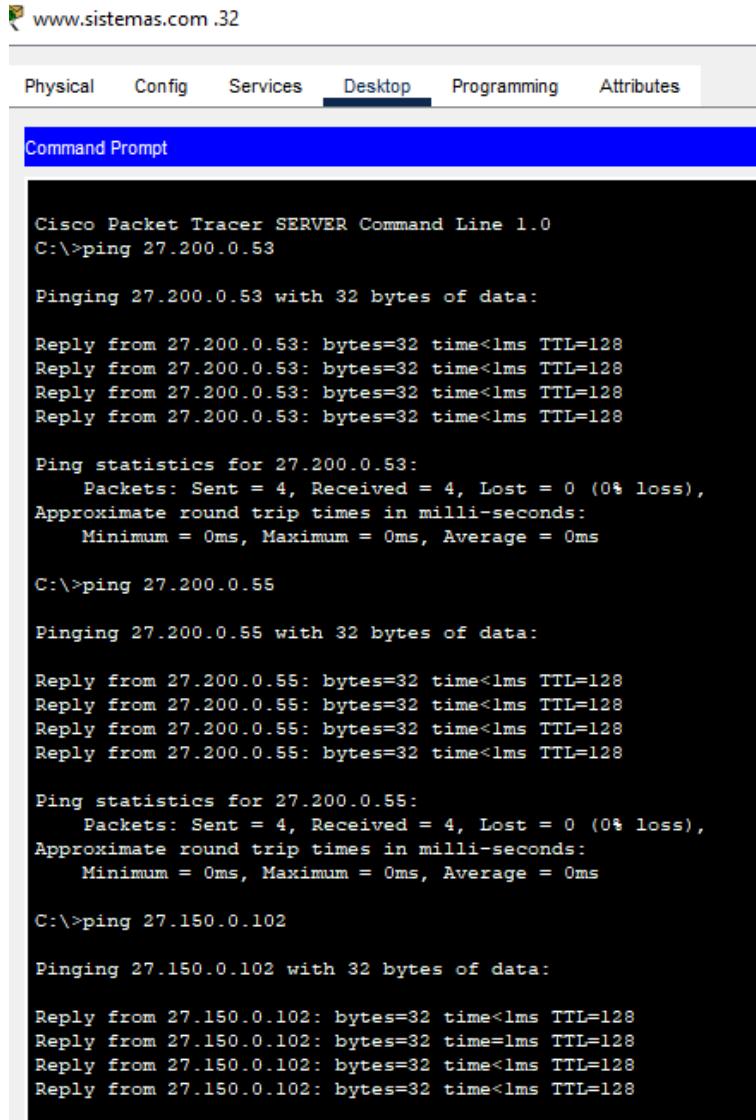


Ilustración 15 configuración cliente EstudianteE2

- A continuación, se envían mensajes entre los equipos de la red y se verifica la conectividad entre todos ellos.
 - Prueba de www.sistemas.com a www.civil.com, EstudianteC1 y Correo



www.sistemas.com .32

Physical Config Services Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 27.200.0.53

Pinging 27.200.0.53 with 32 bytes of data:

Reply from 27.200.0.53: bytes=32 time<lms 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 27.200.0.55

Pinging 27.200.0.55 with 32 bytes of data:

Reply from 27.200.0.55: bytes=32 time<lms TTL=128

Ping statistics for 27.200.0.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

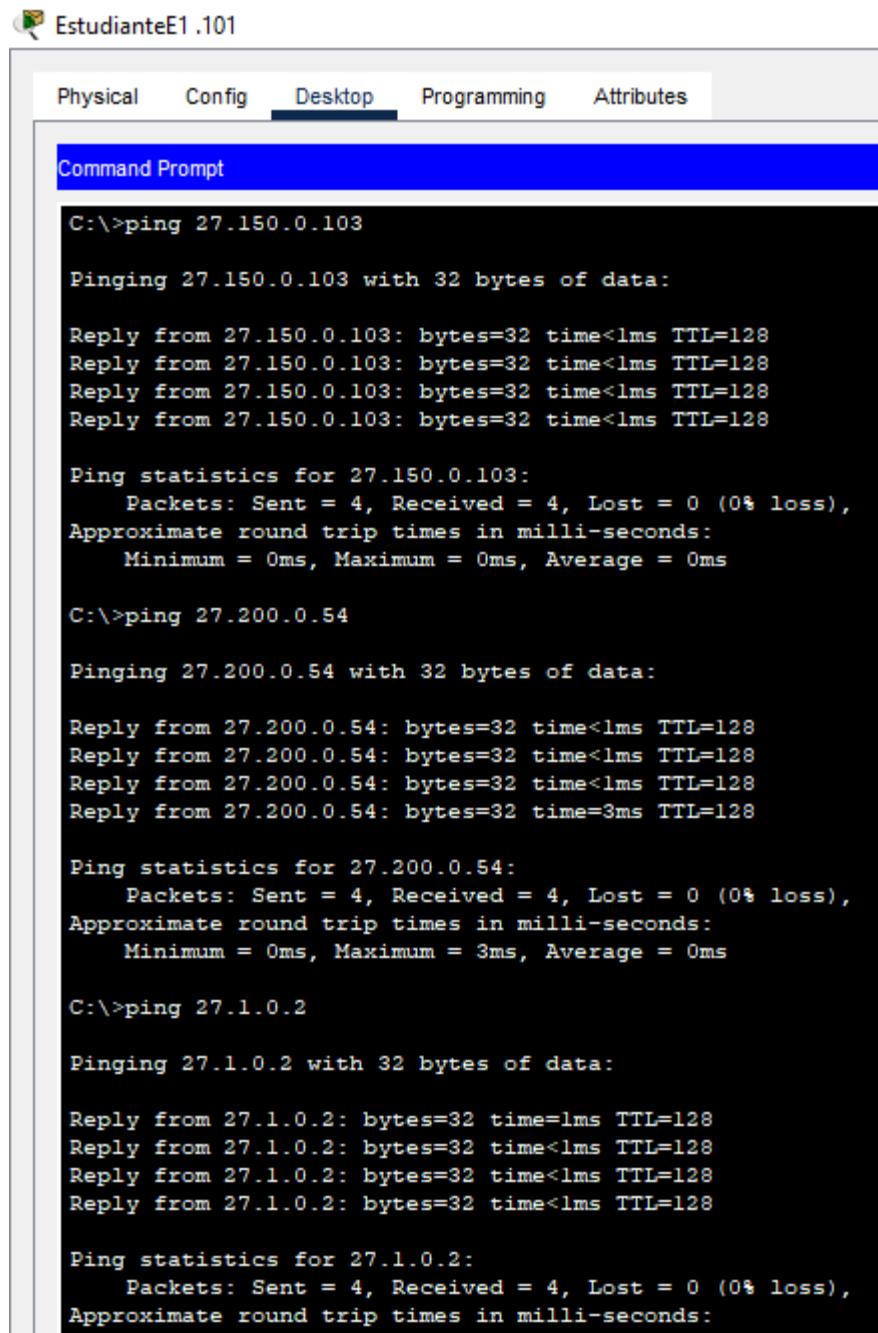
C:\>ping 27.150.0.102

Pinging 27.150.0.102 with 32 bytes of data:

Reply from 27.150.0.102: bytes=32 time<lms TTL=128
Reply from 27.150.0.102: bytes=32 time=lms TTL=128
Reply from 27.150.0.102: bytes=32 time<lms TTL=128
Reply from 27.150.0.102: bytes=32 time<lms TTL=128
```

Ilustración 16 prueba conexión 1

- Prueba de EstudianteE1 a EstudianteE2, EstudianteC2 y DNS



EstudianteE1.101

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 27.150.0.103

Pinging 27.150.0.103 with 32 bytes of data:

Reply from 27.150.0.103: bytes=32 time<1ms TTL=128

Ping statistics for 27.150.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 27.200.0.54

Pinging 27.200.0.54 with 32 bytes of data:

Reply from 27.200.0.54: bytes=32 time<1ms TTL=128
Reply from 27.200.0.54: bytes=32 time<1ms TTL=128
Reply from 27.200.0.54: bytes=32 time<1ms TTL=128
Reply from 27.200.0.54: bytes=32 time=3ms TTL=128

Ping statistics for 27.200.0.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>ping 27.1.0.2

Pinging 27.1.0.2 with 32 bytes of data:

Reply from 27.1.0.2: bytes=32 time=1ms TTL=128
Reply from 27.1.0.2: bytes=32 time<1ms TTL=128
Reply from 27.1.0.2: bytes=32 time<1ms TTL=128
Reply from 27.1.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 27.1.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

Ilustración 17 prueba conexión 2

- De estudianteS1 a www.civil.com, Correo y mail.sistemas.com

1 estudianteS1 .34

Physical	Config	Desktop	Programming	Attributes
----------	--------	---------	-------------	------------

Command Prompt

```
C:\>ping 27.200.0.53

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 27.150.0.102

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 27.100.0.33

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),
```

Ilustración 18 prueba conexión 3

3. Configuración de servicios

DNS

- a. En el servidor DNS con IP 27.1.0.2 se incluyen las siguientes entradas

- i. sistemas.com con IP del servidor de correo de sistemas.com

6	sistemas.com	A Record	27.100.0.33
---	--------------	----------	-------------

Ilustración 19 configuración DNS 1

- ii. pop3.sistemas.com como alias a sistemas.com.

5	pop3.sistemas.com	CNAME	sistemas.com
---	-------------------	-------	--------------

Ilustración 20 configuración DNS 2

- iii. smtp. sistemas.com con alias a sistemas.com

9	smtp.sistemas.com	CNAME	sistemas.com
---	-------------------	-------	--------------

Ilustración 21 configuración DNS 3

- iv. http.sistemas.com con IP del servidor web de sistemas.com

11	http.sistemas.com	A Record	27.100.0.32
----	-------------------	----------	-------------

Ilustración 22 configuración DNS 3

v. www.sistemas.com como alias a http.sistemas.com

12	www.sistemas.com	CNAME	http.sistemas.com
----	------------------	-------	-------------------

Ilustración 23 configuración DNS 4

vi. civil.com con IP del servidor de correo de civil.com

0	civil.com	A Record	27.200.0.52
---	-----------	----------	-------------

Ilustración 24 configuración DNS 5

vii. pop3.civil.com como alias a civil.com.

3	pop3.civil.com	CNAME	civil.com
---	----------------	-------	-----------

Ilustración 25 configuración DNS 6

viii. smtp.civil.com con alias a civil.com

8	smtp.civil.com	CNAME	civil.com
---	----------------	-------	-----------

Ilustración 26 configuración DNS 7

ix. http.civil.com con IP del servidor web de civil.com

11	http.sistemas.com	A Record	27.100.0.32
----	-------------------	----------	-------------

Ilustración 27 configuración DNS 8

x. www.civil.com como alias a http.civil.com

10	www.civil.com	CNAME	http.civil.com
----	---------------	-------	----------------

Ilustración 28 configuración DNS 9

b. En el servidor DNS con IP 27.1.0.2 se incluyen las siguientes entradas para Eléctrica

i. electrica.com con IP del servidor de correo de electrica.com

1	electrica.com	A Record	27.150.0.102
---	---------------	----------	--------------

Ilustración 29 configuración DNS 10

UNIVERSIDAD

ii. pop3.crear.com como alias a electrica.com.

5	pop3.crear.com	CNAME	electrica.com
---	----------------	-------	---------------

Ilustración 30 configuración DNS 11

iii. smtp.crear.com con alias a electrica.com

9	smtp.crear.com	CNAME	electrica.com
---	----------------	-------	---------------

Ilustración 31 configuración DNS 12

c. resultado completo

DNS

DNS Service	<input checked="" type="radio"/> On	<input type="radio"/> Off																																																
Resource Records																																																		
Name	<input type="text"/>	Type <input type="button" value="A Record"/>																																																
Address <input type="text"/>																																																		
<input type="button" value="Add"/>	<input type="button" value="Save"/>	<input type="button" value="Remove"/>																																																
<table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr> <th style="width: 10%;">No.</th> <th style="width: 30%;">Name</th> <th style="width: 30%;">Type</th> <th style="width: 30%;">Detail</th> </tr> </thead> <tbody> <tr><td>0</td><td>civil.com</td><td>A Record</td><td>27.200.0.52</td></tr> <tr><td>1</td><td>electrica.com</td><td>A Record</td><td>27.150.0.102</td></tr> <tr><td>2</td><td>http.civil.com</td><td>A Record</td><td>27.200.0.53</td></tr> <tr><td>3</td><td>pop3.civil.com</td><td>CNAME</td><td>civil.com</td></tr> <tr><td>4</td><td>pop3.crear.com</td><td>CNAME</td><td>electrica.com</td></tr> <tr><td>5</td><td>pop3.sistemas.com</td><td>CNAME</td><td>sistemas.com</td></tr> <tr><td>6</td><td>sistemas.com</td><td>A Record</td><td>27.100.0.33</td></tr> <tr><td>7</td><td>smtp.crear.com</td><td>CNAME</td><td>electrica.com</td></tr> <tr><td>8</td><td>smtp.civil.com</td><td>CNAME</td><td>civil.com</td></tr> <tr><td>9</td><td>smtp.sistemas.com</td><td>CNAME</td><td>sistemas.com</td></tr> <tr><td>10</td><td>www.civil.com</td><td>CNAME</td><td>http.civil.com</td></tr> </tbody> </table>			No.	Name	Type	Detail	0	civil.com	A Record	27.200.0.52	1	electrica.com	A Record	27.150.0.102	2	http.civil.com	A Record	27.200.0.53	3	pop3.civil.com	CNAME	civil.com	4	pop3.crear.com	CNAME	electrica.com	5	pop3.sistemas.com	CNAME	sistemas.com	6	sistemas.com	A Record	27.100.0.33	7	smtp.crear.com	CNAME	electrica.com	8	smtp.civil.com	CNAME	civil.com	9	smtp.sistemas.com	CNAME	sistemas.com	10	www.civil.com	CNAME	http.civil.com
No.	Name	Type	Detail																																															
0	civil.com	A Record	27.200.0.52																																															
1	electrica.com	A Record	27.150.0.102																																															
2	http.civil.com	A Record	27.200.0.53																																															
3	pop3.civil.com	CNAME	civil.com																																															
4	pop3.crear.com	CNAME	electrica.com																																															
5	pop3.sistemas.com	CNAME	sistemas.com																																															
6	sistemas.com	A Record	27.100.0.33																																															
7	smtp.crear.com	CNAME	electrica.com																																															
8	smtp.civil.com	CNAME	civil.com																																															
9	smtp.sistemas.com	CNAME	sistemas.com																																															
10	www.civil.com	CNAME	http.civil.com																																															

Ilustración 32 configuración general parte 1

11	http.sistemas.com	A Record	27.100.0.32
12	www.sistemas.com	CNAME	http.sistemas.com

DNS Cache

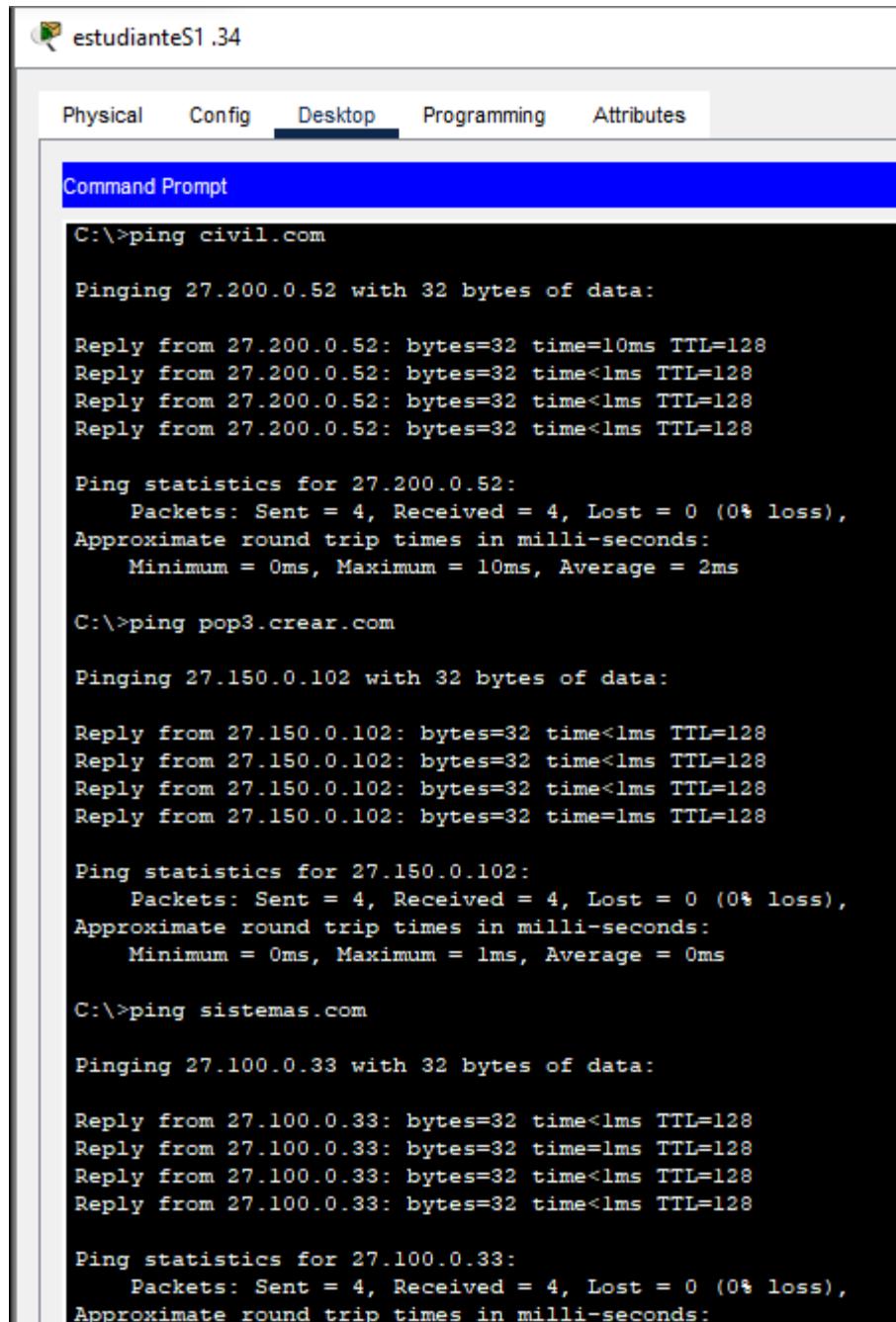
Ilustración 33 configuración general parte 2

- d. ahora se sube el servicio y desde una máquina cliente de cada empresa, se utiliza el comando ping por nombre en la línea de comandos para verificar que el servicio está funcionando bien.
- se sube el servicio



Ilustración 34 activación servicio DNS

- Pruebas:
 - Sistemas: estudianteS1
Hacia civil.com, pop3.crear.com, www.sistemas.com



estudianteS1.34

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping civil.com

Pinging 27.200.0.52 with 32 bytes of data:

Reply from 27.200.0.52: bytes=32 time=10ms TTL=128
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<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 = 10ms, Average = 2ms

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
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128
Reply from 27.150.0.102: bytes=32 time<1ms TTL=128
Reply from 27.150.0.102: bytes=32 time=lms 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 = 1ms, Average = 0ms

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
Reply from 27.100.0.33: bytes=32 time=lms TTL=128
Reply from 27.100.0.33: bytes=32 time<1ms 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:
```

Ilustración 35 prueba DNS 1

- Civil: EstudianteC2
Hacia http.sistemas.com, smtp.crear.com, smtp.civil.com

EstudianteC2

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping http.sistemas.com

Pinging 27.100.0.32 with 32 bytes of data:

Reply from 27.100.0.32: bytes=32 time=10ms TTL=128
Reply from 27.100.0.32: bytes=32 time<1ms TTL=128
Reply from 27.100.0.32: bytes=32 time<1ms TTL=128
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 = 10ms, Average = 2ms

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:\>ping smtp.civil.com

Pinging 27.200.0.52 with 32 bytes of data:

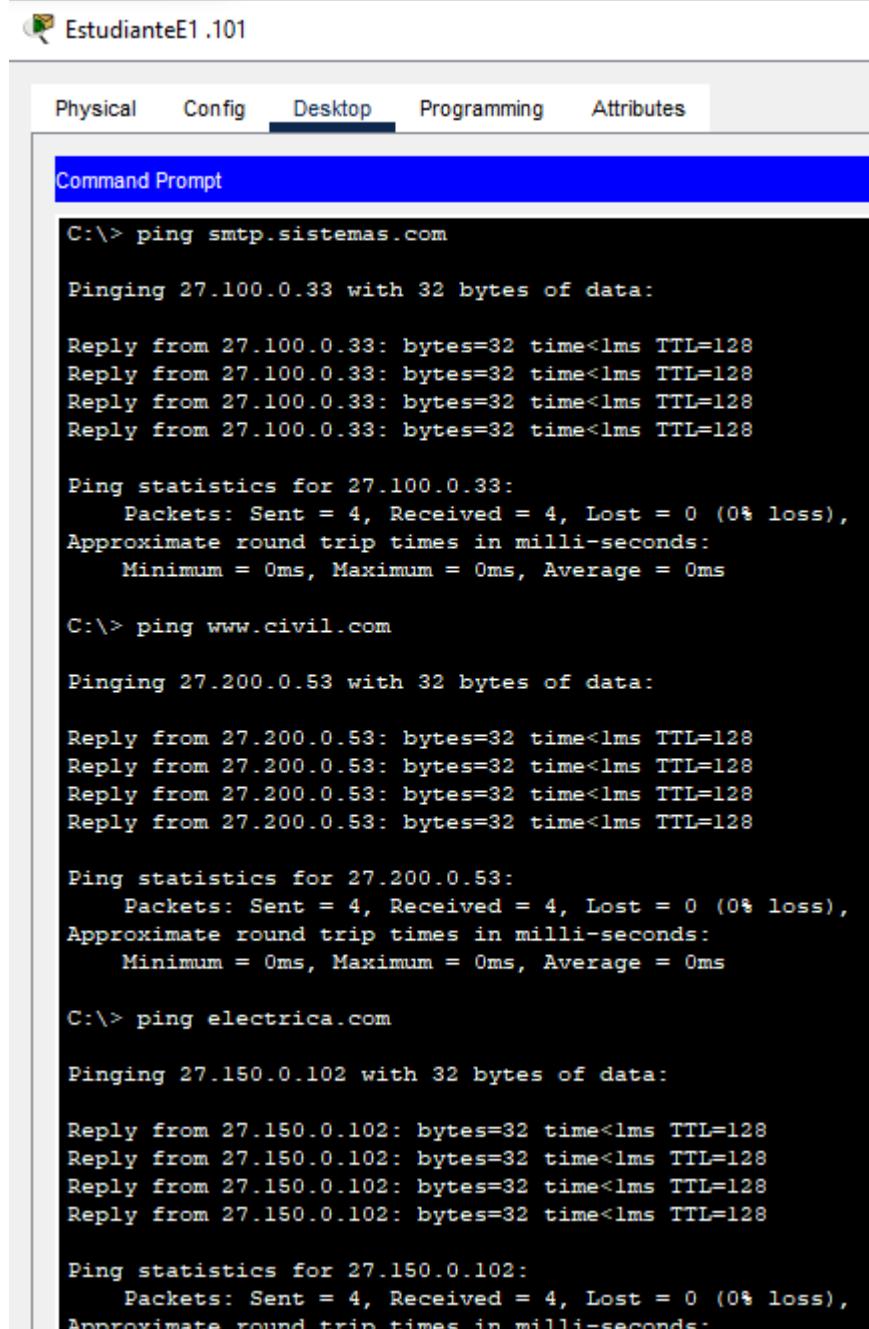
Reply from 27.200.0.52: bytes=32 time<1ms TTL=128

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

Ilustración 36 prueba DNS 2

- Eléctrica: EstudianteE1

Hacia smtp.sistemas.com, www.civil.com, electrica.com



EstudianteE1 .101

Physical Config Desktop Programming Attributes

Command Prompt

```
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

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 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:\> 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

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

Ilustración 37 prueba DNS 3

4. Configuración de servicio HTTP

- a. En los servidores web configuramos el servicio HTTP. Modificamos las páginas web de los servidores para reconocer a qué decanatura pertenecen y subimos el servicio.
 - En el servidor web de sistemas www.sistemas.com
Se abre la opción de servicios y se edita el index.html para personalizarlo

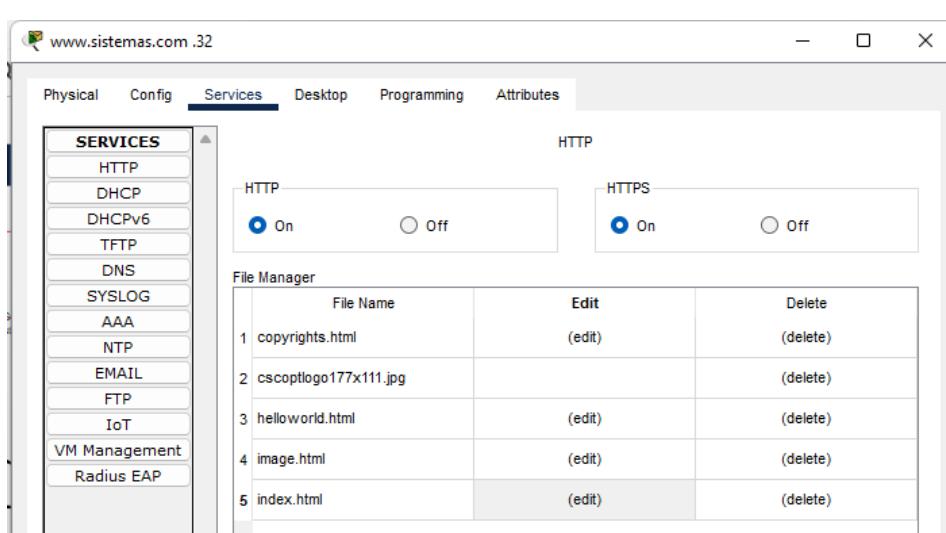
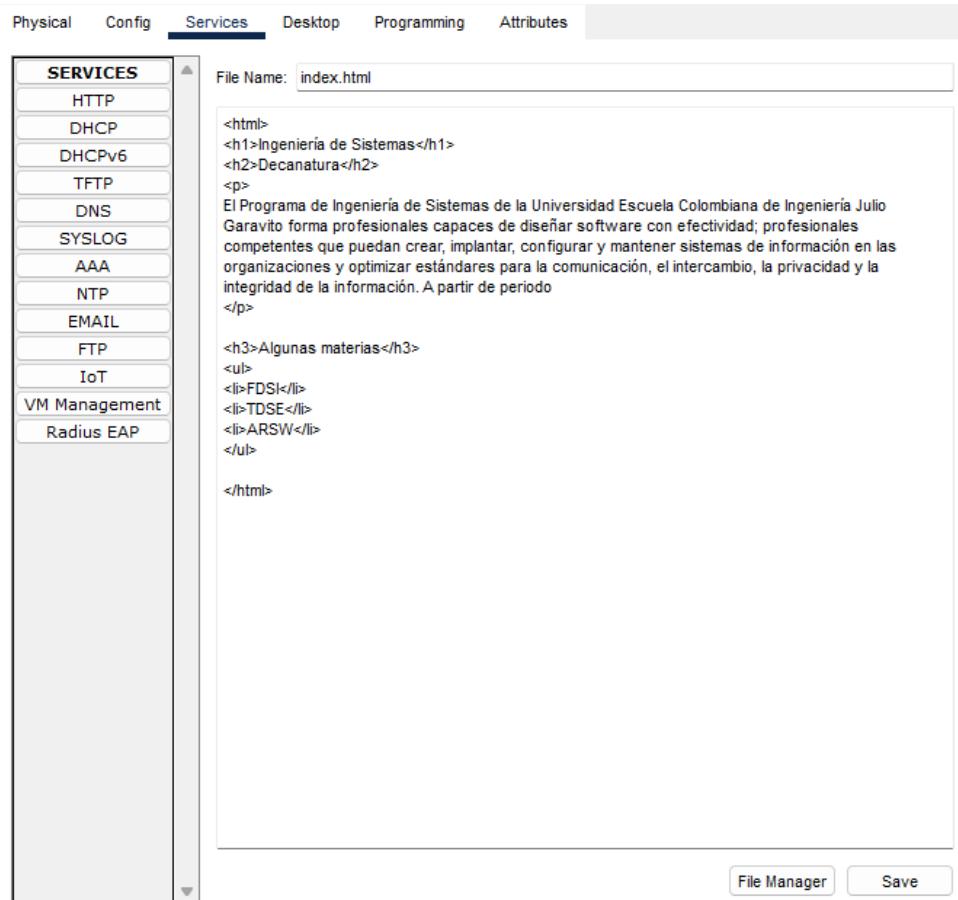


Ilustración 38 configuración servidor web sistemas

Luego personalizamos la página



Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

File Name: index.html

```

<html>
<h1>Ingeniería de Sistemas</h1>
<h2>Decanatura</h2>
<p>
El Programa de Ingeniería de Sistemas de la Universidad Escuela Colombiana de Ingeniería Julio Garavito forma profesionales capaces de diseñar software con efectividad; profesionales competentes que puedan crear, implantar, configurar y mantener sistemas de información en las organizaciones y optimizar estándares para la comunicación, el intercambio, la privacidad y la integridad de la información. A partir de periodo
</p>

<h3>Algunas materias</h3>
<ul>
<li>FDSI</li>
<li>TDSE</li>
<li>ARSW</li>
</ul>

</html>

```

File Manager **Save**

Ilustración 39 personalización página web sistemas

- En el servidor web de sistemas www.civil.com
 Se abre la opción de servicios y se edita el index.html para personalizarlo

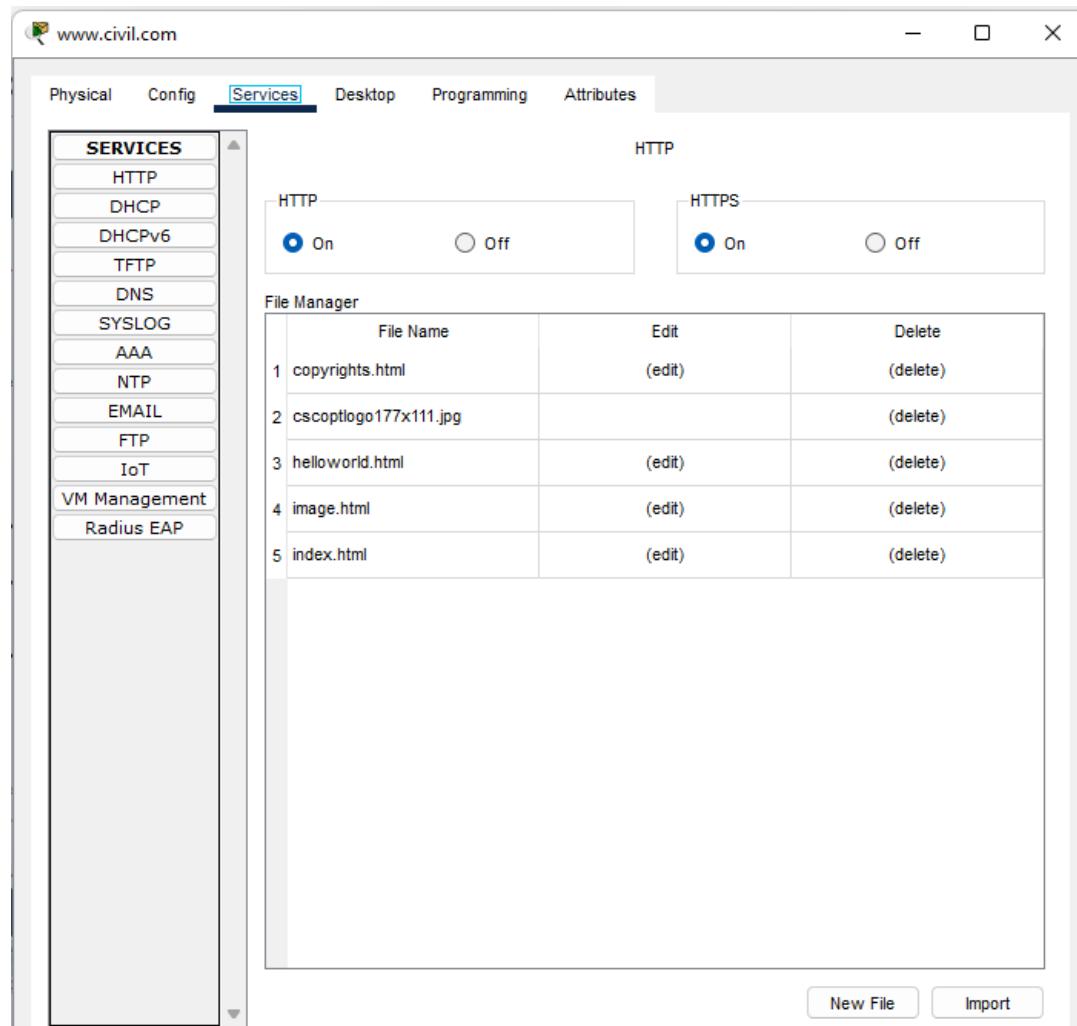


Ilustración 40 configuración servidor web Civil

Personalizamos la página

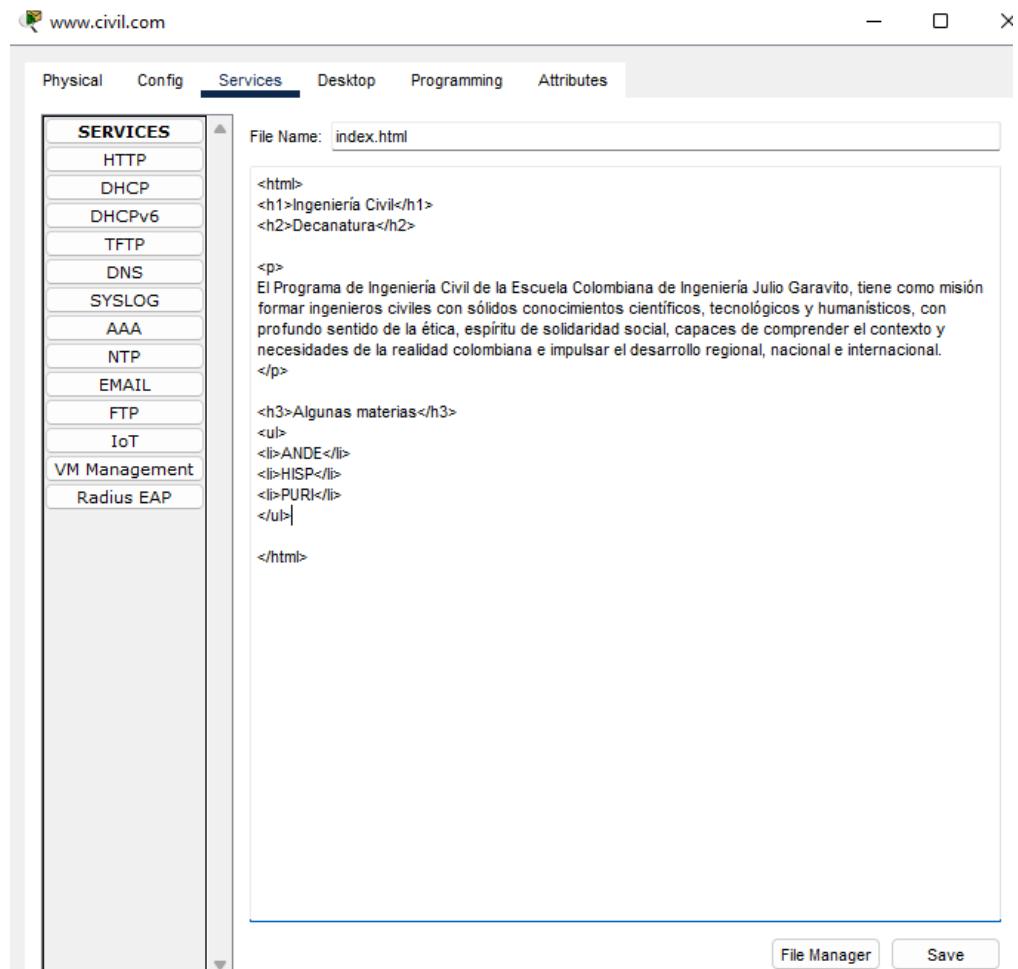


Ilustración 41 personalización página web Civil

- b. Desde las estaciones clientes se prueba la conexión con los servidores web.
 - i. Se hace la solicitud de la página web usando las direcciones IP de cada servidor.
 - De sistemas desde EstudianteC1

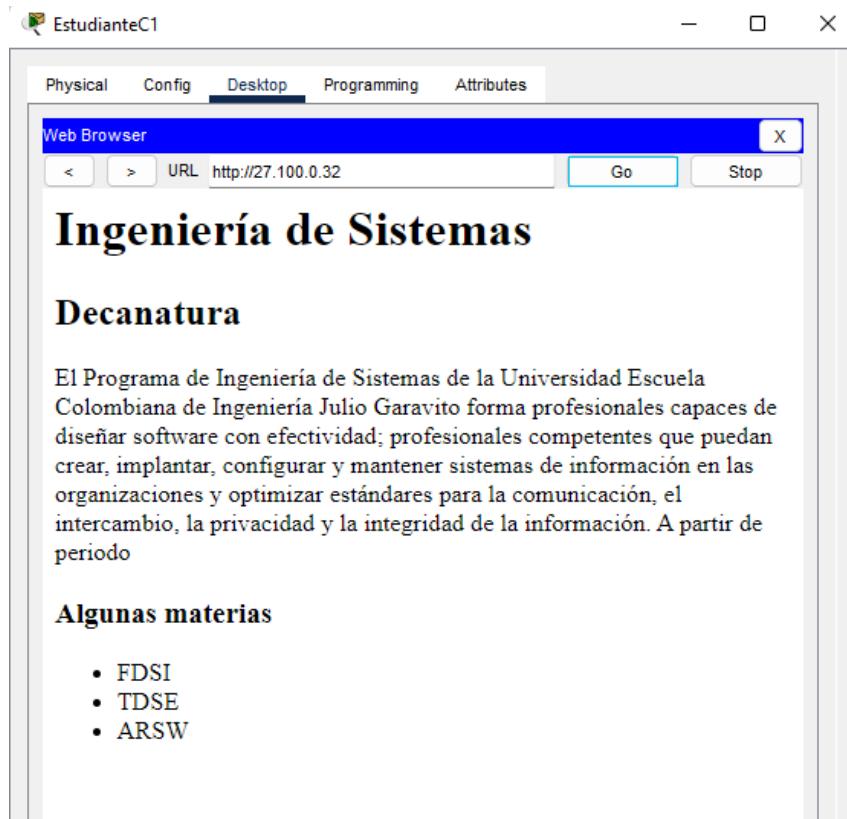


Ilustración 42 consulta 1

- De civil desde EstudianteC2

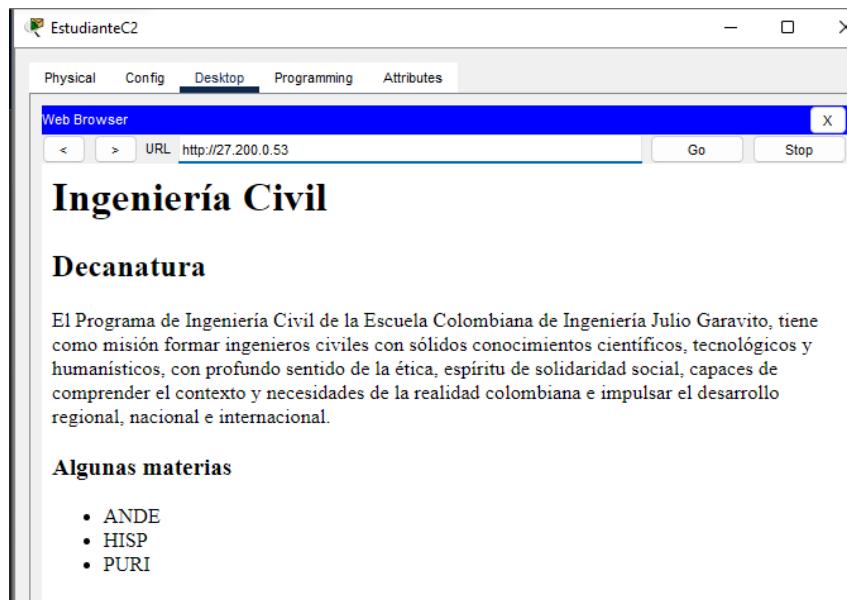


Ilustración 43 consulta 2

ii. Se hace la solicitud de la página web usando el URL de cada servidor.

- De sistemas desde EstudianteC2

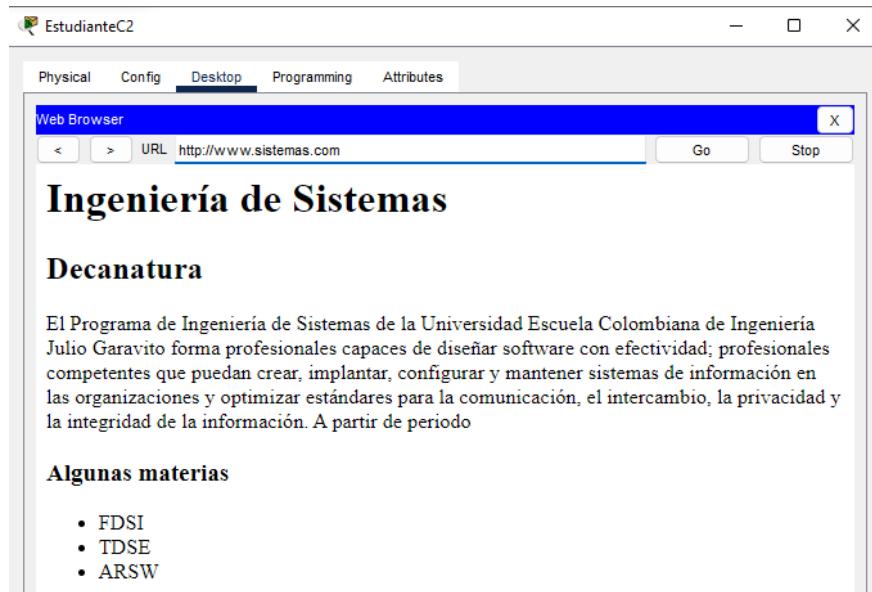


Ilustración 44 consulta 3

- De civil desde EstudianteC1

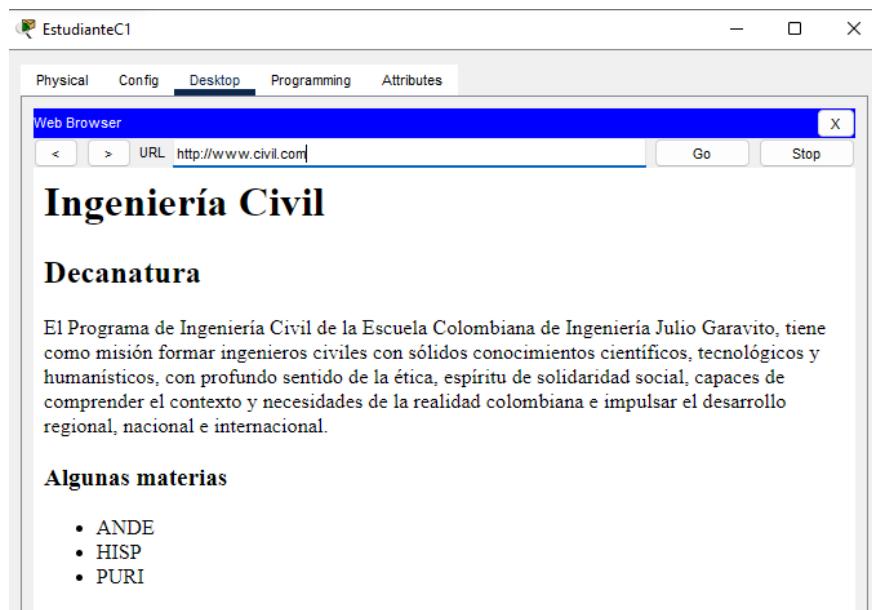


Ilustración 45 consulta 4

- iii. Utilizando el modo simulación se revisa el contenido de los PDU de la capa de aplicación

Haciendo una solicitud desde EstudianteS1 a www.civil.com
 Revisando los PDUs se puede observar lo siguiente

- Se detalla que el protocolo de la capa de transporte a la hora de realizar la consulta http es TCP

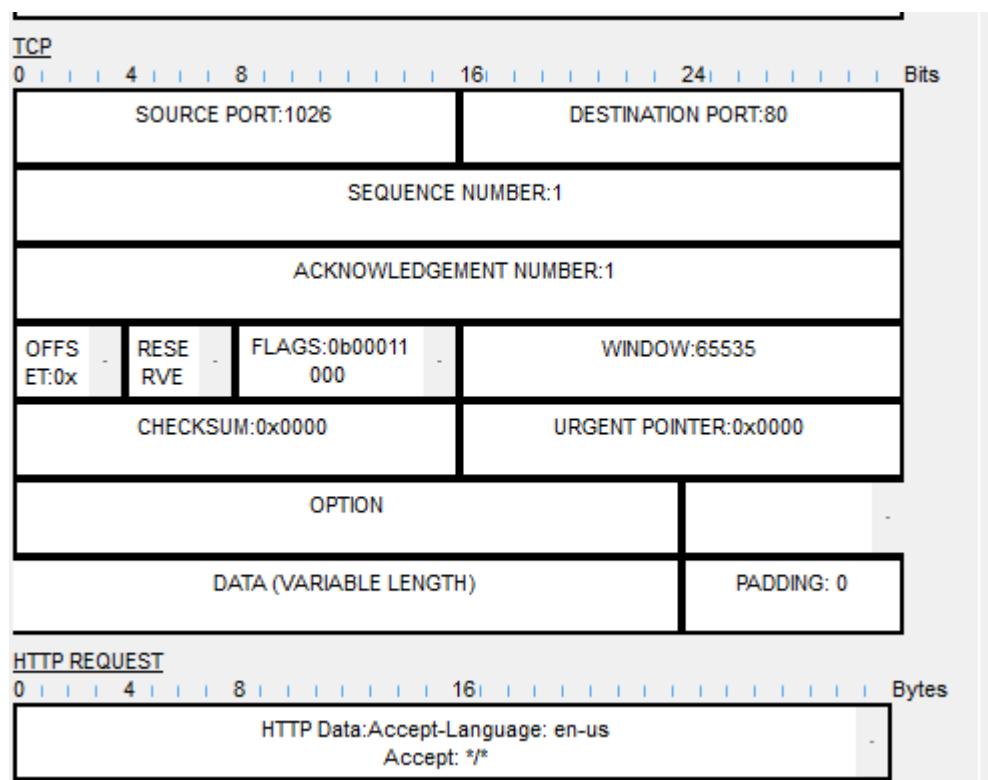


Ilustración 46 PDU consulta HTTP

- También se puede observar dos PDUs de http, uno de REQUEST y otro de RESPONSE

PDU Information at Device: estudianteS1.34

OSI Model [Inbound PDU Details](#)

PDU Formats

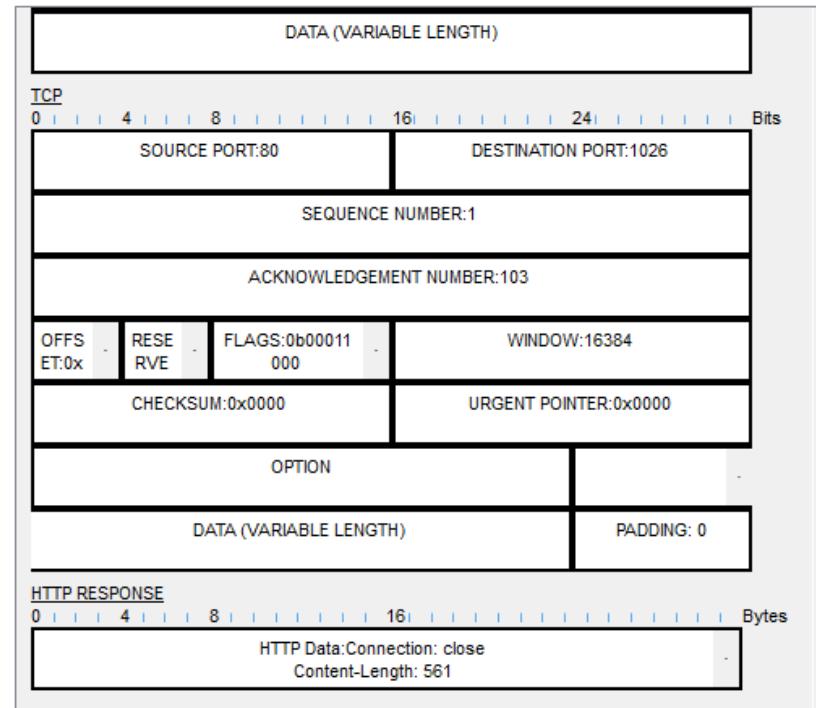


Ilustración 47 DPU cierre conexión HTTP

- Por último, se ve que se uso el protocolo DNS para resolver la solicitud de www.civil.com a la IP 27.200.0.53 y que utiliza UPD como protocolo de la capa de transporte

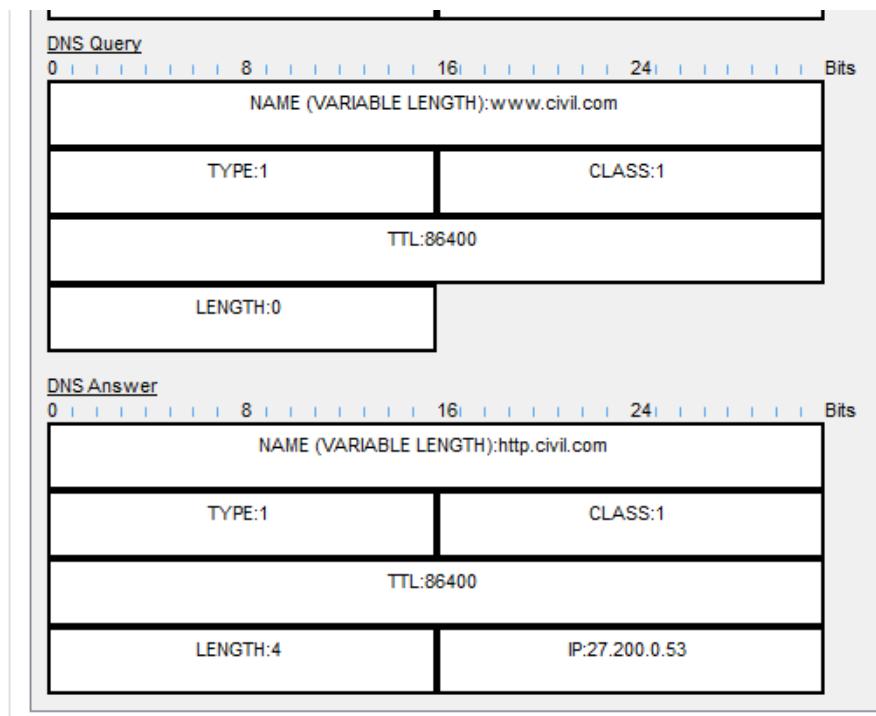


Ilustración 48 DPU consulta DNS

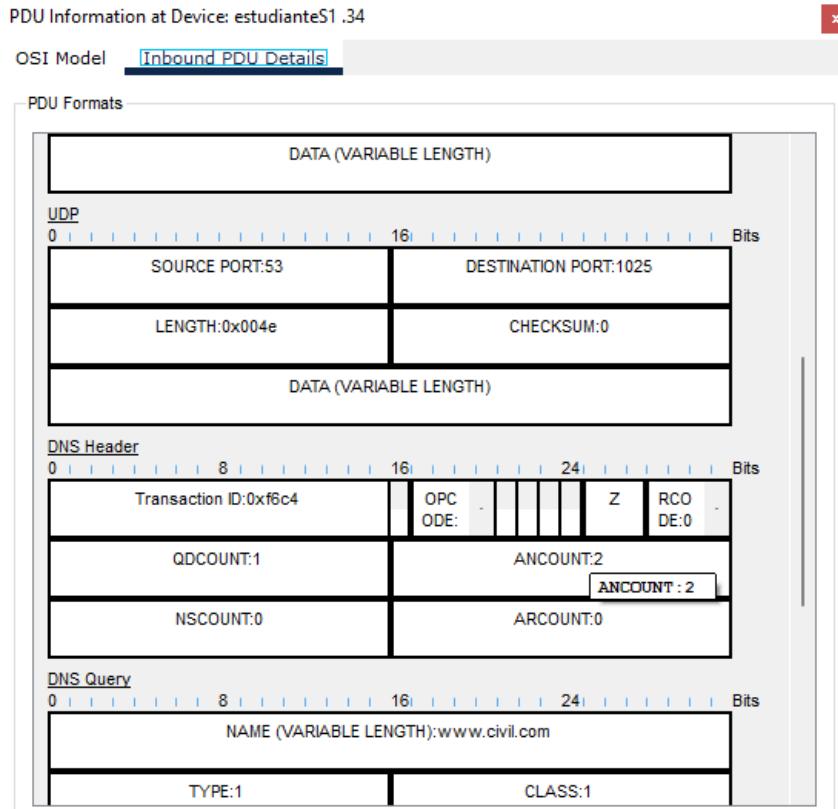


Ilustración 49 PDU resolución de consulta DNS

5. Configuración de servicio de Correo electrónico

- En el servidor de correo de cada decanatura se incluyen las cuentas de correo para los usuarios de cada decanatura. Se usan los nombres de los computadores cliente como nombre de los usuarios

Se establecen los dos usuarios con el nombre y la contraseña del computador cliente al que pertenecen en el servidor de correo. Además, también se configura el Dominio de cada servidor

- Sistemas

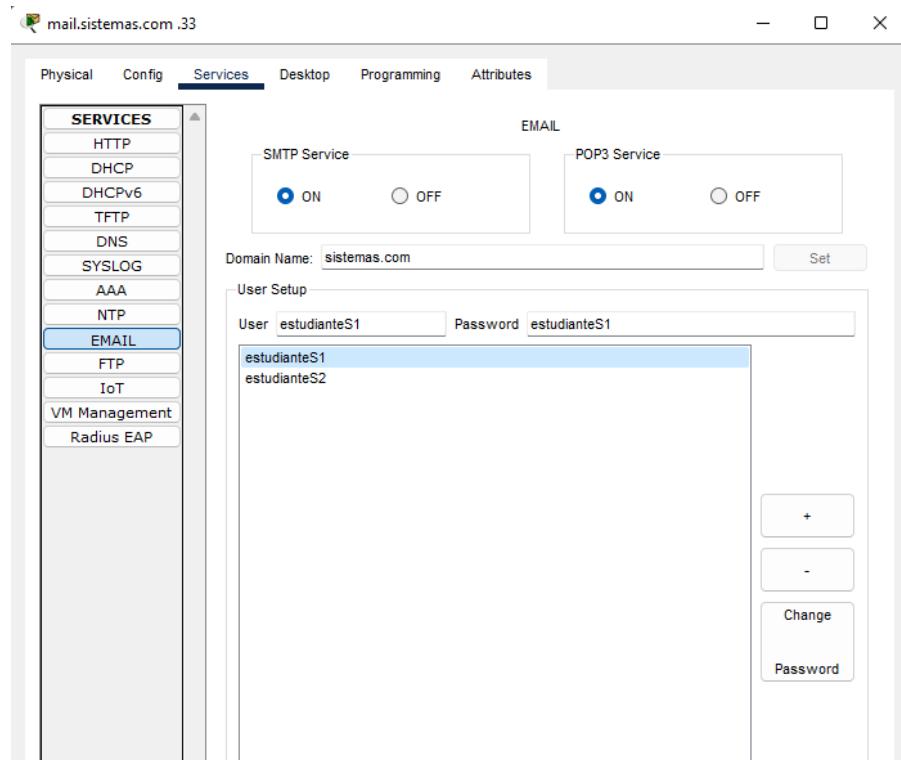


Ilustración 50 configuración usuarios y dominio sistemas

- Civil

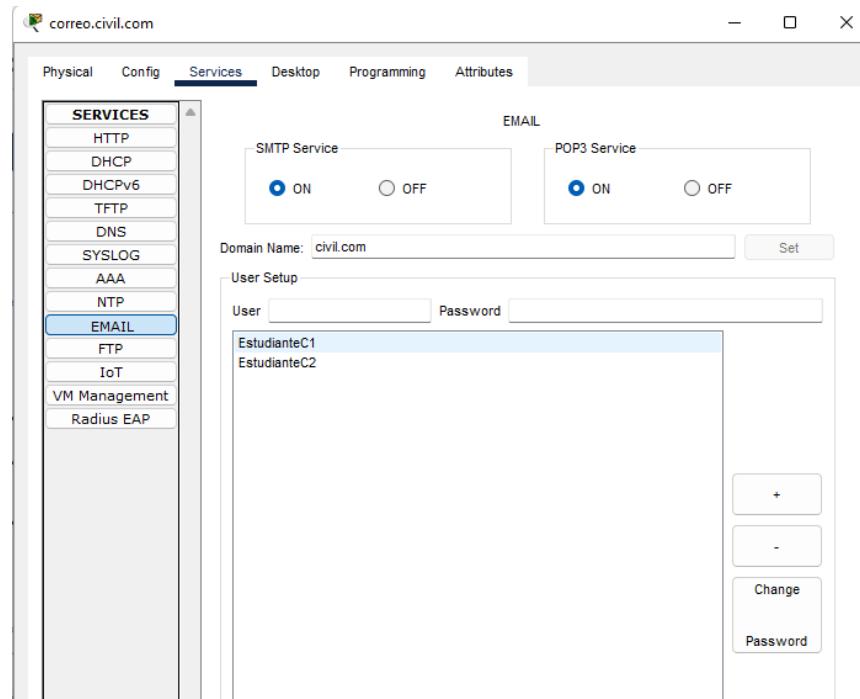


Ilustración 51 configuración usuarios y dominio civil

- **Eléctrica**

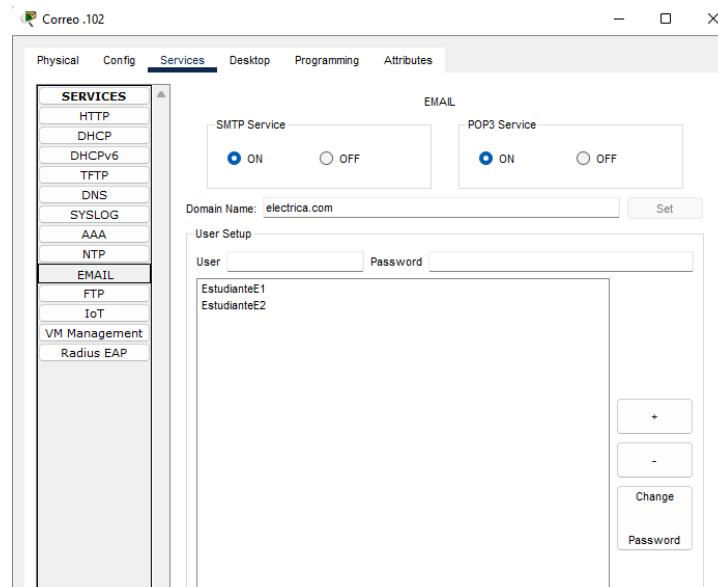


Ilustración 52 configuración usuarios y dominio eléctrica

- b. Desde las estaciones clientes se prueba el servicio
 - a. Se configura los clientes de correo de cada dominio.
 - Sistemas: estudianteS1, estudiante S2

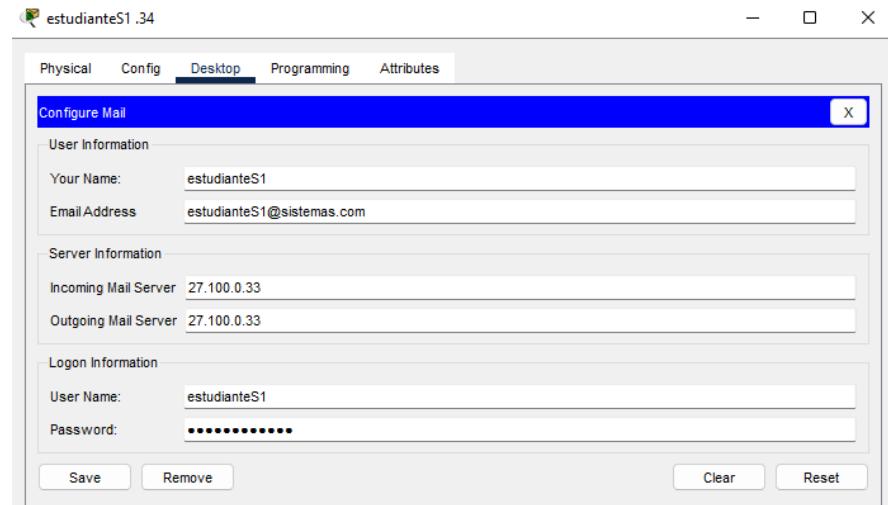


Ilustración 53 configuración correo estudianteS1

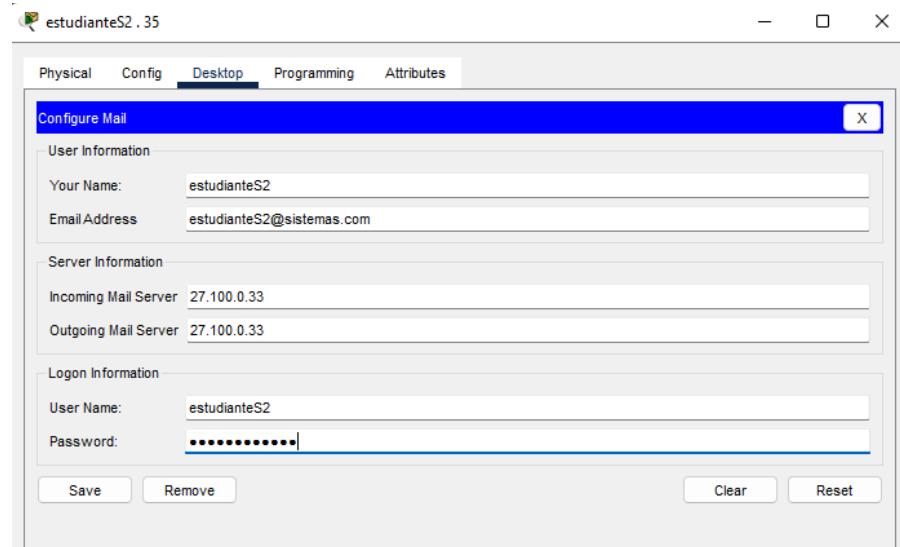


Ilustración 54 configuración correo estudianteS2

- Civil: EstudianteC1, EstudianteC2

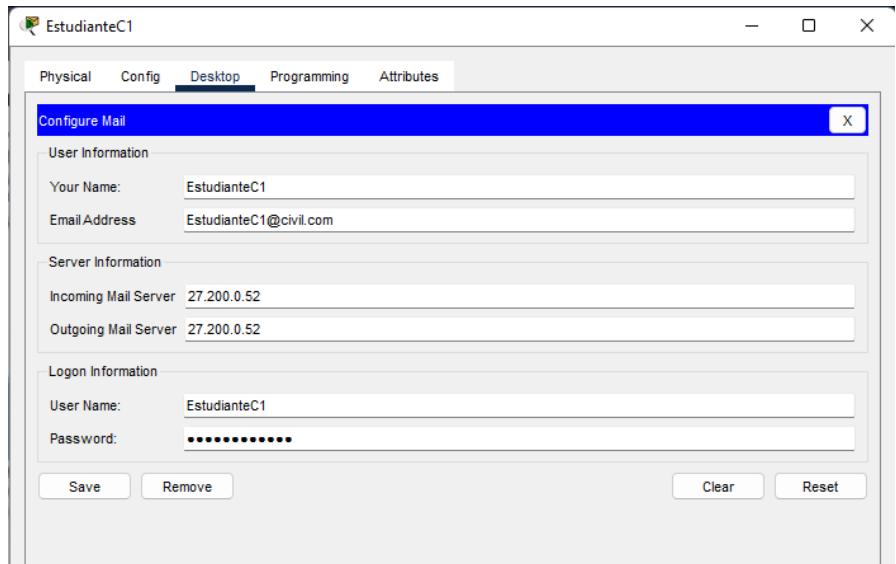


Ilustración 55 configuración correo EstudianteC1

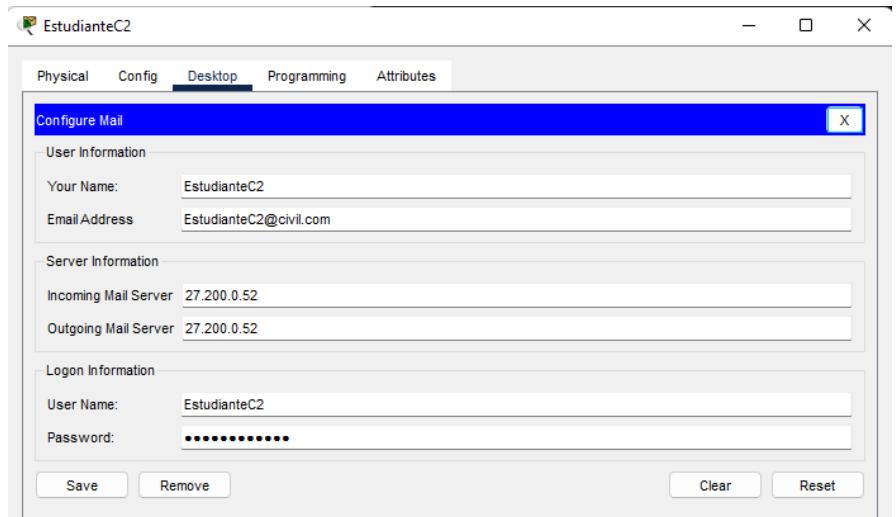


Ilustración 56 configuración correo EstudianteC2

- Eléctrica: EstudianteE1, EstudianteE2

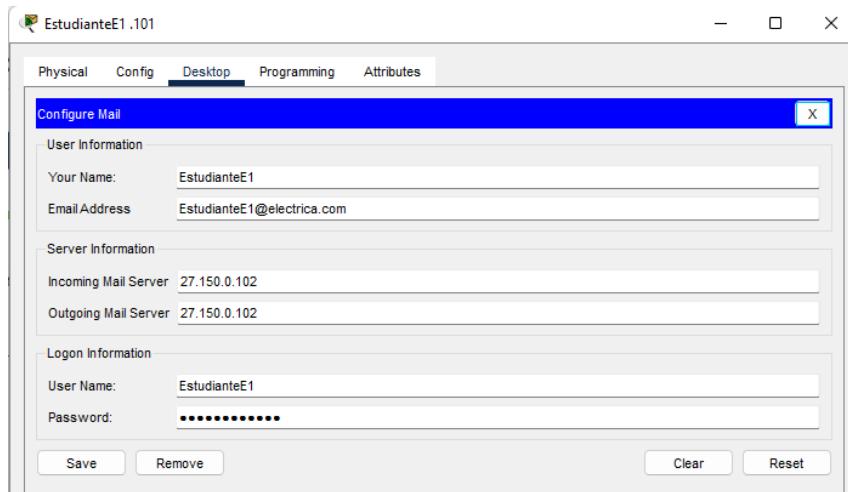


Ilustración 57 configuración correo EstudianteE1

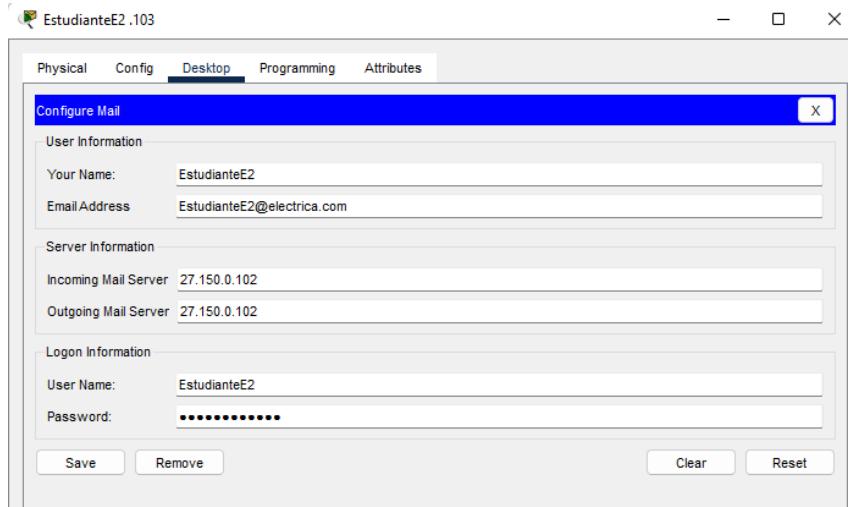


Ilustración 58 configuración correo EstudianteE2

- b. Se envían correo entre las estaciones del mismo dominio.
- Sistemas: de estudianteS1 a estudianteS2

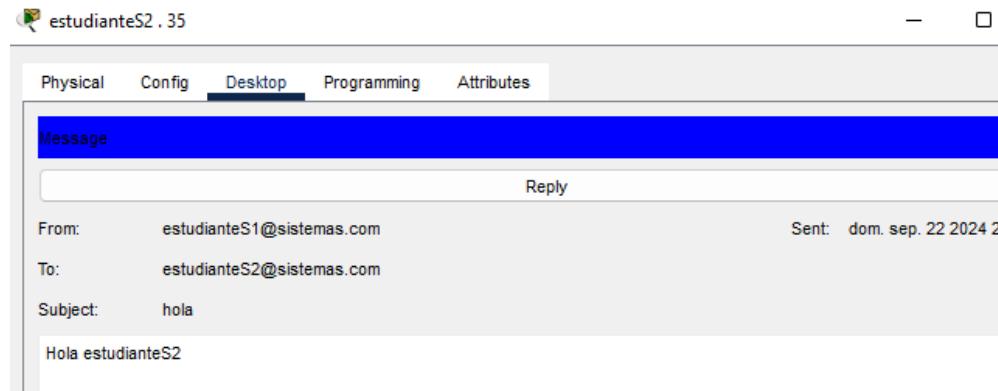


Ilustración 59 envío correo 1

- Civil: de EstudianteC1 a EstudianteC2

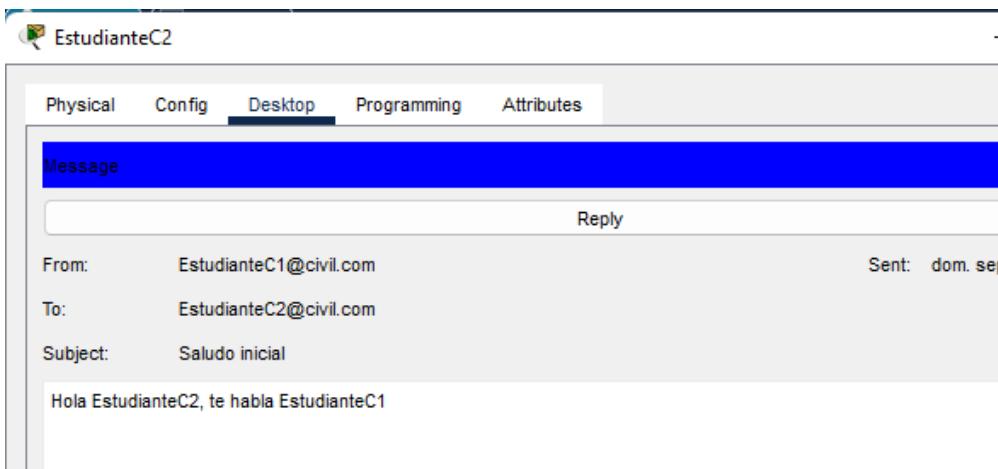


Ilustración 60 envío correo 2

- Eléctrica: de EstudianteE1 a EstudianteE2



Ilustración 61 envío correo 3

- c. Se Verifica el recibo de correo en las estaciones y se responde a los mensajes recibidos.

- Respuesta estudianteS2 a estudianteS1

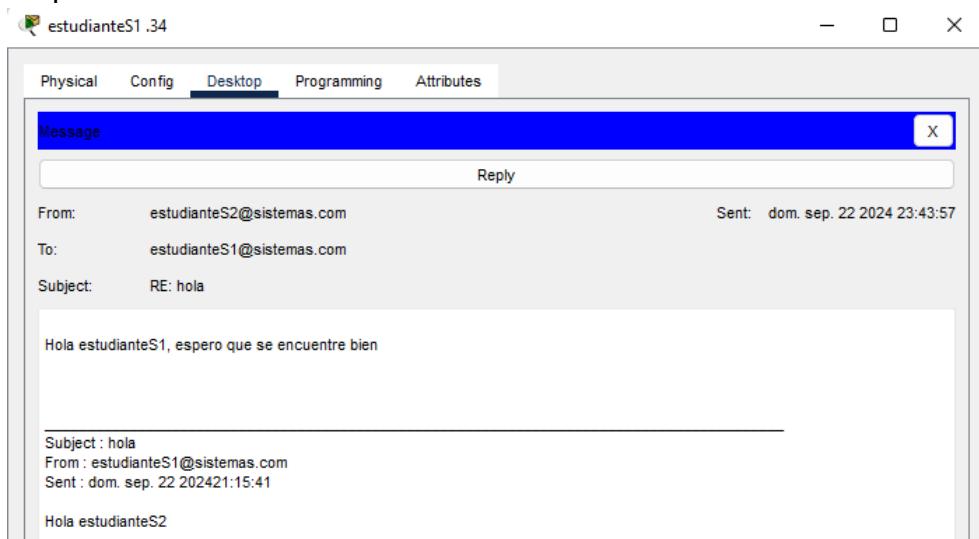


Ilustración 62 respuesta correo 1

- Civil: respuesta EstudianteC2 a EstudianteC1

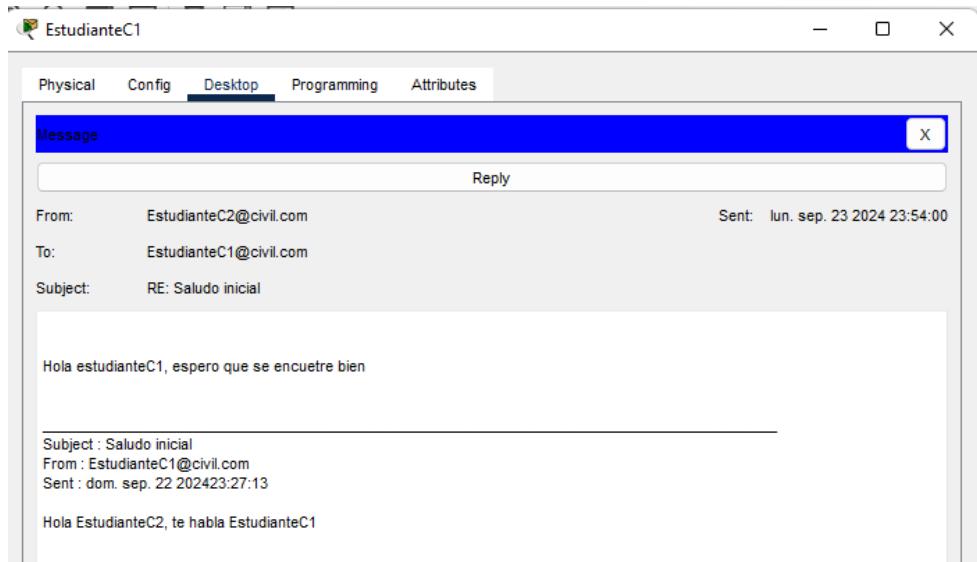


Ilustración 63 respuesta correo 2

- **Eléctrica: respuesta EstudianteE2 a EstudianteE1**

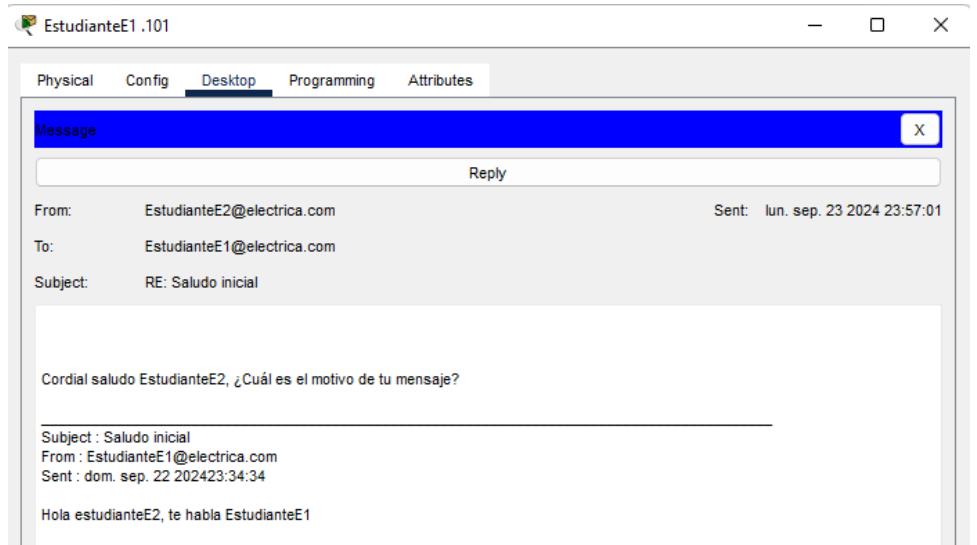


Ilustración 64 respuesta correo 3

d. Se envía correo hacia los clientes de los otros dominios.

- De estudianteS1 a EstudianteC2

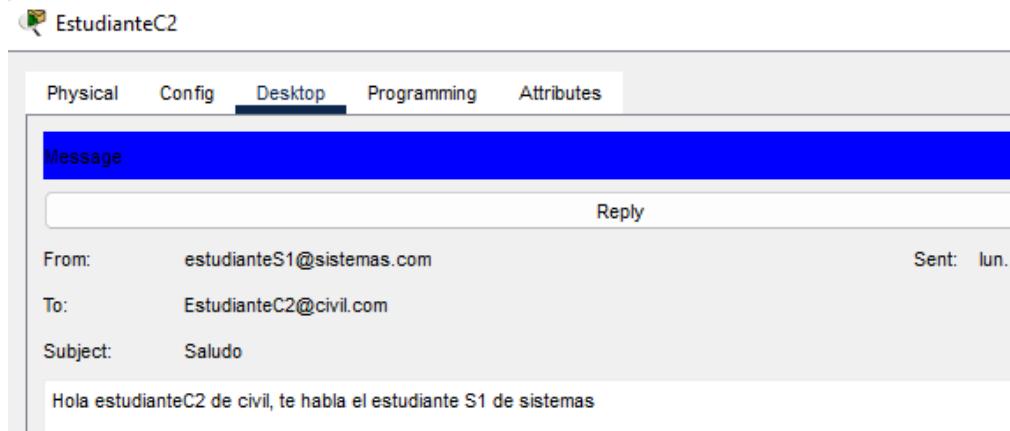


Ilustración 65 envío correo otro dominio 1

- De EstudianteC2 a EstudianteE1

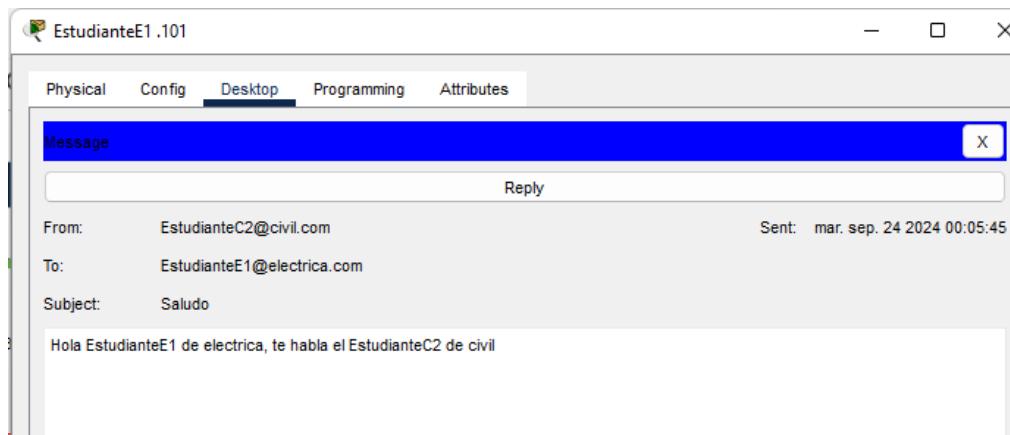


Ilustración 66 envío correo otro dominio 2

- De EstudianteE1 a estudianteS2

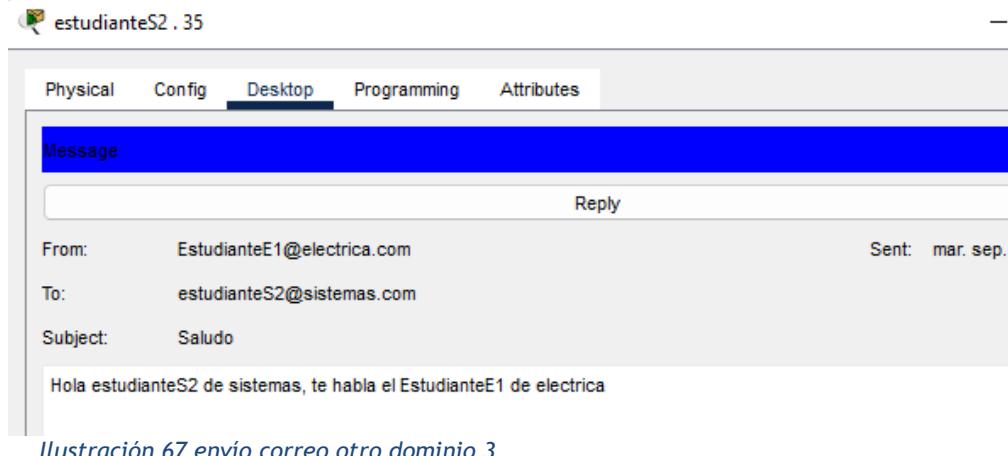


Ilustración 67 envío correo otro dominio 3

- e. Se Verifica el recibo de correo en las estaciones y responda a los mensajes recibidos.

- Respuesta EstudianteC2 a estudianteS1

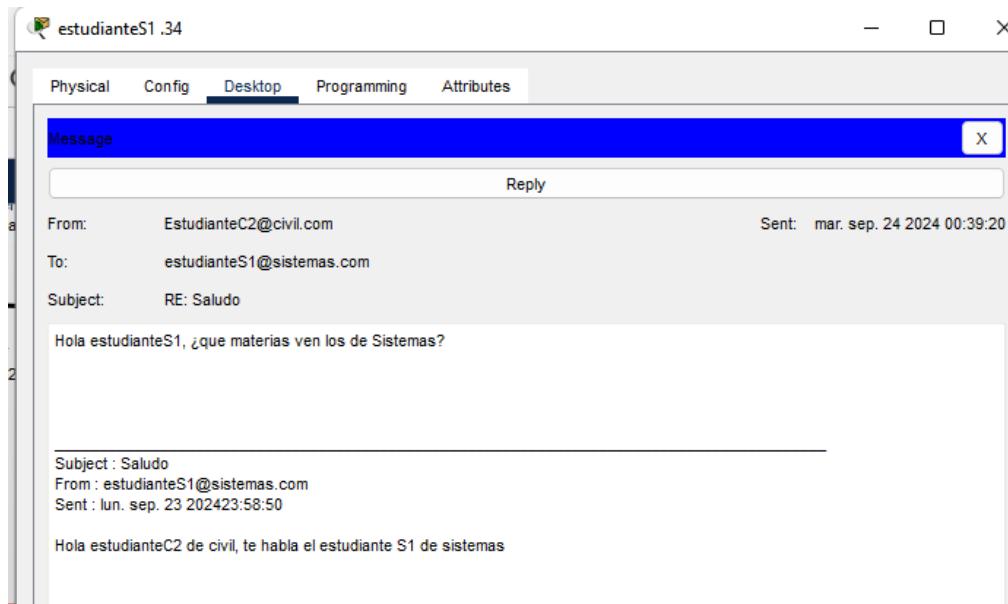


Ilustración 68 envío correo otro dominio 1

- Respuesta EstudianteE1 a estudianteC2

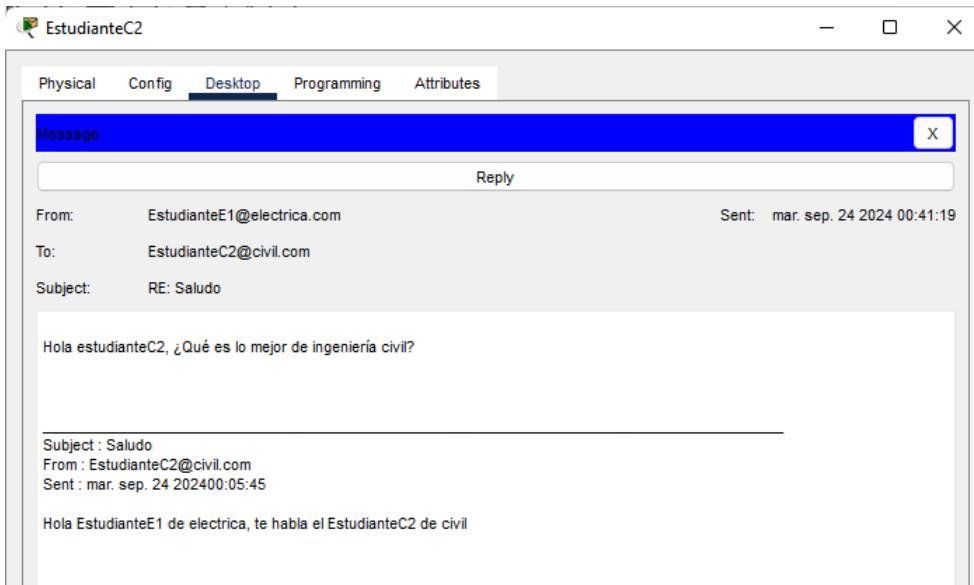


Ilustración 69 respuesta envío correo otro dominio 2

- Respuesta EstudianteS2 a estudianteE1

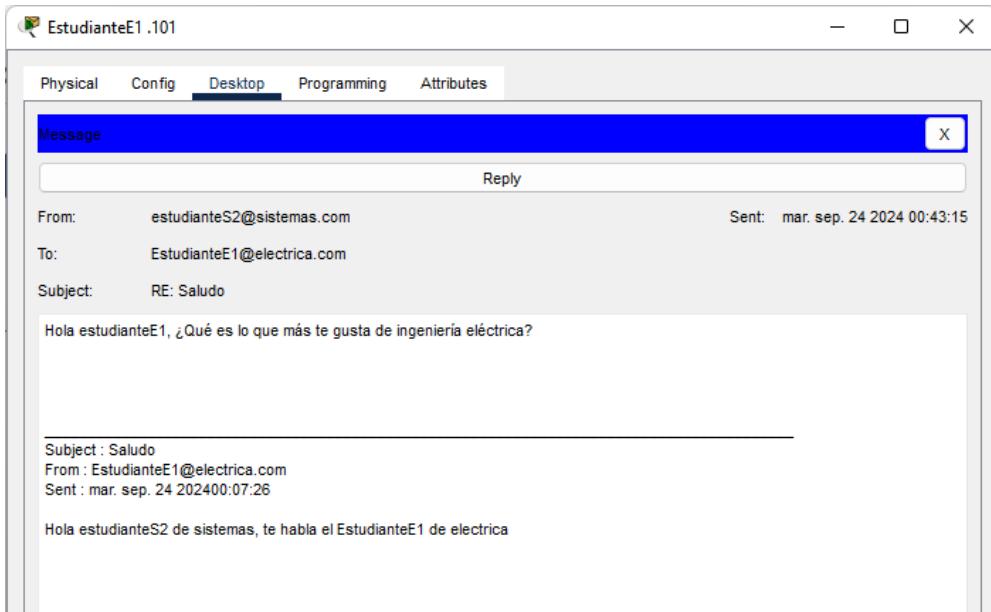


Ilustración 70 respuesta envío correo otro dominio 3

- Utilizando la herramienta de simulación, revisamos el contenido de los PDU a nivel de las capas de transporte y aplicación en el envío de un correo entre el cliente que envía y su servidor SMTP y entre el cliente que recibe y su servidor POP3

- **SMTP**

Se observa como el envío del correo por el protocolo SMTP que usa el protocolo de transporte TCP

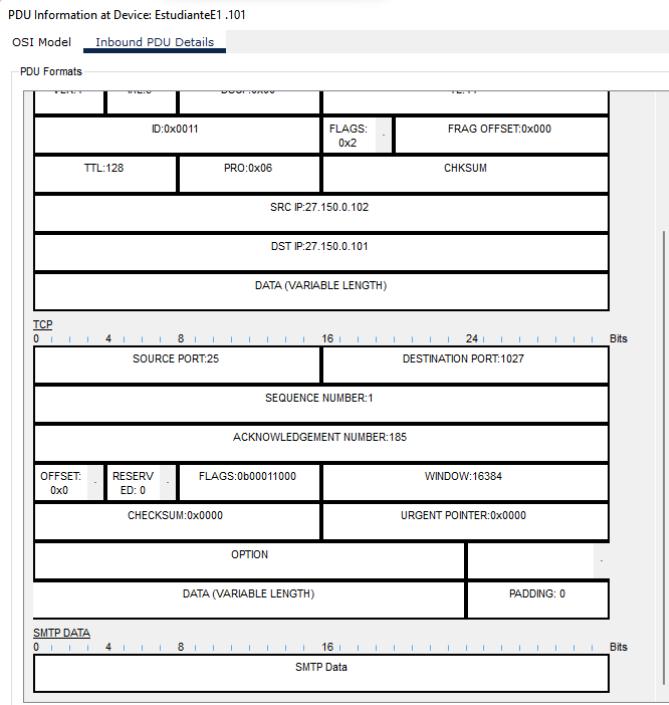


Ilustración 71 PDU SMTP

- **POP3**

Se observa cómo se descargan los correos del mail Box mediante el uso del protocolo POP3 que usa como protocolo de transporte TCP

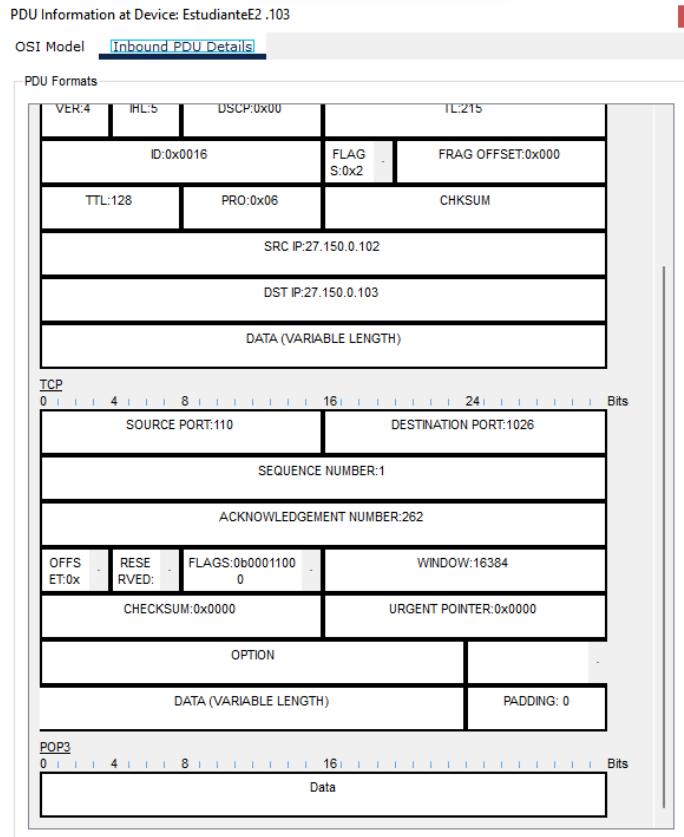


Ilustración 72 PDU POP3

6. Configuración de servicio FTP

- En el servidor web de sistemas en la configuración de red de cada miembro del equipo se configura el servicio FTP. Se crea un usuario con el nombre y clave como apellido de cada miembro del equipo

Configuración de red 1:

usuario: jorge y clave: gamboa

Configuración de red 2:

usuario: camila y clave: torres

Para cada configuración de red se crea un usuario con su respectiva contraseña para brindar el servicio FTP en el servidor web de sistemas, según la configuración de red el usuario y contraseña serán diferentes

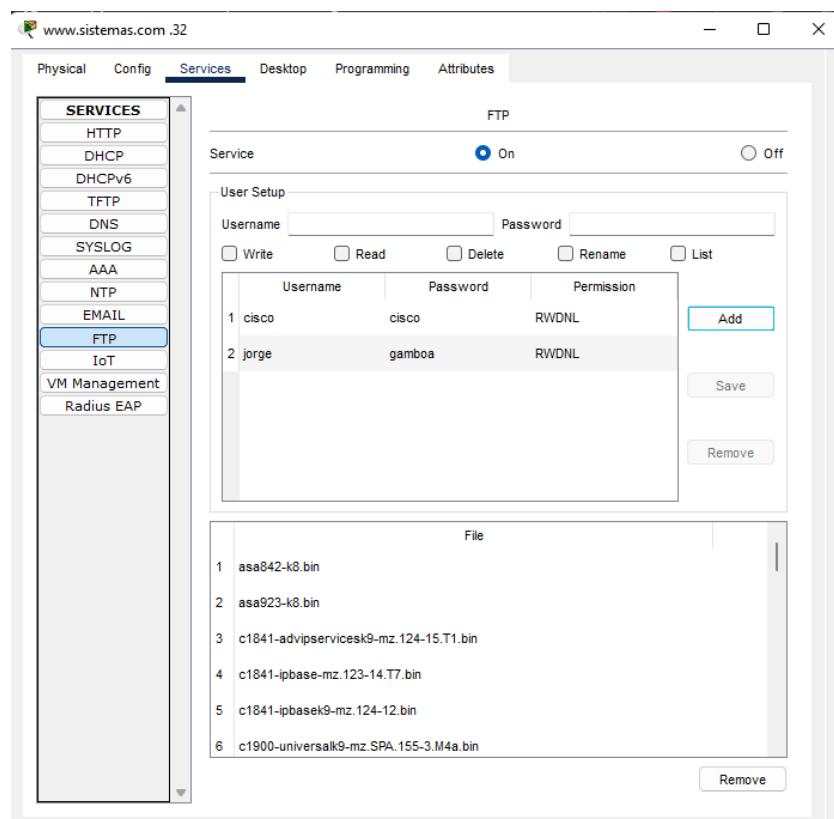


Ilustración 73 configuración FTP usuario y contraseña

- Desde las estaciones clientes se conecta al servidor FTP y se bajar un archivo

- Desde la línea de comando se ingresa al servidor FTP usando el comando telnet.

Desde la terminal de un cliente (estudianteS1) se establece conexión con el servidor que se busca hacer conexión

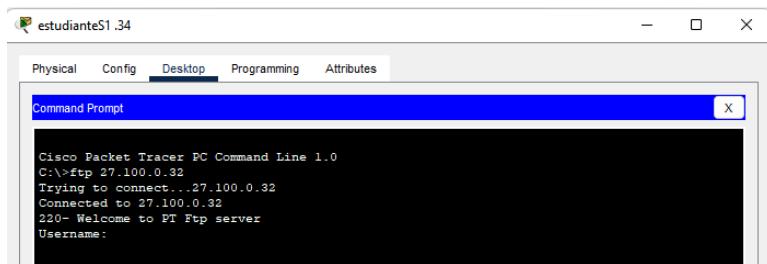


Ilustración 74 inicio FTP

- Se ingresa con el usuario/claves creados.

Se realiza la conexión al servidor con el usuario y contraseña elegidos anteriormente

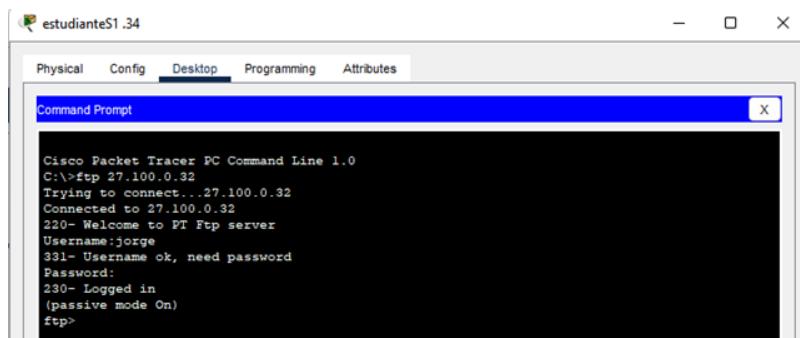


Ilustración 75 ingreso servidor FTP

Se revisan los archivos en el servidor con el comando dir

```
ftp>dir
Listing /ftp directory from 27.100.0.32:
0 : ad100m-adviservicesk9-mz.123-18.71.bin
1 : ad100m-adviservicesk9-mz.123-18.71.bin
2 : c1841-adviservicesk9-mz.124-16.71.bin
3 : c1841-ipbase-mz.123-14.77.bin
4 : c1841-ipbasek9-mz.124-16.71.bin
5 : c1840-universalk9-mz.SPA.156-3.M4a.bin
6 : c2600-adviservicesk9-mz.124-16.71.bin
7 : c2600-i-mz.122-20.bin
8 : c2600-ipbasek9-mz.124-8.bin
9 : c2800nm-adviservicesk9-mz.124-18.T1.bin
10 : c2800nm-adviservicesk9-mz.124-18.T1.bin
11 : c2800nm-ipbase-mz.123-14.77.bin
12 : c2800nm-ipbasek9-mz.124-8.bin
13 : c2900-universalk9-mz.SPA.156-3.M4a.bin
14 : c2950-adviservicesk9-mz.124-16.71.bin
15 : c2950-ig412-mz.121-22.EA9.bin
16 : c2960-lanbase-mz.122-25.FX.bin
17 : c2960-lanbase-mz.122-25.SEE1.bin
18 : c2960-universalk9-mz.122-27.SEE1.bin
19 : c3560-adviservicesk9-mz.122-27.SEE1.bin
20 : c3560-adviservicesk9-mz.122-46.SEE1.bin
21 : c800-universalk9-mz.SPA.152-4.M4.bin
22 : c800-universalk9-mz.SPA.154-3.M6a.bin
23 : c800-universalk9-mz.SPA.154-3.M6a.bin
24 : c8000-universalk9-mz.SPA.154-2.CG
25 : c8000-universalk9-mz.SPA.156-3.CG
26 : c8000-universalk9-mz.SPA.156-3.CG
27 : c8000-universalk9-mz.SPA.156-3.M
28 : c8000-universalk9-mz.SPA.156-3.M
29 : ir800_yocto-1.7.2.tar
30 : ir800_yocto-1.7.2_python-2.7.3.tar
31 : pt1000-i-mz.122-28.bin
32 : pt3000-1eq412-mz.121-22.EA4.bin
```

Ilustración 76 revisión archivos del servidor

- c. Se baja uno de los archivos que se encuentran en el servidor

Con el comando get se descarga un archivo, en este caso el asa842-k8.bin

```
ftp>get asa842-k8.bin
Reading file asa842-k8.bin from 27.100.0.32:
File transfer in progress...
[Transfer complete - 5571584 bytes]
5571584 bytes copied in 20.093 secs (63535 bytes/sec)
ftp>
```

Ilustración 77 descarga de archivo servidor a cliente

- d. Se sale del servidor y se verifica que el archivo esté en el cliente.

Se sale de la sesión con el comando quit y se visualizan los archivos con el comando dir

```
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  19:00 PM           5571584    asa842-k8.bin
12/31/1969  19:00 PM             26      sampleFile.txt
                           5571610 bytes        2 File(s)
C:\>|
```

Ilustración 78 cierre sesión

- c. A continuación, se presenta una bitácora de comandos utilizados. Desde el modo simulación se ingresa nuevamente al servidor FTP y se sube el archivo .TXT que se encuentre en el cliente. Se analizan los encabezados de la capa de aplicación que se producen en donde se indique la conexión, envío de usuario y clave, mensajes de confirmación de aceptación, envío del archivo y fin de la comunicación.

Comandos utilizados

- Dir: lista los archivos
- Get [archivo]: descarga archivo del servidor
- Put [archivo]: sube un archivo al servidor
- ftp [ip] crea la conexión entre cliente y servidor FTP
- quit: sale de la conexión entre cliente y servidor FTP

Explicación proceso

- Nos conectamos al servidor con la clave y contraseña y con el comando put subimos un archivo ya definido en la maquina cliente llamado sampleFile.txt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 27.100.0.32
Trying to connect...27.100.0.32
Connected to 27.100.0.32
220- Welcome to PT Ftp server
Username:jorge
331- Username ok, need password
Password:
230- Logged in
(pассив mode On)
ftp>dir!
Invalid or non supported command.
ftp>!dir
Invalid or non supported command.
ftp>put sampleFile.txt

Writing file sampleFile.txt to 27.100.0.32:
File transfer in progress...

[Transfer complete - 26 bytes]
```

Ilustración 79 conexión y transferencia a servidor

- Luego de eso usamos el comando dir para ver los documentos presentes en el servidor

```
ftp>dir

Listing /ftp directory from 27.100.0.32:
 0 : asa042-k8.bin                               5571584
 1 : asa923-k8.bin                               30468096
 2 : c1841-adviservicesk9-mz.124-15.T1.bin     33591768
 3 : c1841-ipbase-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-i6q412-mz.121-22.EA4.bin           3058048
15 : c2950-i6q412-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       6512000
31 : pt1000-i-mz.122-28.bin                   5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin         3117390
33 : sampleFile.txt                           26
```

Ilustración 80 verificación del archivo subido al servidor

- Finalmente se sale con el comando quit después de ver que el archivo se subió correctamente con el registro

```
ftp>quit
221- Service closing control connection.
```

Ilustración 81 finalización de sesión

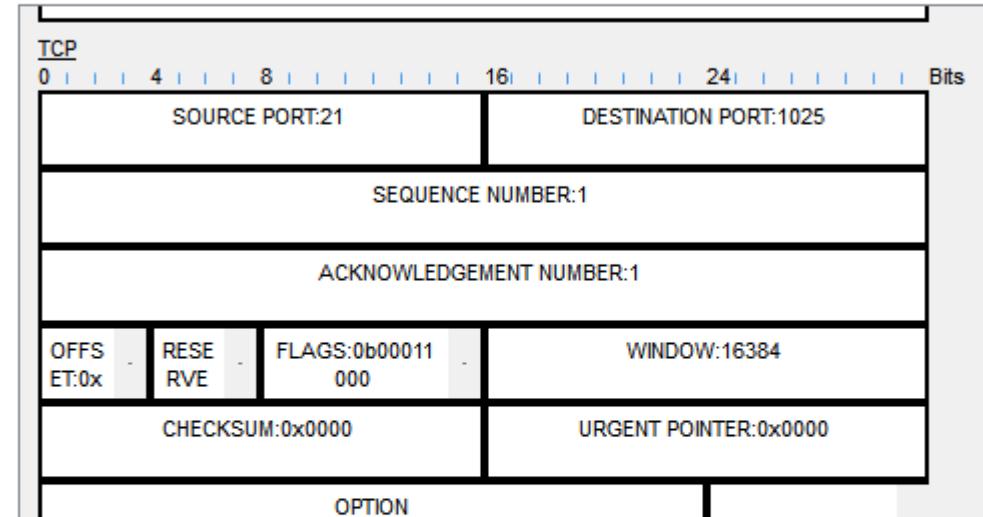
PDUs involucrados en el proceso

- Se establece conexión con el servidor mediante la solicitud con el comando ftp y la ip del servidor

PDU Information at Device: estudianteS1 .34

OSI Model Inbound PDU Details

PDU Formats



FTP Response

0 4 8 16 Bytes

Code:220

Message:Welcome to PT Ftp server

Ilustración 82 solicitud conexión

- Luego de esto se envía la contraseña junto con el usuario para validar la

solicitud

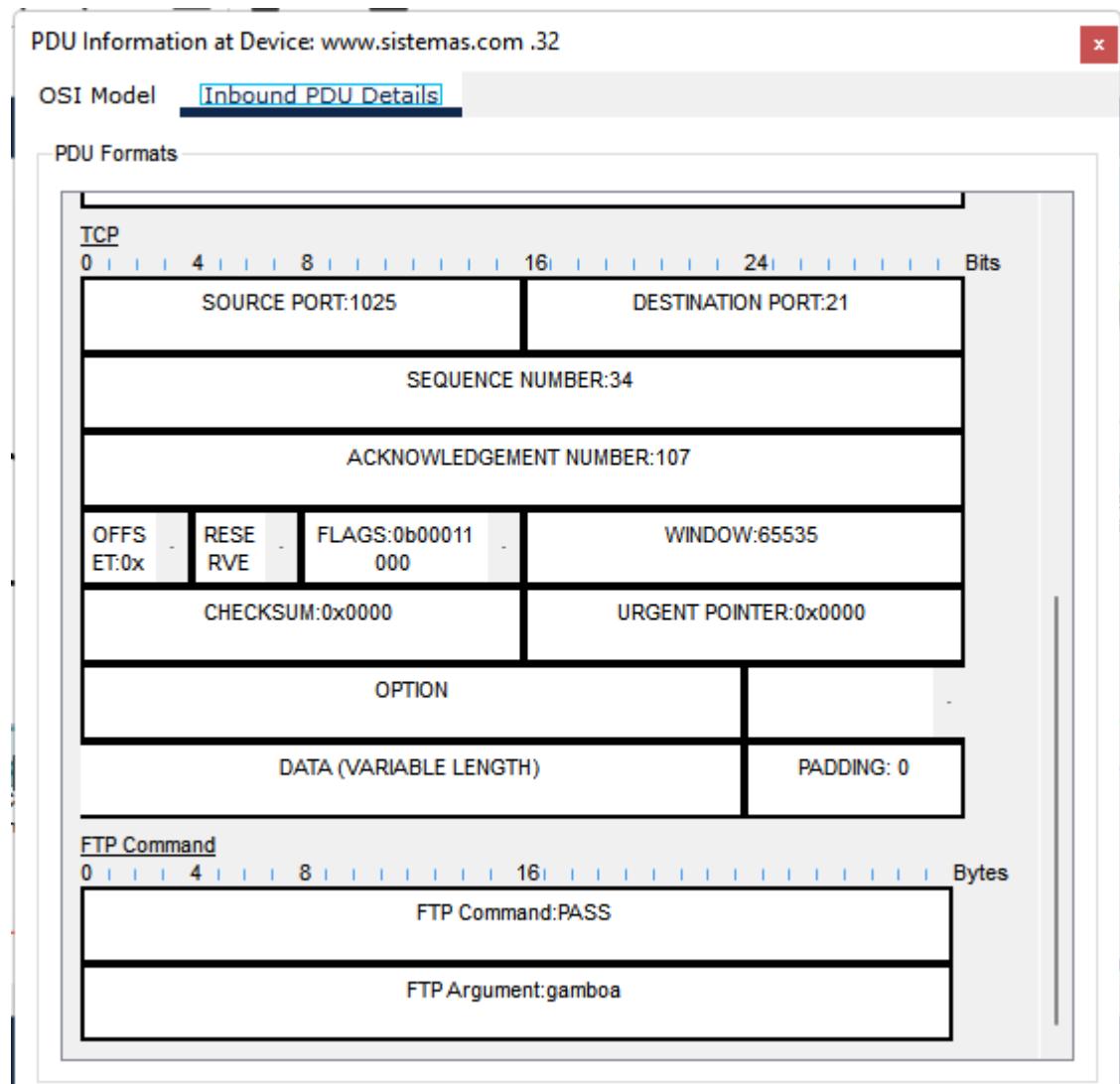


Ilustración 83 validación contraseña correcta

- Se informa que la contraseña y el usuario son correctos

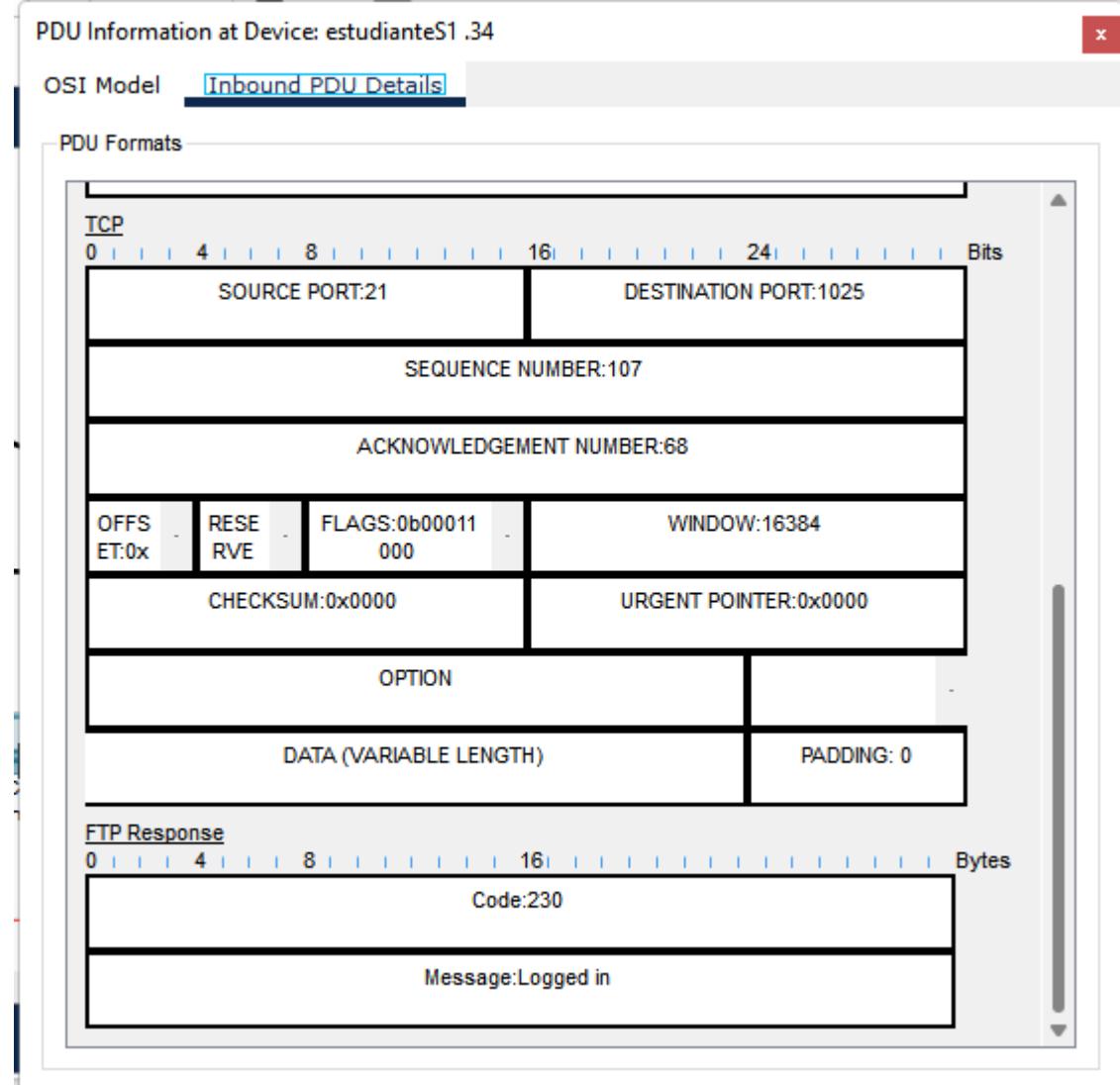


Ilustración 84 validación correcta

- Inicia la transferencia de documentos.

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
0.001		estudianteS1 .34	Switch0	FTP
0.002		Switch0	www.sistemas.com .32	FTP
0.002		--	www.sistemas.com .32	FTP
0.003		www.sistemas.com .32	Switch0	FTP
0.004		Switch0	estudianteS1 .34	FTP
0.004		--	estudianteS1 .34	FTP
0.005		estudianteS1 .34	Switch0	FTP
0.006		Switch0	www.sistemas.com .32	FTP
0.006		--	www.sistemas.com .32	FTP
0.007		www.sistemas.com .32	Switch0	FTP
0.008		Switch0	estudianteS1 .34	FTP
0.008		--	estudianteS1 .34	FTP
0.009		estudianteS1 .34	Switch0	FTP
0.010		Switch0	www.sistemas.com .32	FTP
0.010		--	www.sistemas.com .32	FTP
0.011		www.sistemas.com .32	Switch0	FTP
0.012		Switch0	estudianteS1 .34	FTP
0.016		--	estudianteS1 .34	FTP
0.017		--	estudianteS1 .34	FTP
0.018		estudianteS1 .34	Switch0	FTP
0.019		Switch0	www.sistemas.com .32	FTP
0.019		--	www.sistemas.com .32	FTP
0.028		--	www.sistemas.com .32	FTP
0.029		www.sistemas.com .32	Switch0	FTP
0.030		Switch0	estudianteS1 .34	FTP

Reset Simulation Constant Delay Captured to: 139.956 s

Play Controls:

Ilustración 85 proceso transferencia de documentos

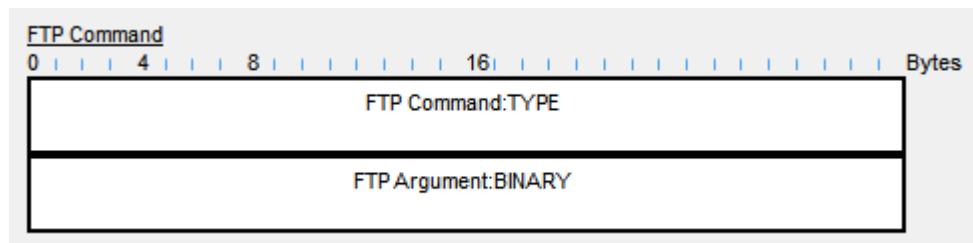


Ilustración 86 transferencia de datos 1

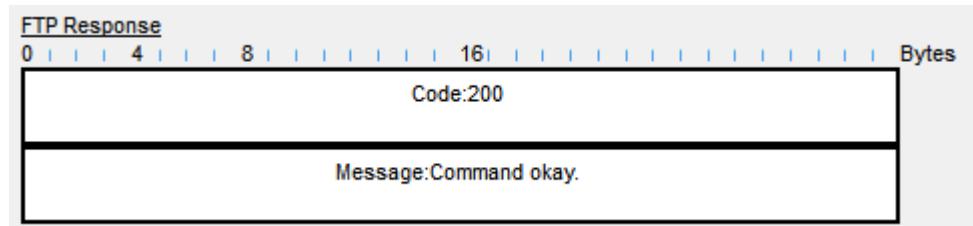


Ilustración 87 transferencia de datos 2

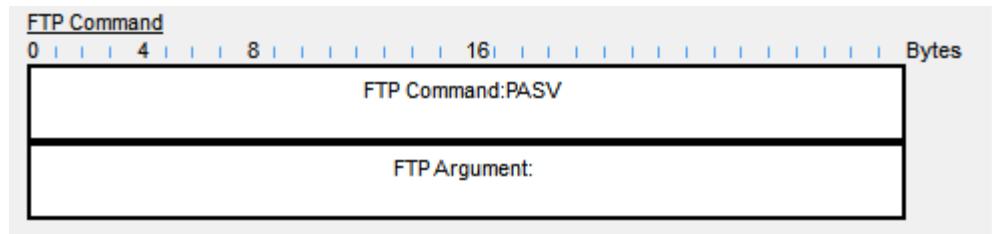


Ilustración 88 transferencia de datos 3

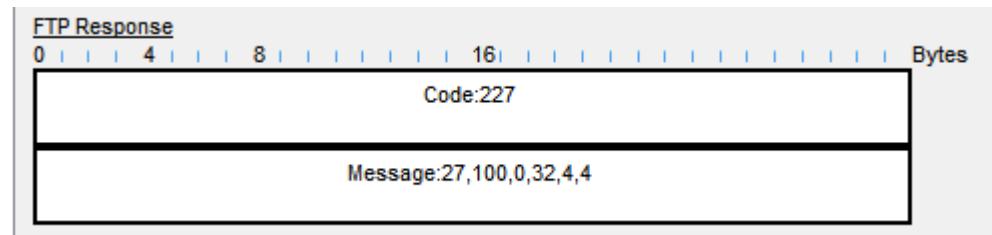


Ilustración 89 transferencia de datos 4

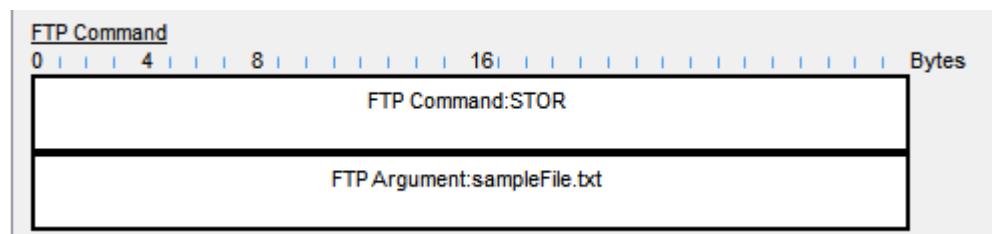


Ilustración 90 transferencia de datos 5

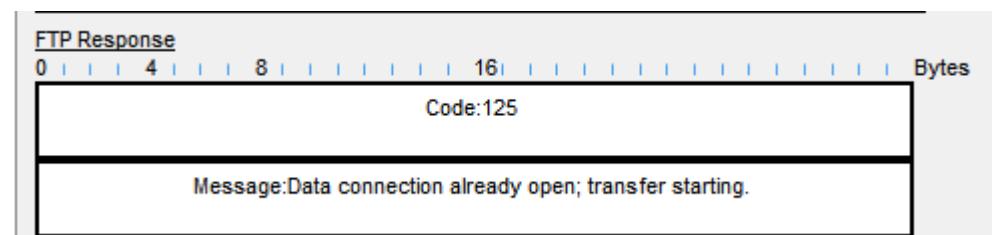


Ilustración 91 transferencia de datos 6

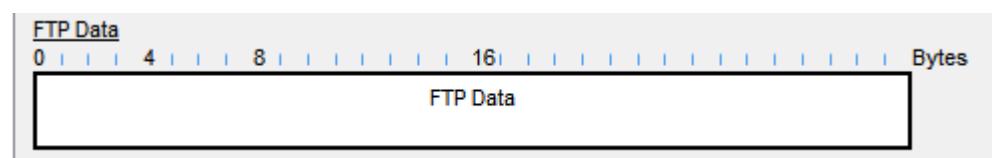


Ilustración 92 transferencia de datos 7

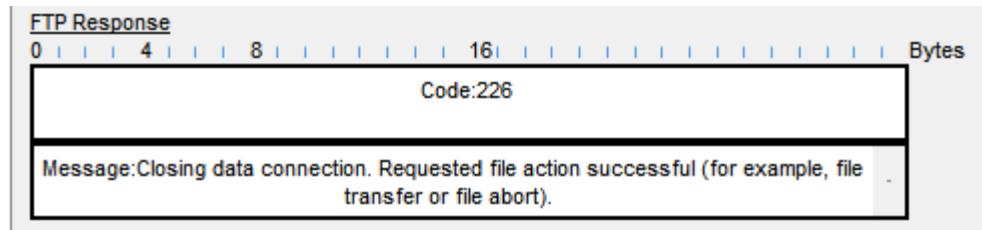


Ilustración 93 transferencia de datos 8

- Se ejecuta el comando dir para revisar los documentos y revisar que se encuentre

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
0.001	estudianteS1_34	Switch0	Switch0	FTP
0.002	--	www.sistemas.com_32	www.sistemas.com_32	FTP
0.003	www.sistemas.com_32	Switch0	Switch0	FTP
0.004	Switch0	estudianteS1_34	estudianteS1_34	FTP
0.004	--	estudianteS1_34	estudianteS1_34	FTP
0.005	estudianteS1_34	Switch0	Switch0	FTP
0.006	Switch0	www.sistemas.com_32	www.sistemas.com_32	FTP
0.006	--	www.sistemas.com_32	www.sistemas.com_32	FTP
0.007	www.sistemas.com_32	Switch0	Switch0	FTP
0.008	Switch0	estudianteS1_34	estudianteS1_34	FTP
0.008	--	estudianteS1_34	estudianteS1_34	FTP
0.009	estudianteS1_34	Switch0	Switch0	FTP
0.010	Switch0	www.sistemas.com_32	www.sistemas.com_32	FTP
0.010	--	www.sistemas.com_32	www.sistemas.com_32	FTP
0.011	www.sistemas.com_32	Switch0	Switch0	FTP
0.012	Switch0	estudianteS1_34	estudianteS1_34	FTP
0.018	--	www.sistemas.com_32	www.sistemas.com_32	FTP
0.019	www.sistemas.com_32	Switch0	Switch0	FTP
0.020	Switch0	estudianteS1_34	estudianteS1_34	FTP
0.020	--	www.sistemas.com_32	www.sistemas.com_32	FTP
0.021	www.sistemas.com_32	Switch0	Switch0	FTP
0.022	Switch0	estudianteS1_34	estudianteS1_34	FTP

Ilustración 94 proceso revisión documentos

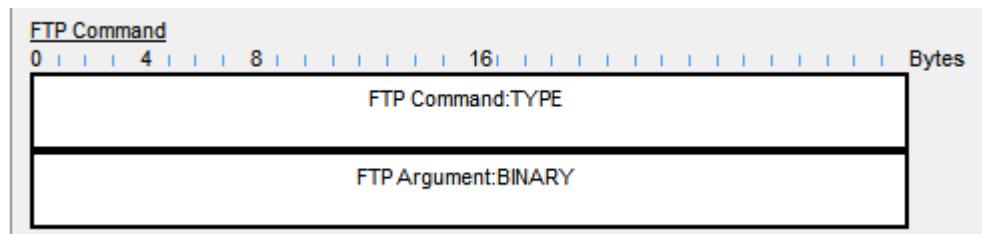


Ilustración 95 traspaso de datos 1

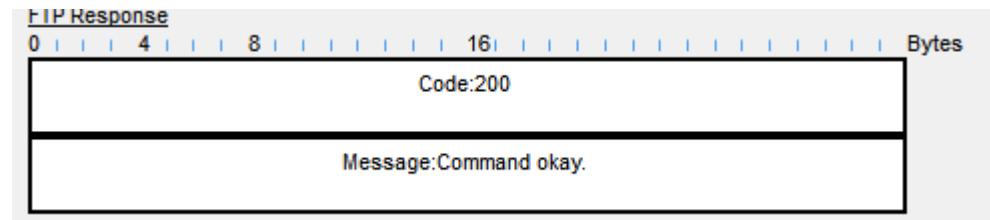


Ilustración 96 traspaso de datos 2

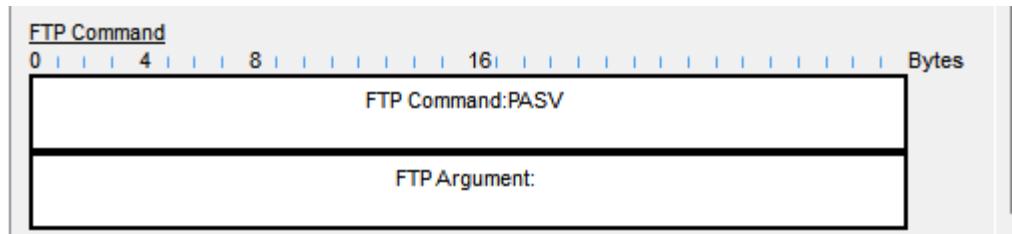


Ilustración 97 traspaso de datos 3

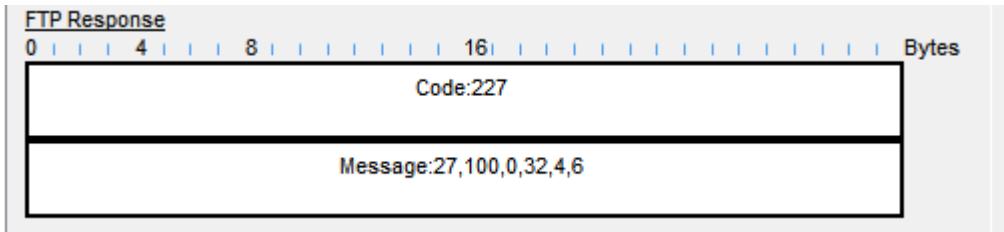


Ilustración 98 traspaso de datos 4

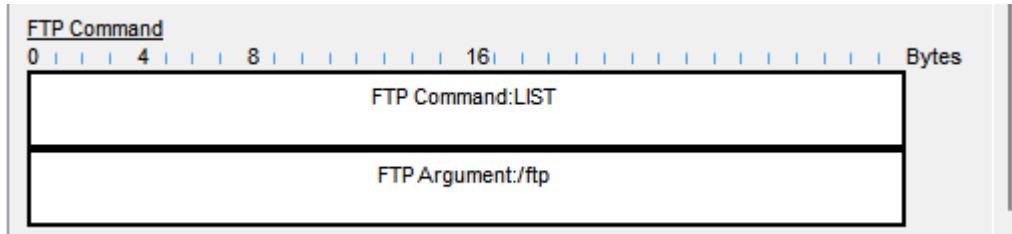


Ilustración 99 traspaso de datos 5

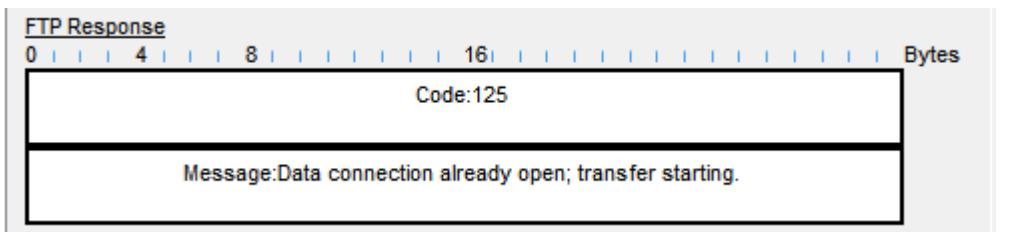


Ilustración 100 traspaso de datos 6

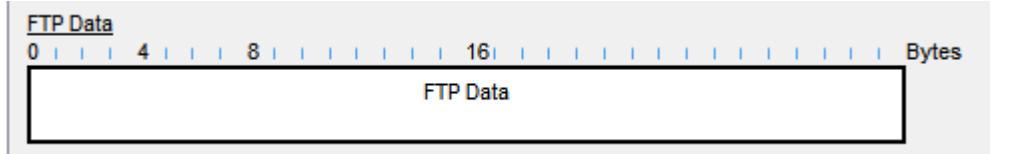


Ilustración 101 traspaso de datos 7

- Se sale de la conexión con el comando quit

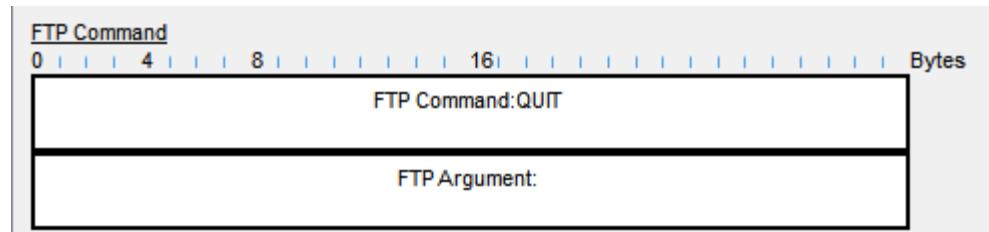


Ilustración 102 cierre sesión 1

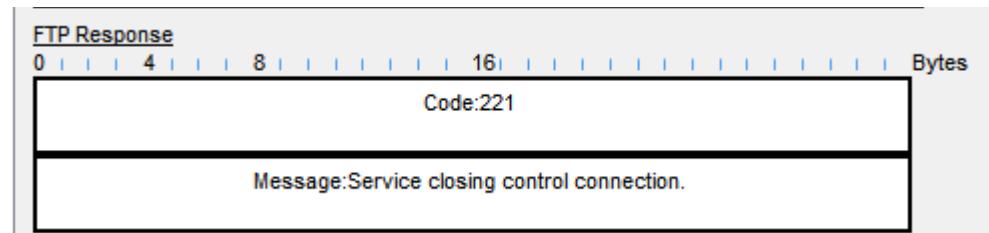


Ilustración 103 cierre sesión 2

En la red real

1. Wireshark

1.1. Captura web <http://laboratorio.is.escuelaing.edu.co/>

- DNS

Al consultar esta página, se realizó una consulta DNS hacia el subdominio del servidor DNS de la escuela. Al realizar la captura, observamos que el DNS se identifica con la dirección ipv6 2800:481:2300::4 así, filtramos por dicha ip escribiendo ipv6.addr == 2800:481:2300::4 y observamos sus paquetes.

Imagen No 104. Capturas DNS del dominio laboratorio.escuelaing.edu.co

Podemos observar un paquete que representa la solicitud de la dirección ipv4 desde el DNS cliente hacia el servidor DNS

6	0.019236	2800:481:2300::4	2800:486:987:4500::7	DNS	172	Standard query response 0x34e5 HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com.
7	3.812631	2800:486:987:4500::7	2800:481:2300::4	DNS	112	Standard query 0x6f7e AAAA laboratorio.is.escuelaing.edu.co
8	3.812866	2800:486:987:4500::7	2800:481:2300::4	DNS	112	Standard query 0xd967 A laboratorio.is.escuelaing.edu.co
9	3.813058	2800:486:987:4500::7	2800:481:2300::4	DNS	112	Standard query 0x9555 HTTPS laboratorio.is.escuelaing.edu.co
10	3.816692	2800:486:987:4500::7	2800:481:2300::4	DNS	103	Standard query 0xa64d AAAA safebrowsing.google.com
11	3.816918	2800:486:987:4500::7	2800:481:2300::4	DNS	103	Standard query 0xdb5f A safebrowsing.google.com

Imagen No 105. Paquetes específicos del funcionamiento DNS

Abrimos el paquete para obtener más detalles, en este podemos observar la consulta realizada desde el DNS cliente por un puerto dinámico 61546 hacia el DNS de laboratorio.is.escuelaing.edu.co el cual se comunica por el puerto 53.

UNIVERSIDAD

```

> Frame 83: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: ASUSTekCOMPU_ad:d9c (7c:10:c9:ad:ed:9c), Dst: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20)
> Internet Protocol Version 6, Src: 2800:486:987:4500:7d4c:5726:42d9:20c0, Dst: 2800:481:2300::4
> User Datagram Protocol, Src Port: 61546, Dst Port: 53
    Source Port: 61546
    Destination Port: 53
    Length: 58
    Checksum: 0x02ea [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (58 bytes)
> Domain Name System (query)

0000  14 82 5b 00 00 20 7c 10 c9 ad ed 9c 86 dd 60 08 ...[... | .....`.
0010  b0 83 00 3a 11 40 28 00 04 86 09 87 45 00 7d 4c ...:@( ...-E )L
0020  57 26 42 d9 20 c0 28 00 04 81 23 00 00 00 00 00 W&B -( ...#.....
0030  00 00 00 00 00 04 f0 6a 00 35 00 3a 02 ea d9 67 .....j 5 :... g
0040  01 00 00 01 00 00 00 00 00 00 0b 6c 61 62 6f 72 .....labor
0050  61 74 6f 72 69 6f 02 69 73 0a 65 73 63 75 65 6c atorio:i s\escuel
0060  61 69 6e 67 03 65 64 75 02 63 6f 00 00 01 00 01 aing.edu.co .....

No.: 83 - Time: 4.588984 - Source: 2800:486:987:4500:7d4c:5726:42d9:20c0 - Destination: 2800:481:2300:4 - Protocol: DNS - Length: 112 - Info: Standard query 0xd967 A laboratorio.is.escuelaing.edu.co
 Mostrar bytes de paquete Layout: Vertical (Stacked)

```

Imagen No 106. Paquete DNS cliente al servidor DNS laboratorio.is.escuelaing.edu.co

Observamos la captura del paquete de la respuesta del servidor DNS desde el puerto 53 al puerto 61546.

Imagen No. 107 Captura de la respuesta del servidor DNS

Para obtener más detalles, abrimos el paquete y dentro de este podemos ver la dirección ipv4 del servidor web al que se está solicitando y que `laboratorio.is.escuelaing.edu.co` es un alias de `jade.is.escuelaing.edu.co`

```

▶ User Datagram Protocol, Src Port: 53, Dst Port: 61546
  ▶ Domain Name System (response)
    Transaction ID: 0xd967
    ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 2
  ▶ Queries
    ▶ laboratorio.is.escuelaing.edu.co: type A, class IN
      Name: laboratorio.is.escuelaing.edu.co
      [Name Length: 32]
      [Label Count: 5]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  ▶ Answers
    ▶ laboratorio.is.escuelaing.edu.co: type CNAME, class IN, cname jade.is.escuelaing.edu.co
    ▶ jade.is.escuelaing.edu.co: type A, class IN, addr 45.239.88.88
  ▶ Authoritative nameservers
    ▶ is.escuelaing.edu.co: type NS, class IN, ns dns2.is.escuelaing.edu.co
    ▶ is.escuelaing.edu.co: type NS, class IN, ns dns1.is.escuelaing.edu.co
  ▶ Additional records
    ▶ dns1.is.escuelaing.edu.co: type A, class IN, addr 45.239.88.97
    ▶ dns2.is.escuelaing.edu.co: type A, class IN, addr 45.239.88.98
  [Request Id: 8]
  [Time: 0.031435000 seconds]

0000 124 16 201 173 237 156 20 130 91 0 0 32 134 221 96 0 |.....[ ... .
0010 0 0 0 163 17 58 40 0 4 129 35 0 0 0 0 0 .....:( .#...
0020 0 0 0 0 0 4 40 0 4 134 9 135 69 0 125 76 .....( .....E ]L
0030 87 38 66 217 32 192 0 53 240 106 0 163 185 12 217 103 W&B ..5 j....g
0040 129 128 0 1 0 2 0 2 0 2 11 108 97 98 111 114 .....labor
0050 97 116 111 114 105 111 2 105 115 10 101 115 99 117 101 108 atorio.i s.escuel
0060 97 105 110 103 3 101 100 117 2 99 111 0 0 1 0 1 aing.edu .co....
0070 192 12 0 5 0 1 0 1 81 128 0 7 4 106 97 100 .....: Q...:jad
0080 101 192 24 192 62 0 1 0 1 0 1 81 128 0 4 45 e...>... .Q...
0090 239 88 88 192 24 0 2 0 1 0 1 81 128 0 7 4 .XX.....Q...
00a0 100 110 115 50 192 24 192 24 0 2 0 1 0 1 81 128 dns2.....Q.
00b0 0 7 4 100 110 115 49 192 24 192 116 0 1 0 1 0 ...dns1. ....t....
00c0 1 81 128 0 4 45 239 88 97 192 97 0 1 0 1 0 .Q....X a-a.....
00d0 1 81 128 0 4 45 239 88 98 .....X b

```

Imagen No. 108 Paquete de respuesta del servidor DNS al cliente

- HTTP

Como primera instancia, filtramos el tráfico por la ip del servidor web. Esta ip fue conocida al capturar el paquete DNS anterior. También la podemos confirmar en la consola digitando nslookup. En Wireshark podemos observar las capturas de esta, entre ellas, http.

No.	Time	Source	Destination	Protocol	Length Info	
861	12.355377	192.168.20.90	192.168.20.90	TCP	66 88 = 57996 [SYN] Seq=0 Wnn=64240 Len=8 HHS=1468 Wn=256 SACK_PERM	
862	12.378353	192.168.20.90	192.168.20.90	TCP	66 88 = 57995 [SYN, ACK] Seq=1 Wnn=29200 Len=8 HHS=1468 SACK_PERM Wn=128	
877	12.378006	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
878	12.379041	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
879	12.379041	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
888	12.375667	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
882	12.378353	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
899	12.378353	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
930	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
931	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
932	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
933	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
934	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
935	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
936	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
937	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
938	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
939	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
940	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
941	12.359666	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
942	12.361286	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
943	12.361286	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
944	12.361286	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
945	12.373991	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
946	12.373991	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
947	12.373991	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
948	12.373991	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
949	12.379448	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
950	12.379448	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
951	12.379448	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
952	12.379448	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
953	12.379448	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
954	12.379448	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
955	12.379448	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
956	12.379448	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
961	12.387709	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
962	12.387755	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
962	12.387755	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
963	12.387782	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
964	12.387782	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
965	12.387802	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
965	12.387802	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
966	12.388891	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
967	12.388891	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
968	12.388816	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
968	12.388816	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
969	13.007508	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
970	13.007508	192.168.20.90	45.239.88.88	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
971	13.007508	45.239.88.88	192.168.20.90	TCP	54 57995 = 80 [ACK] Seq=1 Ack=1 Wnn=26356 Len=0	
Frame 879: 949 bytes on wire (7592 bits), 949 bytes captured (7592 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C6268436} (Intel PRO/100 MT Desktop Adapter) at 00:00:00:00:00:20 [eth0] Ethernet II, Src: ASUSTekCPU (00:0c:29:00:00:20), Dst: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20) > Destination: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20) > Source: ASUSTekCPU (00:0c:29:00:00:20) Type: IPv4 (0x0800) [Stream Index: 1] Internet Protocol Version 4, Src: 192.168.20.90, Dst: 45.239.88.88 Transmission Control Protocol, Src Port: 57095, Dst Port: 80, Seq: 1, Ack: 1, Len: 895 Hypertext Transfer Protocol						

Imagen No. 109 Captura del tráfico del servidor web de laboratorio.is.escuelaing.edu.co

Por tanto, mejoramos el filtro de búsqueda y colocamos “ip.addr==45.239.88.88 && http” y podemos tener una mejor apreciación de los paquetes capturados por http.

No.	Time	Source	Destination	Protocol	Length Info
879	12.373333	192.168.20.90	45.239.88.88	HTTP	949 GET / HTTP/1.1
1003	13.023205	45.239.88.88	192.168.20.90	HTTP	330 HTTP/1.1 200 OK (text/html)
1019	13.156935	192.168.20.90	45.239.88.88	HTTP	910 GET /favicon.ico HTTP/1.1
1021	13.166982	45.239.88.88	192.168.20.90	HTTP	474 HTTP/1.1 404 Not Found (text/html)
Frame 879: 949 bytes on wire (7592 bits), 949 bytes captured (7592 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C6268436} (Intel PRO/100 MT Desktop Adapter) at 00:00:00:00:00:20 Ethernet II, Src: ASUSTekCPU (00:0c:29:00:00:20), Dst: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20) > Destination: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20) > Source: ASUSTekCPU (00:0c:29:00:00:20) Type: IPv4 (0x0800) [Stream Index: 1] Internet Protocol Version 4, Src: 192.168.20.90, Dst: 45.239.88.88 Transmission Control Protocol, Src Port: 57095, Dst Port: 80, Seq: 1, Ack: 1, Len: 895 Hypertext Transfer Protocol					

Imagen No. 110 Captura del tráfico del protocolo HTTP

El primer paquete nos indica cuando nosotros, como clientes realizamos un GET por un puerto dinámico, en este caso, 57095 al servidor web el cual responde por medio del puerto 80.

```

> Frame 879: 949 bytes on wire (7592 bits), 949 bytes captured (7592 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c), Dst: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20)
> Internet Protocol Version 4, Src: 192.168.20.90, Dst: 45.239.88.88
> Transmission Control Protocol, Src Port: 57095, Dst Port: 80, Seq: 1, Ack: 1, Len: 895
    Source Port: 57095
    Destination Port: 80
    [Stream index: 18]
    [Stream Packet Number: 4]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 895]
    Sequence Number: 1      (relative sequence number)
    Sequence Number (raw): 3097176286
    [Next Sequence Number: 896      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 672244451
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0x5ee3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (895 bytes)

0000  14 82 5b 00 00 20 7c 10 c9 ad ed 9c 08 00 45 00  ..[ . | .....E.
0010  03 a7 de 85 40 00 80 06 00 00 c8 a4 5a 2d ef  ... @. ....Z-
0020  58 58 df 07 00 50 68 9b 2d 28 11 a2 e3 50 18  XX...P...(<..P.
0030  04 02 5e e3 00 00 47 45 54 20 2f 20 48 54 54 50  ..^...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6c 61 62 6f  /1.1-Ho st: labo
0050  72 61 74 6f 72 69 6f 2e 69 73 2e 65 73 63 75 65  ratorio. is.escue
0060  6c 61 69 6e 67 2e 65 64 75 26 63 6f 0d 0a 43 6f  laing.ed.u.co.co
0070  6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61  nnection : keep-a
0080  6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e  live--Up grade-In
0090  73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a  secure-e requests:
00a0  20 31 0d 0a b5 73 65 72 2d 41 67 65 66 74 3a 2b  1 -User-Agent:
00b0  4d 6f 7a 69 6c 6c 61 2f 35 2e 30 2b 57 69 6e Mozilla/ 5.0 (Win
00c0  64 6f 77 73 20 4e 54 20 31 3e 2e 30 3b 2b 57 69 dows NT 10.0; Wi
00d0  6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 n64; x64 ) AppleW
00e0  65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 eckKit/53.7.36 (KHTML
00f0  54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29, lik e Gecko)
0100  20 43 68 72 6f 6d 65 2f 31 32 39 2e 30 2e 30 2e Chrome/ 129.0.0.
0110  30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36*
0120  0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74  Accept: text/ht
0130  6d 6c 2a 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,application/x
0140  68 74 6d 6c 2b 78 6d 6c 2c 61 70 6c 69 63 61 html+xml , applica
0150  74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml ;q=0.9,image/
0160  6d 61 67 65 2f 61 76 69 66 2e 69 6d 61 67 65 2f webp,image/png,
0170  77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c */;q=0.8,application/x
0180  2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 /signed-exchange;
0190  61 74 69 6f 6e 2f 73 69 67 66 65 64 2d 65 78 63 hange;v= b3;q=0.7
01a0  68 61 66 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37
01b0  0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e
01c0  67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65
01d0  0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67
01e0  65 3a 20 65 73 2d 45 53 2c 65 73 3b 71 3d 30 2e
01f0  39 0d 0a 43 6f 6f 6b 69 65 3a 20 68 75 62 73 70 9. Cookie: hubsp

```

Imagen No. 111 Paquete del primer GET del cliente al servidor web

En el segundo paquete, observamos cuando el servidor web responde a la solicitud con un mensaje 200 que confirma su solicitud y devuelve los objetos de la página. En este caso, el puerto de origen es el 80 y el de destino el 57095.

UNIVERSIDAD

```

> Frame 1003: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20), Dst: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c)
> Internet Protocol Version 4, Src: 45.239.88.88, Dst: 192.168.20.90
> Transmission Control Protocol, Src Port: 80, Dst Port: 57095, Seq: 48212, Ack: 896, Len: 276
    Source Port: 80
    Destination Port: 57095
    [Stream index: 18]
    [Stream Packet Number: 52]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 276]
    Sequence Number: 48212 (relative sequence number)
    Sequence Number (raw): 672292662
    [Next Sequence Number: 48488 (relative sequence number)]
    Acknowledgment Number: 896 (relative ack number)
    Acknowledgment number (raw): 3097177181
    0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
    Window: 243
    [Calculated window size: 31104]
    [Window size scaling factor: 128]
    Checksum: 0xade9 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (276 bytes)
.....  

0000  7c 10 c9 ad ed 9c 14 82 5b 00 00 20 08 00 45 00 |..... [ ... E·
0010  01 3c 3f ac 40 00 37 06 a7 c6 2d ef 58 58 c0 a8 ·<@ 7 ·-- XX·
0020  14 5a 00 50 df 07 28 12 5f 36 b8 9b 2c 5d 50 18 ·Z·P ·( _6 ·,]P·
0030  00 f3 ad e9 00 00 70 3a 2f 2f 6c 61 62 6f 72 61 ···· p: //labora
0040  74 6f 72 69 6f 2e 69 73 2e 65 73 63 75 65 6c 61 torio.is .escuela
0050  69 6e 67 2e 65 64 75 2e 63 6f 2f 77 70 2d 63 6f ing.edu. co/wp-co
0060  6e 74 65 6e 74 2f 70 6e 75 67 69 6e 73 2f 65 6c ntent/pl ugins/el
0070  65 6d 65 6e 74 6f 72 2f 61 73 73 65 74 73 2f 6a ementor/ assets/j
0080  73 2f 66 72 6f 6e 74 65 6e 64 2e 6d 69 6e 2e 6a s/fronte nd.min.j
0090  73 3f 76 65 72 3d 33 2e 38 2e 31 27 3e 3c 2f 73 s?ver=3. 8.1'>/s
00a0  63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 73 cript> < script s
00b0  72 63 3d 27 68 74 74 70 3a 2f 2f 6c 61 62 6f 72 rc='http ://labor
00c0  61 74 6f 72 69 6f 2e 69 73 2e 65 73 63 75 65 6c atorio.i s.escuel
00d0  61 69 6e 67 2e 65 64 75 2e 63 6f 2f 77 70 2d 63 aing.edu. co/wp-c
00e0  6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 65 ontent/p lugins/e
00f0  6c 65 6d 65 6e 74 6f 72 2f 61 73 73 65 74 73 2f lementor/ assets/
0100  6a 73 2f 70 72 65 6c 6f 61 64 65 64 2d 6d 6f 64 js/prelo aded-mod
0110  75 6c 65 73 2e 6d 69 6e 2e 6a 73 3f 76 65 72 3d ules.min .js?ver=
0120  33 2e 38 2e 31 27 3e 3c 2f 73 63 72 69 70 74 3e 3.8.1'>< /script>
0130  0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 ...</bod y></ht
0140  6d 6c 3e 0d 0a 30 0d 0a 0d 0a ml>...< ...
```

Imagen No. 112 Paquete de respuesta 200 del servidor web al cliente

En el tercer paquete, podemos observar que se realiza otro GET desde el puerto 57095 al 80.

```

> Frame 1019: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: ASUSTekCOMPU_8c:9c (7c:10:c9:ad:ed:9c), Dst: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20)
> Internet Protocol Version 4, Src: 192.168.20.90, Dst: 45.239.88.88
> Transmission Control Protocol, Src Port: 57095, Dst Port: 80, Seq: 896, Ack: 48488, Len: 856
    Source Port: 80
    Destination Port: 80
    [Stream index: 18]
    [Stream Packet Number: 54]
    > [Conversation completeness: Complete, WITH_DATA (31)]
        [TCP Segment Len: 856]
        Sequence Number: 896      (relative sequence number)
        Sequence Number (raw): 3097177181
        Next Sequence Number: 1752      (relative sequence number)
        Acknowledgment Number: 48488      (relative ack number)
        Acknowledgment number (raw): 672292938
        0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0x5ebc [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (856 bytes)
.....
0000 14 82 5b 00 00 20 7c 10 c9 ad ed 9c 08 00 45 00  ..[...|.....E
0010 03 80 0d 93 40 00 88 06 00 00 c0 a8 14 5a 2d ef  ...@.....Z-
0020 58 58 df 07 00 50 b8 9b 2c 5d 28 12 60 4a 50 18  XX---P...](^JP
0030 04 02 5e bc 00 00 47 45 54 20 2f 66 61 76 69 63  ..^...GE T /Favic
0040 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d on.ico H TTP/1.1
0050 0a 48 6f 73 74 3a 28 6c 61 62 6f 72 61 74 6f 72 Host: 1 aborator
0060 69 6f 2e 69 73 2e 65 73 63 75 65 6c 61 69 6e 67 io.is.es cuelaing
0070 2e 65 64 75 2e 63 6f 0d 0a 43 6f 66 6e 65 63 74 .edu.co Connect
0080 69 6f 6e 3a 20 6b 65 65 0d 20 61 6c 69 76 65 0d ion: kee p-alive
0090 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a User-Agent: Moz
00a0 69 6c 6c 63 2f 35 2e 30 20 57 69 6e 64 6f 77 illa/5.0 (Windows
00b0 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 s NT 10. 0; Win64
00c0 3b 20 78 36 34 29 28 41 70 70 6c 65 57 65 62 4b ; x64) A ppleWebK
00d0 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c it/537.3 6 (KHTML
00e0 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 , like G ecko) Ch
00f0 72 6f 6d 65 2f 31 32 39 2e 30 2e 30 2e 30 29 53 rome/129. 0.0.0 S
0100 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/53.7.36 Ac
0110 63 65 70 74 3a 20 69 6d 61 67 65 2f 61 76 69 66 cept: image/avif
0120 2c 69 6d 62 67 65 2f 77 65 62 78 2c 69 6d 61 67 ,image/w ebp,imag
0130 65 2f 61 70 6e 67 2c 69 6d 67 65 2f 73 76 67 e/apng,image/svg
0140 2b 78 6d 6c 2c 69 6d 61 67 65 2f 2a 2c 2a 2f 2a +xml,image/*,*
0150 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 72 3a ;q=0.8 Referer:
0160 20 68 74 70 3a 2f 2f 6c 61 62 6f 72 61 74 6f http:// laborato
0170 72 69 6f 69 73 2e 65 73 63 75 65 6c 61 69 6e rio.is.scuelain
0180 67 2e 65 64 75 2e 63 6f 2f 0d 0a 41 63 63 65 70 g.edu.co / - Accep
0190 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encoding: gzip
01a0 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 , deflate e - Accep
01b0 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 73 2d 45 t-Language: es-E
01c0 53 2c 65 73 3b 71 3d 30 2e 39 0d 0a 43 6f 6f 6b 5,es;q=0.9 - cook
01d0 69 65 3a 20 68 75 62 73 70 6f 74 75 74 6b 3d 36 ie: hubs potatk=6
01e0 64 39 33 36 36 64 37 32 31 61 62 33 39 38 62 34 d9366d72 lab390b4
01f0 37 66 66 62 65 36 34 39 64 63 34 66 63 63 63 3b 7ffbe649 dc4fccc;

```

Imagen No. 113 Segundo GET del cliente al servidor web

Sin embargo, en el cuarto paquete, observamos que el servidor responde con un 404 not found indicando que la URL indicada no se encontró.

```

> Frame 1021: 474 bytes on wire (3792 bits), 474 bytes captured (3792 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20), Dst: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c)
> Internet Protocol Version 4, Src: 45.239.88.88, Dst: 192.168.20.90
> Transmission Control Protocol, Src Port: 80, Dst Port: 57095, Seq: 48488, Ack: 1752, Len: 420
    Source Port: 80
    Destination Port: 57095
    [Stream index: 18]
    [Stream Packet Number: 56]
    > [Conversation completeness: Complete, WITH_DATA (31)]
        [TCP Segment Len: 420]
        Sequence Number: 48488      (relative sequence number)
        Sequence Number (raw): 672292938
        [Next Sequence Number: 48908      (relative sequence number)]
        Acknowledgment Number: 1752      (relative ack number)
        Acknowledgment number (raw): 3097178037
        0101 .... = Header Length: 20 bytes (5)
    > Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 32896]
    [Window size scaling factor: 128]
    Checksum: 0xb693 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (420 bytes)

0000  7c 10 c9 ad ed 9c 14 82 5b 00 00 20 08 00 45 00 |.....[...E-
0010  01 cc 3f ae 40 00 37 06 a7 34 2d ef 58 58 c0 a8 ..?@7-4-XX-
0020  14 5a 00 50 df 07 28 12 60 4a b8 9b 2f b5 50 18 Z P(.J-/P-
0030  01 01 b0 93 00 00 48 54 54 50 2f 31 2e 31 20 34 .....HT TP/1.1.4
0040  30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61 04 Not Found Da
0050  74 65 3a 20 46 72 69 2c 20 32 37 28 53 65 70 20 te: Fri, 27 Sep
0060  32 30 32 34 20 30 30 3a 31 35 3a 35 33 20 47 4d 2024 00: 15:53 GM
0070  54 0d 00 53 65 72 76 65 72 3a 20 41 70 61 63 68 T-Serve r: Apach
0080  65 2f 32 3e 5e 2e 34 33 20 28 55 6e 69 78 29 20 e/2.4.43 (Unix)
0090  50 48 50 2f 37 2e 34 2e 36 0d 0a 43 6f 6e 74 65 PHP/7.4.6 Conte
00a0  6e 74 2d 4c 65 6e 67 74 68 3a 20 31 39 36 0d 0a nt-Lengt h: 196
00b0  4b 65 65 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 Keep-Ali ve: time
00c0  6f 75 74 3d 35 2c 28 6d 61 78 3d 39 39 0d 0a 43 out=5, m ax=99 C
00d0  6f 6e 66 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d connectio n: Keep-
00e0  41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 Alive-C ontent-T
00f0  79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 ype: tex t/html;
0100  63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 charset= iso-8859
0110  2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 -1 ... <!DOCTYPE
0120  48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f HTM< PUB LIC "-//
0130  49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 IETF//DT D HTML 2
0140  2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c .0//EN"> <html><
0150  68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 head><t itle>404
0160  20 3e 0e 4f 74 20 46 75 6e 64 3c 2f 74 69 74 6c Not Fou nd</titl
0170  65 3e 0e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e e></hea d><body>
0180  0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f <h1>Not Found</
0190  68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 h1><p>I he requ
01a0  73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 ested URL was not
01b0  20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 found o n this s
01c0  65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 erver.</ p></bod
01d0  79 3e 3c 2f 68 74 6d 6c 3e 0a y></html >
```

Imagen No. 114 Paquete de respuesta 404 del servidor web al cliente

Si seguimos interactuando con cada una de las páginas de la web, podemos observar el proceso en el que se hace un GET y el servidor web devuelve los objetos correspondientes junto con el mensaje exitoso 200.

o.	Time	So	http	Destination	Protocol	Length	Info
52	4.157473	19	http3	20.90	45.239.88.88	1042	GET /index.php/horarios/ HTTP/1.1
133	4.644911	45.239.88.88		192.168.20.90	HTTP	931	GET /wp-content/uploads/elementor/css/post-80.css?ver=1725905337 HTTP/1.1
152	4.751232	45.239.88.88		192.168.20.90	HTTP	1194	HTTP/1.1 200 OK (text/css)
165	4.751323	192.168.20.90		45.239.88.88	HTTP	93	GET /wp-content/uploads/2024/08/Horario-.png HTTP/1.1
168	4.751970	45.239.88.88		192.168.20.90	HTTP	956	HTTP/1.1 200 OK (text/html)
457	4.815593	45.239.88.88		192.168.20.90	HTTP	1109	HTTP/1.1 200 OK (PNG)
493	10.402471	192.168.20.90		45.239.88.88	HTTP	1019	GET / HTTP/1.1
541	11.062041	45.239.88.88		192.168.20.90	HTTP	330	HTTP/1.1 200 OK (text/html)
567	18.404744	192.168.20.90		45.239.88.88	HTTP	1021	GET /index.php/decanatura/ HTTP/1.1
623	19.012035	45.239.88.88		192.168.20.90	HTTP	221	HTTP/1.1 200 OK (text/html)
625	19.013255	192.168.20.90		45.239.88.88	HTTP	976	GET /wp-content/uploads/2020/09/Plan-de-Estudios-Sistemas.png HTTP/1.1
780	19.086450	45.239.88.88		192.168.20.90	HTTP	458	HTTP/1.1 200 OK (PNG)
831	19.132202	192.168.20.90		45.239.88.88	HTTP	1800	HTTP/1.1 200 OK (periodos-anteriores/ HTTP/1.1
883	24.387977	192.168.20.90		45.239.88.88	HTTP	952	GET /wp-content/uploads/elementor/css/post-195.css?ver=1725905980 HTTP/1.1
894	25.008336	45.239.88.88		192.168.20.90	HTTP	947	HTTP/1.1 200 OK (text/css)
938	25.127780	45.239.88.88		192.168.20.90	HTTP	791	HTTP/1.1 200 OK (text/html)
1058	33.034092	192.168.20.90		45.239.88.88	HTTP	1059	GET /index.php/convenios/ HTTP/1.1
1097	34.178939	192.168.20.90		45.239.88.88	HTTP	932	GET /wp-content/uploads/elementor/css/post-64.css?ver=1724698094 HTTP/1.1
1106	34.209853	45.239.88.88		192.168.20.90	HTTP	621	HTTP/1.1 200 OK (text/css)
1126	34.389303	192.168.20.90		45.239.88.88	HTTP	964	GET /wp-content/uploads/2020/07/icon-cloud-aws.png HTTP/1.1
1127	34.389421	192.168.20.90		45.239.88.88	HTTP	965	GET /wp-content/uploads/2020/10/microsoft-azure.png HTTP/1.1
1152	34.404156	45.239.88.88		192.168.20.90	HTTP	767	HTTP/1.1 200 OK (text/html)
1167	34.408193	192.168.20.90		45.239.88.88	HTTP	99	GET /wp-content/uploads/2020/07/1200px-Cisco_logo_blue_2016.svg.png HTTP/1.1
1256	34.422715	45.239.88.88		192.168.20.90	HTTP	917	HTTP/1.1 200 OK (PNG)
1265	34.423429	192.168.20.90		45.239.88.88	HTTP	956	GET /wp-content/uploads/2020/10/oracle.png HTTP/1.1
1268	34.424111	45.239.88.88		192.168.20.90	HTTP	186	HTTP/1.1 200 OK (PNG)
1271	34.424899	45.239.88.88		192.168.20.90	HTTP	831	HTTP/1.1 200 OK (PNG)
1273	34.425357	192.168.20.90		45.239.88.88	HTTP	963	GET /wp-content/uploads/2020/07/IBM_logo_id20.png HTTP/1.1
1276	34.426168	192.168.20.90		45.239.88.88	HTTP	957	GET /wp-content/uploads/2020/07/tableau.jpg HTTP/1.1
1279	34.426836	192.168.20.90		45.239.88.88	HTTP	955	GET /wp-content/uploads/2020/07/unity.jpg HTTP/1.1
1297	34.437873	45.239.88.88		192.168.20.90	HTTP	1059	HTTP/1.1 200 OK (PNG)
1348	34.446083	45.239.88.88		192.168.20.90	HTTP	949	HTTP/1.1 200 OK (PNG)
1364	34.454646	45.239.88.88		192.168.20.90	HTTP	570	HTTP/1.1 200 OK (JPEG 3IF image)
1431	34.480611	45.239.88.88		192.168.20.90	HTTP	1198	HTTP/1.1 200 OK (JPEG 3IF image)

Imagen No. 115 Capturas del servidor web al interactuar con la página varias veces

1.2. Captura tráfico DHCP

Antes realizar la captura, quitamos la dirección de la máquina digitando ipconfig /release

C:\Users\andre>ipconfig /release "Ethernet"

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

```
Sufijo DNS específico para la conexión. . . : 
Dirección IPv6 . . . . . : 2800:486:987:4500:b6a:87ae:a0d3:11bf
Dirección IPv6 . . . . . : 2800:486:987:4500:ab34:adf2:726e:76f6
Dirección IPv6 temporal. . . . . : 2800:486:987:4500:7d4c:5726:42d9:20c0
Vínculo: dirección IPv6 local. . . . . : fe80::6543:91a3:ba60:5722%17
Puerta de enlace predeterminada . . . . . : fe80::1682:5bff:fe00:20%17
```

Adaptador de Ethernet Ethernet 2:

```
Sufijo DNS específico para la conexión. . . : 
Vínculo: dirección IPv6 local. . . . . : fe80::4dde:5313:2f05:8837%11
Dirección IPv4. . . . . : 192.168.56.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
```

C:\Users\andre>

Imagen No. 116 Desactivar la ip actual del computador

Empezamos la captura y digitamos ipconfig /renew para volver a solicitar la dirección ip

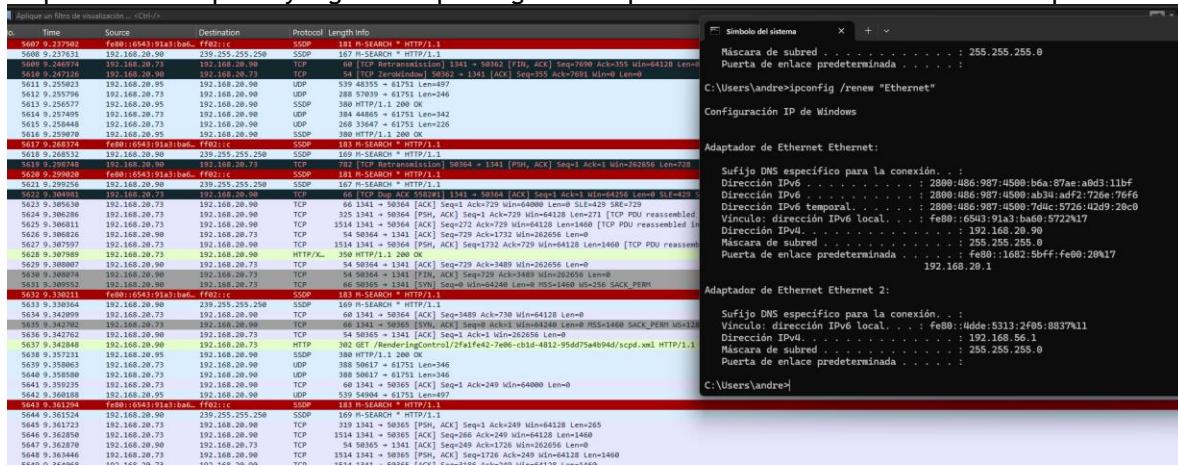


Imagen No. 117 Capturas del servicio DHCP

Filtramos el tráfico digitando dhcp, podemos observar que se realizó el proceso DORA.

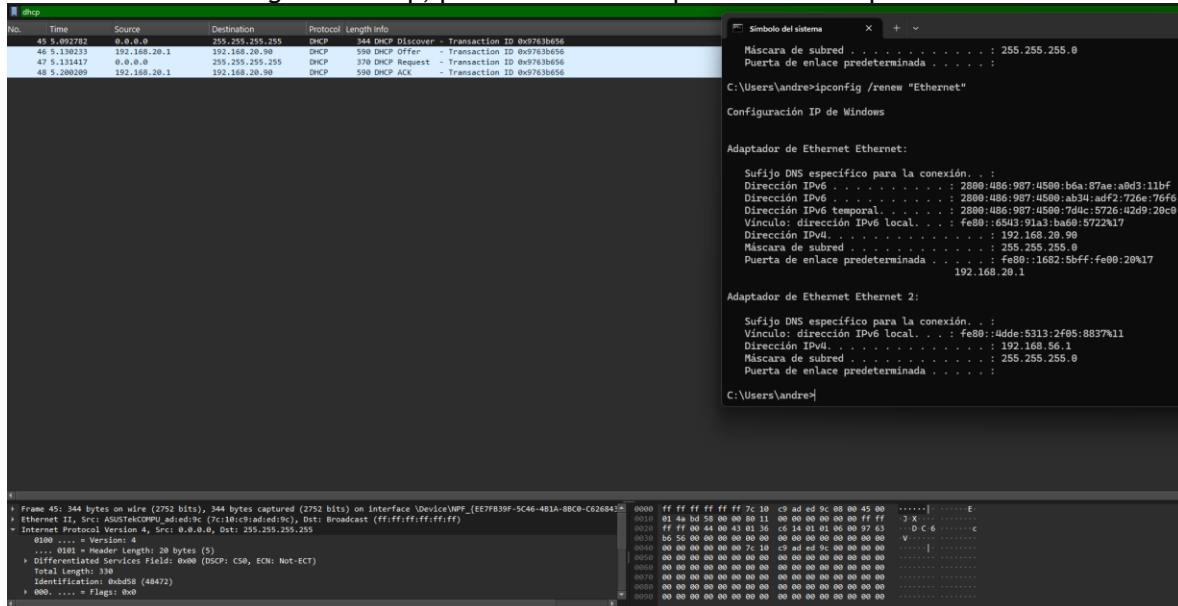


Imagen No. 118 Filtro del protocolo DHCP

En el primer paquete, podemos analizar el mensaje Discover, en este, el cliente hace un broadcast por el puerto 68 hacia los servidores cuyo puerto sea 67.

UNIVERSIDAD

```

> Frame 45: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: ASUSTekCOMP_1ad:ed:9c (7c:10:c9:ad:ed:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
└ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 330
        Identification: 0xbdb58 (48472)
    > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: UDP (17)
        Header Checksum: 0x0000 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 0.0.0.0
        Destination Address: 255.255.255.255
        [Stream index: 7]
    > User Datagram Protocol, Src Port: 68, Dst Port: 67
    > Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff 7c 10 c9 ad ed 9c 08 00 45 00 ..... | . E.
0010 01 4a bd 58 00 00 80 11 00 00 00 00 00 00 ff ff J-X | . .
0020 ff ff 00 44 00 43 01 36 c6 14 01 01 06 00 97 63 .. D C-6 . .
0030 b6 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 V - .
0040 00 00 00 00 00 00 7c 10 c9 ad ed 9c 08 00 00 00 00 ..... | .
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
0110 00 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01 ..... | c Sc5 = .
0120 7c 10 c9 ad ed 9c 32 04 c0 a8 14 5a 0c 0f 4c 41 | . 2 . Z LA
0130 50 54 4f 50 2d 47 53 49 49 36 50 48 45 3c 08 4d PTOP-GSI I6PHE< M
0140 53 46 54 20 35 2e 30 37 0e 01 03 06 0f 1f 21 2b SFT 5.07 !+
0150 2c 2e 2f 77 79 f9 fc ff ..... ,./vy . .

0: 45 - Time: 5.092782 - Source: 0.0.0.0 - Destination: 255.255.255.255 - Protocol: DHCP - Length: 344 - Info: DHCP Discover - Transaction ID 0x9763b656
 Mostrar bytes de paquete      Layout: Vertical (Stacked) ▾

```

Imagen No. 119 Paquete del mensaje Discover

En el segundo paquete observamos el mensaje Offer, donde el dhcp realiza una oferta sobre una ip al cliente. Este mensaje es transmitido por un broadcast del puerto 67 al 68.

UNIVERSIDAD

```

Frame 46: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
Ethernet II, Src: HefeiRadioCo_00:00:20 (14:82:5b:00:00:20), Dst: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c)
Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.90
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
        Total Length: 576
        Identification: 0x0000 (0)
        000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 64
        Protocol: UDP (17)
        Header Checksum: 0xcf01 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.20.1
        Destination Address: 192.168.20.90
        [Stream index: 8]
    > User Datagram Protocol, Src Port: 67, Dst Port: 68
    > Dynamic Host Configuration Protocol (Offer)

0000  7c 10 c9 ad ed 9c 14 82  5b 00 00 20 08 00 45 00  |-----[. . E
0010  02 40 00 00 00 40 11 cf 01 c0 a8 14 01 c0 a8  @ . @
0020  14 5a 00 43 00 44 02 2c b1 7c 02 01 06 00 97 63  Z C D , |-----c
0030  b6 56 00 00 00 00 00 00 00 00 c0 a8 14 5a c0 a8  V . . Z .
0040  14 01 00 00 00 00 7c 10 c9 ad ed 9c 00 00 00 00  . . .
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110  00 00 00 00 00 63 82 53 63 35 01 02 36 04 c0  . . . c Sc5 - 6
0120  a8 14 01 0c 0f 4c 41 50 54 4f 50 2d 47 53 49 49  . . . LAP TOP-GSII
0130  36 50 48 45 33 04 00 0d 2f 00 01 04 ff ff 00 6PHE3  / . .
0140  03 04 c0 a8 14 01 06 08 be 9d 08 6d be 9d 08 65  . . . m . e
0150  ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

a: 46 - Time: 5.130233 - Source: 192.168.20.1 - Destination: 192.168.20.90 - Protocol: DHCP - Length: 590 - Info: DHCP Offer - Transaction ID 0x9763b656
 Mostrar bytes de paquete      Layout: Vertical (Stacked)

```

Imagen No. 120 Paquete del mensaje Offer

En el siguiente paquete, observamos el mensaje Request, donde el cliente acepta la oferta y realiza un broadcast desde el puerto 68 al 67 para confirmarle al servidor que le asignó la ip.

UNIVERSIDAD

```

> Frame 47: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
    Total Length: 356
    Identification: 0xbd59 (48473)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
    [Stream index: 7]
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)

0000 ff ff ff ff ff ff 7c 10 c9 ad ed 9c 08 00 45 00 . . . . E
0010 01 64 bd 59 00 80 11 00 00 00 00 00 ff ff d Y . .
0020 ff ff 00 44 00 43 01 50 5b ec 01 01 06 00 97 63 D C P [ . . . . c
0030 b6 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 V . .
0040 00 00 00 00 00 00 7c 10 c9 ad ed 9c 00 00 00 00 | . .
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . .
0110 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 c Sc5 - . .
0120 7c 10 c9 ad ed 9c 32 04 c0 a8 14 5a 36 04 c0 a8 | . . . 2 . Z6 . .
0130 14 01 0c 0f 4c 41 50 54 4f 50 2d 47 53 49 49 36 LAPT OP-GSII6
0140 50 48 45 51 12 00 00 00 4c 41 50 54 4f 50 2d 47 PHEQ . . . LAPTOP-G
0150 53 49 49 36 50 48 45 3c 08 4d 53 46 54 20 35 2e SII6PHE< MSFT 5 .
0160 30 37 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 07 !.,./vy
0170 fc ff . . . .

No. 47 · Time: 5.131417 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 370 · Info: DHCP Request - Transaction ID 0x9763b656
 Mostrar bytes de paquete   Layout: Vertical (Stacked) ▾

```

Imagen No. 121 Paquete del mensaje Request

En el último paquete, observamos el mensaje de confirmación del servidor Acknowledge, el cual, asigna la ip y le confirma al cliente mediante el puerto 67 al 68.

UNIVERSIDAD

```

> Frame 48: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{EE7FB39F-5C46-4B1A-8BC0-C626843681D9}, id 0
> Ethernet II, Src: HefeiRadioCo 00:00:20 (14:82:5b:00:00:20), Dst: ASUSTekCOMPU_ad:ed:9c (7c:10:c9:ad:ed:9c)
> Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.90
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 576
        Identification: 0x0000 (0)
    > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xcf01 [validation disabled]
        [Header checksum status: Unverified]
    Source Address: 192.168.20.1
    Destination Address: 192.168.20.90
        [Stream index: 8]
    > User Datagram Protocol, Src Port: 67, Dst Port: 68
    > Dynamic Host Configuration Protocol (ACK)

0000  7c 10 c9 ad ed 9c 14 82  5b 00 00 20 08 00 45 00 | ..... [ - . E
0010  02 40 00 00 00 00 40 11  cf 01 c9 a8 14 01 c9 a8 @ . . @ ...
0020  14 5a 00 43 00 44 02 2c  ff 2b 02 01 06 00 97 63 Z C D , + . . c
0030  b6 56 00 00 00 00 00 00  00 00 c9 a8 14 5a c9 a8 V . . . Z .
0040  14 01 00 00 00 00 7c 10  c9 ad ed 9c 00 00 00 00 00 . . . | . . .
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 c0 . . . c Sc5 6
0120  a8 14 01 33 04 00 0d 2f  00 0c 0f 4c 41 50 54 4f . . . 3 . / . LAPTO
0130  50 2d 47 53 49 49 36 50  48 45 01 04 ff ff ff 00 P-GSII6P HE
0140  03 04 c9 a8 14 01 06 08  be 9d 08 6d be 9d 08 65 . . . m . e
0150  ff 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .
01f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00 . . . .

No. 48 Time: 5.200209 Source: 192.168.20.1 Destination: 192.168.20.90 Protocol: DHCP - Length: 590 Info: DHCP ACK - Transaction ID 0x9763b656
 Mostrar bytes de paquete Layout: Vertical (Stacked) ▾

```

Imagen No. 122 Paquete del mensaje Acknowledge

1.3. Captura tráfico TELNET y HTTP

- a. Analizamos la información de la capa de aplicación y puertos (capa de transporte) en el contenido de los paquetes capturados en una conexión HTTP
- Desbloqueamos el uso del protocolo TELNET.

Oprimimos las teclas Windows + r, buscamos control y le damos a aceptar

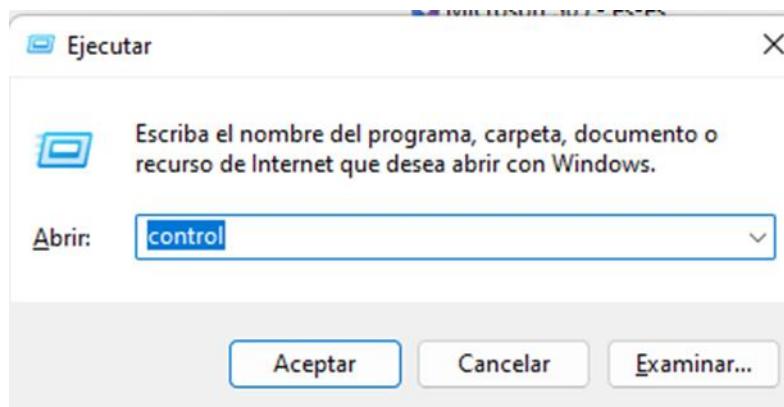


Ilustración 123 configuración cliente Telnet

Luego nos aparecerá un menú en la parte superior izquierda verificamos que se muestre la opción ver por iconos grandes

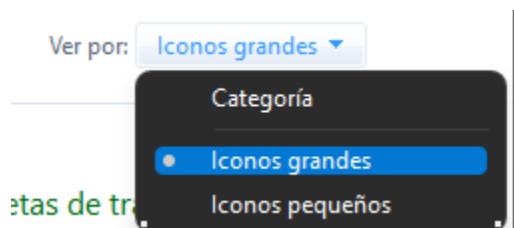


Ilustración 124 configuración ventana de ajustes

Luego de eso hacemos click en Programas y características

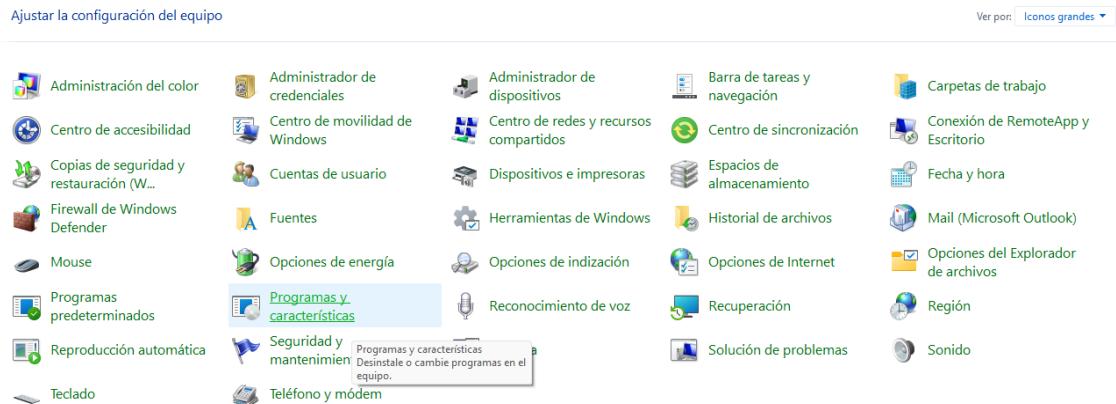


Ilustración 125 Selección programas y características

Damos click en Activar o desactivar las características de Windows



Ilustración 126 activación de características especiales de Windows

Activamos la opción de cliente Telnet y le damos a aceptar

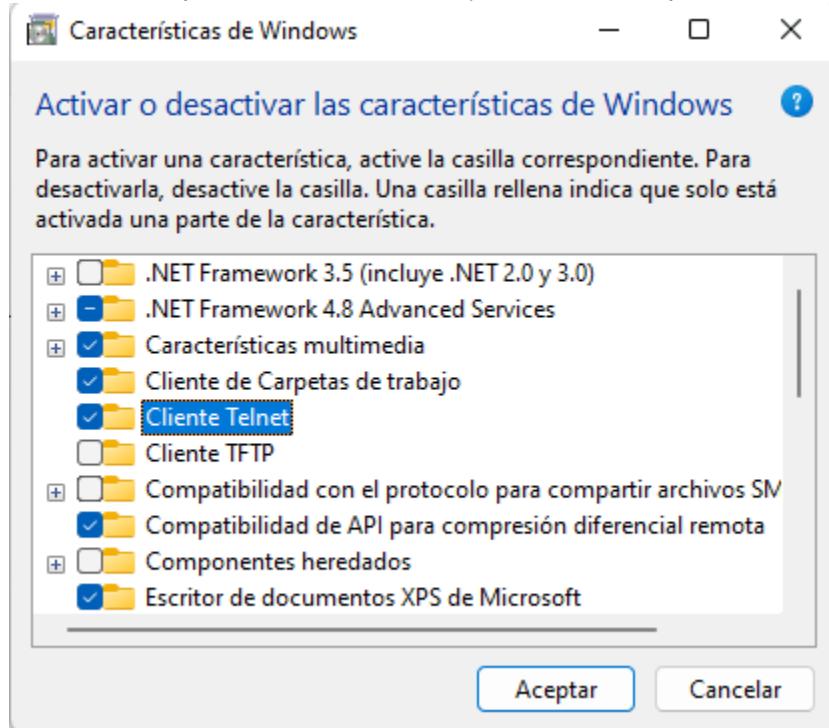


Ilustración 127 activación cliente telnet

- Realizamos la captura de los paquetes con protocolos TELNET y HTTP y luego mostramos los mensajes de la capa de aplicación generados en las siguientes consultas:
- La captura se realizó a la siguiente página web <http://profesores.is.escuelaing.edu.co/~csantiago/RECO/index.html> usando los protocolos:
 - Telnet
 - Se inicia la conexión al servidor con el comando Telnet profesores.is.escuelaing.edu.co 80

PowerShell 7.4.5
Loading personal and system profiles took 1296ms.
jgamb ➤ System32 ➤ telnet profesores.is.escuelaing.edu.co 80

Ilustración 128 inicio conexión mediante telnet

- Se hace la solicitud al recurso index.html con el siguiente comando

```
GET /~csantiago/RECO/index.html HTTP/1.1
Host: profesores.is.escuelaing.edu.co
```

tener en cuenta dejar un espacio en blanco al final para que funcione la consulta, de lo contrario no la aceptara y se finalizara la conexión por un Timeout error o un error de solicitud

```
HTTP/1.1 200 OK
Date: Fri, 27 Sep 2024 23:03:28 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
Content-Type: text/html

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

Se ha perdido la conexión con el host.

Ilustración 129 respuesta solicitud get index.html

Captura WireWhark }
Filtro: tcp.port == 80 && http

No.	Time	Source	Destination	Protocol	Length	Info
223	27.250769	192.168.1.3	45.239.88.86	HTTP	136	GET /~csantiago/RECO/index.html HTTP/1.1
225	27.324484	45.239.88.86	192.168.1.3	HTTP	532	HTTP/1.1 200 OK (text/html)

Ilustración 130 captura paquetes

▼ Transmission Control Protocol, Src Port: 50351, Dst Port: 80, Seq: 2, Ack: 1, Len: 82

- Source Port: 50351
- Destination Port: 80
- [Stream index: 31]
- ▶ [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 82]
- Sequence Number: 2 (relative sequence number)
- Sequence Number (raw): 3271019798
- [Next Sequence Number: 84 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 4214806530
- 0101 = Header Length: 20 bytes (5)
- ▶ Flags: 0x018 (PSH, ACK)
- Window: 513
- [Calculated window size: 131328]
- [Window size scaling factor: 256]
- Checksum: 0x4a0e [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- ▶ [Timestamps]
- ▶ [SEQ/ACK analysis]
- TCP payload (82 bytes)
- TCP segment data (82 bytes)

▶ [2 Reassembled TCP Segments (83 bytes): #221(1), #223(82)]

▼ Hypertext Transfer Protocol

- ▶ GET /~csantiago/RECO/index.html HTTP/1.1\r\n
- Host: profesores.is.escuelaing.edu.co\r\n
- \r\n
- [Full request URI: http://profesores.is.escuelaing.edu.co/~csantiago/RECO/index.html]
- [HTTP request 1/1]
- [Response in frame: 225]

Ilustración 131 captura solicitud index.html

- Se descarga el archivo tipo PDF prueba.pdf. con la siguiente solicitud
GET /~csantiago/RECO/prueba.pdf HTTP/1.1
Host: profesores.is.escuelaing.edu.co

Tener en cuenta la recomendación anterior

Ilustración 132 respuesta solicitud get prueba.pdf

Se puede observar cómo al ser una imagen y ser obtenida por medio de la terminal, esta no termina de verse debido a que la terminal no sabe o no soporta .pdf. por esta razón muestra el archivo codificado

WireShark

Filtro: tcp.port == 80 && http

+ 348 41.542805 192.168.1.3 45.239.88.86 HTTP 136 GET /~csantiago/RECO/prueba.pdf HTTP/1.1
+ 477 41.837351 45.239.88.86 192.168.1.3 HTTP 1444 HTTP/1.1 200 OK (application/pdf)

Ilustración 133 captura de paquetes

```

▼ Transmission Control Protocol, Src Port: 50352, Dst Port: 80, Seq: 2, Ack: 1
  Source Port: 50352
  Destination Port: 80
  [Stream index: 34]
  ▶ [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 82]
    Sequence Number: 2      (relative sequence number)
    Sequence Number (raw): 1700412392
    [Next Sequence Number: 84      (relative sequence number)]
    Acknowledgment Number: 1      (relative ack number)
    Acknowledgment number (raw): 1910200684
    0101 .... = Header Length: 20 bytes (5)
    ▶ Flags: 0x018 (PSH, ACK)
      Window: 513
      [Calculated window size: 131328]
      [Window size scaling factor: 256]
      Checksum: 0x81a0 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    ▶ [Timestamps]
    ▶ [SEQ/ACK analysis]
      TCP payload (82 bytes)
      TCP segment data (82 bytes)
  ▶ [2 Reassembled TCP Segments (83 bytes): #346(1), #348(82)]
  ▼ Hypertext Transfer Protocol
    ▶ GET /~csantiago/RECO/prueba.pdf HTTP/1.1\r\n
      Host: profesores.is.escuelaing.edu.co\r\n
      \r\n
      [Full request URI: http://profesores.is.escuelaing.edu.co/~csantiago/RECO/prueba.pdf]
      [HTTP request 1/1]
      [Response in frame: 477]

```

Ilustración 134 captura solicitud get prueba.pdf

- Se descarga el archivo tipo imagen network.png. con la siguiente solicitud

GET /~csantiago/RECO/network.png HTTP/1.1
 Host: profesores.is.escuelaing.edu.co

Tener en cuenta el formato y la recomendación anterior



Ilustración 135 visualización solicitud network.png

Como en el caso anterior, debido a que la terminal no soporta formato .png, este recurso no se podrá visualizar de manera correcta

WireShark

	2677 109.976236	192.168.1.3	45.239.88.86	HTTP	137 GET /~csantiago/RECO/network.png HTTP/1.1
+	2718 110.149675	192.168.1.3	45.239.88.86	HTTP	57 Continuation
+	2722 110.204321	192.168.1.3	45.239.88.86	HTTP	57 Continuation
+	2734 110.205634	45.239.88.86	192.168.1.3	HTTP	384 HTTP/1.1 200 OK (PNG)

Ilustración 136 consulta wireShark

```

▼ Transmission Control Protocol, Src Port: 50373, Dst Port: 80, Seq: 2, Ack: 1, Len: 83
  Source Port: 50373
  Destination Port: 80
  [Stream index: 63]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 83]
  Sequence Number: 2      (relative sequence number)
  Sequence Number (raw): 2563722452
  [Next Sequence Number: 85      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 2549783252
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
  Window: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x9d43 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  TCP payload (83 bytes)
  TCP segment data (83 bytes)
  ▶ [2 Reassembled TCP Segments (84 bytes): #2675(1), #2677(83)]
  ▶ Hypertext Transfer Protocol
    ▶ GET /~csantiago/RECO/network.png HTTP/1.1\r\n
    Host: profesores.is.escuelaing.edu.co\r\n
    \r\n
    [Full request URI: http://profesores.is.escuelaing.edu.co/~csantiago/RECO/network.png]
    [HTTP request 1/1]
    [Response in frame: 2734]

```

Ilustración 137 visualización solicitud get network.png

- HTTP
 - Usamos el browser para mirar las mismas páginas que consultamos con TELNET

- Index.html



Ilustración 138 visualización index.html

- Prueba.pdf

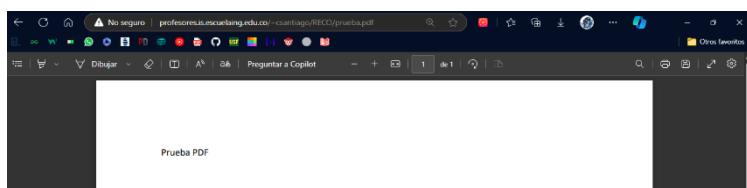


Ilustración 139 visualización prueba.pdf

- Network.png

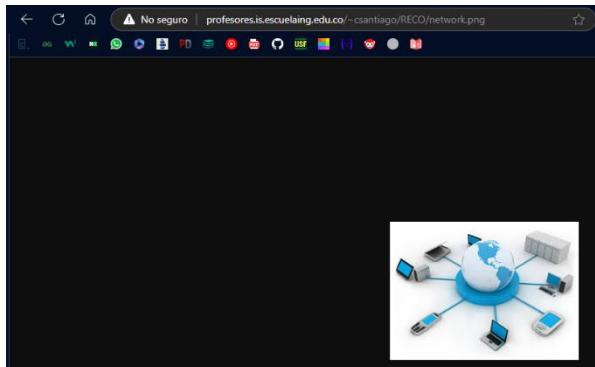


Ilustración 140 visualización network.png

La captura realizada en Wireshark es la siguiente:

http.request.method == "GET" && tcp.port == 80						
No.	Time	Source	Destination	Protocol	Length	Info
68	10.182398	192.168.1.3	45.239.88.86	HTTP	1385	GET /~csantiago/RECO/index.html HTTP/1.1
170	22.630631	192.168.1.3	45.239.88.86	HTTP	1388	GET /~csantiago/RECO/prueba.pdf HTTP/1.1
246	28.296215	192.168.1.3	45.239.88.86	HTTP	1388	GET /~csantiago/RECO/network.png HTTP/1.1

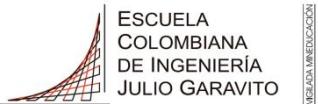
Ilustración 141 captura de telnet con wireShark

Se puede observar la solicitud de los tres recursos el index.html, prueba.pdf y network.png por medio del protocolo HTTP mediante una solicitud GET al Host: profesores.is.escuelaing.edu.co mediante el protocolo de transporte TCP

- ¿Qué diferencia encuentra entre los archivos descargados con el protocolo Telnet y con el browser?

Se puede observar que la transferencia de archivos hecha mediante Telnet tiene problemas, ya que no se puede visualizar de manera correcta los archivos png y pdf, además de que solo se puede ver la estructura del archivo index.html. Para visualizarlo correctamente hay que cambiarles el formato, mientras que el navegador los reconoce y los abre directamente en el formato esperado. Además de que solo se puede ver la estructura del archivo index.html

En cuanto a la captura de paquetes, se puede evidenciar que no varía mucho el uso del protocolo TELNET. Sin embargo, observamos que con TELNET se veían paquetes con la información "continuation", indicando que se estaba descargando un archivo que podía visualizarse en la consola



ESCUELA
COLOMBIANA
DE INGENIERÍA
JULIO GARAVITO

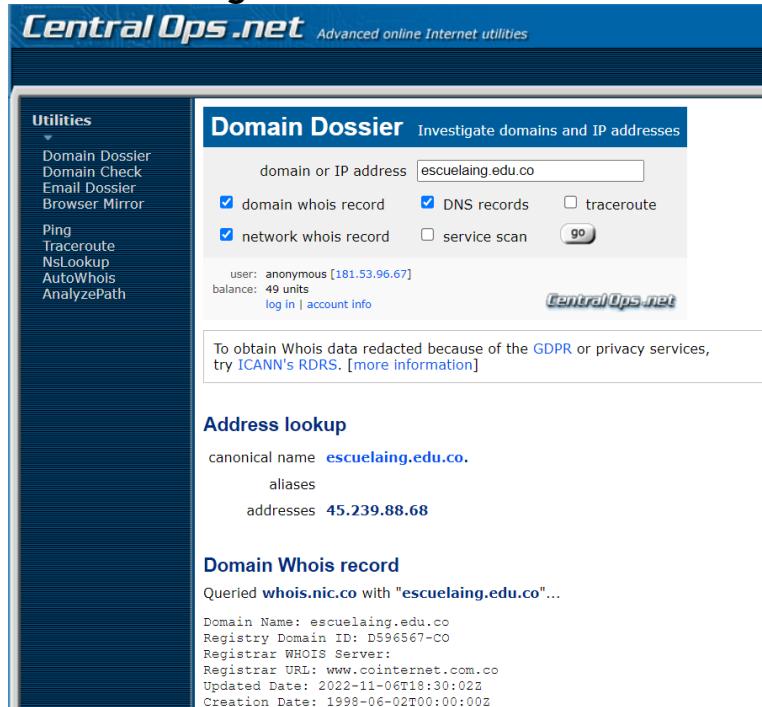
VERIFICACIÓN

UNIVERSIDAD

2. Prueba con equipos servicio DNS

A continuación, se presentan las pruebas DNS realizadas mediante el portal web CentralOps, donde se consultaron los siguientes dominios para verificar la configuración DNS y su correspondiente resolución:

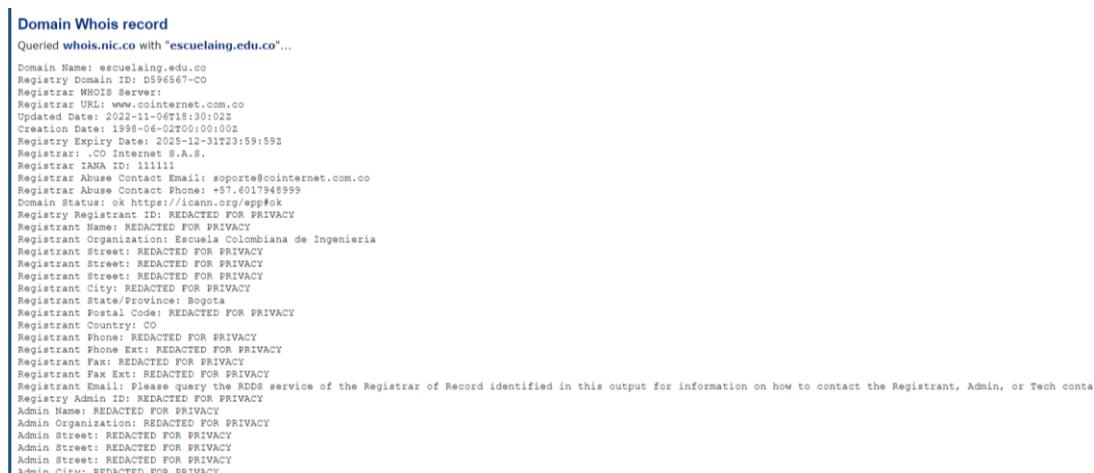
2.1. Escuelaing.edu.co



The screenshot shows the 'Domain Dossier' interface on the Central Ops .net website. The search bar contains 'escuelaing.edu.co'. Under 'Domain Whois record', it shows the domain was queried from whois.nic.co. The WHOIS details include:

- Domain Name: escuelaing.edu.co
- Registry Domain ID: D596567-CO
- Registrar WHOIS Server: Registrar URL: www.cointernet.com.co
- Updated Date: 2022-11-06T18:30:02Z
- Creation Date: 1998-06-02T00:00:00Z
- Registrar: CO Internet S.A.S.
- Registrar IP: 10.11.11.11
- Registrar Abuse Contact Email: soporte@cointernet.com.co
- Registrar Abuse Contact Phone: +57 6017948999
- Domain Status: ok https://icann.org/epp#ok
- Registry Registrant ID: REDACTED FOR PRIVACY
- Registrant Name: REDACTED FOR PRIVACY
- Registrant Organization: Escuela Colombiana de Ingeniería
- Registrant Street: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant City: REDACTED FOR PRIVACY
- Registrant State/Province: Bogota
- Registrant Postal Code: REDACTED FOR PRIVACY
- Registrant Country: CO
- Registrant Phone: REDACTED FOR PRIVACY
- Registrant Fax: REDACTED FOR PRIVACY
- Registrant Fax Ext: REDACTED FOR PRIVACY
- Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contacts.
- Registry Admin ID: REDACTED FOR PRIVACY
- Admin Name: REDACTED FOR PRIVACY
- Admin Organization: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin City: REDACTED FOR PRIVACY

Imagen No. 142 Búsqueda del dominio escuelaing.edu.co



The screenshot shows the 'Domain Whois record' interface on the Central Ops .net website. It displays the same WHOIS information as the previous screenshot, including the domain name, registration date, and contact details, all of which are heavily redacted for privacy.

UNIVERSIDAD

```

Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Postcode: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Tech Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of
Name Server: ns1.escuelaing.edu.co
Name Server: ns2.escuelaing.edu.co
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-09-23T19:08:02Z <<<

```

Network Whois record

Queried whois.lacnic.net with "45.239.88.68"...

inetnum:	45.239.88.0/22
status:	assigned
aut-num:	N/A
name:	ESCUOLA COLOMBIANA DE INGENIERIA

Imagen No. 143 Información general del servicio DNS de escuelaing.edu.co

Utilities	
Domain Dossier	inetnum: 45.239.88.0/22
Domain Check	status: assigned
Email Dossier	aut-num: N/A
Browser Mirror	owner: ESCUELA COLOMBIANA DE INGENIERIA
Ping	ownerid: CO-ECIN2-LACNIC
Traceroute	responsible: JULIAN GARCIA
NsLookup	address: AUTOP NORTE KM 13 / AV 13 205-59, ,
AutoWhois	address: 9999 - BOGOTA - BO
AnalyzePath	country: CO
	phone: +057 01 6683600 [272]
	owner-c: JUG11
	tech-c: JUG11
	abuse-c: JUG11
	created: 20180724
	changed: 20180724
	nic-hdl: JUG11
	person: JULIAN GARCIA
	e-mail: jesus.marint.pr@eth.com.co
	address: AUTOP NORTE KM 13 / AV 13 205-59, ,
	address: 9999 - BOGOTA - BO
	country: CO
	phone: +057 01 6683600 [272]
	created: 20100714
	changed: 20100714
% whois.lacnic.net accepts only direct match queries.	
% Types of queries are: POCs, ownerid, CIDR blocks, IP	
% and AS numbers.	

Imagen No. 144 Información del propietario del servidor DNS de escuelaing.edu.co

DNS records

DNS query for **68.88.239.45.in-addr.arpa** returned an error from the server: **NameError**

name	class	type	data	time to live
escuelaing.edu.co	IN	A	45.239.88.68	300s (00:05:00)
escuelaing.edu.co	IN	MX	preference: 10 exchange: escuelaing-edu-co.mail.protection.outlook.com	300s (00:05:00)
escuelaing.edu.co	IN	TXT	uyuQKTQIB0aPE0tezeYHWIFhqdZtdkvda3a1QGAG9ZnmgXJp2nBwWZKeIVKvqo3lghVM8tyMogc+9zNj1zA==	300s (00:05:00)
escuelaing.edu.co	IN	TXT	MS=ms84725362	300s (00:05:00)
escuelaing.edu.co	IN	TXT	v=spf1 include:spf.protection.outlook.com include:spf.masterbase.com include:_spf.embluemail.com include:21615186.spf05.hubspotemail.net -all	300s (00:05:00)
escuelaing.edu.co	IN	TXT	facebook-domain-verification=7lvadnh3yhinn1ao5hh4lxjjdx2s	300s (00:05:00)
escuelaing.edu.co	IN	TXT	google-site-verification=fuMP0aYdM2WRuBvBsFFFCf5KMp_aPRdnEX_G57AdYc	300s (00:05:00)
escuelaing.edu.co	IN	TXT	_globalsign-domain-verification=7im6sNR168xe5ntvIUbPB0LajxaQM4-mQ4LWh3Oo	300s (00:05:00)
escuelaing.edu.co	IN	TXT	brevo-code:5b1b716f419039c1d521ba9a5f77c4d	300s (00:05:00)
escuelaing.edu.co	IN	TXT	_globalsign-domain-verification=p9HbMN7qZLh-TyXauzq__68cEQfQXfmnz6uF9500T3	300s (00:05:00)
escuelaing.edu.co	IN	TXT	pruebacorreo-escuelaing-edu-co.mail.protection.outlook.com	300s (00:05:00)
escuelaing.edu.co	IN	TXT	owY2ENRuVNXRKQDSmVkg1VAycGd/PLwfdG1KfZwAopk=	300s (00:05:00)
escuelaing.edu.co	IN	SOA	server: ns1.escuelaing.edu.co email: admin@escuelaing.edu.co serial: 2024091001 refresh: 86400 retry: 3600 expire: 604800 minimum ttl: 300	300s (00:05:00)
escuelaing.edu.co	IN	NS	ns1.escuelaing.edu.co	300s (00:05:00)
escuelaing.edu.co	IN	NS	ns2.escuelaing.edu.co	300s (00:05:00)

-- end --

[URL for this output](#) | [return to CentralOps.net](#), a service of Hexillion

Imagen No. 145 Registros de nombres de dominios del servidor DNS escuelaing.edu.co

- ¿Cuántos servidores de dominio tiene?

Tiene 2 servidores de dominio

```
-----  
Name Server: ns1.escuelaing.edu.co  
Name Server: ns2.escuelaing.edu.co  
DNSSEC: unsigned
```

- ¿Hace cuánto fue asignado ese dominio?

Fue asignado el 2 de junio de 1998

```
-----  
Creation Date: 1998-06-02T00:00:00Z
```

- ¿Ante quién está registrado?

Está registrado ante COInternet, la empresa que maneja el top-level-domain .co en Colombia

```
-----  
Registrar: .CO Internet S.A.S.  
Registrar IANA ID: 111111
```

- ¿Cuál es el ID de la entidad de registro?

El ID de la entidad es 111111

```
Registrar: .CO Internet S.A.S.  
Registrar IANA ID: 111111
```

```
Registrar Abuse Contact Email: sonia
```

- ¿Cuándo fue actualizado el registro por última vez?

El registro fue actualizado el 23 de septiembre del 2024

```
-----  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of WHOIS database: 2024-09-23T19:08:02Z <<<
```

- ¿Hasta cuándo está activo dicho registro?

El registro está activo hasta el 31 de diciembre del 2025

UNIVERSIDAD

Creation Date: 1998-06-02T00:00:00Z
Registry Expiry Date: 2025-12-31T23:59:59Z
Registrar: .CO Internet S.A.S.

- ¿Cuál es el rango IP asignado y por cuál autoridad de registro fue dado?
 El rango IP asignado es 45.239.88.0/22 y lo asignó LACNIC (Registro de Direcciones de Internet para América Latina y Caribe)

Queried whois.lacnic.net with "45.239.88.68"...

```
inetnum:      45.239.88.0/22
status:       assigned
aut-num:      N/A
```

- ¿A cuál empresa le fue asignado?

Se le asignó a la empresa ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

```
inetnum:      45.239.88.0/22
status:       assigned
aut-num:      N/A
owner:        ESCUELA COLOMBIANA DE INGENIERIA
ownerid:      CO-ECIN2-LACNIC
responsible:  JULIAN GARCIA
address:      AUTOP NORTE KM 13 / AV 13 205-59, ,
address:      9999 - BOGOTA - BO
country:      CO
phone:        +057 01 6683600 [272]
owner-c:      JUG11
tech-c:       JUG11
abuse-c:      JUG11
created:     20180724
changed:     20180724

nic-hdl:      JUG11
person:       JULIAN GARCIA
e-mail:       jesus.marint.pr@etb.com.co
address:      AUTOP NORTE KM 13 / AV 13 205-59, ,
address:      9999 - BOGOTA - BO
country:      CO
phone:        +057 01 6683600 [272]
created:     20100714
changed:     20100714
```

2.2. jbb.gov.co

Domain Dossier Investigate domains and IP addresses

domain or IP address

domain whois record DNS records traceroute

network whois record service scan

user: anonymous [181.53.96.67]
balance: 47 units

[log in](#) | [account info](#)

[CentralOps.net](#)

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

Address lookup

canonical name [jbb.gov.co](#).

aliases

addresses **20.94.123.146**
20.119.228.39
2603:1030:403:3::a2

Imagen No. 146 Búsqueda del dominio jbb.gov.co

Domain Whois record

Queried whois.nic.co with "jbb.gov.co"...

```

Domain Name: jbb.gov.co
Registry Domain ID: D603102-CO
Registrant WHOIS Server:
Registrant IP Address: 202.112.255.254
Updated Date: 2021-08-14T03:11:03Z
Creation Date: 2000-01-20T00:00:00Z
Registry Entry Date: 2000-01-20T23:59:59Z
Registry Status: OK, no status $A-B.
Registrant IANA ID: 111111
Registrant Abuse Contact Email: support@scinetnet.com.co
Registrant Abuse Contact Phone: +5731234567899
Domain Status: ok https://icann.org/eppok
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: JUAN Bautista Jose Celestino Mutis
Registrant Street: REDACTED FOR PRIVACY
Registrant Street2: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Bogota
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CO
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrant Admin: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street2: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postcode: REDACTED FOR PRIVACY
Admin Country: CO
Admin Phone: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrant Tech: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street2: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Postcode: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: ns31.domaincontrol.com
Name Server: ns32.domaincontrol.com
DNSSEC Unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-09-23T23:23:13Z <<

```

Imagen No. 147 Información general del servicio DNS jbb.gov.co

Network Whois record

Queried whois.arin.net with "n 20.94.123.146"...

```

NetRange: 20.93.0.0 - 20.125.255.255
CIDR: 20.93.0.0/16, 20.94.0.0/14, 20.48.0.0/12, 20.128.0.0/16, 20.34.0.0/15, 20.40.0.0/13, 20.46.0.0/10
NetName: NSFT
NetHandle: NET-20-33-0-0-1
Parent: RIPE-NCC-NS-0-0-0
NetType: Direct Allocation
OriginAS: 
Organization: Microsoft Corporation (MSFT)
RegDate: 2017-10-18
Updated: 2021-12-14
Ref: https://rap.arin.net/registry/ip/20.93.0.0

OrgName: Microsoft Corporation
OrgId: NSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1994-07-10
Updated: 2024-03-18
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft product, please contact:
Comment: * https://cert.microsoft.com.
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment: * abuse@microsoft.com.
Comment: To report security vulnerabilities in Microsoft products and services, please contact:
Comment: * secure@microsoft.com.
Comment: For legal and law enforcement-related requests, please contact:
Comment: * handles@microsoft.com
Comment: For routing, peering or DNS issues, please contact:
Comment: * dns@microsoft.com
Comment: * IOC@microsoft.com
Ref: https://rap.arin.net/registry/entity/NSFT

OrgTechName: SCINAME-434H
OrgTechHandle: Redard, Dawn
OrgTechPhone: +1-425-338-6637
OrgTechEmail: dasedard@microsoft.com

```

OrgTechHandle: BEDAR6-ARIN
OrgTechName: Bedard, Dawn
OrgTechPhone: +1-425-538-6637
OrgTechEmail: dabedard@microsoft.com
OrgTechRef: <https://rdap.arin.net/registry/entity/BEDAR6-ARIN>

OrgAbuseHandle: MAC74-ARIN
OrgAbuseName: Microsoft Abuse Contact
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@microsoft.com
OrgAbuseRef: <https://rdap.arin.net/registry/entity/MAC74-ARIN>

OrgRoutingHandle: CHATU3-ARIN
OrgRoutingName: Chaturmoha, Somesh
OrgRoutingPhone: +1-425-882-8080
OrgRoutingEmail: someshch@microsoft.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/CHATU3-ARIN>

OrgTechHandle: IPHOSS5-ARIN
OrgTechName: IPHostmaster, IPHostmaster
OrgTechPhone: +1-425-538-6637
OrgTechEmail: iphostmaster@microsoft.com
OrgTechRef: <https://rdap.arin.net/registry/entity/IPHOSS5-ARIN>

OrgTechHandle: KIMAV-ARIN
OrgTechName: Kim, Avery
OrgTechPhone: +1-425-882-8080
OrgTechEmail: averykim@microsoft.com
OrgTechRef: <https://rdap.arin.net/registry/entity/KIMAV-ARIN>

OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: <https://rdap.arin.net/registry/entity/MRPD-ARIN>

OrgTechHandle: SINGH683-ARIN
OrgTechName: Singh, Prachi
OrgTechPhone: +1-425-707-5601
OrgTechEmail: pracsin@microsoft.com
OrgTechRef: <https://rdap.arin.net/registry/entity/SINGH683-ARIN>

Imagen No. 148 Información del propietario del servidor DNS jbb.gov.co

DNS records

Imagen No. 149 Registros de los nombres de dominio del servidor DNS jbb.gov.co

- ¿Cuántos servidores de dominio tiene?

Tiene 2 servidores de dominio

jbb.gov.co	IN	NS	ns32.domaincontrol.com	3600s (01:00:00)
jbb.gov.co	IN	NS	ns31.domaincontrol.com	3600s (01:00:00)

- ¿Hace cuánto fue asignado ese dominio?

Fue asignado el 20 de enero del 2000

```
Updated Date: 2021-05-14T03:12:05Z
Creation Date: 2000-01-20T00:00:00Z
DNSSEC Enabled Date: 2021-05-14T03:12:05Z
```

- ¿Ante quién está registrado?

Está registrado ante .CO Internet S.A.S

```
Registry Expiry Date: 2026-01-21
Registrar: .CO Internet S.A.S.
Registrar IANA ID: 111111
```

- ¿Cuál es el ID de la entidad de registro?

El ID de la entidad de registro es 111111

```
Registrar: .CO Internet S.A
Registrar IANA ID: 111111
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
```

- ¿Cuándo fue actualizado el registro por última vez?

Se actualizó el 23 de noviembre del 2024

```
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org
>>> Last update of WHOIS database: 2024-09-23T23:23:13Z <<<
```

- ¿Hasta cuándo está activo dicho registro?

Está activo hasta el 20 de enero del 2026

```
Creation Date: 2000-01-20T00:00:00Z
Registry Expiry Date: 2026-01-20T23:59:59Z
Registrar: .CO Internet S.A.S.
```

- ¿Cuál es el rango IP asignado y por cuál autoridad de registro fue dado?

El rango IP asignado es 20.33.0.0 - 20.168.255.255, fue dado por la autoridad de registro ARIN (American Registry for Internet Numbers), una organización que se encarga de la asignación y gestión de direcciones IP en América Norte.

Queried whois.arin.net with "n 20.94.123.146"...

```
NetRange: 20.33.0.0 - 20.128.255.255
CIDR: 20.33.0.0/16, 20.36.0.0/14, 20.48.0.0/12, 20.128.0.0/16, 20.34.0.0/15, 20.40.0.0/13, 20.64.0.0/10
NetName: MSFT
NetHandle: NET-20-33-0-0-1
Parent: NET20 (NET-20-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2017-10-18
Updated: 2021-12-14
Ref: https://rdap.arin.net/registry/ip/20.33.0.0
```

- ¿A cuál empresa le fue asignado?

Se le asignó a Microsoft Corporation

```

OrgName: Microsoft Corporation
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1998-07-10
Updated: 2024-03-18
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services,
* https://cert.microsoft.com.
Comment:
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment: * abuse@microsoft.com.
Comment:
Comment: To report security vulnerabilities in Microsoft products and services, please contact:
Comment: * secure@microsoft.com.
Comment:
Comment: For legal and law enforcement-related requests, please contact:
Comment: * msndcc@microsoft.com
Comment:
Comment: For routing, peering or DNS issues, please
contact:
Comment: * IOC@microsoft.com
Ref: https://rdap.arin.net/registry/entity/MSFT

```

2.3. google.com

Domain Dossier Investigate domains and IP addresses

domain or IP address

domain whois record
 DNS records
 traceroute

network whois record
 service scan

user: anonymous [181.53.96.67]
 balance: 46 units
[log in](#) | [account info](#)

CentralOps.net

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

Address lookup

canonical name [google.com](#).

aliases

addresses

```

172.253.115.101
172.253.115.138
172.253.115.102
172.253.115.113
172.253.115.100
172.253.115.139
2607:f8b0:4004:c1b::8b
2607:f8b0:4004:c1b::71
2607:f8b0:4004:c1b::66
2607:f8b0:4004:c1b::64

```

Imagen No. 150 Búsqueda del dominio google.com

Domain Whois record

Queried whois.internic.net with "dom google.com"...

```
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_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
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
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: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-09-23T21:43:05Z <<<
```

Queried whois.markmonitor.com with "google.com"...

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-09-23T21:39:20+0000 <<<
```

Imagen No. 151 Información general del servicio DNS de google.com

Network Whois record

Queried whois.arin.net with "n 172.253.115.101"...

```
NetRange:      172.253.0.0 - 172.253.255.255
CIDR:         172.253.0.0/16
NetName:       GOOGLE
NetHandle:     NET-172-253-0-0-1
Parent:        NET172 (NET-172-0-0-0-0)
NetType:       Direct Allocation
OriginsAS:    AS15169
Organization: Google LLC (GOGL)
RegDate:      2013-04-04
Updated:       2013-04-04
Ref:          https://rdap.arin.net/registry/ip/172.253.0.0
```

```
OrgName:       Google LLC
OrgId:         GOGL
Address:       1600 Amphitheatre Parkway
City:          Mountain View
StateProv:    CA
PostalCode:   94043
Country:      US
RegDate:      2009-03-30
Updated:       2019-10-31
Comment:      Please note that the recommended way to file abuse complaints are located in the following links.
Comment:      To report abuse and illegal activity: https://www.google.com/contact/
Comment:      For legal requests: http://support.google.com/legal
Comment:      Regards,
Comment:      The Google Team
Ref:          https://rdap.arin.net/registry/entity/GOGL
```

```
OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:  Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef:   https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

Imagen No. 152 Información del propietario del servidor DNS google.com

DNS records

name	class	type	data	time to live
google.com	IN	A	142.251.116.102	300s (00:05:00)
google.com	IN	A	142.251.116.100	300s (00:05:00)
google.com	IN	A	142.251.116.138	300s (00:05:00)
google.com	IN	A	142.251.116.113	300s (00:05:00)
google.com	IN	A	142.251.116.101	300s (00:05:00)
google.com	IN	A	142.251.116.139	300s (00:05:00)
google.com	IN	AAAA	2607:f8b0:4023:1009::8a	300s (00:05:00)
google.com	IN	AAAA	2607:f8b0:4023:1009::65	300s (00:05:00)
google.com	IN	AAAA	2607:f8b0:4023:1009::64	300s (00:05:00)
google.com	IN	AAAA	2607:f8b0:4023:1009::66	300s (00:05:00)
google.com	IN	CAA	[no interpretation available] 00 05 69 73 73 75 65 70 ..issuem hex dump: EB 69 2E 67 6F 6F 67 K1.qoog (15 bytes)	86400s (1:00:00:00)
google.com	IN	TXT	google-site-verification=wB8N7lJTNtKezJ49swvWW48f8_9xveREV4oB-0Hf5o	3600s (01:00:00)
google.com	IN	SOA	server: ns1.google.com email: dns-admin@google.com serial: 677421491 refresh: 900 retry: 900 expire: 1800 minimum ttl: 60	60s (00:01:00)
google.com	IN	TXT	onetrust-domain-verification=de01ed21f2fa4d8781cbc3ff89cf4ef	3600s (01:00:00)
google.com	IN	TXT	v=spf1 include:_spf.google.com ~all	3600s (01:00:00)
google.com	IN	TXT	docusign=1b0a6754-49b1-4db5-8540-d2c12664b289	3600s (01:00:00)
google.com	IN	NS	ns3.google.com	345600s (4:00:00:00)
google.com	IN	TXT	facebook-domain-verification=22rm551cu4k0ab0bxsw536tlids4h95	3600s (01:00:00)

UNIVERSIDAD

google.com	IN	NS	ns4.google.com	345600s (4.00:00:00)
google.com	IN	NS	ns1.google.com	345600s (4.00:00:00)
google.com	IN	TXT	MS=EA468B9AB2BB9670BCE15412F62916164C0B20BB	3600s (01:00:00)
google.com	IN	MX	preference: 10 exchange: smtp.google.com	300s (00:05:00)
google.com	IN	TYPE65	[no interpretation available] 00 01 00 00 01 00 06 02 hex dump: 68 32 02 68 33 h2.h3 (13 bytes)	21600s (06:00:00)
google.com	IN	TXT	disco-ci-domain-verification=479146de172eb01dde3e8b1a455ab9e0bb51542dd7f1fa298557dfa7b22d963	3600s (01:00:00)
google.com	IN	TXT	google-site-verification=4lPUFUb-wxLQ_S7vsXvomSTVanmuXBvA2pR51Z87D0	3600s (01:00:00)
google.com	IN	TXT	google-site-verification=TV9-Dbe4R80X4v0M4U_b_d_9cpOJM0nikft0Agjm8Q	3600s (01:00:00)
google.com	IN	TXT	apple-domain-verification=30af1BcvSuDV2PLX	3600s (01:00:00)
101.115.253.172.in-addr.arpa	IN	PTR	bg-in-f101.e1e00.net	3600s (01:00:00)
253.172.in-addr.arpa	IN	SOA	server: ns1.google.com email: dns-admin@google.com serial: 677709978 refresh: 900 retry: 900 expire: 1800 minimum ttl: 60	60s (00:01:00)
b.8.0.0.0.0.0.0.0.0.0.0.0.b.1.c.0.4.0.0.4.0.b.8.f.7.0.6.2.ip6.arpa	IN	PTR	wv-in-f139.le100.net	3600s (01:00:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	SOA	server: ns1.google.com email: dns-admin@google.com	60s (00:01:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	SOA	server: ns1.google.com email: dns-admin@google.com serial: 677709978 refresh: 900 retry: 900 expire: 1800 minimum ttl: 60	60s (00:01:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	NS	ns3.google.com	345600s (4.00:00:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	NS	ns4.google.com	345600s (4.00:00:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	NS	ns2.google.com	345600s (4.00:00:00)
4.0.b.8.f.7.0.6.2.ip6.arpa	IN	NS	ns1.google.com	345600s (4.00:00:00)

Imagen No. 153 Registro de los nombres de dominio del servidor DNS google.com

- ¿Cuántos servidores de dominio tiene?

Tiene 4 servidores de dominio

```
Name Server: ns1.google.com  
Name Server: ns2.google.com  
Name Server: ns3.google.com  
Name Server: ns4.google.com  
DNSSEC: unsigned
```

- ¿Hace cuánto fue asignado ese dominio?

Fue asignado el 15 de septiembre de 1997

Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2026

- ¿Ante quién está registrado?

Está registrado ante MarkMonitor Inc. Una empresa estadounidense destinada a proteger las marcas corporativas de falsificación, fraude, piratería y ciberocupación.

Registry Expiry Date: 2028-09-14TO

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

- ¿Cuál es el ID de la entidad de registro?

El ID de registro es 292

REGISTRATION NUMBER 1110.

Registrar IANA ID: 292

- Registrar Abuse Contact Email
¿Cuándo fue actualizado el registro por última vez?

El registro fue actualizado el 23 de septiembre del 2024

DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2024-09-23T21:39:20+0000 <<<

- ¿Hasta cuándo está activo dicho registro?

Está activo hasta el 14 de septiembre del 2028

Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.

- ¿Cuál es el rango IP asignado y por cuál autoridad de registro fue dado?

El rango de IP asignado es 172.253.0.0-172.253.255.255 y la autoridad de registro es ARIN

NetRange: 172.253.0.0 - 172.253.255.255
CIDR: 172.253.0.0/16
NetName: GOOGLE
NetHandle: NET-172-253-0-0-1
Parent: NET172 (NET-172-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS15169
Organization: Google LLC (GOGL)
RegDate: 2013-04-04
Updated: 2013-04-04
Ref: <https://rdap.arin.net/registry/ip/172.253.0.0>

- ¿A cuál empresa le fue asignado?

Le fue asignado a Google LLC

OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2019-10-31
Comment: Please note that the recommended way to file abuse complaints are located in the following links.
Comment: To report abuse and illegal activity: <https://www.google.com/contact/>
Comment: For legal requests: <http://support.google.com/legal>
Comment: Regards,
Comment: The Google Team
Ref: <https://rdap.arin.net/registry/entity/GOGL>

2.4. Ikea.com

Domain Dossier Investigate domains and IP addresses

domain or IP address

domain whois record DNS records traceroute

network whois record service scan

user: anonymous [181.53.96.67]
balance: 43 units
[log in](#) | [account info](#)

[CentralOps.net](#)

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

Address lookup

canonical name [ikea.com](#).

aliases

addresses **104.69.113.197**
2600:1404:1800:686::2eb6
2600:1404:1800:697::2eb6
2600:1404:1800:69f::2eb6
2600:1404:1800:69e::2eb6

Imagen No. 154 Búsqueda del dominio ikea.com

Domain Whois record

Queried [whois.internic.net](#) with "dom [ikea.com](#)"...

```
Domain Name: IKEA.COM
Registry Domain ID: 1501324_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-07-01T05:17:09Z
Creation Date: 1995-07-29T04:00:00Z
Registry Expiry Date: 2025-07-05T08:40:23Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
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: UDNS1.CSCDNS.NET
Name Server: UDNS2.CSCDNS.UK
DNSSEC: signedDelegation
DNSSEC DS Data: 45802 13 2 9D14F9103B63F55B2B4E6668896D68FEEF86BB27067B577D97D07A40AFBC58AD
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-09-24T00:18:59Z <<<
```

Queried [whois.corporatedomains.com](#) with "ikea.com"...

```
Domain Name: ikea.com
Registry Domain ID: 1501324_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2024-07-01T01:17:09Z
Creation Date: 1995-07-29T00:00:00Z
Registrar Registration Expiration Date: 2025-07-05T08:40:23Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Administration
Registrant Organization: Inter IKEA Systems B.V.
Registrant Street: Olof Palmestraat 1
Registrant City: Delft
```

UNIVERSIDAD

```
-----  
Registrant State/Province: NL  
Registrant Postal Code: 2616 LN  
Registrant Country: NL  
Registrant Phone: +32.23574111  
Registrant Phone Ext:  
Registrant Fax: +32.23574498  
Registrant Fax Ext:  
Registrant Email: DNSadmin@inter.ikea.com  
Registry Admin ID:  
Admin Name: Domain Administration  
Admin Organization: Inter IKEA Systems B.V.  
Admin Street: Olof Palmestraat 1  
Admin City: Delft  
Admin State/Province: NL  
Admin Postal Code: 2616 LN  
Admin Country: NL  
Admin Phone: +32.23574111  
Admin Phone Ext:  
Admin Fax: +32.23574498  
Admin Fax Ext:  
Admin Email: DNSadmin@inter.ikea.com  
Registry Tech ID:  
Tech Name: Domain Administration  
Tech Organization: Inter IKEA Systems B.V.  
Tech Street: Olof Palmestraat 1  
Tech City: Delft  
Tech State/Province:  
Tech Postal Code: NL-2616 LN  
Tech Country: NL  
Tech Phone: +32.23574111  
Tech Phone Ext:  
Tech Fax: +32.23574498  
Tech Fax Ext:  
Tech Email: domainadm@INTER-IKEA.COM  
Name Server: udns1.cscdns.net  
Name Server: udns2.cscdns.uk  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2024-07-01T01:17:09Z <<<
```

Imagen No. 155 Información general del servicio DNS ikea.com

Network Whois record

Queried whois.arin.net with "n 104.69.113.197"...

```

NetRange:      104.64.0.0 - 104.127.255.255
CIDR:         104.64.0.0/10
NetName:       AKAMAI
NetHandle:    NET-104-64-0-0-1
Parent:        NET104 (NET-104-0-0-0-0)
NetType:       Direct Allocation
OrigAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate:      2014-04-22
Updated:       2014-04-22
Ref:          https://rdap.arin.net/registry/ip/104.64.0.0
  
```

```

OrgName:      Akamai Technologies, Inc.
OrgId:        AKAMAI
Address:      145 Broadway
City:         Cambridge
StateProv:   MA
PostalCode:  02142
Country:     US
RegDate:    1999-01-21
Updated:     2023-10-24
Ref:          https://rdap.arin.net/registry/entity/AKAMAI
  
```

```

OrgTechHandle: IPADM11-ARIN
OrgTechName: ipadmin
OrgTechPhone: +1-617-444-0017
OrgTechEmail: ip-admin@akamai.com
OrgTechRef:  https://rdap.arin.net/registry/entity/IPADM11-ARIN

OrgTechHandle: SJS98-ARIN
OrgTechName: Schechter, Steven Jay
OrgTechPhone: +1-617-274-7134
OrgTechEmail: ip-admin@akamai.com
OrgTechRef:  https://rdap.arin.net/registry/entity/SJS98-ARIN

OrgAbuseHandle: NUS-ARIN
OrgAbuseName: NOC United States
OrgAbusePhone: +1-617-444-2535
OrgAbuseEmail: abuse@akamai.com
OrgAbuseRef:  https://rdap.arin.net/registry/entity/NUS-ARIN
  
```

Imagen No. 156 Información del propietario del servidor DNS ikea.com

DNS records

name	class	type	data	time to live
ikea.com	IN	NS	udns1.cscdns.net	86400s (1:00:00:00)
ikea.com	IN	NS	udns2.cscdns.uk	86400s (1:00:00:00)
ikea.com	IN	RRSIG	type covered: NS (2) algorithm: ECDSA Curve P-256 with SHA-256 (13) labels: 2 original ttl: 86400 (1:00:00:00) signature expiration: 2024-10-07 04:39:42Z signature inception: 2024-09-23 04:39:42Z key tag: 37296 signer's name: ikea.com signature: 94822626490E244F7FC50A0462396208 (512 bits) 184548D2B1FF75FB6E2ZB048379AE303 729A50E2BD32F3D94E1FTB8E4950564B 0287B64599DB3A4372932687E2E263211	86400s (1:00:00:00)
197.113.69.104.in-addr.arpa	IN	PTR	a104-69-113-197.deploy.static.akamaltechnologies.com	43200s (12:00:00)
6.b.e.2.0.0.0.0.0.0.0.0.0.0.6.8.6.0.0.0.8.1.4.0.4.1.0.0.6.2.ip6.arpa	IN	PTR	g2600-1404-1800-0686-0000-0000-0000-2eb6.deploy.static.akamaltechnologies.com	43200s (12:00:00)

Imagen No. 157 Registros de los nombres de dominio de ikea.com

- ¿Cuántos servidores de dominio tiene?

Tiene 2 servidores de dominio

```

Tech Email: domainadm@INTER-1M
Name Server: udns1.cscdns.net
Name Server: udns2.cscdns.uk
  
```

- ¿Hace cuánto fue asignado ese dominio?

Fue asignando el 29 de julio de 1995

```

Updated Date: 2024-07-01T01:17:09Z
Creation Date: 1995-07-29T00:00:00Z
Registrar Registration Expiration Date
  
```

- ¿Ante quién está registrado?

Está registrado ante CSC CORPORATE DOMAINS, INC.

Registrar Registration Expiration Date:
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299

- ¿Cuál es el ID de la entidad de registro?

El ID de la entidad de registro es 299

Registrar Registration Expiration Date:
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainat

- ¿Cuándo fue actualizado el registro por última vez?

Fue actualizado el 1 de septiembre del 2024

URL of the ICANN WHOIS Data Problem Reporting System: http://wdj
>> Last update of WHOIS database: 2024-07-01T01:17:09Z <<

- ¿Hasta cuándo está activo dicho registro?

Está activo hasta el 5 de julio del 2025

Creation Date: 1995-07-29T04:00:00Z
Registry Expiry Date: 2025-07-05T08:40:23Z
Registrar: CSC Corporate Domains Inc

- ¿Cuál es el rango IP asignado y por cuál autoridad de registro fue dado?

El rango IP asignado es 104.64.0.0 - 104.127.255.255 y la autoridad de registro fue dado por ARIN

Queried whois.arin.net with "n 104.69.113.197"...

NetRange: 104.64.0.0 - 104.127.255.255
CIDR: 104.64.0.0/10
NetName: AKAMAI
NetHandle: NET-104-64-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate: 2014-04-22
Updated: 2014-04-22
Ref: https://rdap.arin.net/registry/ip/104.64.0.0

- ¿A cuál empresa le fue asignado?

Fue asignada a la empresa Akamai Technologies, Inc.

OrgName: Akamai Technologies, Inc.
OrgId: AKAMAI
Address: 145 Broadway
City: Cambridge
StateProv: MA
PostalCode: 02142
Country: US
RegDate: 1999-01-21
Updated: 2023-10-24
Ref: https://rdap.arin.net/registry/entity/AKAMAI

3. NTP Server

¿Por qué es importante lograr que todos los equipos de cómputo de una infraestructura tengan la misma hora?

Es importante que todos los equipos de cómputo en una infraestructura estén sincronizados con la misma hora para evitar inconsistencias en el sistema. La sincronización horaria asegura que los registros de eventos, archivos y transacciones se realicen en el orden correcto, lo cual es fundamental para el diagnóstico de problemas, la auditoría de sistemas y la seguridad. Además, garantiza que los usuarios y aplicaciones trabajen con una línea de tiempo coherente, evitando conflictos en la ejecución de procesos, autenticaciones y transferencias de datos, que pueden verse afectados si los equipos no tienen una hora sincronizada. Esto también ayuda en la correcta operación de los sistemas distribuidos y evita errores que podrían generarse por diferencias horarias.

3.1. Configuración Servidor NTP en Linux Slackware

Montamos el disco Óptico para instalar el servicio NTP, usamos mount /dev/sr0 /mnt/cdrom

```
root@andrea:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda     8:0    0  20G  0 disk
└─sda1  8:1    0  16G  0 part /
└─sda2  8:2    0   4G  0 part [SWAP]
sr0    11:0   1 1024M  0 rom
root@andrea:~# mount /dev/sr0 /mnt/cdrom
mount: /mnt/cdrom: no medium found on /dev/sr0.
root@andrea:~# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda     8:0    0  20G  0 disk
└─sda1  8:1    0  16G  0 part /
└─sda2  8:2    0   4G  0 part [SWAP]
sr0    11:0   1 1024M  0 rom
root@andrea:~# mount /dev/sr0 /mnt/cdrom
mount: /mnt/cdrom: WARNING: source write-protected, mounted read-only.
root@andrea:~# cd /mnt/cdrom
root@andrea:/mnt/cdrom# ls
ANNOUNCE.15.0          ChangeLog.txt      README_LUM.TXT    extra/
CHANGES_AND_HINTS.TXT  EFI/                README_RAID.TXT  isolinux/
CHECKSUMS.md5           FILELIST.TXT     README_UEFI.TXT  kernels/
CHECKSUMS.md5.asc       GPG-KEY            RELEASE_NOTES   pasture/
COPYING                PACKAGES.TXT     SPEAKUP_DOCS.TXT patches/
COPYING3               README.TXT        SPEAK_INSTALL.TXT slackware64/
COPYRIGHT.TXT          README.initrd    Slackware-HOWTO  testing/
CRYPTO_NOTICE.TXT      README_CRYPT.TXT  UPGRADE.TXT     usb-and-pxe-installers/
root@andrea:/mnt/cdrom#
```

Imagen No. 158 Montaje del disco óptico

Navegamos a /mnt/cdrom/slackware64/n y buscamos el paquete con ls | grep ntp,

Luego, usamos installpkg y esperamos a que se instale.

```
root@andrea:/mnt/cdrom# cd slackware64/n
root@andrea:/mnt/cdrom/slackware64/n# ls | grep ntp
ntp-4.2.8p15-x86_64-8.txt
ntp-4.2.8p15-x86_64-8.txz
ntp-4.2.8p15-x86_64-8.txz.asc
root@andrea:/mnt/cdrom/slackware64/n# installpkg ntp-4.2.8p15.x86_64-8.txz
```

Imagen No. 159 Navegación entre las carpetas del disco óptico

```
Verifying package ntp-4.2.8p15-x86_64-8.txz.
Installing package ntp-4.2.8p15-x86_64-8.txz [OPT]:
PACKAGE DESCRIPTION:
# ntp (Network Time Protocol daemon)
#
# The Network Time Protocol (NTP) is used to synchronize the time of a
# computer client or server to another server or reference time source,
# such as a radio or satellite receiver or modem. It provides client
# accuracies typically within a millisecond on LANs and up to a few tens
# of milliseconds on WANs relative to a primary server synchronized to
# Coordinated Universal Time (UTC) via a Global Positioning Service
# (GPS) receiver, for example.
#
# Homepage: http://www.ntp.org
Executing install script for ntp-4.2.8p15-x86_64-8.txz.
Package ntp-4.2.8p15-x86_64-8.txz installed.
root@andrea:/mnt/cdrom/slackware64/n#
```

Imagen No. 160 Instalación NTP

Abrimos el archivo /etc/ntp.conf y descomentamos los servidores NTP externos, estos son: server 0.pool.ntp.org iburst, server 1.pool.ntp.org iburst, server 2.pool.ntp.org iburst, server 3.pool.ntp.org iburst

```
GNU nano 6.0                               /etc/ntp.conf                                         Modified
# Sample /etc/ntp.conf: Configuration file for ntpd.

#
# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available. The
# default stratum is usually 3, but in this case we elect to use stratum
# 0. Since the server line does not have the prefer keyword, this driver
# is never used for synchronization, unless no other other
# synchronization source is available. In case the local host is
# controlled by some external source, such as an external oscillator or
# another protocol, the prefer keyword would cause the local host to
# disregard all other synchronization sources, unless the kernel
# modifications are in use and declare an unsynchronized condition.
#
#server 127.127.1.0      # local clock
#fudge  127.127.1.0 stratum 10

#
# 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

#
# 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
#
logfile /var/log/ntp

^G Help      ^O Write Out  ^W Where Is   ^X Cut          ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^H Replace   ^U Paste        ^J Justify   ^- Go To Line M-E Redo
```

Imagen No. 161 Configuración NTP Server

De igual manera, descomentamos las líneas restrict que permite que los clientes accedan a nuestro servidor.

Finalmente, especificamos las IP's de los clientes que queremos que tengan acceso a nuestro servidor.

```
GNU nano 6.0                               /etc/ntp.conf                                         Modified
# Set an optional compensation for broadcast packet delay:
#broadcastdelay 0.008

#
# Keys file. If you want to diddle your server at run time, make a
# keys file (mode 640 owned by root:ntp) and define the key number to
# be used for making requests.
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will.
#
#keysdir      /etc
#keys        /etc/ntp.keys
#trustedkey   65535
#requestkey   65535
#controlkey   65535

#
# Don't serve time or stats to anyone else by default (more secure)
restrict default limited kod nomodify notrap nopeer noquery
restrict -6 default limited kod nomodify notrap nopeer noquery

#
# Use these lines instead if you do want to serve time and stats to
# other machines on the network:
restrict default limited kod nomodify notrap nopeer
restrict -6 default limited kod nomodify notrap nopeer

#
# Trust ourselves. :-)
restrict 127.0.0.1
restrict ::1
restrict 192.168.20.101 mask 255.255.255.0 modifi notrap_

^G Help      ^O Write Out  ^W Where Is    ^X Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^E Replace     ^P Paste     ^J Justify   ^L Go To Line M-E Redo
```

Imagen No. 162 Configurar clientes en el servidor

Salvamos el archivo y usamos chmod +x /etc/rc.d/rc.ntpd para permitir ejecutar este archivo. Finalmente, iniciamos el servicio con /etc/rc.d/rc.ntpd start

```
root@andrea:~# /etc/rc.d/rc.ntpd start
Starting NTP daemon: /usr/sbin/ntpd -g -u ntp:ntp
root@andrea:~#
```

Imagen No. 163 Iniciar servicio NTP

Verificamos que el servidor NTP esté funcionando correctamente con el comando ntpq -p

```
root@andrea:~# ntpq -p
      remote           refid      st t when poll reach   delay    offset  jitter
-----+
 200.25.20.50    169.229.128.142  2 u    2   64    1  68.437  -179486   0.377
 200.25.3.17    169.229.128.134  2 u    1   64    1   2.035  -179486   0.364
 200.25.3.11    .STEP.          16 u   426   64    0    0.000   +0.000   0.000
root@andrea:~# date
Tue Sep 24 11:02:47 -05 2024
root@andrea:~# date
Tue Sep 24 11:02:53 -05 2024
```

Imagen No. 164 Prueba del funcionamiento del servidor NTP

3.2. Configuración Cliente NTP en Solaris

Necesitamos crear el archivo ntp.conf, para realizar esto, nos dirigimos al archivo /etc/inet y usamos cp

ntp.client ntp.conf para copiar el archivo ntp client como ntp.conf.

Luego, editamos el archivo ntp.conf y descomentamos el apartado “server server_name1 iburst”, cambiamos name_server1 por la ip de la máquina slackware.

```

Modificado

# get the correct time at boot.
#
# For a list of Internet NTP servers see
# http://support.ntp.org/bin/view/Servers/WebHome
# If you use this list, be sure to read, understand and abide by the rules
# each server has published for accessing themselves.
#
# There is also a DNS round-robin pool of public access NTP servers. The
# instructions for accessing these are at http://www.pool.ntp.org
# Please consider adding your own servers to the pool if possible.
#
# Many ISP's also provide NTP servers for use by their customers.

server 10.2.77.193 iburst
# server server_name2 iburst
# server server_name3 iburst

# Always configure the drift file. It can take days for ntpd to completely
# stabilize and without the drift file, it has to start over on a reboot
# of if ntpd restarts.

driftfile /var/ntp/ntp.drift

# It is always wise to configure at least the loopstats and peerstats files.
# Otherwise when ntpd does something you don't expect there is no way to
# find out why.

statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
¿Guardar el bÃºfer modificado? (Responder "No" DESCARTARÃ los cambios.)
```

S SÃ–
 N No Cancelar

Imagen No. 165 Archivo de configuración NTP cliente en Solaris

Iniciamos el servicio NTP usando **svcadm enable ntp**, luego probamos si el servicio está funcionando con **ntpq -p**

```

root@solaris:/etc/inet# ntpq -p
      remote          refid      st t when poll reach   delay    offset  jitter
=====
  10.2.77.193    200.25.20.50    3 u    2   64    1   0.329  1372.13   0.750
root@solaris:/etc/inet# date
martes, 24 de septiembre de 2024, 11:17:55 (-05)
root@solaris:/etc/inet# date
martes, 24 de septiembre de 2024, 11:17:58 (-05)
root@solaris:/etc/inet#
```

Imagen No. 166 Prueba como cliente NTP en Solaris

3.3. Configuración Cliente NTP en Windows con GUI

Abrimos el panel de control y elegimos ‘Date and Time’

UNIVERSIDAD

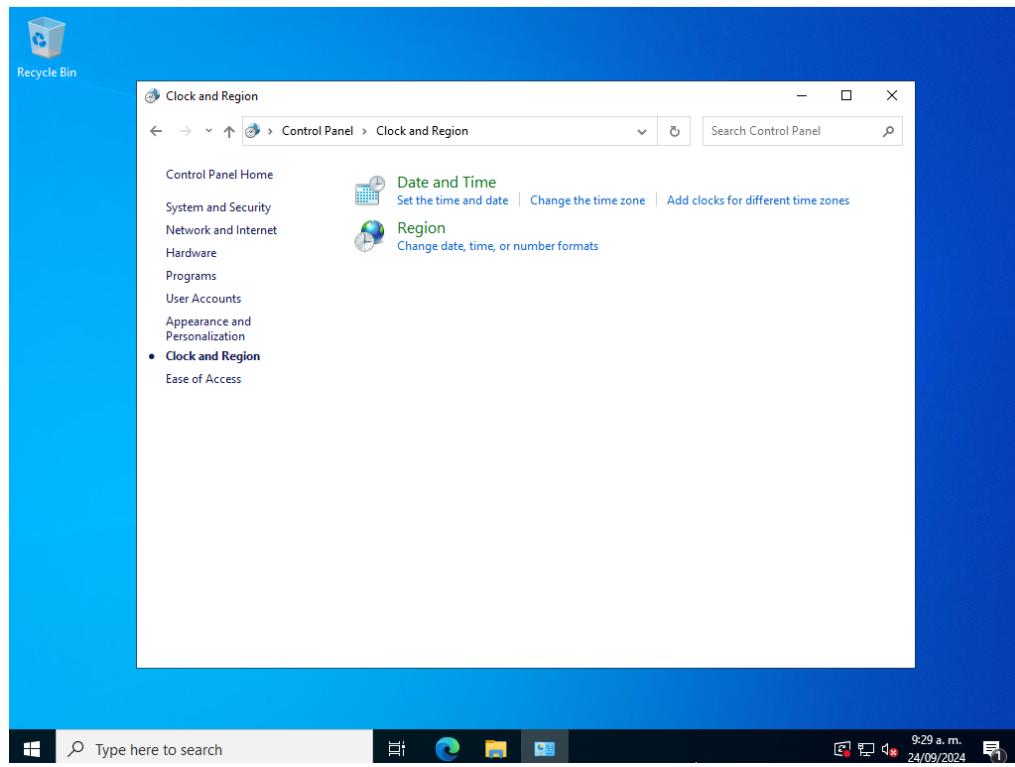


Imagen No. 167 Panel de control de Windows

Vamos a la pestaña 'Internet Time'

UNIVERSIDAD

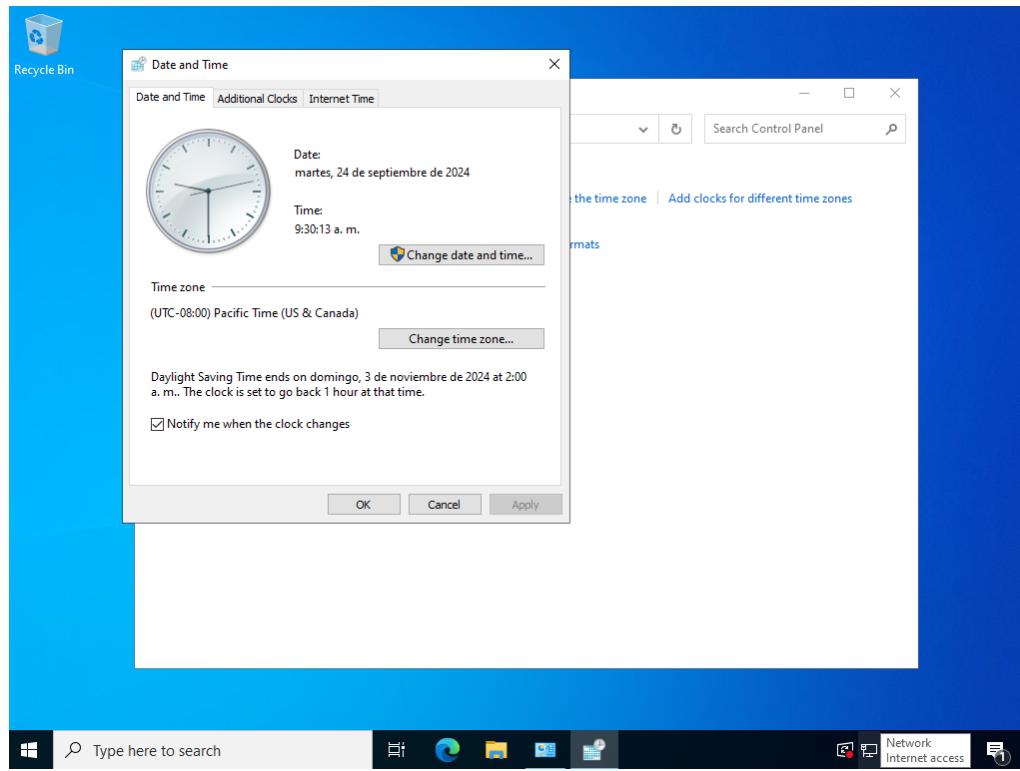


Imagen No. 168 Configuración NTP cliente en Windows

Damos clic en ‘Change Settings’ y digitamos la ip del servidor. Luego, para confirmar que se sincronizó damos clic en ‘Update now’ y debe aparecer un mensaje de confirmación indicando que se ha realizado la sincronización correctamente

UNIVERSIDAD

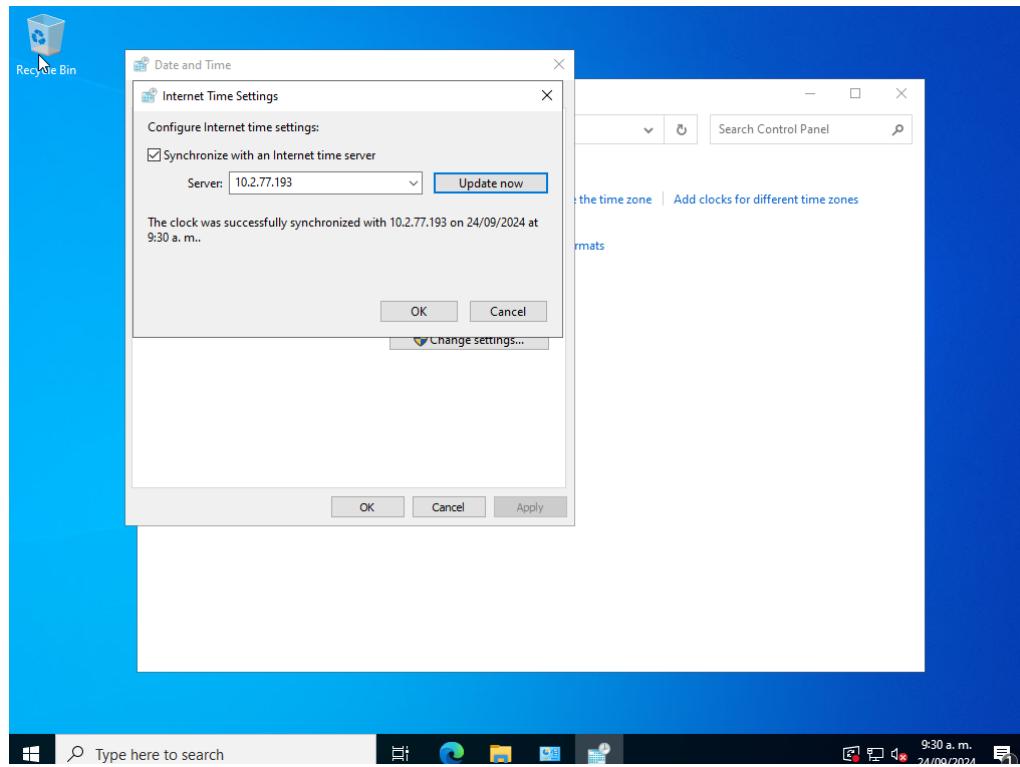


Imagen No. 169 Configuración del servidor NTP en Windows

Damos clic en OK y nos dirigimos a la pestaña ‘Date and Time’ para cambiar la zona horaria a Bogotá.

UNIVERSIDAD

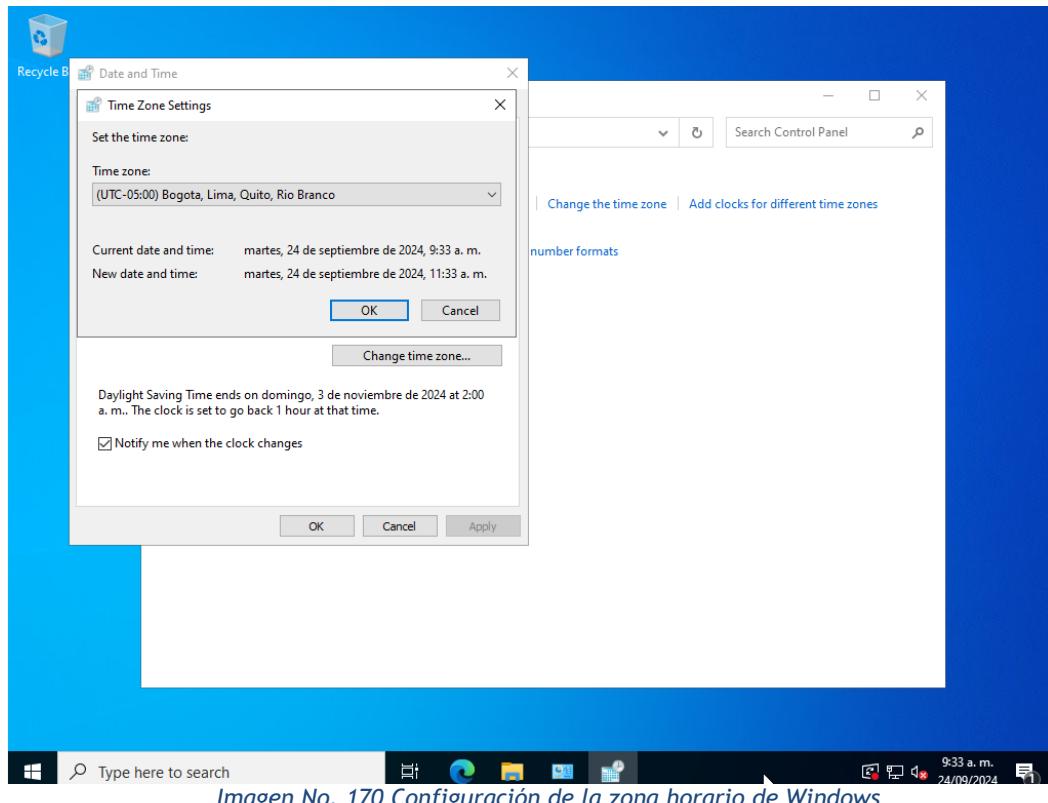


Imagen No. 170 Configuración de la zona horario de Windows

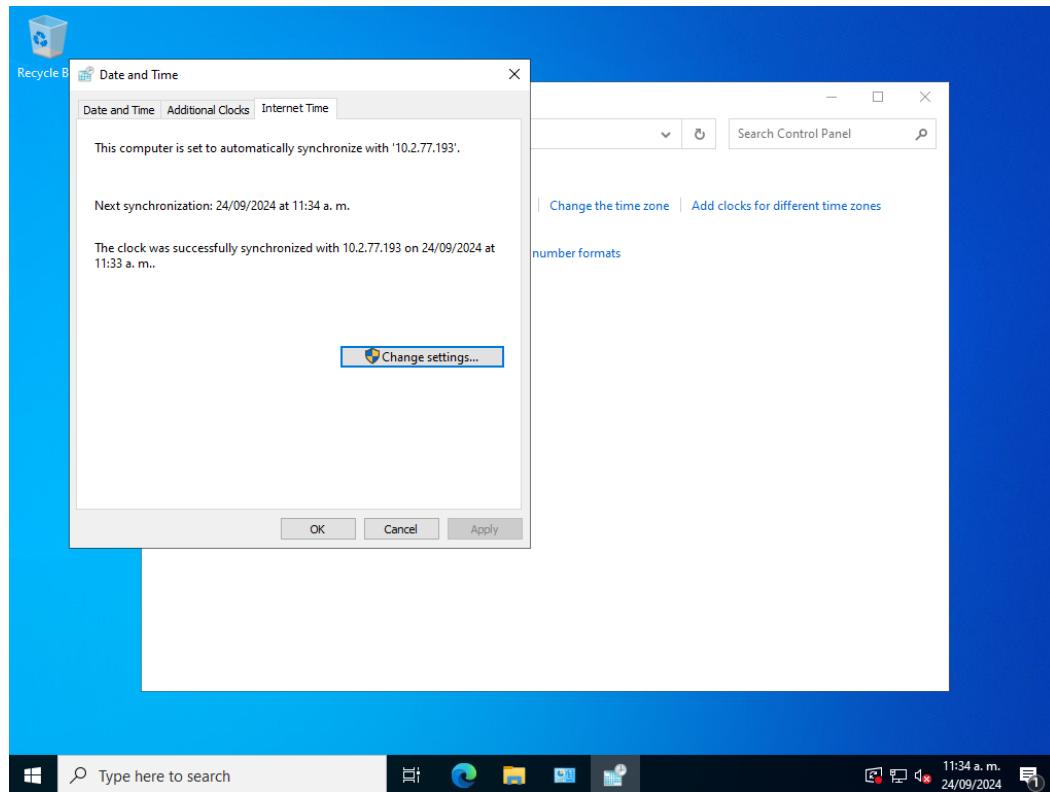


Imagen No. 171 Sincronización con el servidor NTP en Windows

3.4. Configuración Cliente NTP en Windows sin GUI

Digitamos la opción 9 para abrir la configuración del tiempo del sistema

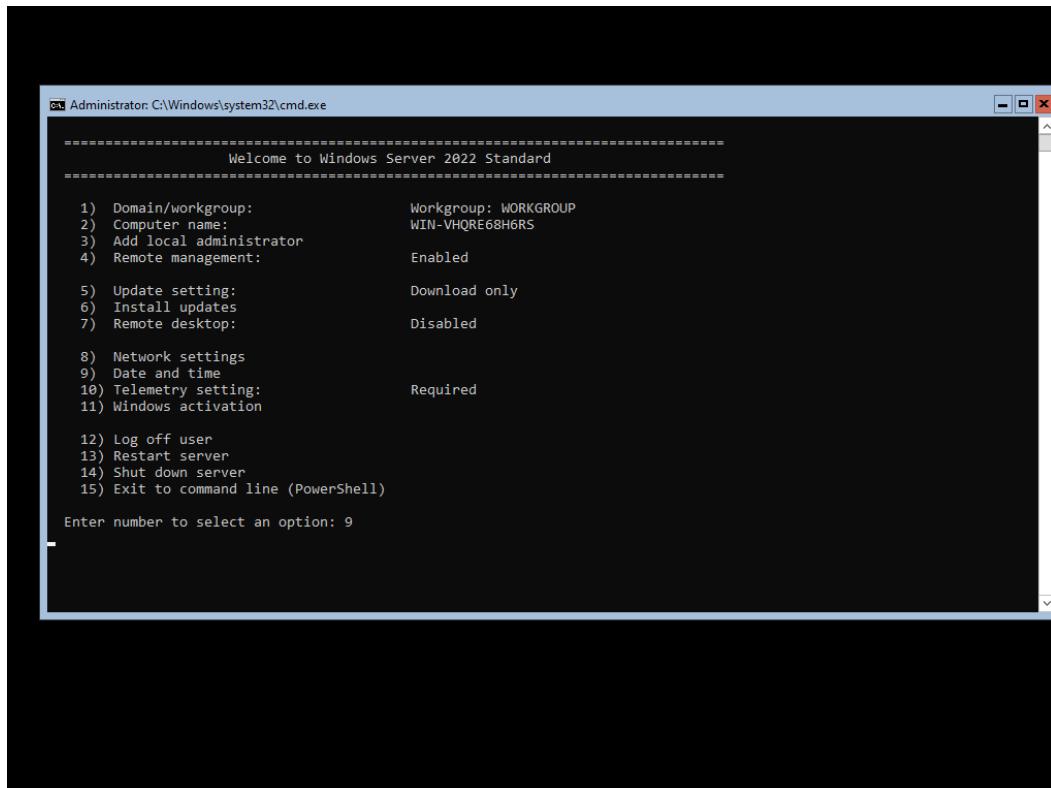


Imagen No. 172 Interfaz de configuración de Windows

Realizamos los mismos pasos que se realizaron con Windows GUI, cambiamos la zona horaria a Bogotá

UNIVERSIDAD

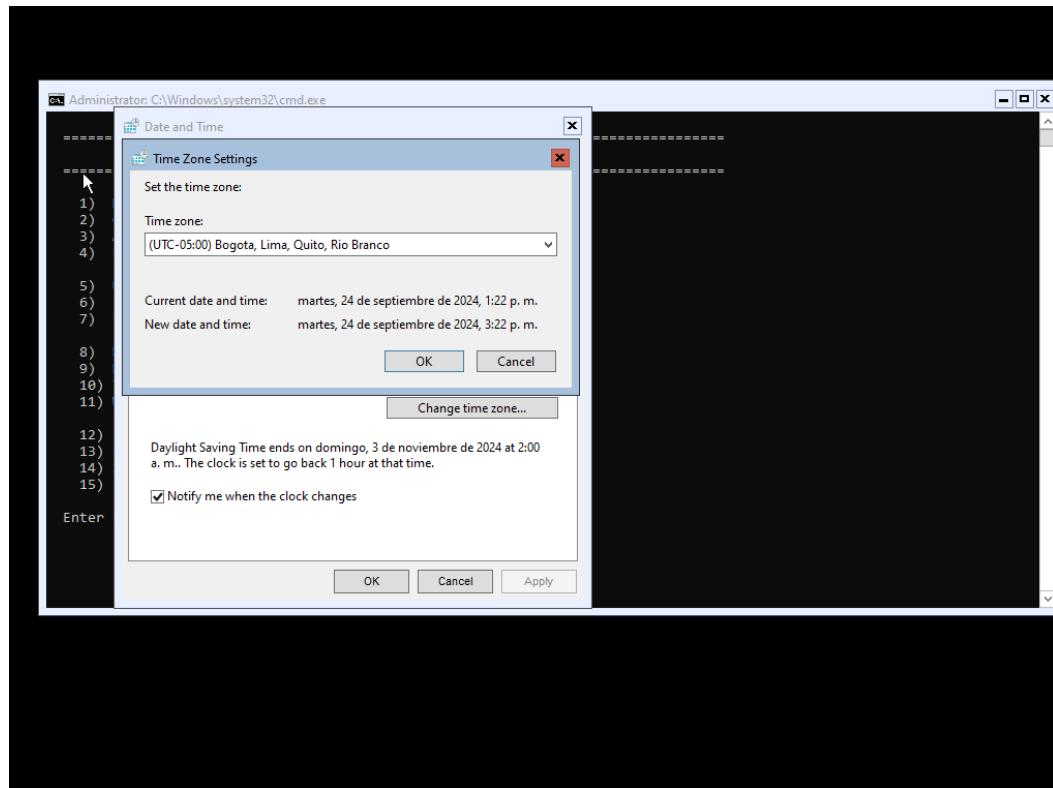


Imagen No. 173 Zona horaria de Windows

Vamos a la pestaña Internet Time y digitamos la ip del servidor. Aparecerá el mensaje de confirmación indicando que la sincronización con la máquina fue correcta

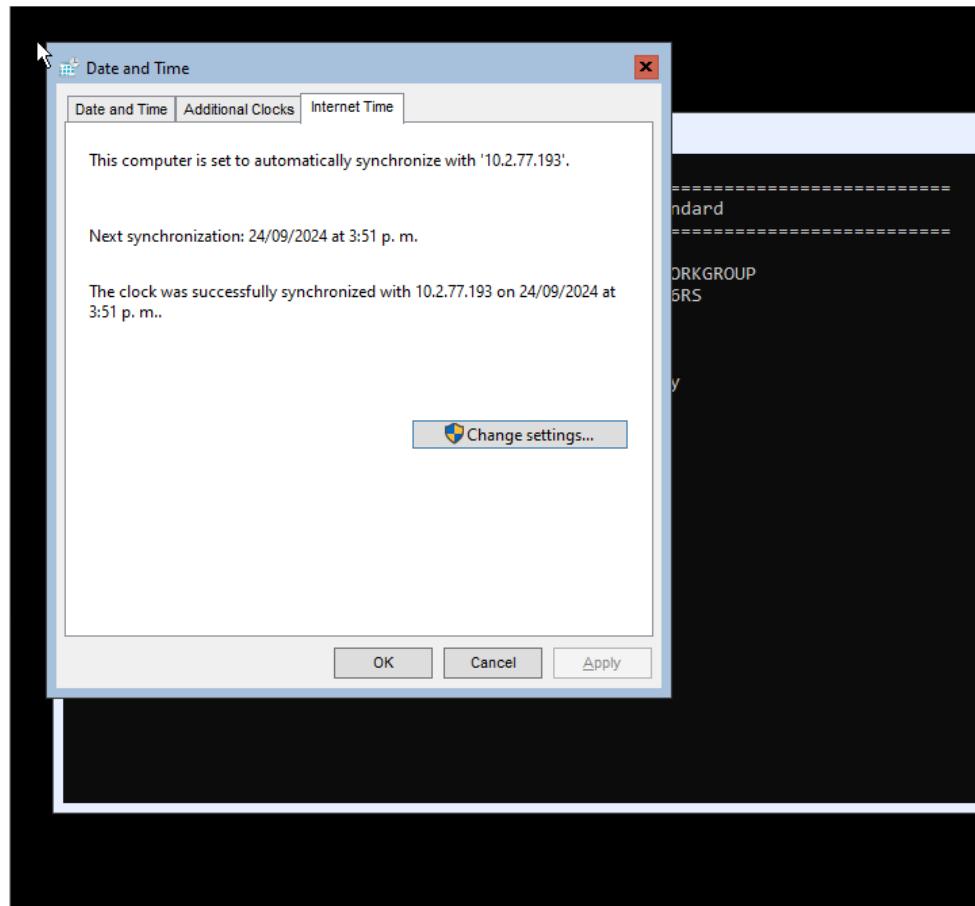


Imagen No. 174 Sincronización con el servidor NTP en Windows sin GUI

3.5. Configuración Cliente NTP en Android

Abrimos Play Store, buscamos ntp e instalamos la siguiente aplicación:

UNIVERSIDAD

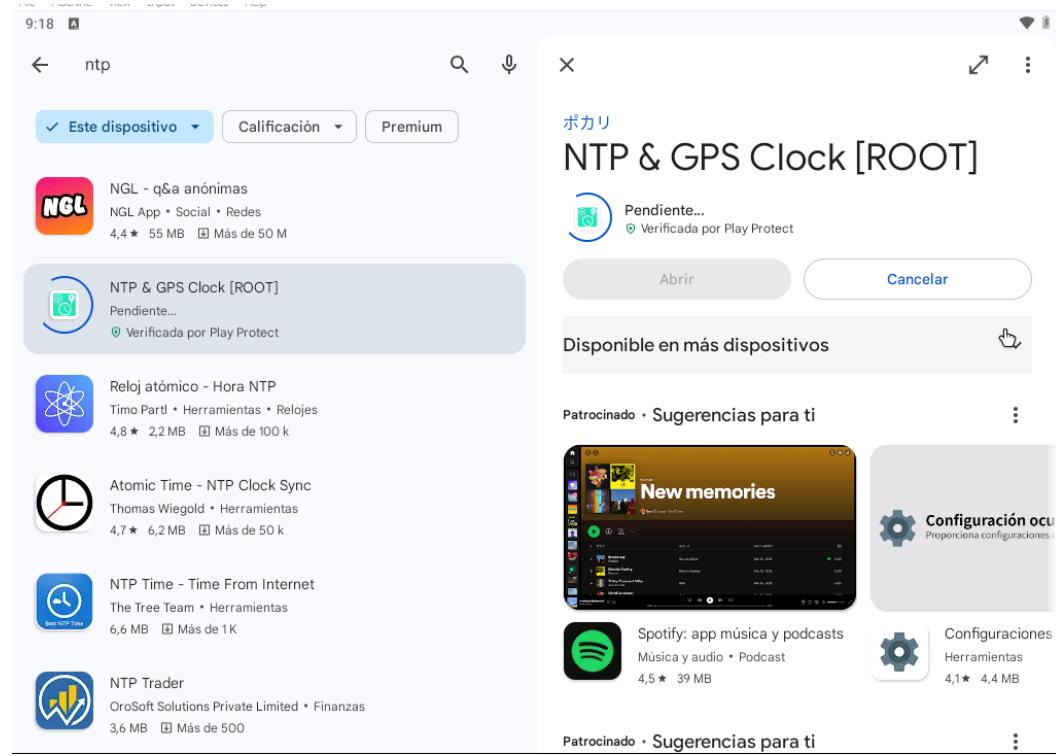


Imagen No. 175 Instalación de la aplicación NTP en Android

Una vez instalada la aplicación, la abrimos y, para acceder a las configuraciones o herramientas adicionales, hacemos clic en el ícono que representa una herramienta o llave inglesa.

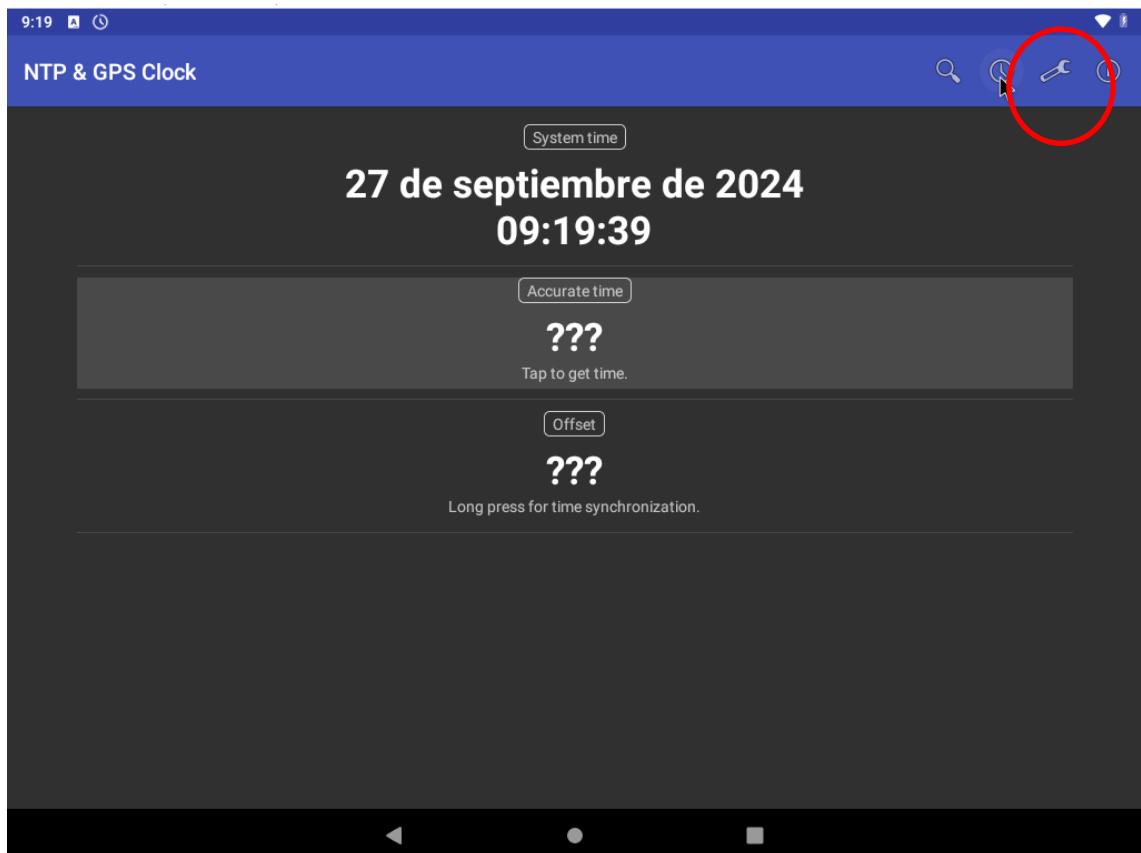


Imagen No. 176 Interfaz de la aplicación NTP en Android

Damos clic en ‘NTP Sever’ y digitamos la IP del servidor

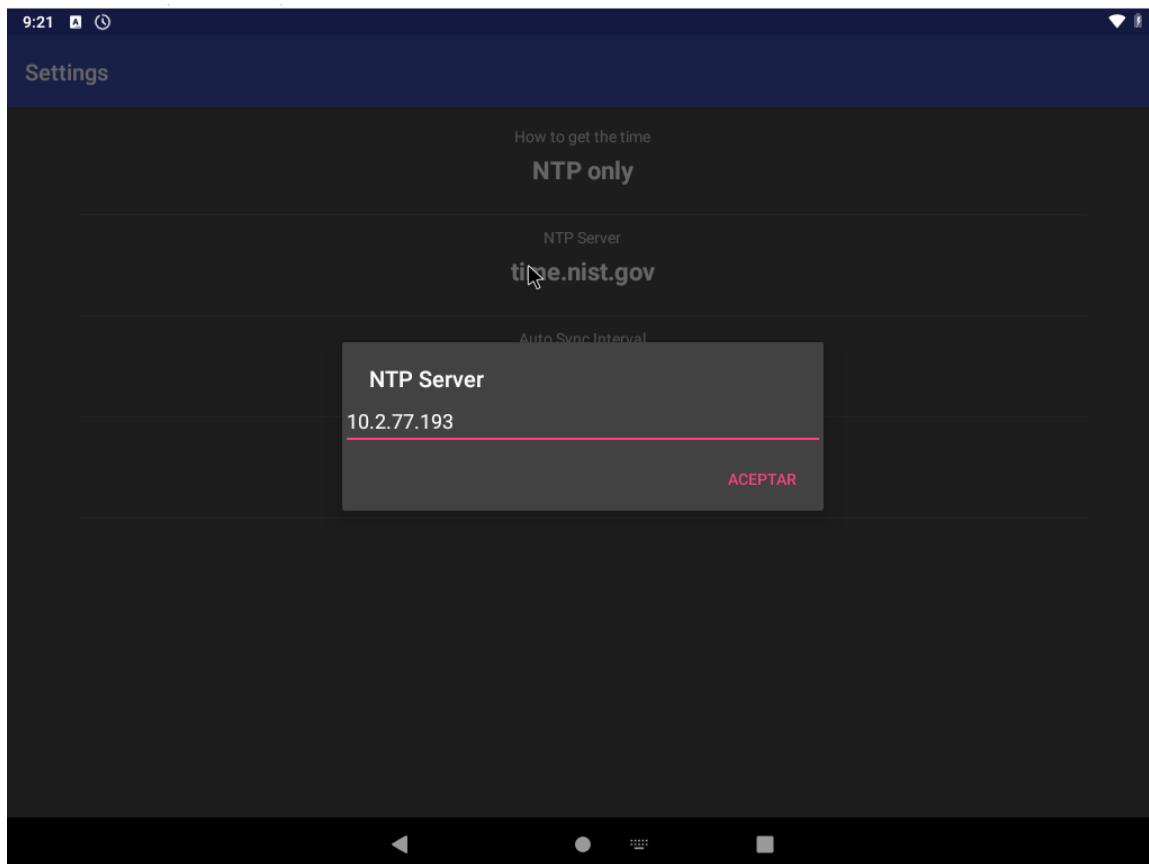


Imagen No. 177 Vinculo con el servidor NTP en Android

Guardamos y volvemos al inicio de la aplicación. Observamos que se sincronizó con la hora del servidor.

UNIVERSIDAD

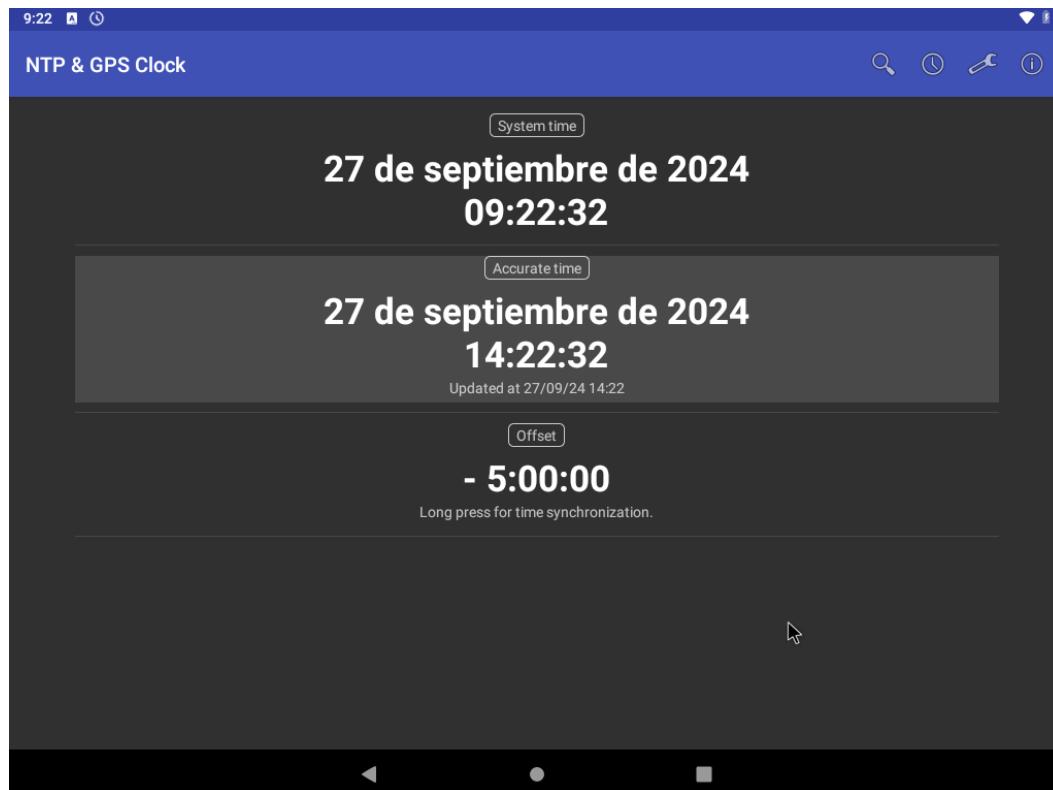


Imagen No. 178 Sincronización con el servidor NTP en Android

UNIVERSIDAD

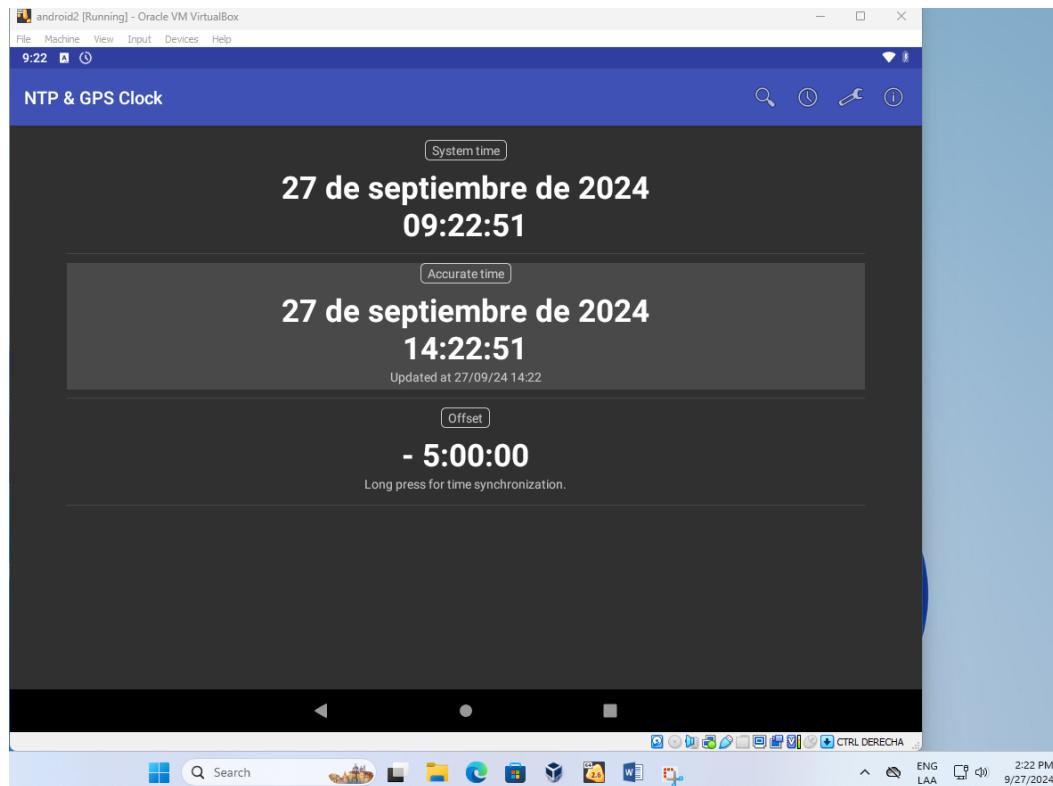


Imagen No. 179 Comprobación de la hora de Android con la hora del sistema

4. Cableado estructurado y construcción de cables

Para construir una infraestructura tecnológica, se debe contar con elementos que permitan la conexión de los equipos de cómputo, y para su organización se cuenta con los estándares de cableado estructurado, los cuales permiten conectar elementos, mantener orden, facilitar el crecimiento y favorecer la gestión de los elementos físicos de la red. A continuación, se plantean diferentes actividades enfocadas a conocer dicha estructura.

¿Para qué se utilizan cada uno de ellos?

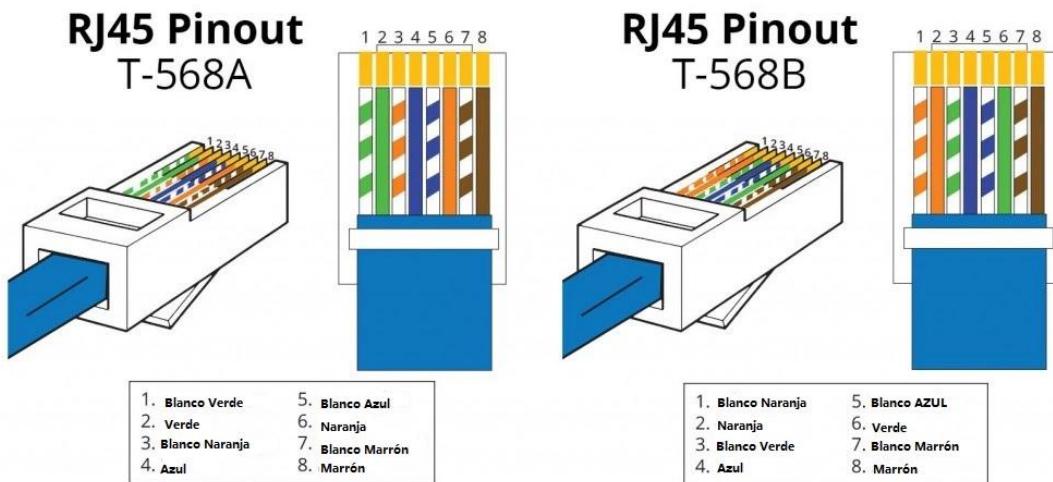


Imagen No. 180 Estandarización de la disposición de cables de red

La *Imagen No. 180* nos facilita la estandarización de la disposición de los cables para la construcción de cables de red ya sea un cable directo o cable cruzado, según el tipo de conexión que necesitemos realizar.

- **Cable directo:** Se utiliza para conectar dispositivos diferentes, como una computadora a un switch o router. Para su construcción, ambos extremos deben seguir el mismo estándar, ya sea T-568A o T-568B.
- **Cable cruzado:** Este tipo de cable se utiliza para conectar dispositivos similares, como computadora a computadora o switch a switch. Para construirlo, se sigue el estándar T-568A en un extremo y T-568B en el otro.

4.1. Construcción de patch cord

Para la construcción de los cables de red, se necesitan dos cables cada uno con una medida de aproximadamente 1m, conectores RJ45, y pinza ponchadora RJ45.

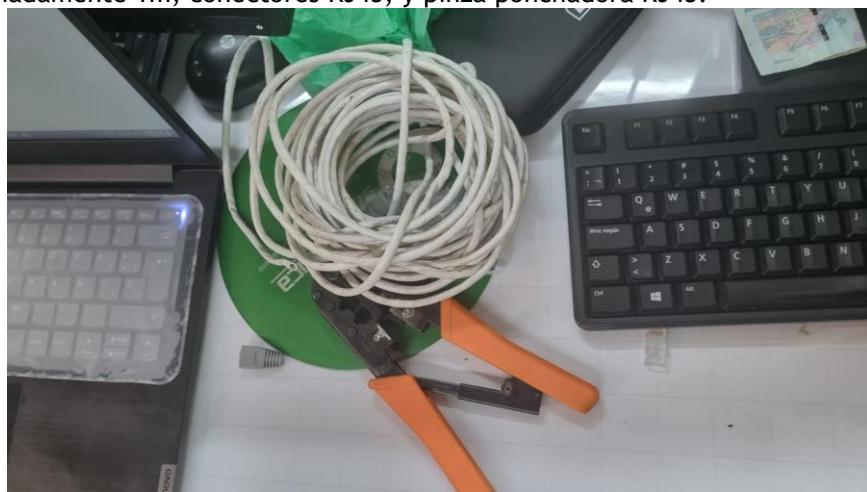


Imagen No. 181 Materiales para la construcción de los cables de red

4.1.1. Cable cruzado

- Pelamos el cable en ambos extremos para exponer los ocho conductores internos.



Imagen No. 182 Conductores internos del cable rj45

- Organizamos los cables siguiendo el esquema de colores del estándar T-568A-T-568B.



Imagen No. 183 Ordenamiento de los cables siguiendo el estándar

- Introducimos los cables en el conector RJ45 en el orden adecuado, asegurando que lleguen al final del conector.



Imagen No. 184 Acomodación de los cables en el conector rj45

- Con la pinza ponchadora, crimpeamos el conector RJ45, fijando los cables en su lugar.



Imagen No. 185 Empalme del conector rj45 de un cable cruzado

- Realizamos el mismo procedimiento con el otro extremo asegurando que un extremo tenga el estándar T568A y el otro T568B.



Imagen No. 186 Resultado final de la construcción del cable cruzado

- Para revisar que el cable fue correctamente construido, utilizamos el probador de cables. Este dispositivo verifica la continuidad y el orden de los hilos en ambos extremos del cable de red.



Imagen No. 187 Prueba 1 y 2 del cable cruzado



Imagen No. 188 Prueba 3 y 4 del cable cruzado



Imagen No. 189 Prueba 5 y 6 del cable cruzado



Imagen No. 190 Prueba 7 y 8 del cable cruzado

4.1.2. Cable directo

- Realizamos el mismo proceso anterior para el ponchado de cables, aseguramos que ambos extremos del cable sigan el mismo estándar T568A-T568A o T568B-T568B.



Imagen No. 191 Empalme del conector rj45 de un cable directo



Imagen No. 192 Resultado final de la construcción del cable directo

- Utilizamos el probador de cables para verificar que ha sido correctamente construido. Las luces deben encenderse en el mismo orden en ambos extremos, lo que indica que los hilos están alineados y conectados correctamente.

UNIVERSIDAD



Imagen No. 193 Prueba 1 del cable directo



Imagen No. 194 Prueba 2 del cable directo

UNIVERSIDAD



Imagen No. 195 Prueba 3 del cable directo



Imagen No. 196 Prueba 4 del cable directo



Imagen No. 197 Prueba 5 del cable directo



Imagen No. 198 Prueba 6 y 7 del cable directo



Imagen No. 199 Prueba 7 y 8 del cable directo

4.2. Ponchado de patch panel

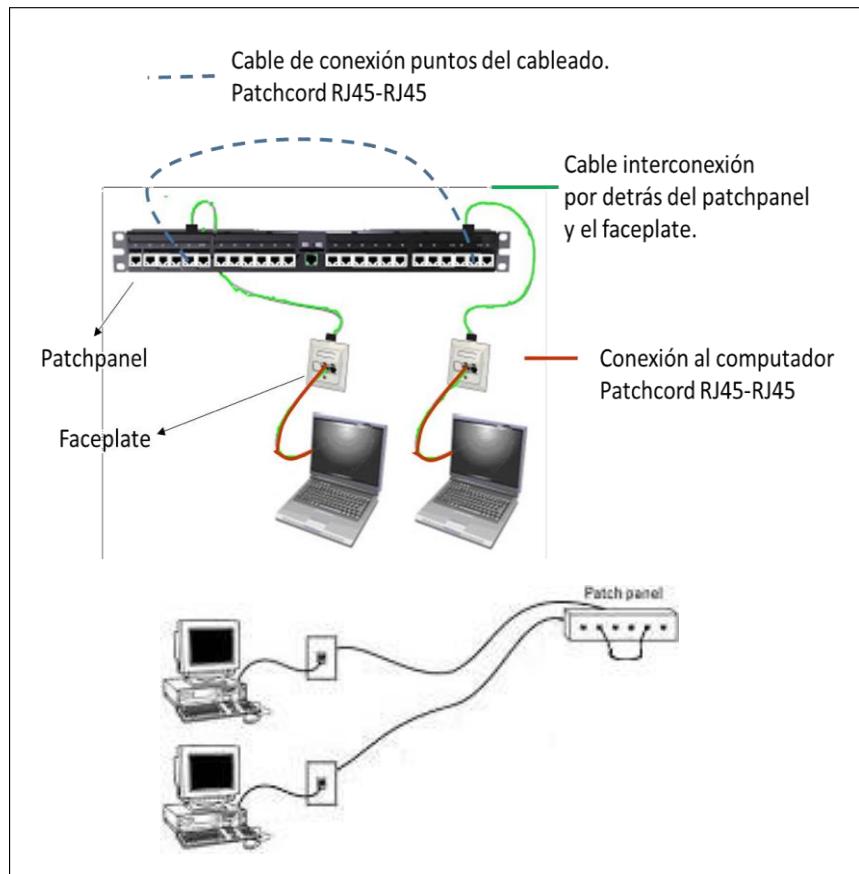
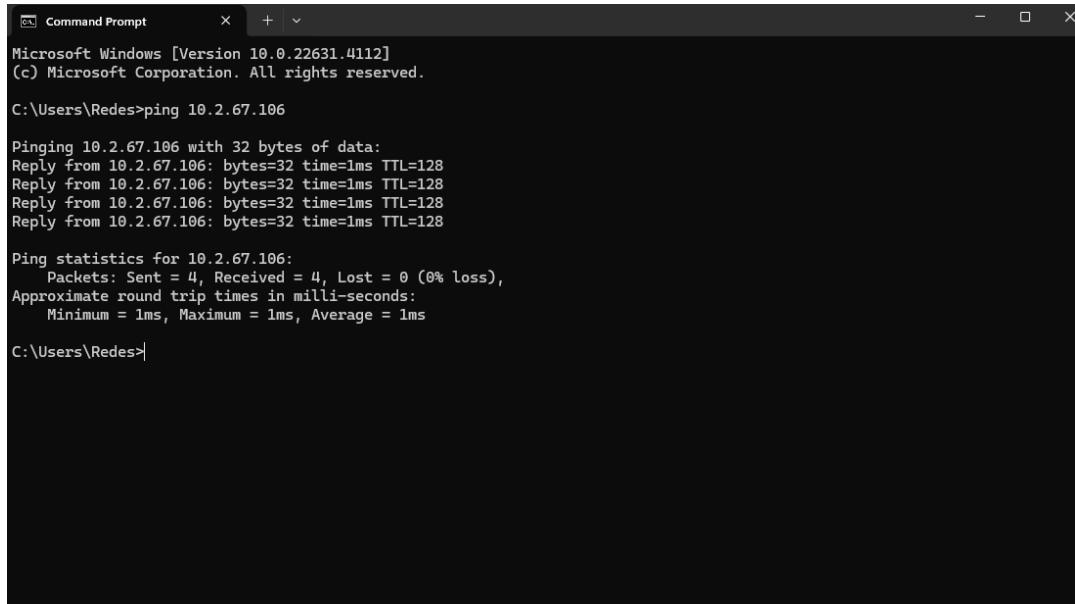


Imagen No. 200 Modelo para la prueba del cableado horizontal

La imagen 200 nos permitió realizar la prueba de ponchado de cableado horizontal, asegurando que se pueda establecer una conexión entre dos computadoras mediante el uso de un patch panel y dos faceplates.

4.2.1. Prueba de ponchado en patch panel y faceplate con cable directo

- Antes de realizar la prueba, asignamos una ip estática a ambas máquinas y verificamos que hagan ping entre ellas.



```
c:\ Command Prompt      x  +  v
Microsoft Windows [Version 10.0.22631.4112]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 10.2.67.106

Pinging 10.2.67.106 with 32 bytes of data:
Reply from 10.2.67.106: bytes=32 time=1ms TTL=128

Ping statistics for 10.2.67.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Redes>
```

Imagen No. 201 Prueba de conexión de dos computadoras antes de cambiar el cable de red

- Desconectamos los cables de red que se encontraban conectados en la entrada izquierda del faceplate. Podemos observar que son cables directos debido a que ambos extremos sigue el estándar T568B.



Imagen No. 202 Desconexión del cable de red de ambas computadoras

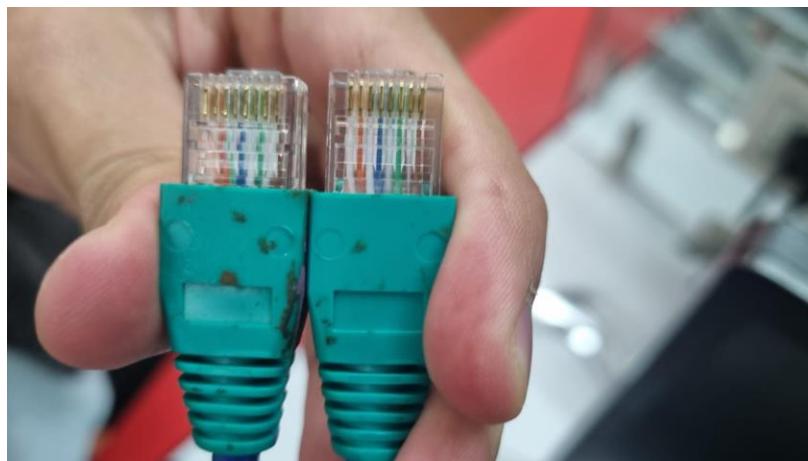


Imagen No. 203 Estándar de cableado en ambos extremos del cable de red

- Conectamos los cables de red al centro de los faceplates. Observamos que ambos números en la entrada central corresponden a las categorías 5E y 6E.



Imagen No. 204 Conexión en el faceplate de la máquina 1



Imagen No. 205 Conexión en el faceplate de la máquina 2

- Volvemos a hacer ping entre las máquinas y observamos que no hay conexión.

```
C:\Users\Redes>PING 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
Reply from 10.2.77.193: Destination host unreachable.

Ping statistics for 10.2.77.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Imagen No. 206 Prueba errónea de la conexión en ambas computadoras

- Conectamos el cable directo al patch panel en las entradas que observamos anteriormente: 5E y 6E.



Imagen No. 207 Conexión del cable directo en el patch panel

- Volvemos a realizar un ping entre las máquinas y confirmamos que la conexión se estableció correctamente, ya que el ping se realizó con éxito.

```
C:\Users\Redes>PING 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
Reply from 10.2.77.194: bytes=32 time=1ms TTL=128

Ping statistics for 10.2.77.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Redes>
```

Imagen No. 208 Prueba de comunicación entre dos máquinas después de la conexión del cable directo

UNIVERSIDAD

0.000000	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=39/9984, ttl=128 (reply in 27)
1.018800	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=40/10240, ttl=128 (reply in 28)
2.026412	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=41/10496, ttl=128 (reply in 29)
3.033787	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=42/10752, ttl=128 (reply in 31)
4.885259	10.2.77.193	10.2.77.194	TCP	66 7680 → 50889 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
4.891728	10.2.77.193	10.2.77.194	MS-DO	129 Handshake Message (Reply)	
4.897664	10.2.77.193	10.2.77.194	MS-DO	113 BitField Message (has 44 of 432 pieces)	
4.897877	10.2.77.193	10.2.77.194	TCP	54 7680 → 50889 [FIN, ACK] Seq=135 Ack=135 Win=525312 Len=0	
4.903730	10.2.77.193	10.2.77.194	TCP	54 7680 → 50889 [ACK] Seq=136 Ack=135 Win=525312 Len=0	
30.762497	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=16/4096, ttl=128
31.774106	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=17/4352, ttl=128
32.783974	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=18/4608, ttl=128
33.797963	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=19/4864, ttl=128
215.191639	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=21/5376, ttl=128
216.206640	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=22/5632, ttl=128
217.223297	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=23/5888, ttl=128
219.080657	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=43/11008, ttl=128 (reply in 36)
220.092265	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=44/11264, ttl=128 (reply in 37)
221.112920	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=45/11520, ttl=128 (reply in 38)
222.126352	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=46/11776, ttl=128 (reply in 39)
230.590962	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=24/6144, ttl=128
231.601581	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=25/6400, ttl=128

Imagen No. 209 Captura de red en Wireshark con la prueba 1

4.2.2. Prueba de ponchado en patch panel con cable cruzado y faceplate con cable directo

- Con los cables de red conectados en el centro, realizamos ping entre las máquinas para confirmar que no tengan conexión.

```
C:\Users\Redes>PING 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.
General failure.

Ping statistics for 10.2.77.194:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Imagen No. 210 Prueba errónea de conexión entre dos máquinas

- Conectamos el cable cruzado al patch panel en las mismas entradas.

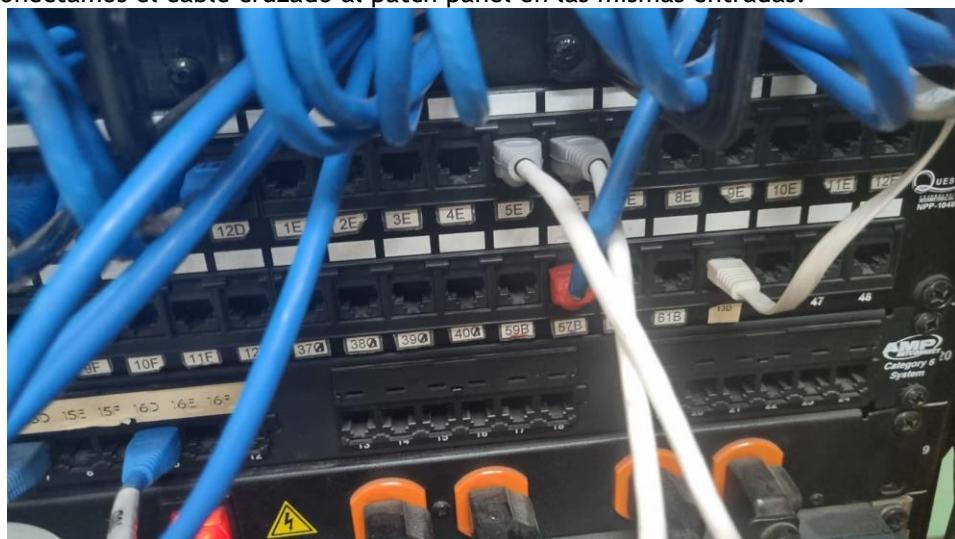


Imagen No. 211 Conexión del cable cruzado al patch panel

- Realizamos la prueba de ping y observamos que hubo conexión entre ellas.

```
C:\Users\Redes>ping 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
Reply from 10.2.77.194: bytes=32 time=5ms TTL=128
Reply from 10.2.77.194: bytes=32 time=6ms TTL=128
Reply from 10.2.77.194: bytes=32 time=6ms TTL=128
Reply from 10.2.77.194: bytes=32 time=6ms TTL=128

Ping statistics for 10.2.77.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

Imagen No. 212 Prueba de conexión entre las máquinas después de la conexión del cable cruzado

231.601581	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=25/6400, ttl=128
232.612678	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=26/6656, ttl=128
233.622246	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=27/6912, ttl=128
270.195629	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=37/9472, ttl=128
271.203390	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=38/9728, ttl=128
272.160619	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=39/9984, ttl=128 (request in 1)
273.172573	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=40/10240, ttl=128 (request in 2)
274.180125	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=41/10496, ttl=128 (request in 3)

Imagen No. 213 Captura de la red en Wireshark con la prueba 2

4.2.3. Pruebas de ponchado con cable directo en patch panel y cruzado en faceplate

- Conectamos las máquinas a los faceplates con cables cruzados y el patch panel con cable directo



Imagen No. 214 Cable cruzado conectado al faceplate

- Realizamos ping entre las máquinas y observamos que hay conexión entre ellas

```
C:\Users\Redes>ping 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
Reply from 10.2.77.194: bytes=32 time=1ms TTL=128
Reply from 10.2.77.194: bytes=32 time=1ms TTL=128
Reply from 10.2.77.194: bytes=32 time=1ms TTL=128
Reply from 10.2.77.194: bytes=32 time<1ms TTL=128

Ping statistics for 10.2.77.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Imagen No. 215 Conexión entre las máquinas después de la conexión del cable directo en el patch panel

345.168767	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=53/13568, ttl=128 (reply in 51)
347.083799	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=43/11008, ttl=128 (request in 17)
348.092464	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=44/11264, ttl=128 (request in 18)
349.106153	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=45/11520, ttl=128 (request in 19)
350.122292	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=46/11776, ttl=128 (request in 20)
350.176873	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=54/13824, ttl=128 (reply in 52)
353.704995	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=55/14080, ttl=128 (reply in 53)
354.712450	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=56/14336, ttl=128 (reply in 54)
355.728244	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=57/14592, ttl=128 (reply in 55)
356.741011	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) request	id=0x0001, seq=58/14848, ttl=128 (reply in 56)

Imagen No. 216 Captura de la red en Wireshark con la prueba 3

4.2.4. Prueba de ponchado en patch panel y faceplate con cable cruzado

- Con los cables cruzados conectados en el faceplate, conectamos ahora un cable cruzado en el patch panel, realizamos ping entre ellas y observamos que hay conexión

```
C:\Users\Redes>ping 10.2.77.194

Pinging 10.2.77.194 with 32 bytes of data:
Reply from 10.2.77.194: bytes=32 time=1ms TTL=128

Ping statistics for 10.2.77.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Imagen No. 217 Conexión entre las máquinas después de la conexión del cable directo en el patch panel

49 921.272924	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=51/13056, ttl=128
50 922.282330	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=52/13312, ttl=128
51 923.297345	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=53/13568, ttl=128 (request in 35)
52 924.312791	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=54/13824, ttl=128 (request in 40)
53 1311.952872	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=55/14080, ttl=128 (request in 41)
54 1312.963073	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=56/14336, ttl=128 (request in 42)
55 1313.972223	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=57/14592, ttl=128 (request in 43)
56 1314.987840	10.2.77.193	10.2.77.194	ICMP	74 Echo (ping) reply	id=0x0001, seq=58/14848, ttl=128 (request in 44)

Imagen No. 218 Captura de la red en Wireshark con la prueba 4

En nuestras pruebas, hemos observado que en todos los escenarios la conexión entre las dos computadoras funciona correctamente. Sin embargo, esto no es del todo correcto, pues la prueba consiste en analizar la conexión correcta entre las dos máquinas cuando se conecta en los faceplates cables directos y en el patch panel un cable cruzado o cuando todos son cruzados. Debido a la configuración de la tarjeta de red que se encontraba en los equipos de la Escuela (Realtek Family Controller) no se permitió observar su funcionamiento correctamente.

4.3. Conocimiento el Cableado estructurado de la Escuela

A continuación, se presenta el cableado estructurado del edificio I de la Escuela:



Imagen No. 219 Cableado estructurado del Edificio I



Imagen No. 220 segunda imagen cableado I

En la *imagen 219* y *220*, podemos observar varios componentes esenciales para la infraestructura de red de una organización:

Patch Panels: contienen múltiples puertos para conectar cables de red, facilitando la organización y gestión eficiente de las conexiones.

Cables de Red: transportan datos entre dispositivos y están conectados a los paneles de parcheo y otros equipos de red, utilizando diferentes categorías según las necesidades de velocidad y ancho de banda.

Switches de Red: gestionan el tráfico de red entre dispositivos, asegurando la transmisión eficiente de datos mediante tablas de conmutación.

Organizadores de Cables: mantienen los cables agrupados y ordenados, reduciendo enredos, facilitando el acceso y mejorando la ventilación y el flujo de aire en el rack para un funcionamiento óptimo de los equipos de red.

Conclusiones

- Durante el laboratorio, configuramos exitosamente una red en Cisco Packet Tracer que incluyó servicios web, correo, FTP y DNS. Al conectar distintos dominios y utilizar el modo de simulación, verificamos la correcta comunicación y transmisión de mensajes, observando los paquetes enviados a través de los diversos protocolos. Esto nos permitió confirmar el funcionamiento adecuado de los servicios en los diferentes equipos de la red.
- El uso de Wireshark nos facilitó la captura y visualización de los protocolos involucrados al realizar consultas en la red. Al realizar una conexión por TELNET para obtener recursos de una URL, pudimos comparar esta interacción con la realizada a través de un navegador web, destacando las diferencias en la visualización y manejo de los datos.

- Analizamos características de varios dominios según lo propuesto en la guía del laboratorio, lo que nos permitió identificar el número de servidores, las entidades de registro y los rangos de IP asignados, entre otros detalles relevantes.
- Desarrollamos habilidades prácticas en la creación y manejo de cables, patch panels y faceplates, siguiendo los estándares de cableado. Este proceso resaltó la importancia de la precisión y la paciencia en el ponchado de cables, especialmente para principiantes.
- La exploración del cableado estructurado en el edificio I del campus universitario nos enseñó a identificar las diferentes partes de un sistema de cableado estructurado, como los patch panels y los Switches. Además, aprendimos la importancia de seguir las normas de cableado y las buenas prácticas para asegurar instalaciones eficientes y ordenadas.

Bibliografía

1. (S/f). Digikey.com. Recuperado el 29 de septiembre de 2024, de <https://www.digikey.com/en/articles/rj45-connectors-what-you-need-to-know?msockid=2d5072e1fade69892d3a663bfbc46887>
2. T568A y T568B: dos estándares de cable de red RJ45. (2018, noviembre 6). Knowledge. <https://community.fs.com/es/article/t568a-vs-t568b-difference-between-straight-through-and-crossover-cable.html>
3. Code, B. (n.d.). Conexión Telnet en windows - eleventa.com. Eleventa.com. Retrieved September 30, 2024, from <https://eleventa.com/aprender/conexion-telnet>
4. Fernández, Y. (2024, April 18). FTP: qué es y cómo funciona. Xataka.com; Xataka Basics. <https://www.xataka.com/basics/ftp-que-como-funciona>
5. Laprovittera, C. (2023, December 24). Guía Rápida de Wireshark: todos los comandos, filtros y sintaxis. - Álvaro Chirou. Álvaro Chirou; Alvaro Chirou. <https://achirou.com/guia-rapida-de-wireshark-todos-los-comandos-filtros-y-sintaxis/>
6. marketing. (2017, June 26). Diferencias entre los cables de par trenzado UTP, STP y FTP. Blog de TelecOcable: actualidad en cables y conexión electrónica; TELEOCABLE. <https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374>
7. Servidor NTP (Network Time Protocol) Servidor de tiempo - 2023. (2017, August 18). tecnozero Soluciones Informáticas; tecnozero. <https://www.tecnozero.com/servidor/ntp/>
8. T568A y T568B: dos estándares de cable de red RJ45. (2018, November 6). Knowledge. <https://community.fs.com/es/article/t568a-vs-t568b-difference-between-straight-through-and-crossover-cable.html>
9. (N.d.-a). Cloudflare.com. Retrieved September 30, 2024, from <https://www.cloudflare.com/es-es/learning/dns/what-is-dns/>
10. (N.d.-b). Cloudflare.com. Retrieved September 30, 2024, from <https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/>

11. (N.d.-c). Cloudflare.com. Retrieved September 30, 2024, from <https://www.cloudflare.com/es-es/learning/email-security/what-is-a-mail-server/>