

## Examen Final

Alumno: Bryan Mariano Salazar Sanchez

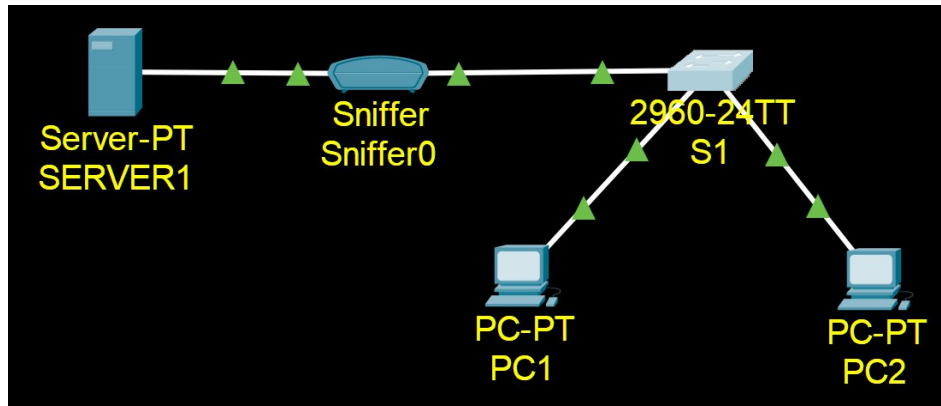


Figura 1. Topología a utilizar.

### Objetivos

- Configurar servicios de infraestructura.
- Configurar servicios de aplicaciones.
- Uso de un sniffer.

### Información básica/situación

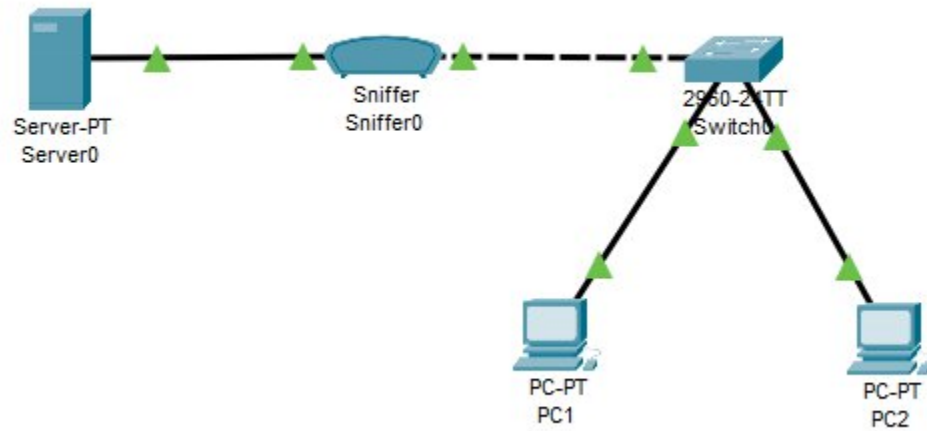
Usted es contratado como analista en un Centro de Operaciones de Seguridad SOC, con la misión de analizar el tráfico de los servicios de infraestructura y de aplicaciones de la red, para lo cual deberá utilizar un sniffer.

### Recursos necesarios

- Computador personal con Windows
- Software Packet Tracer
- Conexión a Internet

## Procedimiento

### Parte 1: Arme la red mostrada en la Figura 1.



**Parte 2: Configure los servicios de infraestructura DHCP y DNS en el servidor SERVER1.**

Examen de Habilidades 2: Creación de una red local

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

**DHCP**

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0Service ☒ On ☐ Off

Pool NameserverPool

Default Gateway192.168.1.1

DNS Server192.168.1.1

Start IP Address : 1921681100

Subnet Mask: 2552552550

Maximum Number of Users :156

TFTP Server:0.0.0.0

WLC Address:0.0.0.0

AddSaveRemove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	192.168....	192.168....	255.255....	156	0.0.0.0	0.0.0.0

☐ Top

Examen de Habilidades 2: Creación de una red local

Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name  Type A Record

Address

AddSaveRemove

No.	Name	Type	Detail
0	pc1.local	A Record	192.168.1.100
1	pc2.local	A Record	192.168.1.101

DNS Cache

☐ Top

**Parte 3: Configure los servicios de aplicaciones HTTP, HTTPS, FTP y EMAIL en el servidor SERVER1.**

Examen de Habilidades 2: Creación de una red local

Server0

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

HTTP

☒ On

☐ Off

HTTPS

☒ On

☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

New File

Import

☐ Top

## Examen de Habilidades 2: Creación de una red local

The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. The 'FTP' service is enabled (radio button selected). The 'User Setup' section shows a table with two users: 'cisco' and 'Prueba'. The 'Prueba' user is highlighted in blue. Below the table, there is a 'File' section listing several files. At the bottom left, there is a 'Top' button.

**Services**

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

**FTP**

Service: ☒ On ☐ Off

**User Setup**

Username:  Password:

☒ Write ☒ Read ☒ Delete ☒ Rename ☒ List

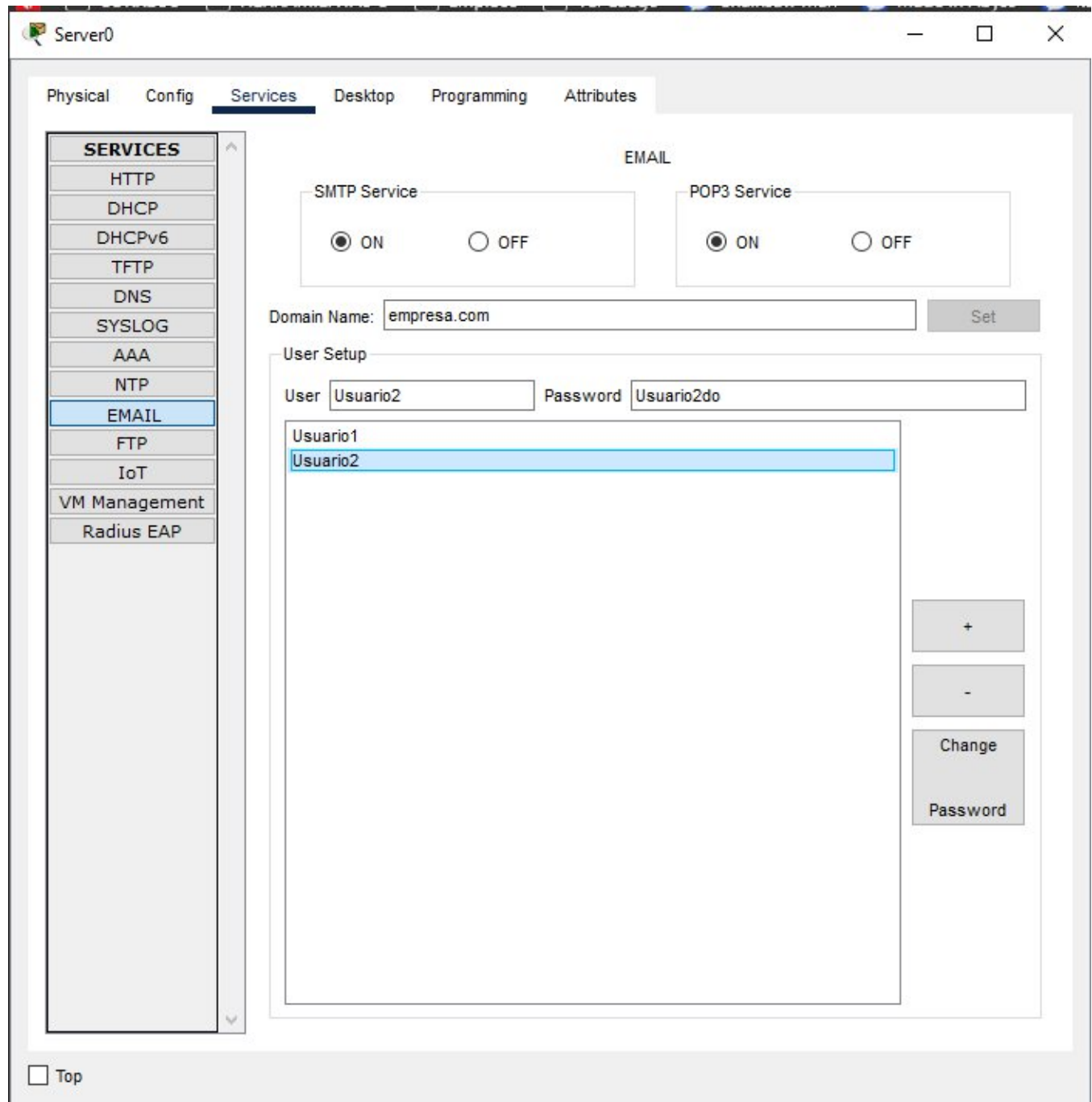
	Username	Password	Permission
1	cisco	cisco	RWDNL
2	Prueba	Prueba132	RWDNL

**File**

1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin

☐ Top

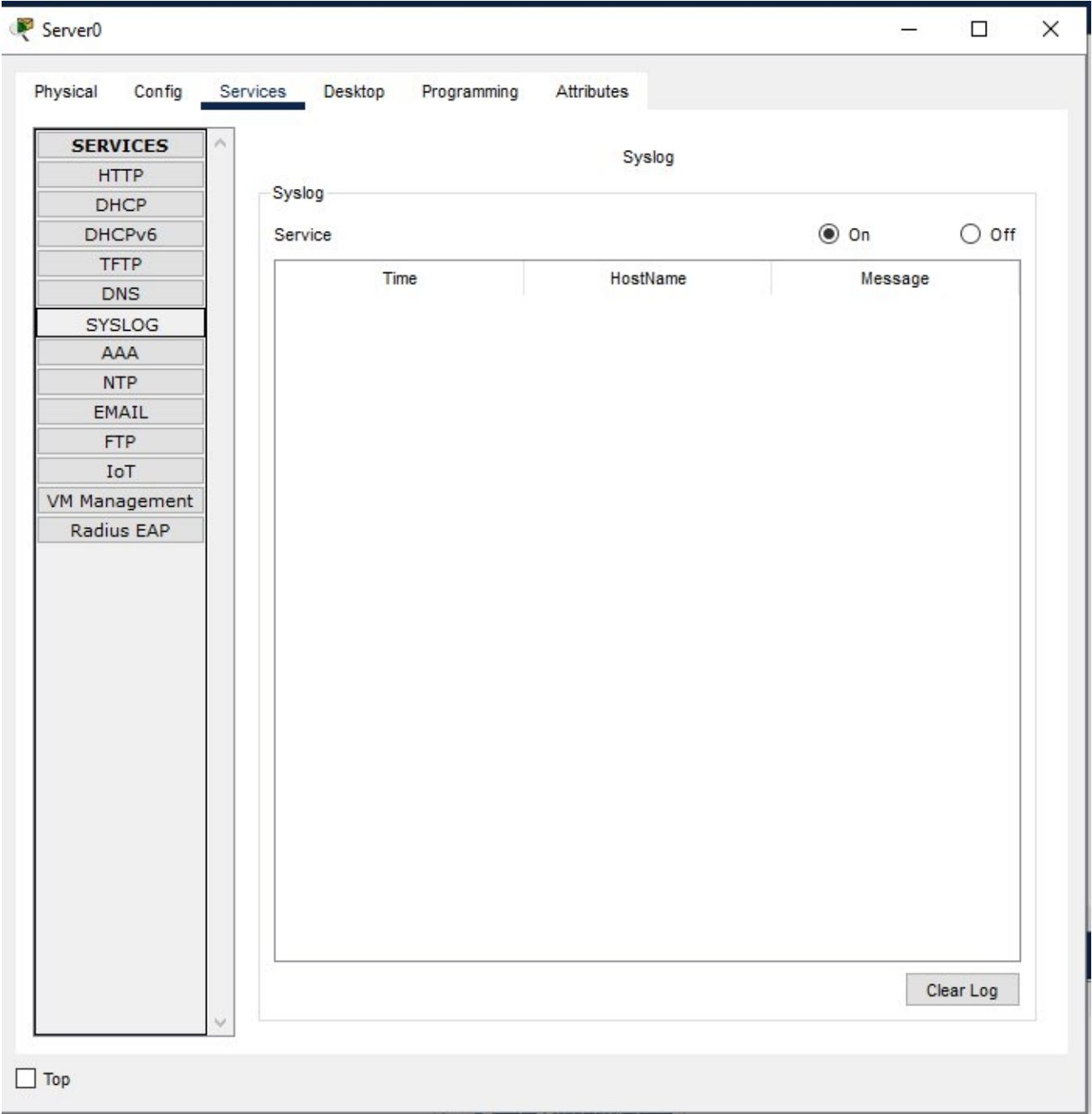




#### Parte 4: Uso de un sniffer.

*(Inserte la captura de pantalla del sniffer capturando paquetes)*

Parte 5: Configuración de un servidor SYSLOG.



Cuestionario

Con respecto al procedimiento realizado, responda las siguientes preguntas:

- 1. Incluya la tabla de direcciones.

## Examen de Habilidades 2: Creación de una red local

Dispositivo	Dirección IP	Máscara de Subred	Puerta de Enlace
Server0	192.168.1.1	255.255.255.0	-
Switch0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	DHCP	DHCP	DHCP
PC2	DHCP	DHCP	DHCP

2. En el servidor SERVER1 configure y active los servicios de infraestructura DHCP y DNS.

Examen de Habilidades 2: Creación de una red local

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

**DHCP**

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0ServiceOnOff

Pool NameserverPool

Default Gateway192.168.1.1

DNS Server192.168.1.1

Start IP Address :1921681100

Subnet Mask:2552552550

Maximum Number of Users :156

TFTP Server:0.0.0.0

WLC Address:0.0.0.0

AddSaveRemove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	192.168....	192.168....	255.255....	156	0.0.0.0	0.0.0.0

☐ Top

## Examen de Habilidades 2: Creación de una red local

Server0

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

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

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name  Type **A Record** ▼

Address

Add Save Remove

No.	Name	Type	Detail
0	pc1.local	A Record	192.168.1.100
1	pc2.local	A Record	192.168.1.101

DNS Cache

☐ Top

3. En el servidor SERVER1 configure y active los servicios de aplicaciones HTTP, HTTPS, FTP y EMAIL

## Examen de Habilidades 2: Creación de una red local

Server0

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

HTTP

☒ On ☐ Off

HTTPS

☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

New File

Import

☐ Top

## Examen de Habilidades 2: Creación de una red local

Server0

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

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

FTP

Service ☒ On ☐ Off

User Setup

Username  Password

☐ Write ☐ Read ☐ Delete ☐ Rename ☐ List

	Username	Password	Permission	
1	Prueba	Prueba132	RWDNL	Add
2	cisco	cisco	RWDNL	Save
				Remove

File

1	asa842-k8.bin
2	asa923-k8.bin
3	c1841-advipservicesk9-mz.124-15.T1.bin
4	c1841-ipbase-mz.123-14.T7.bin
5	c1841-ipbasek9-mz.124-12.bin
6	c1900-universalk9-mz.SPA.155-3.M4a.bin

Remove

☐ Top

## Examen de Habilidades 2: Creación de una red local

Server0

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

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

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User  Password

Usuario1  
Usuario2

☐ Top

4. Configure a la PC1 como cliente DHCP.



## Examen de Habilidades 2: Creación de una red local

PC1

Physical Config **Desktop** Programming Attributes

**IP Configuration** X

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address: 192.168.1.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::20C:85FF:FEB9:AC39

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

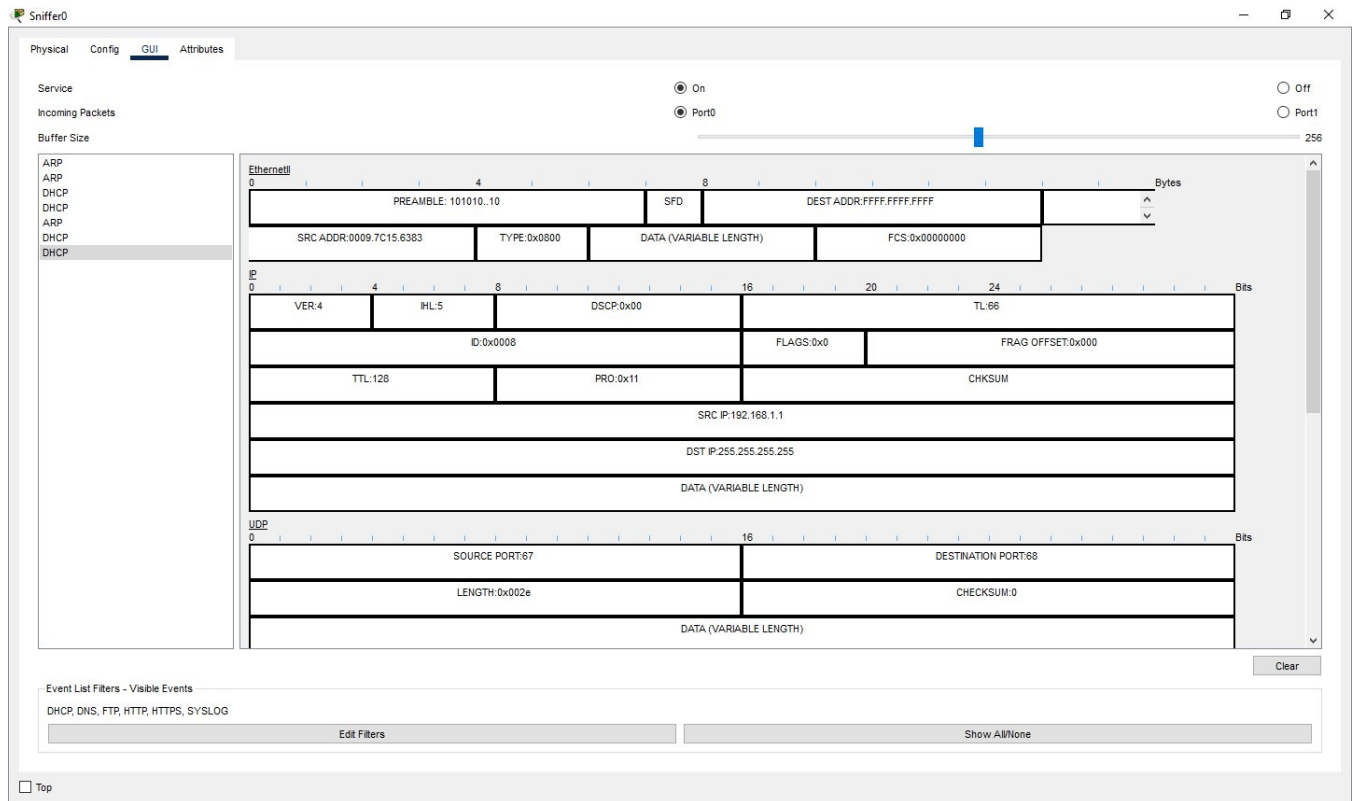
Username:

Password:

☐ Top

5. Use el sniffer para capturar el tráfico DHCP y describa el proceso DORA del tráfico DHCP capturado.

## Examen de Habilidades 2: Creación de una red local



### Descripción:

**Discover:** El cliente envía un mensaje de descubrimiento a la red para localizar servidores DHCP disponibles. En la captura podemos identificar que el cliente con dirección de hardware MAC 00:0C:85:B9:AC:39 ha iniciado este proceso.

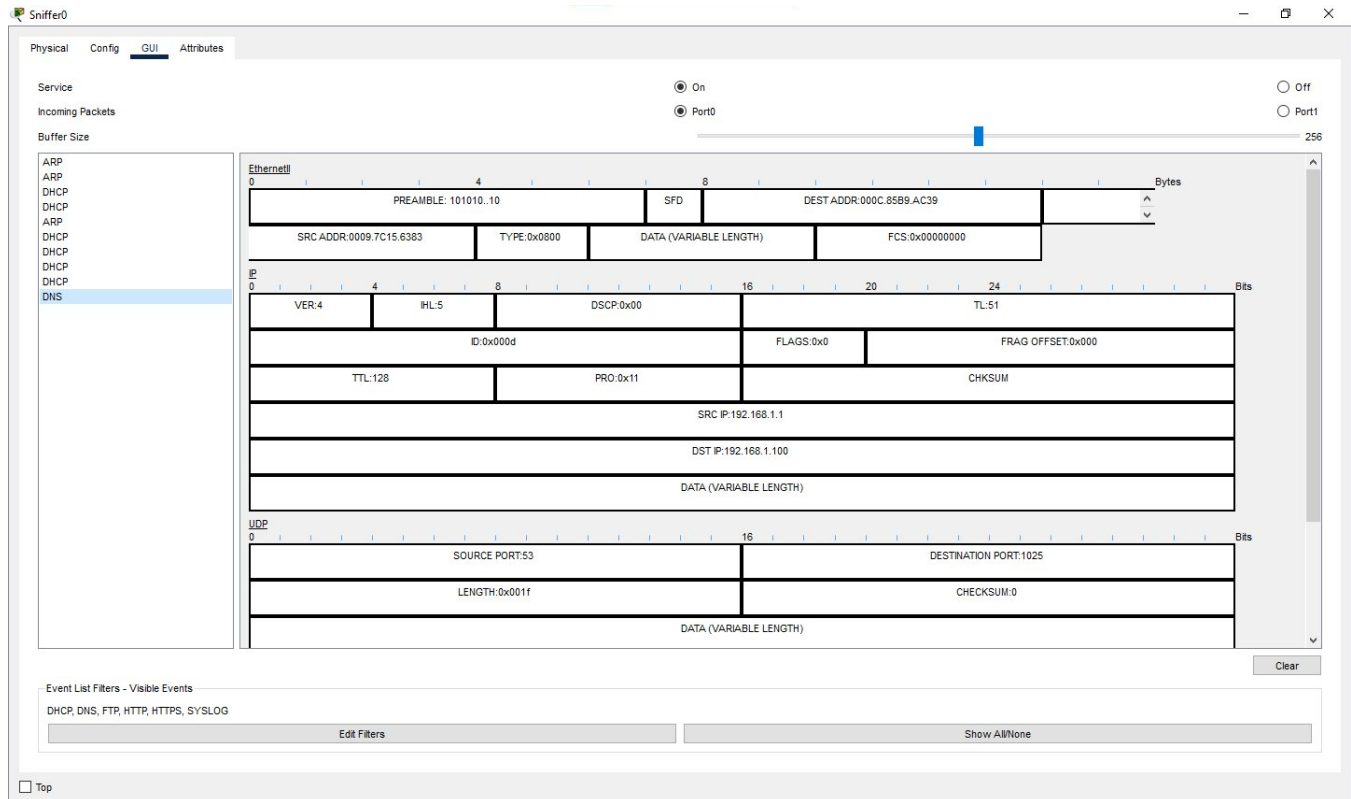
**Offer:** El servidor DHCP (en este caso con dirección IP 192.168.1.1) responde con una oferta que incluye una dirección IP disponible (192.168.1.100) y otras configuraciones de red.

**Request:** El cliente selecciona la oferta y envía una solicitud formal para usar la dirección IP ofrecida (192.168.1.100). Este mensaje confirma que el cliente desea utilizar la configuración propuesta por el servidor.

**Acknowledge:** Finalmente, el servidor DHCP confirma la asignación de la dirección IP enviando un mensaje de reconocimiento, completando así la configuración del cliente.

- Realice una consulta DNS al servidor, capture el tráfico DNS y describa los campos del tráfico DNS capturado.

## Examen de Habilidades 2: Creación de una red local



### Descripción:

**Nivel de transporte:** El tráfico DNS está utilizando UDP como protocolo de transporte (visible en la sección UDP).

**Puerto de origen:** 53 (puerto estándar del servidor DNS)

**Puerto de destino:** 1025 (puerto efímero del cliente)

**Longitud del paquete UDP:** 0x001f (17 bytes en decimal)

**Nivel de red:** La comunicación ocurre entre:

**IP de origen (SRC IP):** 192.168.1.1 (probablemente el router o servidor DNS local)

**IP de destino (DST IP):** 192.168.1.100 (el cliente que realizó la consulta)

**Cabecera DNS:** En la segunda imagen podemos ver la cabecera DNS que muestra:

**ID de transacción:** 0x2e75

**OPCODE:** 0x1 (código de operación, donde 0 es una consulta estándar)

**RCODE:** 0x3 (código de respuesta, posiblemente indicando un error de nombre no existente - NXDOMAIN)

## Examen de Habilidades 2: Creación de una red local

**QDCOUNT: 1 (1 pregunta en la consulta)**

**ANCOUNT: 0 (no hay respuestas)**

**NSCOUNT: 0 (no hay registros de servidor de nombres)**

**ARCOUNT: 0 (no hay registros adicionales)**

**Parámetros de IP:**

**TTL: 128 (Time To Live)**

**Protocolo: 0x11 (17 en decimal, que corresponde a UDP)**

**ID: 0x00d4**

7. Use el sniffer para capturar el tráfico HTTP y describa los campos del tráfico HTTP capturado.

The screenshot shows the Sniffer0 application interface. On the left, a list of protocols includes ARP, DHCP, DNS, and HTTP, with HTTP selected. The main area displays the packet structure in a hierarchical view on the left and a detailed field view on the right. The Ethernet II header shows a destination MAC of 000C:85B9:AC39 and a source MAC of 0009:7C15:6383. The IP header shows a source IP of 192.168.1.1 and a destination IP of 192.168.1.100. The TCP header shows a source port of 80 and a destination port of 1025. The sequence number is 1 and the acknowledgment number is 101.

**Descripción:**

**Nivel de transporte (TCP):**

**Puerto de origen: 80 (puerto estándar para servicio HTTP)**

**Puerto de destino: 1025 (puerto efímero del cliente)**

**Número de secuencia: 1**

**Número de reconocimiento (ACK): 101**

**Ventana TCP: 16384 bytes**

**Flags: 0x00011000 (probablemente ACK y PSH activados)**

**Checksum: 0x0000**

**Sin puntero de urgencia (Urgent Pointer: 0x0000)**

**Nivel de red (IP):**

**IP de origen (SRC IP): 192.168.1.1 (servidor web)**

**IP de destino (DST IP): 192.168.1.100 (cliente)**

**TTL: 128**

**Protocolo: 0x06 (TCP)**

**Versión IP: 4**

**Nivel de enlace (Ethernet):**

**Dirección MAC de destino: 00:0C:85:B9:AC:39 (cliente)**

**Tipo: 0x0800 (IPv4)**

**Preámbulo: 101010..10**

**Contenido HTTP:**

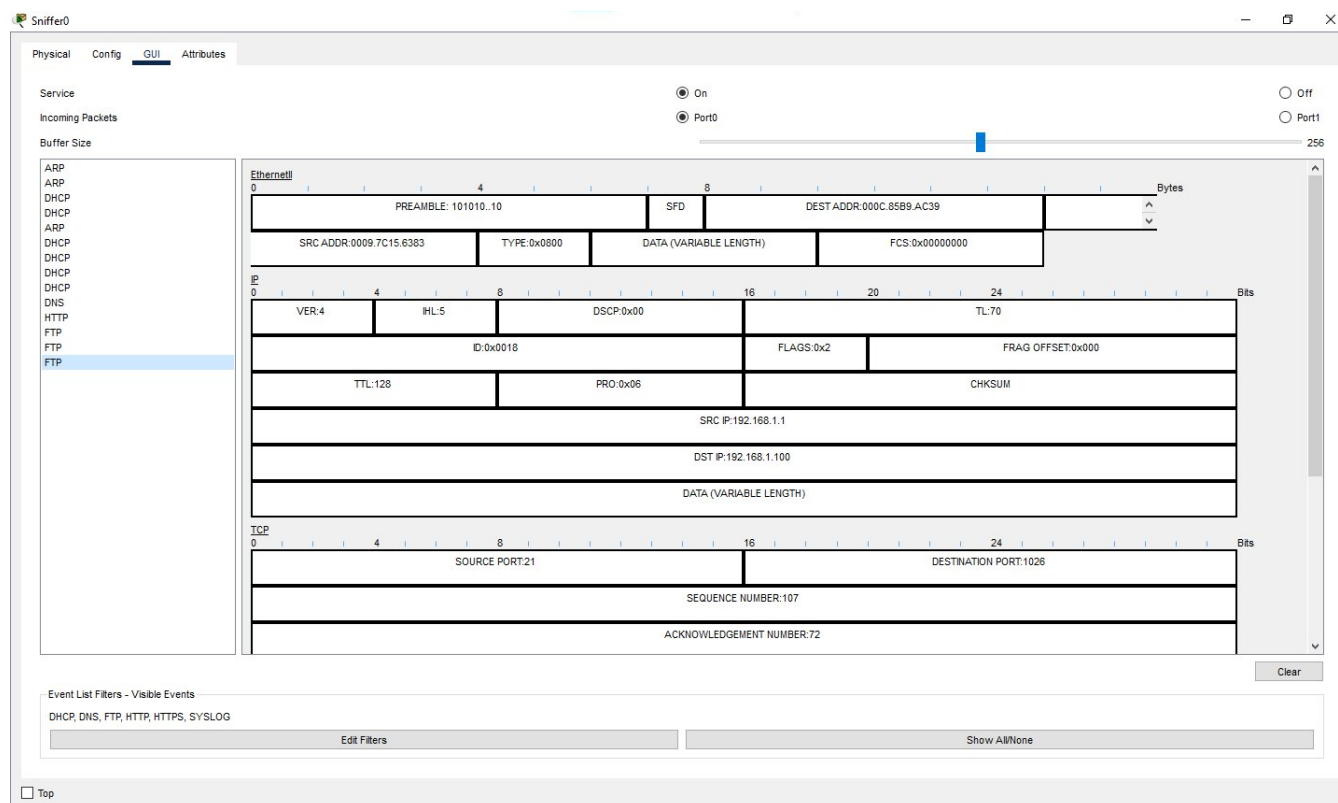
**Respuesta HTTP identificada como "HTTP RESPONSE"**

**Cabecera "Connection: close" (indica que el servidor cerrará la conexión después de esta respuesta)**

**Content-Length: 369 bytes**

8. Capture el tráfico FTP y describa los campos del tráfico FTP capturado. ¿Cuáles son las vulnerabilidades que puede advertir en este tipo de comunicación?

## Examen de Habilidades 2: Creación de una red local

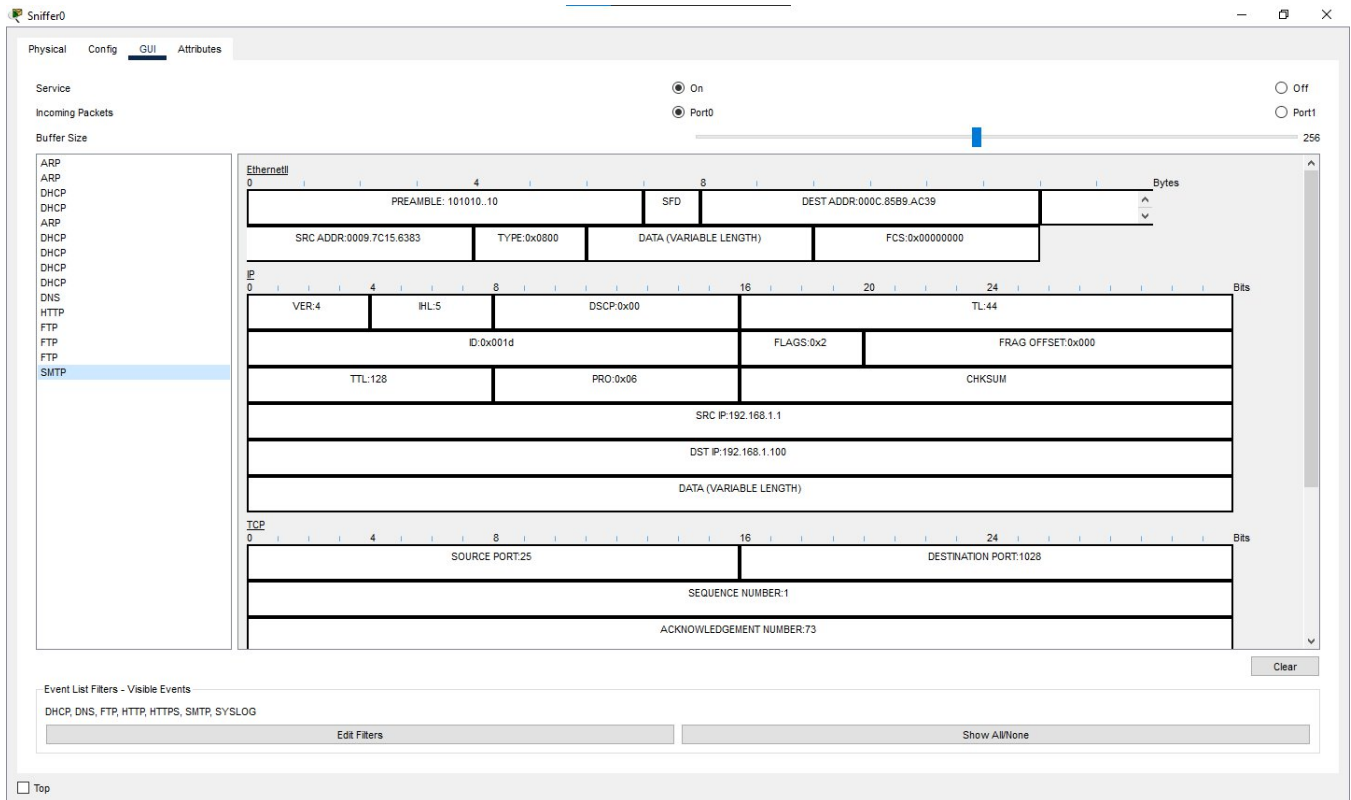


### Vulnerabilidades:

- **Tráfico no cifrado:** *FTP estándar (puerto 21) transmite todos los datos, incluidas las credenciales de autenticación, en texto plano. Cualquier atacante que pueda capturar el tráfico de red (como se está haciendo con Sniffer) podría ver nombres de usuario, contraseñas y todos los datos transferidos.*
- **Autenticación débil:** *Se observa un mensaje "Need account for login", lo que indica un proceso de autenticación básico que podría ser susceptible a ataques de fuerza bruta o diccionario.*
- **Conexiones separadas para control y datos:** *FTP utiliza canales separados para comandos y transferencia de datos, lo que complica la seguridad y puede causar problemas con firewalls.*
- **Comunicación en red local sin seguridad adicional:** *La comunicación ocurre en una red 192.168.1.x que, si bien es privada, no muestra señales de segmentación o protecciones adicionales.*
- **Metadatos expuestos:** *Información sobre la estructura del servidor y el cliente (como direcciones MAC, direcciones IP, puertos y configuración) está disponible para cualquiera que pueda monitorear el tráfico.*
- **Potencial para ataques Man-in-the-Middle:** *Sin cifrado ni verificación de certificados, un atacante podría interceptar y modificar la comunicación.*

## Examen de Habilidades 2: Creación de una red local

9. Configure a la PC1 como cliente de correo y capture el tráfico de correo. ¿Cuáles son los protocolos que utilizó?



### Protocolos:

**Ethernet** - Se observa la capa de enlace de datos con información como:

**Preámbulo:** 101010..10

**Direcciones MAC origen y destino** (SRC ADDR: 0009.7C15.6383, DEST ADDR: 000C.85B9.AC39)

**Tipo:** 0x0800 (indica IPv4)

**IPv4** - Protocolo de capa de red con:

**Versión:** 4

**IHL (Internet Header Length):** 5

**DSCP:** 0x00

**TTL:** 44 y 128 (para diferentes paquetes)

**Protocolo:** 0x06 (TCP)

**Direcciones IP origen y destino** (SRC IP: 192.168.1.1, DST IP: 192.168.1.100)

***TCP - Protocolo de transporte con:***

***Puerto origen: 25 (puerto estándar SMTP)***

***Puerto destino: 1028 (puerto cliente asignado dinámicamente)***

***Número de secuencia: 1***

***Número de reconocimiento (ACK): 73***

***Flags: 0x00011000 (en una imagen) y 0x00001000 (en otra)***

***Ventana: 16384***

***Checksum y puntero urgente***

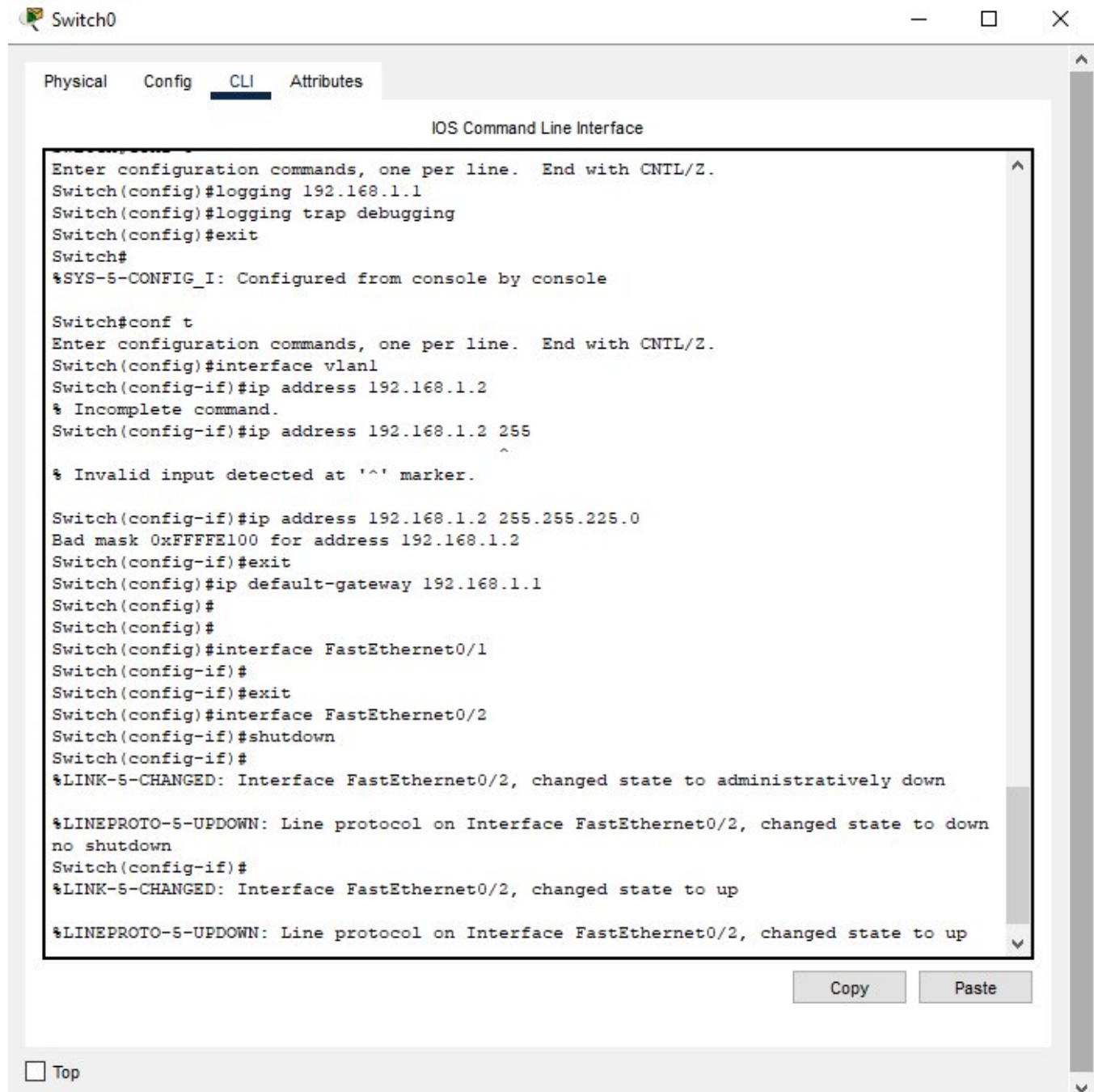
***SMTP - Protocolo de aplicación:***

***Se muestra la sección "SMTP DATA" que contiene la información del correo electrónico***

***La comunicación está ocurriendo a través del puerto 25, que es el puerto estándar para SMTP***

10. Configure el switch S1 para que use como servidor SYSLOG al servidor SERVER1.





The screenshot shows a network switch interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the IOS Command Line Interface. The terminal shows the following sequence of commands and outputs:

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#logging 192.168.1.1
Switch(config)#logging trap debugging
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.2
% Incomplete command.
Switch(config-if)#ip address 192.168.1.2 255

% Invalid input detected at '^' marker.

Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Bad mask 0xFFFFE100 for address 192.168.1.2
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#
Switch(config)#
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons. Below the CLI window, there is a 'Top' button.

## Calificación

Para la calificación se tomará en cuenta la documentación del procedimiento con capturas de pantalla que evidencien lo siguiente:

## Examen de Habilidades 2: Creación de una red local

Criterio		Puntaje
1	Armado de la red	2
2	Configuración de servicios	2
3	Uso del sniffer	2
4	Descripción del tráfico.	2
5	Resolución del cuestionario	12
TOTAL		20