ACTIVIDAD 1. ENLACE DE DATOS: ANÁLISIS DE TRÁFICO

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

LUIS MIGUEL POLO 20182020158

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

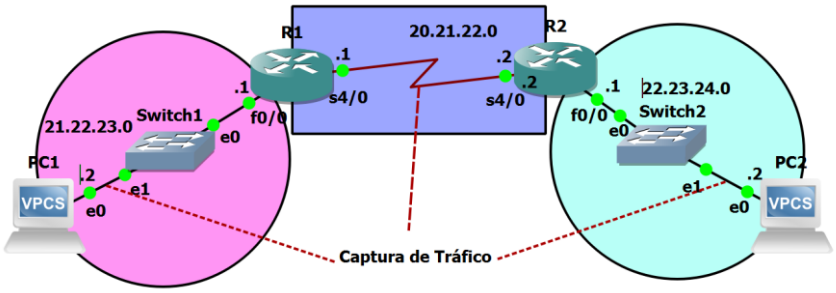
TELEINFORMATICA I

ANDRES ALEXANDER FONSECA

2024-III

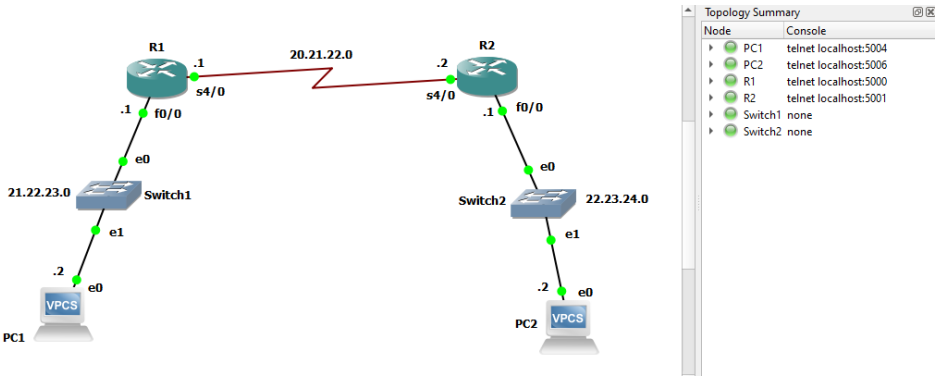
Enunciado

Capturar y analizar el tráfico en los puntos señalados de la siguiente topología:



Procedimiento

En primer lugar, fue necesario crear un nuevo proyecto siguiendo las indicaciones del diagrama físico y lógico del enunciado.



A continuación, se realizó la configuración de los dispositivos

Direccionamiento R1

```
R1(config)#int fa0/0
R1(config-if)#ip add 21.22.23.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#i
*Aug 20 08:34:28.123: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Aug 20 08:34:29.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#interface serial 4/0
R1(config-if)#ip add 20.21.22.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#exit
```

Direccionamiento R2

```
R2(config)#interface fa0/0
R2(config-if)#ip add 22.23.24.1 255.0.0.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#
*Aug 20 08:35:15.279: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Aug 20 08:35:16.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#interface s4/0
R2(config-if)#ip add 20.21.22.2 255.0.0.0
R2(config-if)#no sh
```

Direccionamiento PC1

```
NAME        : PC1[1]
IP/MASK     : 21.22.23.2/8
GATEWAY     : 21.22.23.1
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10018
RHOST:PORT  : 127.0.0.1:10019
MTU:        : 1500
```

Direccionamiento PC2

```
NAME        : PC2[1]
IP/MASK     : 22.23.24.2/8
GATEWAY     : 22.23.24.1
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 10020
RHOST:PORT  : 127.0.0.1:10021
MTU:        : 1500
```

CONFIGURACIÓN OSPF R1

```
R1(config)#router ospf 1
R1(config-router)#network 20.21.22.0 0.0.0.255 area 0
R1(config-router)#network 21.22.23.0 0.0.0.255 area 0
R1(config-router)#exit
R1(config)#exit
```

CONFIGURACIÓN OSPF R2

```
R2(config)#router ospf 1
R2(config-router)#network 20.21.22.0 0.0.0.255 area 0
R2(config-router)#netw
*Aug 21 09:49:39.691: %OSPF-5-ADJCHG: Process 1, Nbr 21.22.23.1 on Serial4/0 fro
m LOADING to FULL, Loading Done
R2(config-router)#network 22.23.24.0 0.0.0.255 area 0
R2(config-router)#exit
R2(config)#exit
```

VERIFICACIÓN PING ENTRE PC1 Y PC2

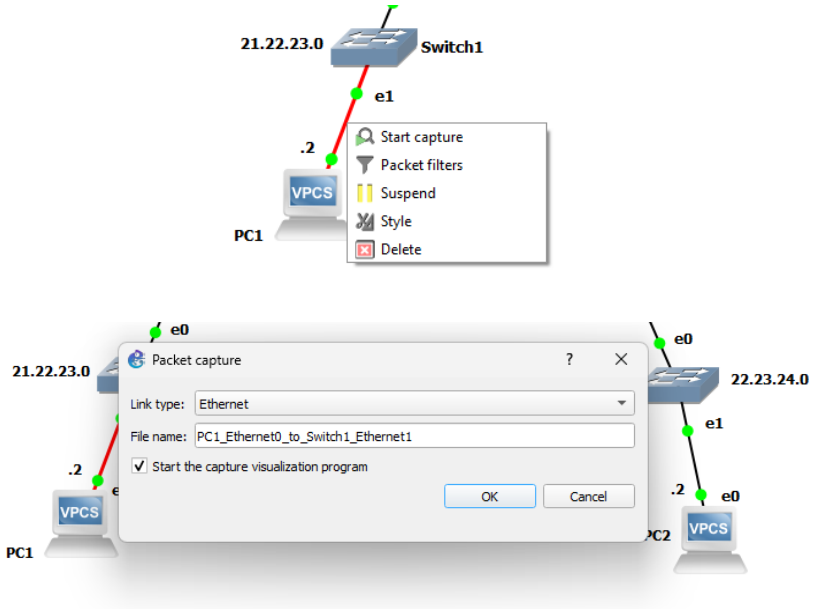
```
PC1> ping 22.23.24.2
84 bytes from 22.23.24.2 icmp_seq=1 ttl=62 time=45.373 ms
84 bytes from 22.23.24.2 icmp_seq=2 ttl=62 time=47.225 ms
84 bytes from 22.23.24.2 icmp_seq=3 ttl=62 time=43.343 ms
84 bytes from 22.23.24.2 icmp_seq=4 ttl=62 time=48.601 ms
84 bytes from 22.23.24.2 icmp_seq=5 ttl=62 time=51.171 ms
```

```
PC2> ping 21.22.23.2
84 bytes from 21.22.23.2 icmp_seq=1 ttl=62 time=45.675 ms
84 bytes from 21.22.23.2 icmp_seq=2 ttl=62 time=63.013 ms
84 bytes from 21.22.23.2 icmp_seq=3 ttl=62 time=64.828 ms
84 bytes from 21.22.23.2 icmp_seq=4 ttl=62 time=46.523 ms
84 bytes from 21.22.23.2 icmp_seq=5 ttl=62 time=49.066 ms
```

Análisis de Tráfico

Enlace entre PC1 Y Switch1 (Ethernet)

Se realizó el análisis de tráfico en los enlaces Ethernet y Serial de la topología

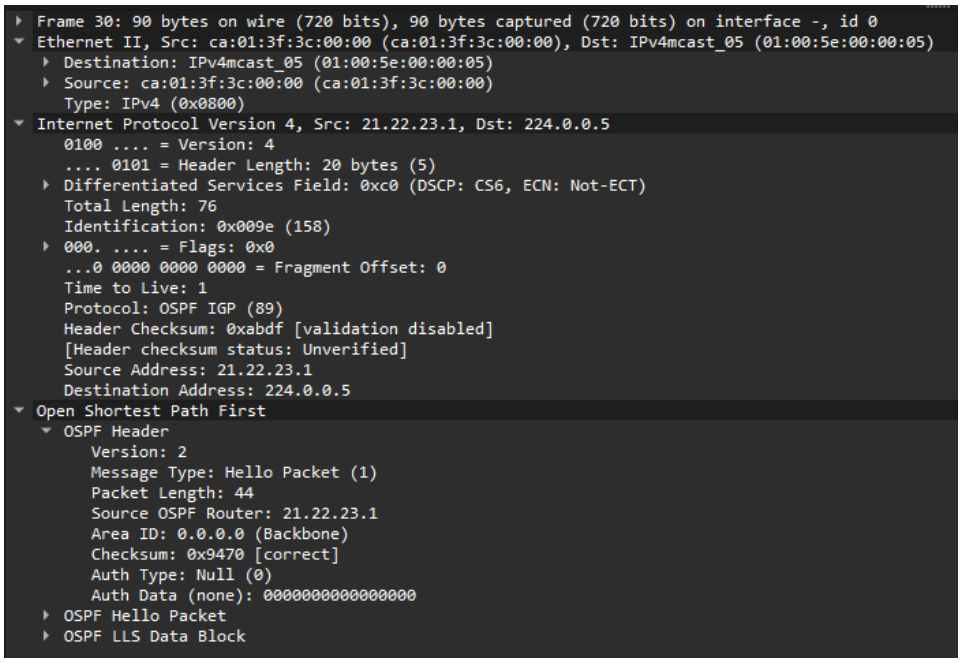


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
2	9.762716	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
3	19.613084	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
4	21.531768	ca:01:3f:3c:00:00	CDP/VTP/DTP/PAgP/UDLD	CDP	350	Device ID: R1 Port ID: FastEthernet0/0
5	29.392234	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
6	39.160824	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
7	48.602702	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
8	57.925541	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
9	67.695248	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
10	76.808221	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
11	81.553526	ca:01:3f:3c:00:00	CDP/VTP/DTP/PAgP/UDLD	CDP	350	Device ID: R1 Port ID: FastEthernet0/0
12	85.985194	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
13	95.872061	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
14	105.442192	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet
15	115.153550	21.22.23.1	224.0.0.5	OSPF	90	Hello Packet

La captura de paquetes muestra un intercambio de información predominantemente entre dos dispositivos de red. La mayoría de los paquetes utilizan el protocolo OSPF, lo que indica que ambos dispositivos están involucrados en un proceso de enrutamiento dinámico. El destino de estos paquetes, 224.0.0.5, es una dirección multicast utilizada específicamente para el protocolo OSPF.

La frecuencia de los paquetes OSPF sugiere que los dispositivos están intercambiando información de enrutamiento de manera regular para mantener actualizadas sus tablas de enrutamiento.

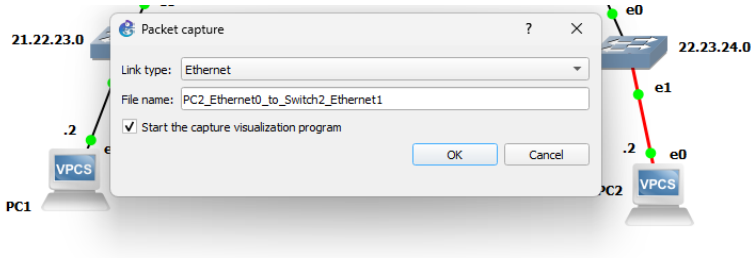
Los paquetes CDP (Cisco Discovery Protocol) presentes, por otro lado, indican que al menos uno de los dispositivos es un router Cisco y se está utilizando para descubrir otros dispositivos Cisco en la red. La información contenida en estos paquetes CDP, como el ID del dispositivo y el puerto de interfaz, puede ser utilizada para construir una topología parcial de la red.



Esta imagen muestra la captura de un paquete de red de tipo OSPF de la captura anterior. El paquete se origina en la dirección MAC ca:01:3f:3c:00:00 y tiene como destino la dirección de multidifusión IPv4 224.0.0.5, una dirección utilizada comúnmente para la comunicación entre enrutadores OSPF. El protocolo utilizado es IPv4, con una dirección IP de origen 21.22.23.1 y un TTL de 1, lo que indica que el paquete está destinado a la red local.

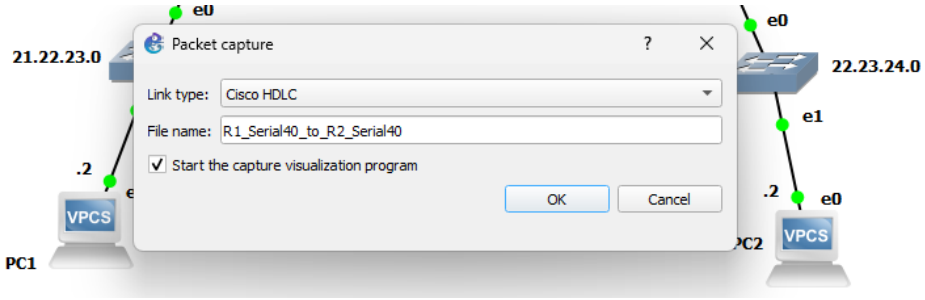
Este paquete contiene un mensaje de tipo "Hello", que es un tipo de mensaje utilizado por OSPF para descubrir y mantener relaciones de enrutamiento entre los routers de una red. El router que envía el paquete tiene el ID 21.22.23.1 y está en el área 0.0.0.0 (el área Backbone en OSPF). El checksum del paquete es válido, lo que confirma que no hay errores en su contenido.

Enlace entre PC2 Y Switch2 (Ethernet)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
2	9.235006	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
3	18.906387	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
4	28.184104	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
5	37.610867	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
6	38.067408	ca:02:2f:a0:00:00	CDP/VTP/DTP/PAgP/UDLD	CDP	350	Device ID: R2 Port ID: FastEthernet0/0
7	47.055390	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
8	56.183774	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
9	65.271425	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
10	74.767475	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
11	84.069934	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
12	93.527902	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
13	98.054554	ca:02:2f:a0:00:00	CDP/VTP/DTP/PAgP/UDLD	CDP	350	Device ID: R2 Port ID: FastEthernet0/0
14	102.896044	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet
15	112.212180	22.23.24.1	224.0.0.5	OSPF	90	Hello Packet

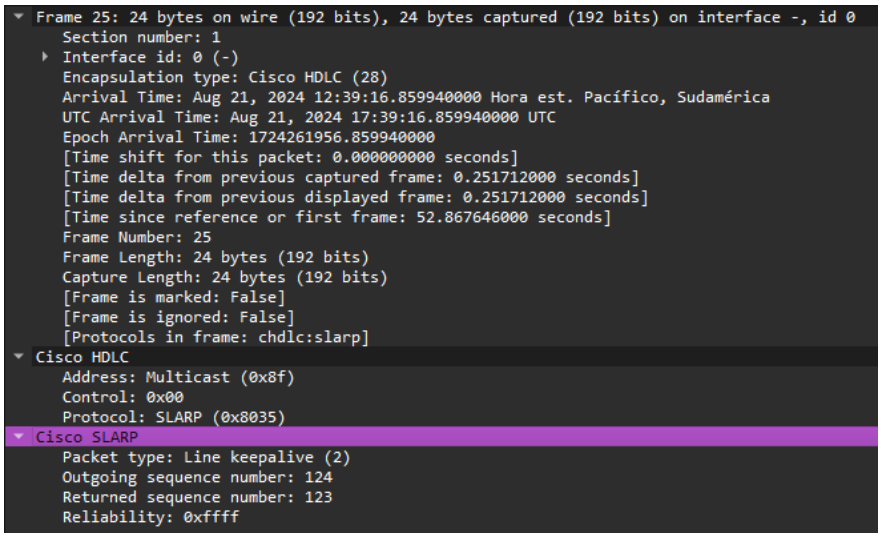
Enlace entre R1 Y R2 (Cisco HDLC)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
2	0.427981	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
3	4.882503	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 220, returned sequence 199
4	4.927199	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 200, returned sequence 220
5	9.092274	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
6	9.646261	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
7	14.838934	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 221, returned sequence 200
8	14.905692	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 201, returned sequence 221
9	18.117362	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
10	18.800828	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
11	24.865495	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 222, returned sequence 201
12	24.912469	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 202, returned sequence 222
13	27.377200	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
14	28.756032	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
15	34.880364	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 223, returned sequence 202
16	34.942535	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 203, returned sequence 223
17	36.534692	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
18	37.941666	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
19	44.874189	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 224, returned sequence 203
20	44.924215	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 204, returned sequence 224

Algunos paquetes de este enlace utilizan el protocolo OSPF, lo que indica que ambos dispositivos están involucrados en un proceso de enrutamiento dinámico. El destino de estos paquetes, 224.0.0.5, es una dirección multicast utilizada específicamente para el protocolo OSPF, confirmando así su función en el enrutamiento. La frecuencia de los paquetes OSPF sugiere que los dispositivos están intercambiando información de enrutamiento de manera regular para mantener actualizadas sus tablas de enrutamiento.

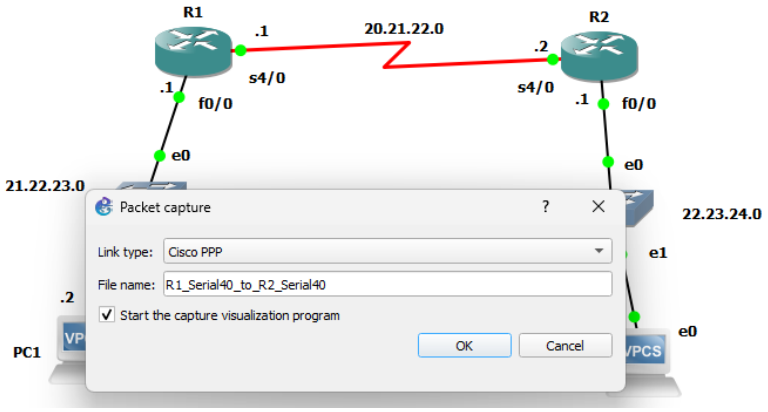
Por otro lado, también tenemos el protocolo SLARP. Este protocolo se utiliza típicamente en enlaces seriales para descubrir y mantener la conectividad con otros dispositivos. Los paquetes SLARP en la captura indican que existe al menos un enlace serial entre los dispositivos involucrados. Los campos de secuencia en los paquetes SLARP sugieren un intercambio de información de mantenimiento de enlace en curso.



La anterior imagen muestra una captura de un paquete de red que utiliza el protocolo Cisco HDLC, encapsulado con el protocolo SLARP. El paquete tiene una longitud total de 24 bytes, y fue capturado en un enlace serial utilizando encapsulación HDLC. Se identifica como un paquete de tipo multicast (0x8f) con un protocolo SLARP (0x8035). Este paquete fue enviado para mantener la conexión en una interfaz serie en un dispositivo Cisco, con detalles de tiempo precisos, como la hora de captura en UTC y la hora local (Pacífico, Sudamérica).

El paquete específico es un mensaje SLARP de keepalive, utilizado para verificar la conectividad en un enlace serie. Los números de secuencia indican que el número de salida es 124 y el número de retorno es 123, lo que sugiere que los paquetes están fluyendo correctamente entre los dispositivos en la red.

R1 Y R2 (Cisco PPP)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
2	1.329111	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 288, returned sequence 267
3	1.380769	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 268, returned sequence 288
4	2.225453	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
5	9.382201	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
6	11.326182	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 289, returned sequence 268
7	11.384490	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 269, returned sequence 289
8	11.434941	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet
9	18.760365	20.21.22.1	224.0.0.5	OSPF	84	Hello Packet
10	21.322300	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 290, returned sequence 269
11	21.389799	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 270, returned sequence 290
12	21.439634	20.21.22.2	224.0.0.5	OSPF	84	Hello Packet

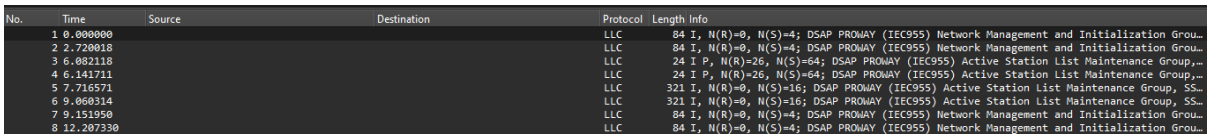
R1 Y R2 (Frame Relay)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			FR	84	DLCI 0, I, N(R)=4, N(S)=0
2	3.387253			FR	84	DLCI 0, I, N(R)=4, N(S)=0
3	3.387253			FR	24	DLCI 0, I, N(R)=64, N(S)=0
4	3.418376			FR	24	DLCI 0, I, N(R)=64, N(S)=0
5	9.800868			FR	84	DLCI 0, I, N(R)=4, N(S)=0
6	12.976609			FR	84	DLCI 0, I, N(R)=4, N(S)=0
7	13.385184			FR	24	DLCI 0, I, N(R)=64, N(S)=0
8	13.421003			FR	24	DLCI 0, I, N(R)=64, N(S)=0
9	15.053241			FR	321	DLCI 0, I, N(R)=16, N(S)=0
10	16.373678			FR	321	DLCI 0, I, N(R)=16, N(S)=0
11	19.705864			FR	84	DLCI 0, I, N(R)=4, N(S)=0
12	22.676197			FR	84	DLCI 0, I, N(R)=4, N(S)=0
13	23.367422			FR	24	DLCI 0, I, N(R)=64, N(S)=0
14	23.430154			FR	24	DLCI 0, I, N(R)=64, N(S)=0
15	28.875371			FR	84	DLCI 0, I, N(R)=4, N(S)=0
16	31.731972			FR	84	DLCI 0, I, N(R)=4, N(S)=0
17	33.378772			FR	24	DLCI 0, I, N(R)=64, N(S)=0
18	33.424608			FR	24	DLCI 0, I, N(R)=64, N(S)=0

La captura muestra un tráfico de red compuesto por un solo tipo de protocolo, identificado como "FR". Los paquetes FR se envían y reciben a intervalos relativamente regulares, sugiriendo una comunicación continua entre dos o más dispositivos. Los campos DLCI (Data Link Connection Identifier) y los valores N(R) y N(S) indican que este es un protocolo de enlace de datos, probablemente utilizado para transmitir información a través de una línea serie o una red de área local (LAN) pequeña.

Los valores de DLCI, N(R) y N(S) son típicos de protocolos de enlace de datos como HDLC o PPP. Estos valores se utilizan para controlar el flujo de datos, detectar y corregir errores, y mantener la sincronización entre los dispositivos. La variedad de valores de DLCI sugiere que puede haber múltiples conexiones lógicas múltiples o canales virtuales multiplexados sobre el enlace físico.

R1 Y R2 (ATM)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			LLC	84	I, N(R)=0, N(S)=4; DSAP PROWAY (IEC955) Network Management and Initialization Grou…
2	2.720018			LLC	84	I, N(R)=0, N(S)=4; DSAP PROWAY (IEC955) Network Management and Initialization Grou…
3	6.082118			LLC	24	I P, N(R)=26, N(S)=64; DSAP PROWAY (IEC955) Active Station List Maintenance Group,…
4	6.141711			LLC	24	I P, N(R)=26, N(S)=64; DSAP PROWAY (IEC955) Active Station List Maintenance Group,…
5	7.716571			LLC	321	I, N(R)=0, N(S)=16; DSAP PROWAY (IEC955) Active Station List Maintenance Group, SS…
6	9.060314			LLC	321	I, N(R)=0, N(S)=16; DSAP PROWAY (IEC955) Active Station List Maintenance Group, SS…
7	9.151950			LLC	84	I, N(R)=0, N(S)=4; DSAP PROWAY (IEC955) Network Management and Initialization Grou…
8	12.207330			LLC	84	I, N(R)=0, N(S)=4; DSAP PROWAY (IEC955) Network Management and Initialization Grou…

La captura muestra un tráfico de red compuesto por un solo tipo de protocolo, identificado como "LLC". Los paquetes LLC se envían y reciben a intervalos relativamente regulares, sugiriendo una comunicación continua entre dos o más dispositivos.

Preguntas

- **¿Cuáles son las principales diferencias entre las tramas Ethernet y las tramas Cisco HDLC en términos de estructura y uso?**

  Estructura de la trama

a. **Trama Ethernet**

   Encabezado (Header): La trama Ethernet tiene un encabezado que incluye varias secciones importantes:

   Dirección MAC de destino: 6 bytes.

   Dirección MAC de origen: 6 bytes.

   Tipo de EtherType/Longitud: 2 bytes (identifica el protocolo de la capa superior, como IPv4, IPv6, etc.)

   Datos/Payload: Contiene los datos a ser transmitidos. La longitud máxima de los datos en una trama Ethernet es de 1500 bytes (MTU - Unidad Máxima de Transferencia).

   CRC (Cyclic Redundancy Check): 4 bytes para verificar la integridad de la trama.

   Tamaño de la trama: La trama Ethernet puede variar entre 64 bytes (tamaño mínimo) y 1518 bytes (tamaño máximo, excluyendo las tramas Jumbo).

b. **Trama Cisco HDLC**

   Bandera (Flag): 1 byte (valor hexadecimal 0x7E), indica el comienzo y el final de la trama.

Dirección: 1 byte. Se usa para identificar el dispositivo de destino en un entorno punto a punto.

Control: 1 byte. Este campo se usa en algunas variantes de HDLC para identificar el tipo de trama (comando o respuesta). En Cisco HDLC, generalmente se fija en un valor estático (0x00).

Protocolo: 2 bytes. Este campo identifica el protocolo de capa superior que transporta la trama (similar al campo EtherType en Ethernet).

Datos/Payload: Los datos reales que están siendo enviados. La longitud varía.

FCS (Frame Check Sequence): 2 o 4 bytes para la verificación de errores, que garantiza la integridad de la trama.

Uso

a. **Ethernet**

Ethernet es ampliamente utilizado en redes LAN. Es el protocolo estándar para la mayoría de las redes cableadas domésticas, empresariales y de centros de datos.

Ethernet puede soportar varias topologías como bus, estrella o malla. También puede trabajar en redes punto a punto, aunque no es su uso principal.

Ethernet está diseñado para redes con varios dispositivos, donde se requiere direccionamiento MAC y la capacidad de manejar colisiones mediante protocolos como CSMA/CD.

b. **Cisco HDLC**

HDLC, especialmente la variante de Cisco HDLC, se utiliza principalmente en conexiones punto a punto entre routers, a menudo en WAN (Wide Area Network). Está optimizado para la transmisión de datos en enlaces seriales.

Es ideal para enlaces punto a punto donde no se requiere direccionamiento adicional, ya que solo hay dos dispositivos en la comunicación.

Este protocolo es simple y eficiente para la transmisión de datos entre dos nodos en un enlace serial, sin la necesidad de características avanzadas como el manejo de colisiones o el direccionamiento.

- **¿Cómo se configura la encapsulación HDLC en los routers Cisco, y cuáles son las implicaciones de esta configuración en la comunicación entre los dispositivos?**

Pasos para configurar HDLC en un router Cisco:

1. **Acceder al modo de configuración de la interfaz serial:** Ingresar al modo de configuración global y luego a la interfaz serial que se va a configurar.

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0/0/0
```

2. **Configurar la encapsulación HDLC:** Una vez en el modo de configuración de la interfaz serial, se establece HDLC como el protocolo de encapsulación. HDLC suele ser el protocolo predeterminado, pero se puede volver a configurar explícitamente con el siguiente comando:

```
Router(config-if)# encapsulation hdlc
```

3. **Verificación de la configuración:** Para asegurarse de que la encapsulación HDLC se ha configurado correctamente, se puede utilizar el siguiente comando de verificación:

```
Router# show interface serial 0/0/0
```

El resultado debe mostrar algo como:

```
Serial0/0/0 is up, line protocol is up
Encapsulation HDLC, loopback not set
...
```

Implicaciones de la configuración de HDLC en la comunicación

Comunicación punto a punto: HDLC está diseñado para conexiones punto a punto, lo que significa que solo habrá dos dispositivos en la misma conexión (generalmente dos routers). No se necesita direccionamiento MAC, ya que el router sabe que el tráfico está destinado directamente al otro dispositivo en el enlace.

Compatibilidad: Cisco HDLC es una versión propietaria del estándar HDLC, por lo que ambos dispositivos en el enlace deben ser routers Cisco o dispositivos que

entiendan la variante de HDLC de Cisco. Si se intenta usar HDLC de Cisco con dispositivos de otro fabricante, es posible que los dispositivos no se comuniquen correctamente, ya que las implementaciones no siempre son compatibles.

Eficiencia y simplicidad: Dado que HDLC es un protocolo simple y eficiente, no introduce mucho overhead (sobrecarga) en la comunicación. Esto lo hace ideal para enlaces seriales WAN de baja velocidad, donde la eficiencia es clave.

Soporte limitado para múltiples protocolos: Aunque HDLC puede transportar varios protocolos de capa 3 (como IP), no tiene la misma flexibilidad que otros protocolos de encapsulación como PPP (Point-to-Point Protocol), que es más robusto y soporta características adicionales como autenticación (PAP, CHAP), compresión y encapsulación de múltiples protocolos.

Confiabilidad básica: HDLC proporciona detección de errores mediante el uso de una secuencia de verificación de trama (FCS), lo que asegura que los datos se entreguen sin errores. Sin embargo, no ofrece mecanismos avanzados de control de errores o retransmisión en caso de fallos, a diferencia de otros protocolos de nivel superior.

- **¿Qué tipo de información se puede capturar y analizar de las tramas Ethernet y Cisco HDLC utilizando herramientas de captura de tráfico, como Wireshark?**

  Con herramientas de captura de tráfico como Wireshark, es posible capturar una variedad de información relevante de las tramas Ethernet. Entre los datos más importantes se encuentran las direcciones MAC de origen y destino, el tipo de protocolo de capa superior (como IPv4 o IPv6), y los datos encapsulados (payload).

  Además, se puede analizar el Frame Check Sequence (FCS) para detectar errores en la transmisión de datos. Wireshark también permite examinar el tráfico de red a nivel de protocolo, como ARP, ICMP, TCP y otros, lo que es útil para identificar problemas de conectividad, colisiones, y tráfico de broadcast o multicast en redes LAN.

  En el caso de las tramas Cisco HDLC, Wireshark también permite capturar y analizar información importante para redes punto a punto en entornos WAN. Se pueden observar campos como la dirección del dispositivo, el campo de control, y el protocolo de capa superior encapsulado (por ejemplo, IP).

Además, es posible verificar la integridad de las tramas mediante el FCS y detectar errores de transmisión. Este análisis es clave para monitorear el rendimiento de enlaces seriales y resolver problemas de conectividad o errores de configuración en conexiones punto a punto entre routers.

- **¿Cuáles son las ventajas y desventajas de utilizar Cisco HDLC en lugar de Ethernet para la conexión entre los routers R1 y R2 en tu configuración?**

  Ventajas de utilizar Cisco HDLC

  Simplicidad en la configuración: Cisco HDLC es un protocolo de encapsulación más sencillo, diseñado específicamente para conexiones punto a punto, lo que elimina la necesidad de direccionamiento MAC y simplifica la configuración y el mantenimiento.

  Menor sobrecarga: Cisco HDLC tiene una estructura de trama más ligera en comparación con Ethernet, ya que no incluye campos adicionales como las direcciones MAC. Esto lo hace más eficiente en conexiones WAN de baja velocidad, donde el ancho de banda puede ser limitado. La menor sobrecarga mejora el rendimiento en enlaces seriales punto a punto, asegurando que la mayoría del tráfico se utilice para los datos en lugar de la encapsulación.

  Desventajas de utilizar Cisco HDLC

  Compatibilidad limitada: Cisco HDLC es una versión propietaria del estándar HDLC, por lo que ambos routers deben ser dispositivos Cisco o equipos que soporten esta variante. Si en algún momento uno de los dispositivos no es Cisco, la interoperabilidad puede ser un problema, requiriendo que se cambie a un protocolo más estándar como PPP.

  Falta de funciones avanzadas: A diferencia de Ethernet o protocolos como PPP, Cisco HDLC no ofrece características avanzadas como autenticación, compresión, o soporte para múltiples protocolos de capa superior de manera flexible. Esto puede ser una limitación en escenarios más complejos, donde se necesitan estas funciones adicionales para mejorar la seguridad o el rendimiento de la red.

- **¿Qué problemas comunes podrías encontrar al capturar y analizar tramas en esta configuración de red, y cómo podrías resolverlos?**

  Al capturar y analizar tramas en una topología punto a punto, es común enfrentar problemas como la falta de visibilidad del tráfico, debido a la naturaleza directa de los enlaces seriales, o configuraciones de encapsulación incompatibles entre los routers, lo que impide la comunicación. Además, pueden surgir errores de transmisión o

problemas de sincronización de reloj, que afectan la integridad de las tramas y el rendimiento del enlace.

Para resolverlos, se podría usar herramientas de monitoreo en los routers (como comandos de debug), asegurar que ambos dispositivos utilicen el mismo protocolo de encapsulación (HDLC, PPP), y verificar la configuración de reloj y velocidad de transmisión en las interfaces seriales.