Enlace WAN

Scaravilli Sandro

20 de septiembre de 2024

1. Introduccion - Capa de Enlace

La capa de enlace de datos (capa 2 del modelo OSI) es responsable de asegurar que los datos se transmitan de manera confiable a través de un medio físico entre dos nodos adyacentes. Su principal función es organizar los datos en tramas, controlar el acceso al medio y gestionar la corrección de errores en la transmisión. Además, gestiona la sincronización entre emisor y receptor para asegurar que los datos lleguen de forma íntegra.

2. HDLC

HDLC es un protocolo orientado a la conexión que organiza los datos en tramas para la comunicación a través de enlaces punto a punto o multipunto. Se utiliza en enlaces seriales, donde la comunicación entre dos dispositivos depende de los roles de DTE y DCE.

DTE (Data Terminal Equipment)
DTE se refiere al equipo terminal de datos, que generalmente es un dispositivo final, como una computadora, un router o una terminal. El DTE es el origen o destino de los datos y depende del DCE para establecer la conexión y realizar la transmisión.

DCE (Data Communication Equipment)
DCE es el equipo de comunicaciones de datos, y generalmente es un dispositivo intermediario, como un módem o un switch, que facilita la transmisión de datos entre dos puntos. El DCE proporciona la interfaz física y lógica para la transmisión de datos, sincronizando la comunicación con el DTE.

En un enlace serial, el DCE suele ser el dispositivo que proporciona el reloj (señal de sincronización) para la transmisión, mientras que el DTE sigue este reloj. En una conexión punto a punto, como la que se configura con HDLC, el DCE maneja el aspecto físico de la comunicación, mientras que el DTE gestiona los datos

2.1. Practica Escenario 1 - HDLC

Primero dentro de cada uno de los routers dentro de la configuracion de la interfaz serial 0/1/0 ingresamos el comando no shutdown para dar de alta el estado de ella. A continuacion pasamos a cambiar el clockrate del DCE a 250.000.Luego gracias a la informacion que nos provee do show interfaces brief podemos ver el estado de la interfaz.

Comandos Utilizados

```
show controllers
show interfaces
no shutdown
clock rate 250000
do show interfaces brief
```

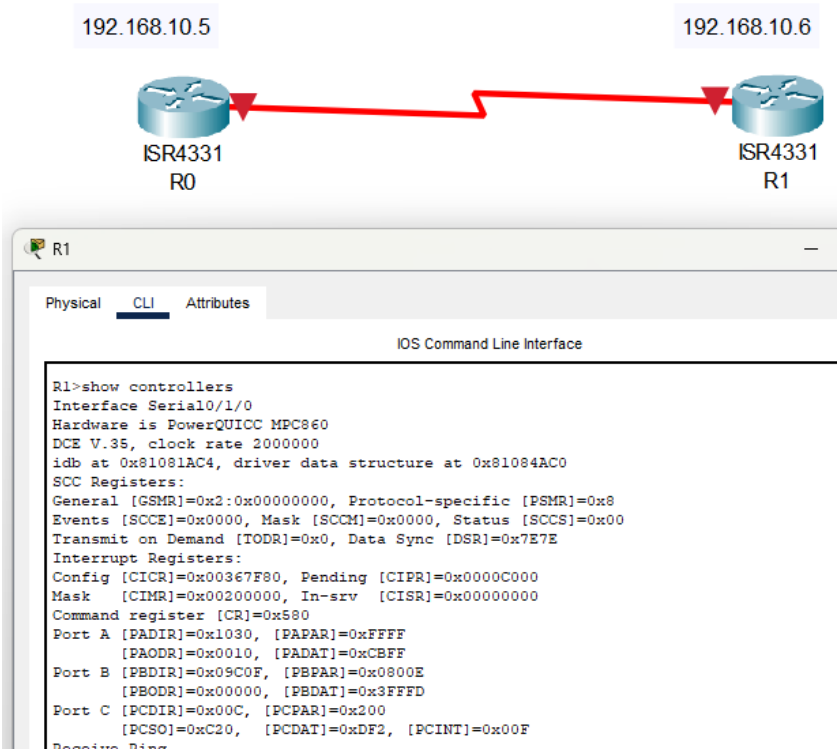

Figura 1: Informacion de comando Show Controllers en R1

Luego de estas configuraciones podemos realizar el ping de R0 a R1 mediante el comando ping 192.168.10.6 y visualizamos la concrecion de dicho envio.

```
ping 192.168.10.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/9 ms

R0#
```

Figura 2: Ping satisfactorio de R0 a R1

3. Trama cHDLC

A continuacion se prosigue a hacer el analisis de la informacion requerida a traves del enlace provisto.

1. Tipos de mensajes SLARP.
Existen tres tipos principales de mensajes en SLARP:
Request (Solicitud): Un router que no conoce su dirección IP envía este mensaje para pedir una dirección IP a través de la línea serial.
Reply (Respuesta): El router que recibe la solicitud y tiene la información requerida responde con la dirección IP solicitada.
Keepalive: Este mensaje es utilizado para verificar que el enlace esté activo y funcionando correctamente, ya que no tiene relación directa con la resolución de direcciones.

2. Secuencia de los mensajes SLARP.
La secuencia de mensajes SLARP sigue este flujo básico:
1 - Un router envía un SLARP Request en la interfaz serial, solicitando información de la dirección IP.
2 - Si el router conectado tiene una IP configurada en la interfaz, responderá con un SLARP Reply, proporcionando la dirección IP solicitada.
3 - Posteriormente, ambos routers pueden enviar mensajes SLARP Keepalive para monitorear la disponibilidad del enlace.

3. Timing de los mensajes SLARP.
El timing de los mensajes SLARP depende de las condiciones de la red y de la configuración de la interfaz serial.

El SLARP Request es enviado poco después de que la interfaz serial esté habilitada y lista para transmisión.
El SLARP Reply se recibe inmediatamente después de que el router receptor procesa la solicitud.
SLARP Keepalive se envían periódicamente para mantener la sincronización y monitorear la integridad del enlace.

4. Valor de protocol para los mensajes SLARP.
El identificador de protocolo para los mensajes SLARP en la capa de enlace HDLC es **0x8035**.

5. Valor de protocol para los mensajes unicast.
El identificador de protocolo para IP sobre HDLC, utilizado en tramas unicast cuando se está enviando tráfico IP entre routers, es **0x8000**.

6. Secuencia de los mensajes unicast.
La secuencia de los mensajes unicast en una comunicación HDLC es más simple que la de SLARP, ya que se basa en la transmisión normal de paquetes IP.

El flujo sería:

1 - El router envía una trama HDLC con un paquete IP encapsulado, dirigido a la dirección unicast del router receptor.
2 - El router receptor procesa la trama y extrae el paquete IP, manejando la información según la tabla de enrutamiento.
3 - El router receptor puede enviar una respuesta (como un ping reply) de vuelta al emisor en otra trama unicast.

En nuestro escenario se realizan 5 intercambios entre Requests y Replies.

4. Conclusiones

El comando show interfaces muestra el estado actual de la interfaz, incluyendo información clave como la cantidad de tramas enviadas/recibidas, errores, y keepalives tal como figura en la imagen siguiente.

```
Serial0/1/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.5/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 640 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 640 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Figura 3: Informacion de comando show interfaces

Importancia del Secuenciamiento
En SLARP:
El secuenciamiento de los mensajes SLARP (Request, Reply, y Keepalive) es fundamental para establecer y mantener la comunicación. La solicitud de dirección (Request) debe preceder a la respuesta (Reply). Si el secuenciamiento se altera o falla (por ejemplo, si el Request no recibe un Reply), el router no podrá obtener una dirección IP, y la interfaz podría permanecer inactiva.
Los SLARP Keepalives también deben seguir un secuenciamiento regular, ya que son esenciales para verificar el estado del enlace. Si los keepalives fallan o no se envían/reciben correctamente, el protocol status en show interfaces cambiaría a down.

En Unicast:
En las transmisiones unicast, el secuenciamiento asegura que los paquetes IP encapsulados en tramas HDLC lleguen de manera ordenada al destino. El secuenciamiento es importante especialmente en conexiones con mecanismos de control de flujo y corrección de errores. Si los paquetes unicast se reciben fuera de orden o se pierden, el rendimiento del enlace se verá afectado. Si hay problemas de secuenciamiento, estos pueden ser observados mediante el incremento de errores de transmisión en show interfaces, lo que indicaría una pérdida de paquetes o problemas en la recepcion.

Identificacion de Origen y Destino
En las conexiones seriales (HDLC o PPP), los routers conectados directamente, en este caso por interfaz serial, no necesitan direcciones físicas (como MAC) para identificar el origen o destino en la capa de enlace. Estas conexiones son exclusivas entre dos dispositivos, y el protocolo asume que cualquier trama enviada desde un extremo está destinada al otro. En Wireshark, los campos de origen y destino de la capa 2 (que normalmente contendrían direcciones MAC en una red Ethernet) no son aplicables, ya que la comunicación es implícita entre los dos dispositivos en el enlace serial.

5. Autenticacion PAP

La configuración de PAP (Password Authentication Protocol) en routers sigue una lógica de autenticación basada en el intercambio de nombres de usuario y contraseñas. En PAP, los routers se autentican mutuamente usando nombres de usuario y contraseñas. El router que está enviando los datos debe decir quién es (mediante un username) y presentar una contraseña para ser autenticado por el router receptor. Es por ello que primero se cambio la encapsulation de HDLC a PPP, luego se setearon los usernames y passwords en ambos routers (de forma opuesta entre ellos) con los siguientes comandos

```
En ambos routers encapsulation ppp
R0(config)#username R1 password cisco1
R0(config)#interface serial 0/1/0
R0(config-if)#ppp authentication pap
R0(config-if)#ppp pap sent-username R0 password cisco0
```

Esto significa que el R0 se configuro para recibir username R1 y password cisco1. A su vez tambien se establecio que dicho router envie su username (R0) y su password (cisco0) al otro router. En el R1 se hizo lo mismo pero inversamente, es decir que reciba R0 y password cisco 0, y que envie R1 y cisco1 al otro.

Luego algunos comandos adicionales utiles para comprobar el proceso de autenticacion y para ver las configuraciones seteadas fueron

```
En ambos routers encapsulation ppp
R0(config)#show running-config
R0(config)#debug ppp authentication
```

A continuacion se presenta la comprobacion de que el ping fue enviado satisfactoriamente.

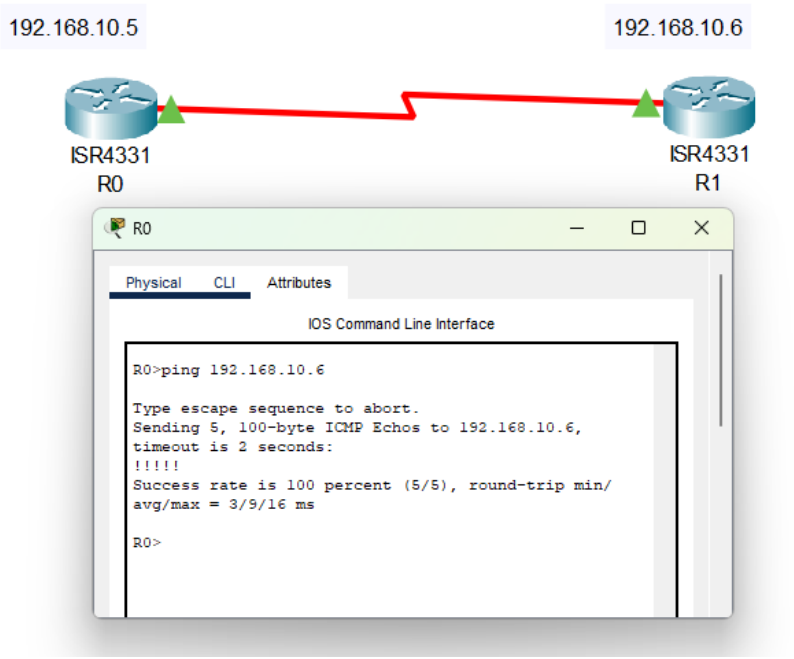

Figura 4: Ping exitoso con autenticacion PAP

https://github.com/Sandrosca/LaTeX