SEGURIDAD EN NETWORKING

Unidad 1

Seguridad para las redes

ESCUELA DE INGENIERÍA Y CONSTRUCCIÓN

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Luis Jaque Zúñiga

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Francisca Aránguiz Jiménez

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Implementan soluciones mediante redes privadas virtuales, considerando normativa vigente.

Fuente: Freepick (s/f).

Introducción

Durante esta segunda semana abordaremos conceptos relacionados con la implementación de soluciones de seguridad en enlaces WAN, mediante protocolos HDLC y PPP.

Así podrán:

- **¿Cómo Identificar protocolos y opciones de configuración de un enlace serial para un enrutamiento seguro, según estándares?**
- **¿Cómo aplicar técnicas de configuración de opciones básicas de protocolo HDLC-LCP?**
- **¿Cómo aplicar técnicas de configuración de opciones básicas de protocolo PPP más seguridad PAP?**
- **¿Cómo aplicar aplica técnicas de configuración de opciones básicas de protocolo PPP más seguridad CHAP?**

1. Conexiones punto a punto[1]

1.1. Puertos serie y paralelos

Un tipo común de conexiones WAN es la conexión punto a punto. Como se muestra en la figura 1, las conexiones punto a punto se utilizan para conectar redes LAN a redes WAN de un proveedor de servicios, así como para conectar segmentos LAN dentro de una red empresarial.

Una conexión punto a punto de LAN a WAN también se denomina "conexión serial" o "conexión de línea arrendada". Esto se debe a que las líneas se arriendan de una prestadora de servicios (generalmente, una compañía telefónica) y se las dedica para que las utilice la empresa que arrienda las líneas. Las empresas pagan una conexión continua entre dos sitios remotos, y la línea está continuamente activa y disponible. Las líneas arrendadas son un tipo de acceso WAN que se usa con frecuencia y, generalmente, el precio se basa en el ancho de banda requerido y en la distancia entre los dos puntos conectados.

Es importante comprender cómo funciona la comunicación serial punto a punto a través de una línea arrendada para tener un concepto general de cómo funcionan las WAN.

[1] Cisco Networking Academy. (2022). Conexión de redes. Capítulo 2: Conexiones punto a punto.

Las comunicaciones a través de una conexión serial son un método de transmisión de datos en el que los bits se transmiten en forma secuencial por un único canal. Esto equivale a una tubería con un ancho suficiente para que pase de a una pelota por vez. Pueden entrar varias pelotas en la tubería, pero de a una sola, y solo tienen un punto de salida (el otro extremo de la tubería). Los puertos serie son bidireccionales y a menudo se los denomina "puertos bidireccionales" o "puertos de comunicaciones".

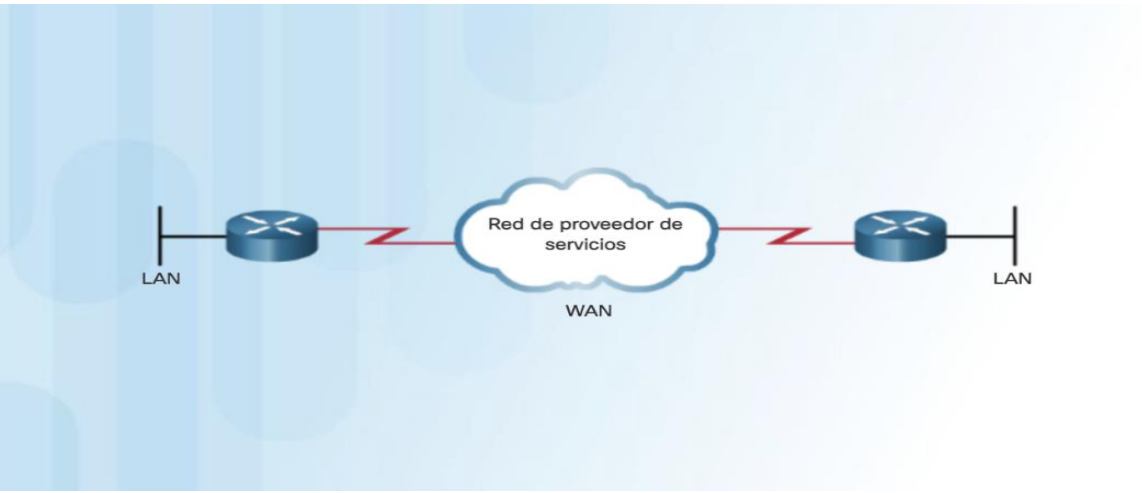


Figura 1: Conexión serial punto a punto.
Fuente: Cisco Networking Academy (2022)

Esto es distinto de las comunicaciones paralelas, en las que los bits se pueden transmitir simultáneamente por varios cables. En la siguiente figura se muestra una ilustración de la diferencia entre las conexiones seriales y las conexiones paralelas.

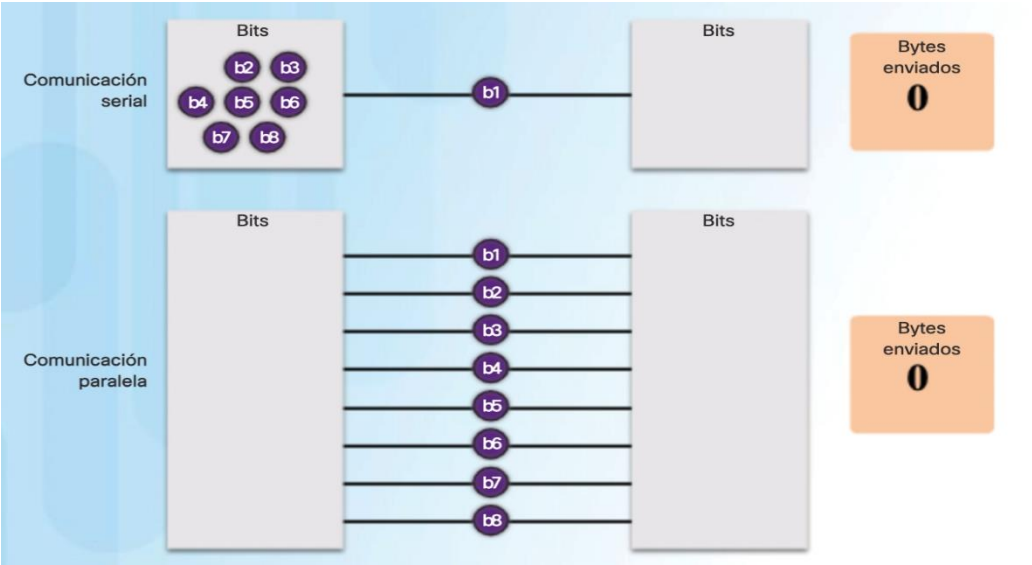


Figura 2: Comunicación serial y paralela.

Fuente: Cisco Networking Academy (2022)

En teoría, una conexión paralela transfiere datos ocho veces más rápido que una conexión serial. De acuerdo con esta teoría, una conexión paralela envía 1 byte (8 bits) en el tiempo en que una conexión serial envía un único bit. Sin embargo, las comunicaciones paralelas tienen problemas con el *crosstalk* a través de los cables, especialmente a medida que la longitud de estos aumenta. El sesgo de reloj también es un problema con las comunicaciones paralelas. El sesgo de reloj ocurre cuando los datos no llegan al mismo tiempo a través de los diferentes cables, lo que crea problemas de sincronización. Por último, muchas comunicaciones paralelas admiten solamente la comunicación unidireccional saliente, pero algunas admiten la comunicación semidúplex (comunicación bidireccional, solo en una dirección a la vez).

En una época, la mayoría de las computadoras incluían puertos serie y paralelos. Los puertos paralelos se utilizaban para conectar impresoras, computadoras y otros dispositivos que requerían un ancho de banda relativamente alto. Los puertos paralelos también se utilizaban entre los componentes internos. Para las comunicaciones externas, se utilizó

principalmente un bus serial para conectarse a las líneas telefónicas y los dispositivos que podrían estar a una distancia adicional de lo que una transferencia paralela podría permitir. Debido a que las comunicaciones seriales son menos complejas y requieren circuitos más simples, las comunicaciones seriales son mucho menos costosas de implementar. Las comunicaciones seriales usan menos hilos, cables más económicos y menos pines de los conectores.

En la mayoría de las computadoras, los puertos paralelos y los puertos serie RS-232 se reemplazaron por las interfaces de bus serial universal (USB), de mayor velocidad. Para las comunicaciones de larga distancia, muchas WAN también usan la transmisión serial.

1.2. Enlaces de comunicación punto a punto

Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una única ruta de comunicaciones WAN preestablecida. Esta ruta va desde las instalaciones del cliente, a través de la red del proveedor, a un destino remoto, como se muestra en la siguiente figura.

Un enlace punto a punto puede conectar dos sitios geográficamente distantes, como una oficina corporativa en Nueva York y una oficina regional en Londres. Para una línea punto a punto, la portadora dedica recursos específicos a una línea que arrienda el cliente (línea arrendada).

Nota: las conexiones punto a punto no se limitan a las conexiones por tierra. Existen cientos de miles de kilómetros de cables de fibra óptica submarinos que conectan países y continentes en todo el mundo. Una búsqueda en Internet de "mapa de cables submarinos de Internet" presenta varios mapas de cables de estas conexiones submarinas.

En general, los enlaces punto a punto son más costosos que los servicios compartidos. El costo de las soluciones de línea arrendada puede llegar a ser considerable cuando se utiliza para conectar varios sitios a través de distancias cada vez mayores. Sin embargo, hay ocasiones en las que los beneficios superan el costo de la línea arrendada. La capacidad dedicada elimina la latencia o fluctuación entre los terminales. La disponibilidad constante es fundamental para algunas aplicaciones, como VoIP o video sobre IP.

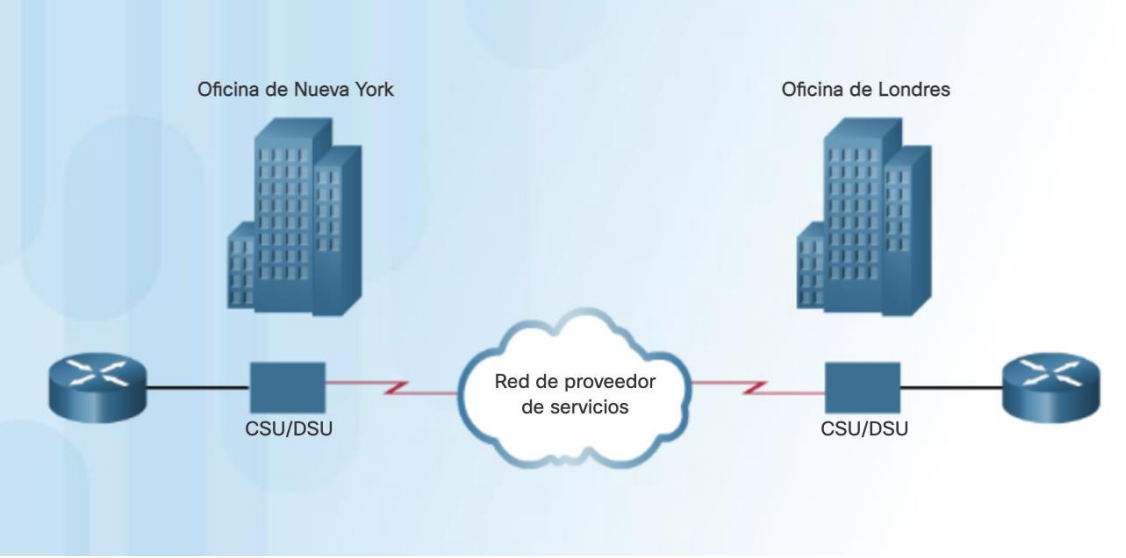


Figura 3: Enlaces de comunicación punto a punto.

Fuente: Cisco Networking Academy (2022).

1.3. Ancho de banda serial

El ancho de banda se refiere a la velocidad a la que se transfieren los datos a través del enlace de comunicación. La tecnología subyacente del proveedor de servicios dictará cuánto ancho de banda estará disponible. Existe una diferencia en los puntos de ancho de banda entre la especificación norteamericana (portadora T) y el sistema europeo (portadora E). Las redes ópticas también utilizan otra jerarquía de ancho de banda, que también

difiere entre América del Norte y Europa. En los EE. UU., la portadora óptica (OC) define los puntos de ancho de banda.

En América del Norte, el ancho de banda generalmente se expresa como un número de nivel de señal digital (DS0, DS1, etc.), el cual se refiere a la velocidad y el formato de la señal. La velocidad de línea más fundamental es 64 kb/s, o DS0, que es el ancho de banda requerido para una llamada telefónica digitalizada sin comprimir. Los anchos de banda de las conexiones seriales pueden aumentar cada vez más para satisfacer la necesidad de una transmisión más rápida. Por ejemplo, se pueden agrupar 24 DS0 para obtener una línea DS1 (también denominada "línea T1") con una velocidad de 1,544 Mb/s. Asimismo, se pueden agrupar 28 DS1 para obtener una línea DS3 (también denominada "línea T3") con una velocidad de 44,736 Mb/s. Hay líneas arrendadas disponibles de distintas capacidades y, por lo general, su precio depende del ancho de banda necesario y de la distancia entre los dos puntos conectados.

Las velocidades de transmisión de OC son un conjunto de especificaciones estandarizadas para la transmisión de señales digitales que se transportan por redes de fibra óptica SONET. La designación utiliza OC seguida de un número entero que representa la velocidad de transmisión básica de 51,84 Mb/s. Por ejemplo, OC-1 tiene una capacidad de transmisión de 51,84 Mb/s, mientras que un medio de transmisión OC-3 sería 51,84 Mb/s por tres, o 155,52 Mb/s.

En la siguiente figura, se muestran los tipos de línea más comunes y la capacidad de velocidad de bits asociada de cada uno.

Tipo de línea	Capacidad de la velocidad de transmisión
56	56 kb/s
64	64 kb/s
T1	1,544 Mb/s
E1	2,048 Mb/s
J1	1,544 Mb/s
E3	34,368 Mb/s
T3	44,736 Mb/s
OC-1	51,84 Mb/s
OC-3	155,52 Mb/s
OC-9	466,56 Mb/s
OC-12	622,08 Mb/s
OC-18	933,12 Mb/s
OC-24	1,244 Gb/s
OC-36	1,866 Gb/s
OC-48	2,488 Gb/s
OC-96	4,976 Gb/s
OC-192	9,954 Gb/s
OC-768	39,813 Gb/s

Figura 4: Velocidades de transmisión de portadora.

Fuente: Cisco Networking Academy (2022)

Nota: E1 (2,048 Mb/s) y E3 (34,368 Mb/s) son estándares europeos como T1 y T3, pero con anchos de banda y estructuras de trama diferentes.

1.4. Protocolos de encapsulación WAN

En cada conexión WAN, se encapsulan los datos en las tramas antes de cruzar el enlace WAN. Para asegurar que se utilice el protocolo correcto, se debe configurar el tipo de encapsulación de capa 2 correspondiente. La opción de protocolo depende de la tecnología WAN y el equipo de comunicación. En la figura 4, se muestran los protocolos WAN más comunes y dónde se utilizan. Las siguientes son descripciones breves de cada tipo de protocolo WAN:

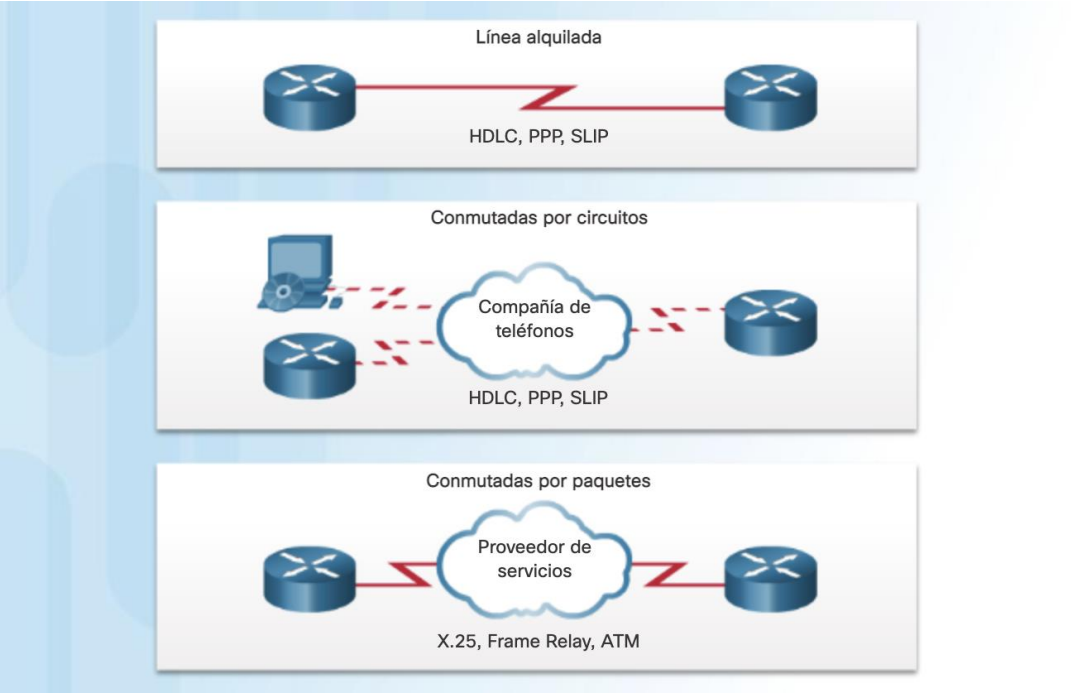


Figura 5: Protocolos de encapsulación WAN.
Fuente: Cisco Networking Academy (2022).

- **HDLC**: es el tipo de encapsulación predeterminado en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuitos cuando el enlace utiliza dos dispositivos de Cisco. Ahora, HDLC es la base para PPP síncrono que usan muchos servidores para conectarse a una WAN, generalmente Internet.

- **PPP:** proporciona conexiones de *router* a *router* y de host a red a través de circuitos síncronos y asíncronos. PPP funciona con varios protocolos de capa de red, como IPv4 e IPv6. PPP se basa en el protocolo de encapsulamiento HDLC, pero también tiene mecanismos de seguridad incorporados como PAP y CHAP.

- **Protocolo de Internet de línea serial (SLIP):** es un protocolo estándar para conexiones seriales punto a punto mediante TCP/IP. PPP reemplazó ampliamente al protocolo SLIP.

- **Procedimiento de acceso al enlace balanceado (LAPB) X.25:** es un estándar del UIT-T que define cómo se mantienen las conexiones entre un DTE y un DCE para el acceso remoto a terminales y las comunicaciones por computadora en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un antecesor de *Frame Relay*.

- ***Frame Relay:*** es un protocolo de capa de enlace de datos conmutado y un estándar del sector que maneja varios circuitos virtuales. *Frame Relay* es un protocolo de última generación posterior a X.25. *Frame Relay* elimina algunos de los procesos prolongados (como la corrección de errores y el control del flujo) empleados en X.25.

- **ATM:** es el estándar internacional de retransmisión de celdas en el que los dispositivos envían varios tipos de servicios (como voz, video o datos) en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento se lleve a cabo en el hardware, lo que disminuye las demoras en el tránsito. ATM aprovecha los medios de transmisión de alta velocidad, como E3, SONET y T3.

1.5. Encapsulación de HDLC

HDLC es un protocolo sincrónico de capa de enlace de datos orientado a *bits* desarrollado por la Organización Internacional para la Estandarización (ISO). El estándar actual para HDLC es ISO 13239. HDLC se desarrolló a partir del estándar de control de enlace de datos síncronos (SDLC) propuesto en la década de los setenta. HDLC proporciona servicio orientado a la conexión y sin conexión.

HDLC utiliza la transmisión serial síncrona, que proporciona una comunicación sin errores entre dos puntos. HDLC define una estructura de trama de capa 2 que permite el control del flujo y de errores mediante el uso de acuses de recibo. Cada trama presenta el mismo formato ya sea una trama de datos o una trama de control.

Cuando las tramas se transmiten por enlaces síncronos o asíncronos, esos enlaces no tienen ningún mecanismo para marcar ni el principio ni el fin de las tramas. Por este motivo, HDLC utiliza un delimitador de trama, o indicador, para marcar el principio y el fin de cada trama.

Cisco desarrolló una extensión del protocolo HDLC para resolver la incapacidad de proporcionar compatibilidad multiprotocolo. Si bien HDLC de Cisco (también conocido como cHDLC) es un protocolo exclusivo, Cisco permitió que muchos otros proveedores de equipos de red lo implementen. Las tramas HDLC de Cisco contienen un campo para identificar el protocolo de red que se encapsula. En la figura 5, se compara el estándar HDLC con HDLC de Cisco.

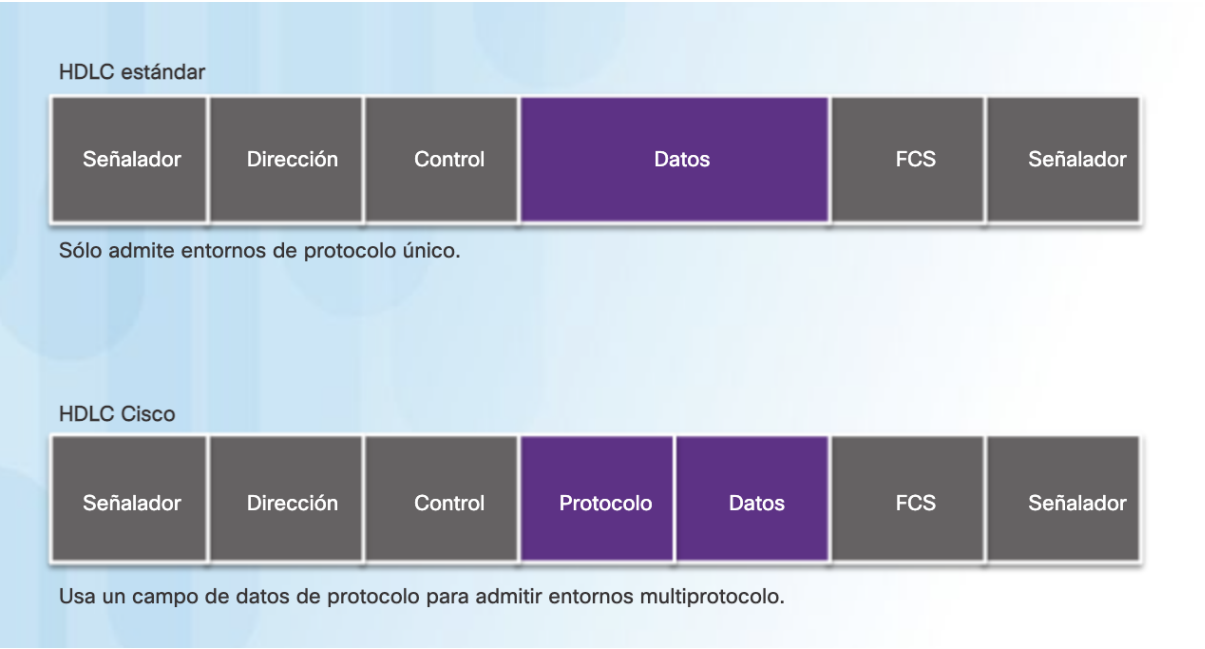


Figura 6: Formato de trama estándar y HDLC Cisco.

Fuente: Cisco Networking Academy (2022).

1.5.1. Configuración del encapsulamiento de HDLC

HDLC de Cisco es el método de encapsulación predeterminado que usan los dispositivos de Cisco en las líneas seriales síncronas.

Utilice HDLC de Cisco como protocolo punto a punto en las líneas arrendadas entre dos dispositivos de Cisco. Si conecta dispositivos que no son de Cisco, utilice PPP síncrono.

Si se modificó el método de encapsulación predeterminado, utilice el comando *encapsulation hdlc en* el modo EXEC privilegiado para volver a habilitar HDLC.

Como se muestra en la siguiente figura, se deben seguir dos pasos para volver a habilitar la encapsulación HDLC:

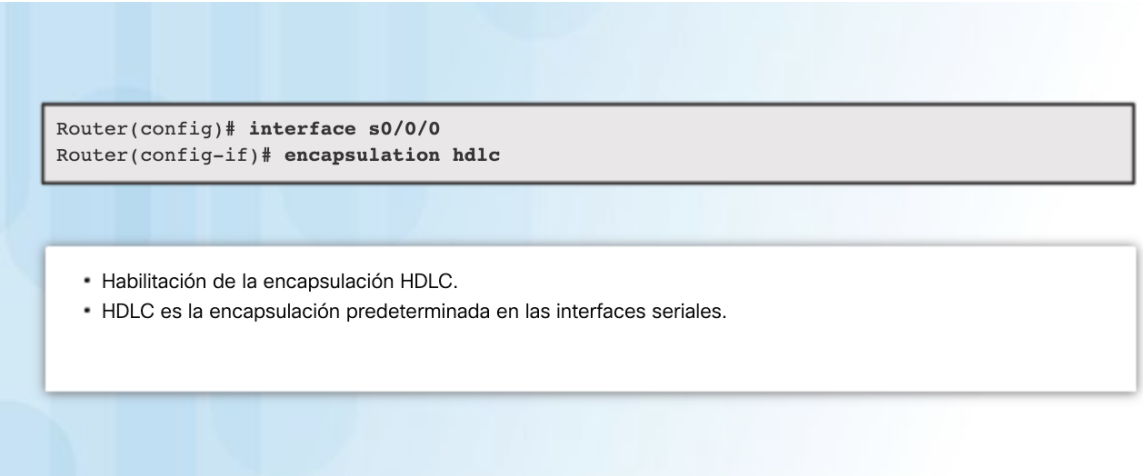


Figura 7: Configuración de encapsulamiento HDLC.

Fuente: Cisco Networking Academy (2022)

- **Paso 1.** Ingrese al modo de configuración de interfaz de la interfaz serial.
- **Paso 2.** Introduzca el comando ***encapsulation hdlc*** para especificar el protocolo de encapsulación en la interfaz.

1.5.2. Resolución de problemas de una interfaz serial

El resultado del comando *show interfaces* serial muestra información específica de las interfaces seriales. Agregue el número de interfaz específico que desea investigar, por ejemplo, *show interface serial 0/0/0*. Cuando se configura HDLC, debe figurar "*encapsulation HDLC*" en la salida, como se resalta en la siguiente figura. "*Serial 0/0/0 is up, line protocol is up*" indica que la línea está activa y en funcionamiento; "*encapsulation HDLC*" indica que está habilitado el encapsulamiento serial predeterminado (HDLC).

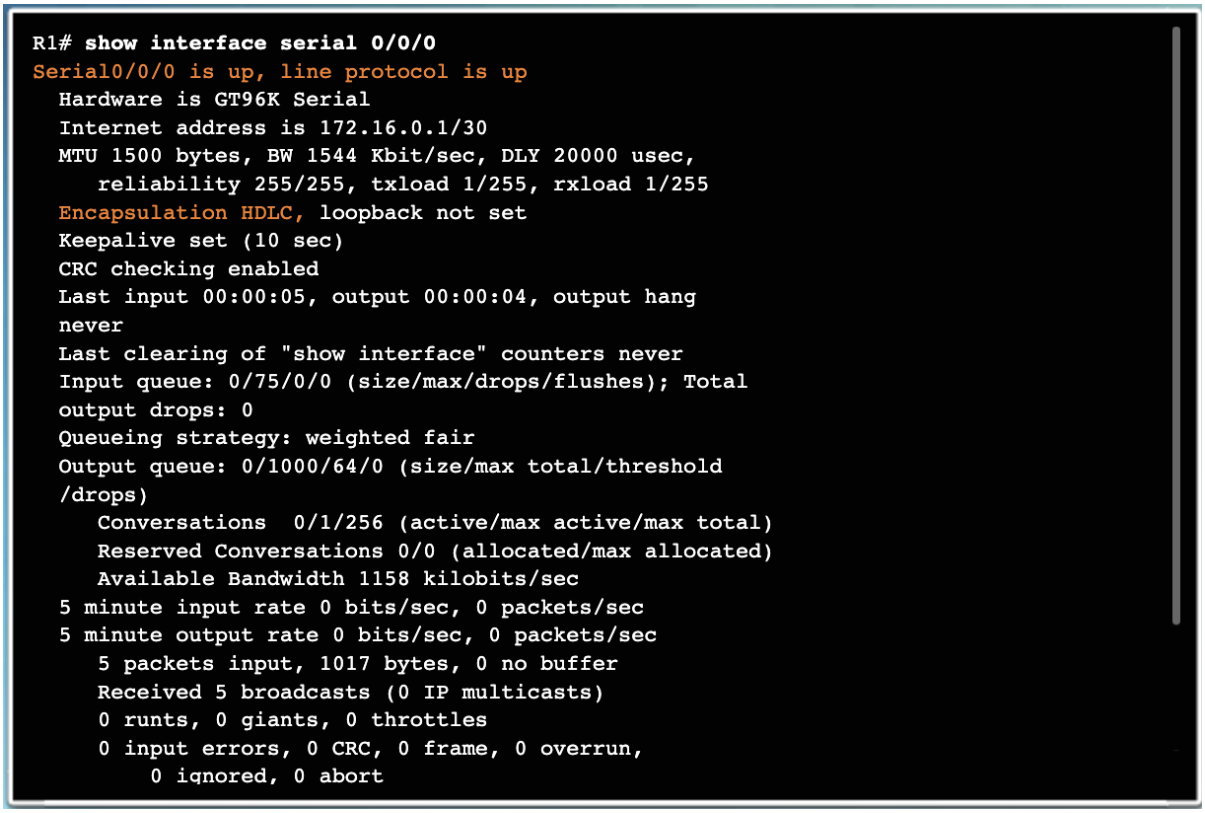


Figura 8: Resolución de problemas de una interfaz serial - 1.

Fuente: Cisco Networking Academy (2022)

El comando ***show interfaces serial*** devuelve uno de seis estados posibles:

- Serial x *is up, line protocol is up*.
- Serial x *is down, line protocol is down*.
- Serial x is *up, line protocol is down*.
- Serial x *is up, line protocol is up (looped)*.
- Serial x *is up, line protocol is down (disabled)*.
- Serial x *is administratively down, line protocol is down*.

De los seis estados posibles, cinco son estados problemáticos. En la figura 8, se muestran los cinco estados problemáticos, los problemas asociados a cada estado y la forma de resolver el problema.

Línea de estado	Condición posible	Problema / Solución
Serial x is up, line protocol is up	Esta es la condición de línea de estado adecuada.	No requiere ninguna acción.
Serial x is down, line protocol is down (DTE mode)	El router no detecta ninguna señal de detección de portadora (CD, carrier detect), lo que significa que la CD no está activa. Se produjo un problema con el proveedor de servicios de portadora WAN, lo que significa que la línea está inactiva o no está conectada a la CSU/DSU. El cableado presenta una falla o es incorrecto.	1. Verifique los LED en la CSU/DSU para ver si la CD está activa, o inserte una caja de interconexión en la línea a fin de verificar la señal de CD. 2. Verifique que se utilice el cable y la interfaz correspondientes en la documentación de instalación del hardware. 3. Inserte una caja de interconexión y revise todos los conectores de control. 4. Comuníquese con el servicio de línea arrendada o de otro proveedor para ver si existe algún problema. 5. Cambie las piezas que presenten fallas. 6. Si se sospecha que el hardware del router presenta una falla, cambie la línea serial a otro puerto. Si la conexión se activa, la interfaz conectada anteriormente tiene un problema.

Figura 9: Resolución de problemas de una interfaz serial - 2.

Fuente: Cisco Networking Academy (2022).

El comando *show controllers* es otra herramienta de diagnóstico importante para la resolución de problemas de líneas seriales, como se muestra en la figura 9. El resultado indica el estado de los canales de la interfaz y si hay un cable conectado a la interfaz o no. En la ilustración, la interfaz serial 0/0/0 tiene un cable DCE V.35 conectado. La sintaxis de los comandos varía, según la plataforma. Los *routers* Cisco serie 7000 utilizan una tarjeta controladora cBus para conectar enlaces seriales. Con estos *routers*, utilice el *comando show controllers cbus*.

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x0000064A,
CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000,
CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x0DBD2DB0, CTDP=0x0DBD31D0, FTDB=0x0DBD31D0
Main Routing Register=0x0003FE38 BRG Conf
Register=0x0005023F
Rx Clk Routing Register=0x76543818 Tx Clk
Routing Register=0x76543910
GPP Registers:
Conf=0x430002  , Io=0x46C050  , Data=0x7F4BBFAD,
Level=0x80004
Conf0=0x430002  , Io0=0x46C050  , Data0=0x7F4BBFAD,
Level0=0x80004
0 input aborts on receiving flag sequence
```

Figura 10: Resolución de problemas de una interfaz serial - 3.

Fuente: Cisco Networking Academy (2022).

Si el resultado de la interfaz eléctrica aparece como "*UNKNOWN*" en lugar de "V.35", "EIA/TIA-449" o algún otro tipo de interfaz eléctrica, es probable que el problema sea un cable mal conectado. También es posible que exista un problema con el cableado interno de la tarjeta. Si la interfaz eléctrica es desconocida, el resultado correspondiente del comando show interfaces serial muestra que la interfaz y el protocolo de línea están inactivos.

2. Introducción a PPP

Recuerde que HDLC es el método de encapsulamiento serial predeterminado al conectar dos *routers* Cisco. Con un campo agregado de tipo de protocolo, la versión de HDLC de Cisco es exclusiva. Por eso, HDLC de Cisco solo puede funcionar con otros dispositivos de Cisco. Sin embargo, cuando existe la necesidad de conectarse a un *router* que no es de Cisco, se debe usar la encapsulación PPP, como se muestra en la siguiente figura.

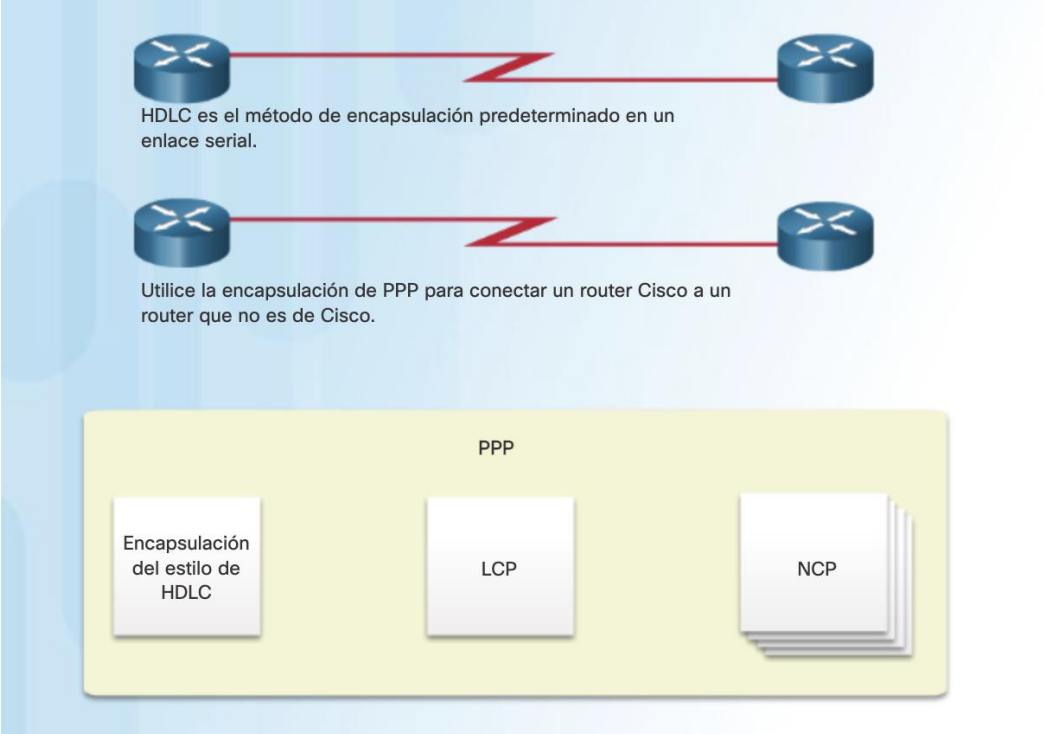


Figura 11: ¿Qué es encapsulación PPP?

Fuente: Cisco Networking Academy (2022).

La encapsulación PPP se diseñó cuidadosamente para conservar la compatibilidad con el *hardware* más usado que la admite. PPP encapsula tramas de datos para transmitirlas a través de enlaces físicos de capa 2. PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.

PPP contiene tres componentes principales:

- Entramado del estilo de HDLC para transportar paquetes multiprotocolo a través de enlaces punto a punto.
- Protocolo de control de enlace (LCP) extensible para establecer, configurar y probar la conexión de enlace de datos.
- Familia de protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP permite el uso simultáneo de varios protocolos de capa de red. Los NCP más comunes son el protocolo de control IPv4 y el protocolo de control IPv6.

Nota: Otros NCP incluyen el protocolo de control *AppleTalk*, el protocolo de control Novell IPX, el protocolo de control de Cisco *Systems*, el protocolo de control SNA y el protocolo de control de compresión.

2.1. Ventajas de PPP

PPP surgió originalmente como protocolo de encapsulación para transportar tráfico IPv4 a través de enlaces punto a punto. PPP proporciona un método estándar para transportar paquetes multiprotocolo a través de enlaces punto a punto.

El uso de PPP presenta muchas ventajas, incluido el hecho de que no es exclusivo. PPP incluye muchas funciones que no están disponibles en HDLC:

- La función de administración de calidad del enlace (LQM) monitorea la calidad del enlace. La LQM se puede configurar con el comando **PPP *quality percentage***. Si el porcentaje de error está por debajo del umbral configurado, el enlace se desactiva y los paquetes se descartan o se envían por otra ruta.

- PPP admite la autenticación PAP y CHAP.

Figura 12: Ventajas de PPP.

Fuente: Cisco Networking Academy (2022).

2.2. Arquitectura de capas PPP

Una arquitectura en capas es un modelo, un diseño, o un plano lógico que ayuda en la comunicación de las capas que se interconectan. En la figura 12, se compara la arquitectura en capas de PPP con el modelo de interconexión de sistema abierto (OSI). PPP y OSI comparten la misma capa física, pero PPP distribuye las funciones de LCP y NCP de manera diferente.

En la capa física, puede configurar PPP en un rango de interfaces. El único requisito absoluto impuesto por PPP es un circuito de dúplex completo, ya sea dedicado o conmutado, que pueda operar en modo serial de bits asíncrono o síncrono. Los estándares de la capa física son transparentes para las tramas de la capa de enlaces PPP. PPP no impone restricciones con respecto a la velocidad de transmisión. La mayoría del trabajo realizado por PPP sucede en las capas de red y enlace de datos, por LCP y NCP.

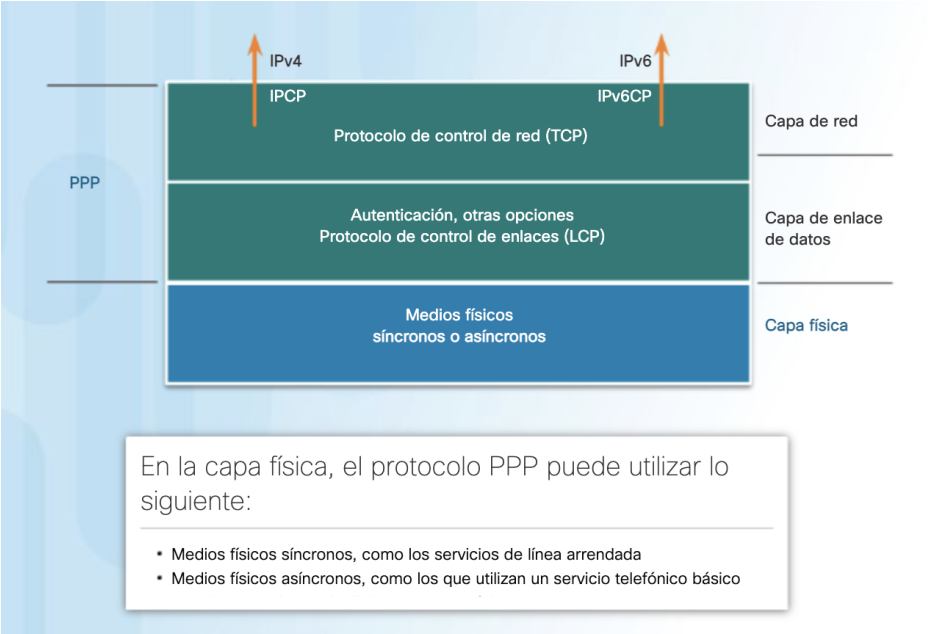


Figura 13: Arquitectura en capas PPP: capa física.

Fuente: Cisco Networking Academy (2022).

2.3. PPP: protocolo de control de enlace (LCP)

LCP funciona dentro de la capa de enlace de datos y cumple una función en el establecimiento, la configuración y la prueba de la conexión de enlace de datos. LCP establece el enlace de punto a punto. LCP también negocia y configura las opciones de control del enlace de datos de WAN, administradas por los NCP.

LCP proporciona la configuración automática de las interfaces en cada extremo:

- Manejo de distintos límites en el tamaño de paquete.
- Detección de errores comunes de configuración.
- Finalización del enlace.
- Determinación de cuándo un enlace funciona correctamente o cuándo falla.

Una vez establecido el enlace, PPP también usa LCP para acordar automáticamente los formatos de encapsulamiento, como la autenticación, la compresión y la detección de errores.

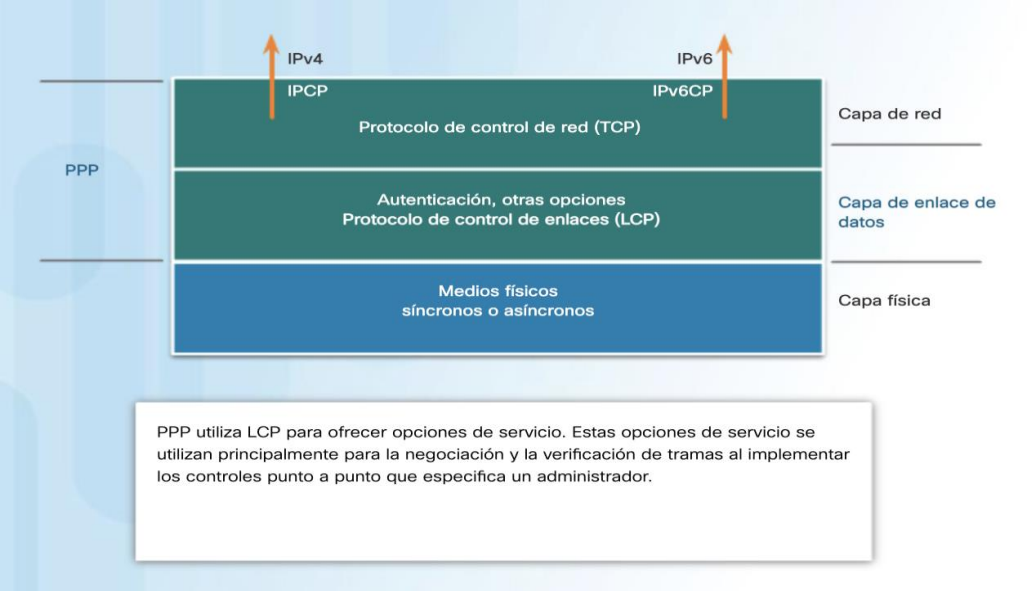


Figura 14: Arquitectura en capas PPP: capa LCP.

Fuente: Cisco Networking Academy (2022).

2.4. PPP: protocolo de control de red (NCP)

PPP permite que varios protocolos de capa de red funcionen en el mismo enlace de comunicación. Para cada protocolo de capa de red que se usa, PPP utiliza un NCP separado, como se muestra en la figura 14. Por ejemplo, IPv4 utiliza el protocolo de control IP (IPCP) e IPv6 utiliza el protocolo de control IPv6 (IPv6CP).

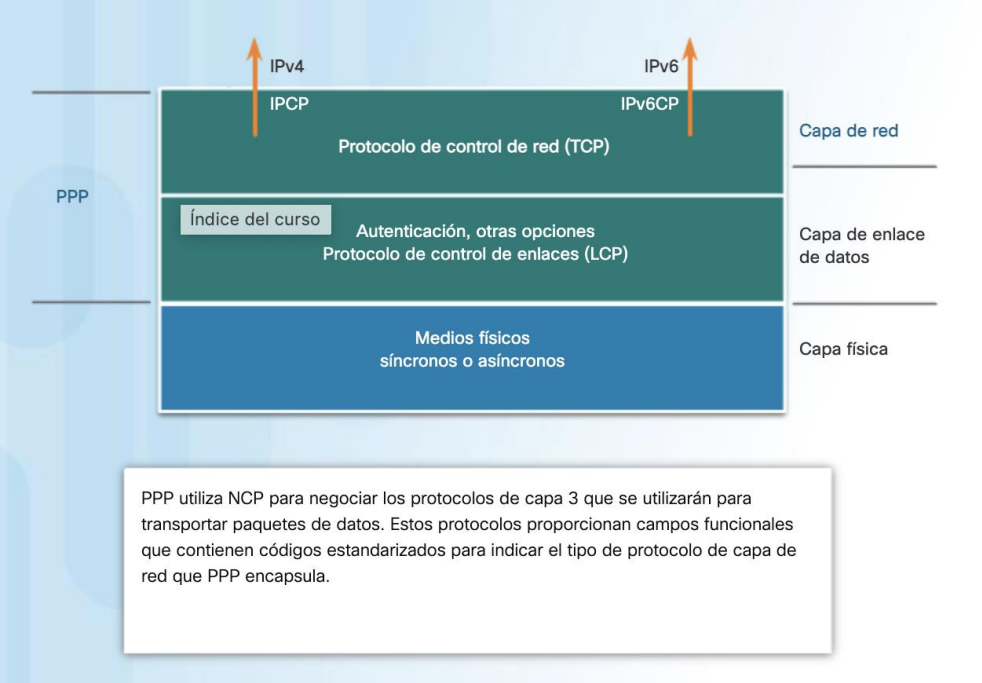


Figura 15: Arquitectura PPP: capa de red.

Fuente: Cisco Networking Academy (2022).

Los protocolos NCP incluyen campos funcionales que contienen códigos estandarizados para indicar el protocolo de capa de red que PPP encapsula. En la figura 15, se indican los números de los campos de protocolo PPP. Cada NCP administra las necesidades específicas requeridas por sus respectivos protocolos de capa de red. Los distintos componentes NCP encapsulan y negocian las opciones para varios protocolos de capa de red.

Valor (en hex)	Nombre del protocolo
8021	Protocolo de control del protocolo de Internet (IPv4)
8057	Protocolo de control del protocolo de Internet versión 6 (IPv6)
8023	Protocolo de control de capa de red OSI
8029	Protocolo de control Appletalk
802b	Protocolo de control Novell IPX
c021	Protocolo de control de enlace
c023	Protocolo de autenticación de contraseña
c223	Protocolo de autenticación de intercambio de señales

Figura 16: Números de campo de protocolo.

Fuente: Cisco Networking Academy (2022).

2.5. Estructura de la trama PPP

Las tramas PPP constan de seis campos. Las siguientes descripciones resumen los campos de las tramas PPP, que se muestran en la siguiente figura:

Figura 17: Campos de trama PPP.

Fuente: Cisco Networking Academy (2022).

- **Señalador:** un único byte que indica el inicio y el final de una trama. El campo indicador está formado por la secuencia binaria 01111110.

- **Dirección:** un único byte que contiene la secuencia binaria 11111111, la dirección de difusión estándar. PPP no asigna direcciones a estaciones individuales.

- **Control:** un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial.

- **Protocolo:** dos bytes que identifican el protocolo encapsulado en el campo de información de la trama. El campo Protocolo de 2 bytes identifica al protocolo del contenido PPP.

- **Datos:** cero o más bytes que contienen el datagrama para el protocolo especificado en el campo Protocolo.

- **Secuencia de verificación de trama (FCS):** normalmente de 16 bits (2 bytes). Si el cálculo de la FCS que realiza el receptor no coincide con la FCS de la trama PPP, esta se descarta sin aviso.

Los protocolos LCP pueden negociar modificaciones a la estructura de la trama PPP estándar. No obstante, las tramas modificadas siempre se distinguen de las tramas estándar.

2.6. Establecimiento de una sesión PPP

Hay tres fases de establecimiento de una sesión PPP, como se muestra en la siguiente figura:

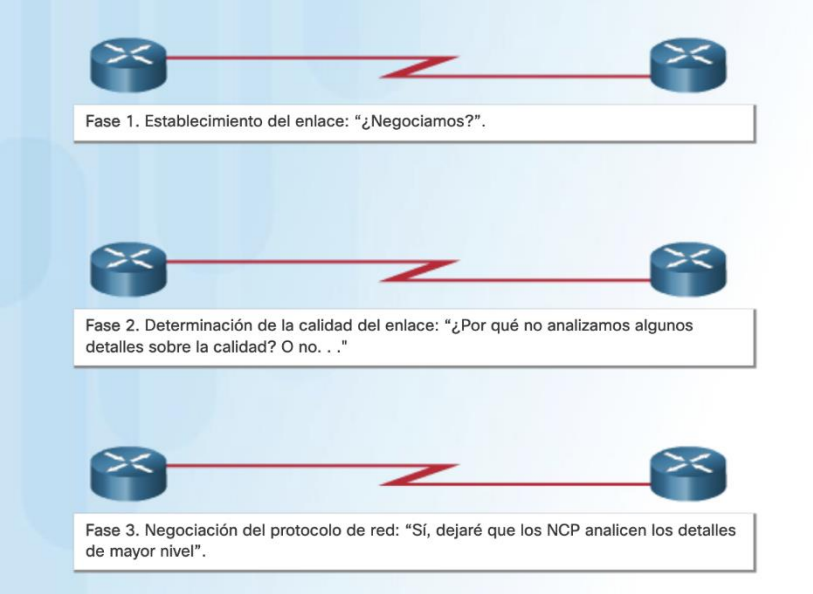


Figura 18: Establecimiento de una sesión PPP.

Fuente: Cisco Networking Academy (2022).

- **Fase 1, establecimiento del enlace y negociación de la configuración:** antes de que PPP intercambie cualquier datagrama de capa de red (como IP) LCP primero debe abrir la conexión y negociar las opciones de configuración. Esta fase se completa cuando el *router* receptor envía una trama de acuse de recibo de configuración de vuelta al *router* que inicia la conexión.

- **Fase 2, determinación de la calidad del enlace (optativa):** LCP prueba el enlace para determinar si la calidad de este es suficiente para activar protocolos de capa de red. LCP puede retrasar la transmisión de la

información del protocolo de capa de red hasta que se complete esta fase.

- **Fase 3, negociación de la configuración del protocolo de capa de red:** una vez que LCP terminó la fase de determinación de la calidad del enlace, el protocolo NCP correspondiente puede configurar por separado los protocolos de capa de red, activarlos y desactivarlos en cualquier momento. Si LCP cierra el enlace, informa a los protocolos de capa de red para que puedan tomar las medidas adecuadas.

El enlace permanece configurado para las comunicaciones hasta que las tramas LCP o NCP explícitas cierren el enlace, o hasta que ocurra algún evento externo, por ejemplo, que caduque un temporizador de inactividad o que intervenga un administrador.

LCP puede finalizar el enlace en cualquier momento. Por lo general, esto se realiza cuando uno de los *routers* solicita la finalización, pero puede suceder debido a un evento físico, como la pérdida de una portadora o el vencimiento de un temporizador de período inactivo.

2.7. Opciones de configuración del PPP

PPP se puede configurar para admitir diversas funciones opcionales, como se muestra en la siguiente figura. Existen tres funciones opcionales:

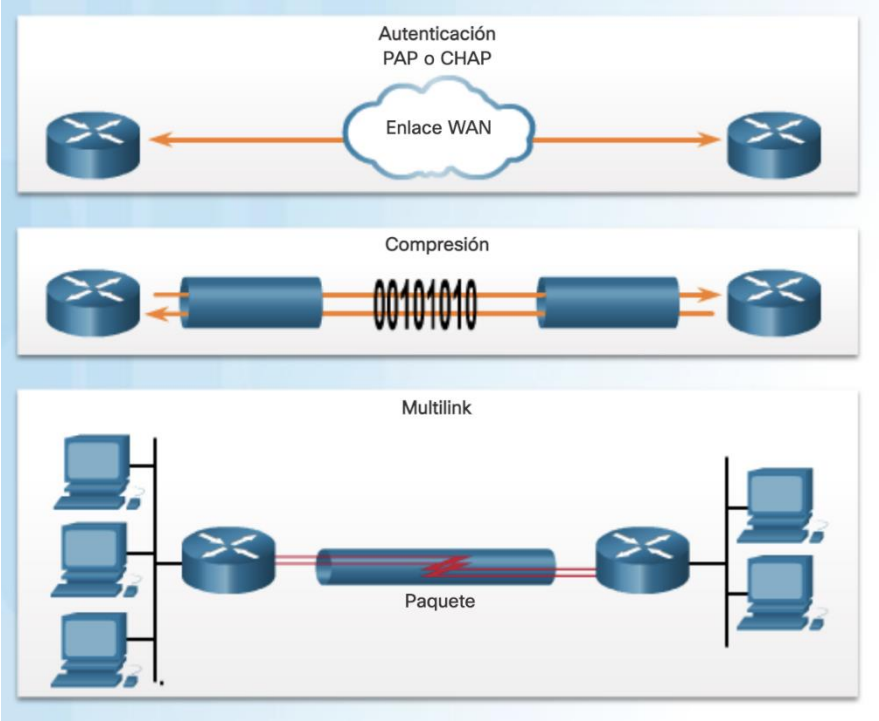


Figura 19: Opciones de configuración PPP.
Fuente: Cisco Networking Academy (2022).

- Autenticación mediante PAP o CHAP.
- Compresión mediante Stacker o Predictor.
- Multienlace que combina dos o más canales para aumentar el ancho de banda WAN.

PPP puede incluir varias opciones de LCP:

- **Autenticación:** los *routers peers* intercambian mensajes de autenticación. Las dos opciones de autenticación son: el protocolo de autenticación de contraseña *(PAP, Password Authentication Protocol*) y el protocolo de autenticación de intercambio de señales (*CHAP, Challenge Handshake Authentication Protocol*).

- **Compresión:** aumenta el rendimiento eficaz en las conexiones PPP, pues reduce la cantidad de bits que deben desplazarse por el enlace. El protocolo descomprime la trama al llegar a su destino. Dos protocolos de compresión disponibles en los *routers Cisco son Stacker y Predictor*.

- **Detección de errores:** identifica fallas, las opciones de calidad y número mágico contribuyen a asegurar el establecimiento de un enlace de datos confiable y sin bucles. El campo de número mágico ayuda a detectar enlaces que se encuentran en una condición de *loop back*. Hasta que no se negocie correctamente la opción de configuración de número mágico, este se debe transmitir como cero. Los números mágicos se generan de forma aleatoria en cada extremo de la conexión.

- **Devolución de llamada PPP:** la devolución de llamada PPP se usa para mejorar la seguridad. Con esta opción de LCP, un *router* Cisco puede funcionar como cliente o servidor de devolución de llamada. El cliente realiza la llamada inicial, solicita que el servidor le devuelva la llamada y termina la comunicación inicial. El *router* de devolución de llamada responde la llamada inicial y se comunica con el cliente sobre la base de sus instrucciones de configuración.

- **Multienlace:** esta alternativa proporciona balanceo de carga a través de las interfaces del *router* que PPP utiliza. El protocolo PPP multienlace, también conocido como MP, MPPP, MLP o multienlace, proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos a la vez que proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

Cuando se configuran las opciones, se inserta el valor de campo correspondiente en el campo de opción de LCP.

Nombre de la opción	Tipo de opción	Longitud de la opción	Descripción
Protocolo de autenticación	3	5 o 6	Este campo indica el protocolo de autenticación, ya sea el PAP o el CHAP.
Compresión de protocolo	7	2	Un señalador que indica que la ID del protocolo PPP se comprimirá a un solo octeto cuando la ID del protocolo de 2 bytes se encuentre en el rango de 0x00-00 a 0x00-FF.
Compresión de campos de dirección y control	8	2	Un señalador que indica que el campo Dirección de PPP (siempre establecido en 0xFF) y el campo Control de PPP (siempre establecido en 0x03) se eliminarán del encabezado PPP.
Número mágico (detección de errores)	5	6	Es un número elegido de manera aleatoria para distinguir un par y detectar las líneas de loopback.
Devolución de llamada	13 o 0x0D	3	Un indicador de 1 octeto que muestra cómo se determinan las devoluciones de llamadas.

Figura 20: Código de campos de opciones configurables.

Fuente: Cisco Networking Academy (2022).

2.8. Comando de configuración básica de PPP

Para establecer PPP como el método de encapsulación que usa una interfaz serial, utilice el comando de configuración de interfaz *encapsulation* PPP. El comando no tiene ningún argumento. Recuerde que, si no se configura PPP en un router Cisco, la encapsulación predeterminada para las interfaces seriales es HDLC.

En la siguiente figura, se muestra que los *routers* R1 y R2 se configuraron con una dirección IPv4 y una dirección IPv6 en las interfaces seriales. PPP es una encapsulación de capa 2 que admite varios protocolos de capa 3, incluidos IPv4 e IPv6.

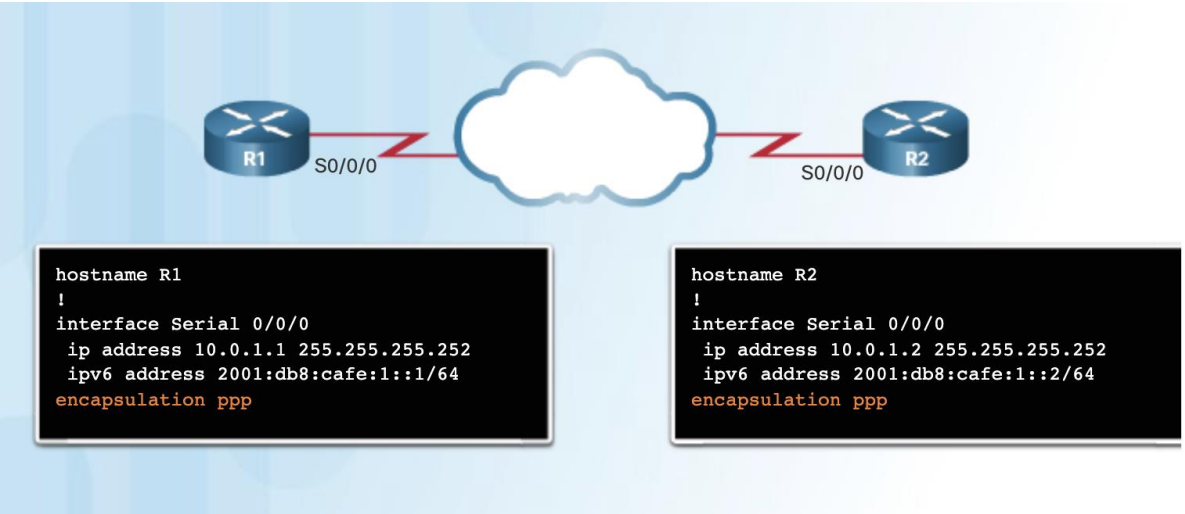


Figura 21: Config1ración básica de PPP.

Fuente: Cisco Networking Academy (2022).

2.9. Comandos de compresión de PPP

La compresión de software de punto a punto en las interfaces seriales se puede configurar después de que se habilita la encapsulación PPP. Dado que esta opción invoca un proceso de compresión de software, puede afectar el rendimiento del sistema. Si el tráfico ya consta de archivos comprimidos, como .zip, .tar, o .mpeg, no utilice esta opción. En la siguiente figura, se muestra la sintaxis del comando ***compress***.

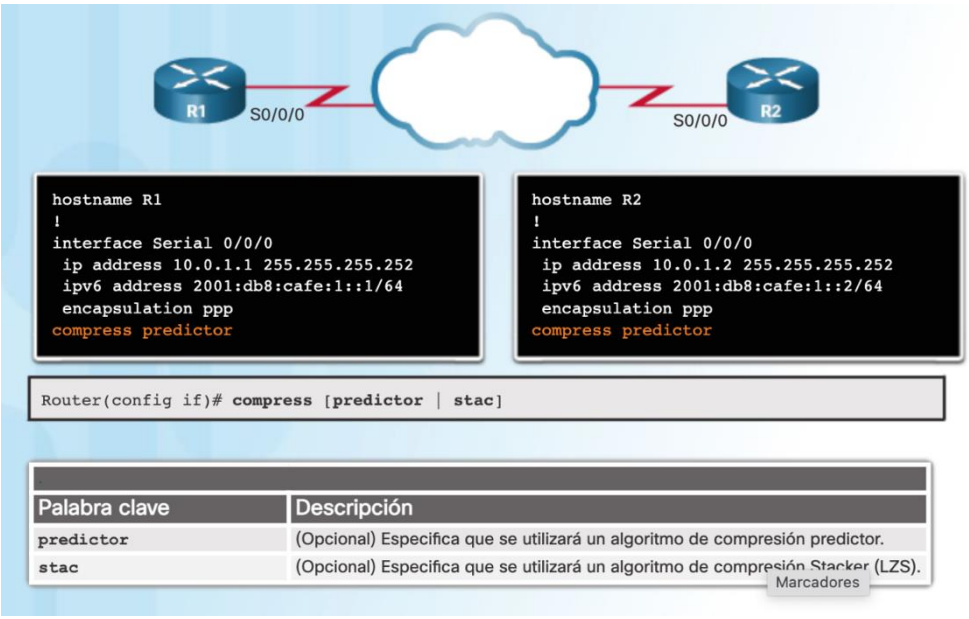


Figura 22: Compresión de PPP.

Fuente: Cisco Networking Academy (2022).

2.10. Comando de control de calidad del enlace PPP

LCP proporciona una etapa de determinación de la calidad del enlace. En esta fase, LCP prueba el enlace para determinar si la calidad de este es suficiente para usar protocolos de capa 3.

El comando ***PPP quality*** porcentaje asegura que el enlace cumpla con el requisito de calidad establecido; de lo contrario, el enlace queda inactivo.

Los porcentajes se calculan para las direcciones entrantes y salientes. La calidad de la salida se calcula comparando la cantidad total de paquetes y bytes enviados con la cantidad total de paquetes y bytes que recibe el nodo de destino. La calidad de entrada se calcula comparando la cantidad total de paquetes y bytes recibidos con la cantidad total de paquetes y bytes que envía el nodo de destino.

Si no se mantienen el porcentaje de la calidad del enlace y el umbral configurado, el enlace se considera de baja calidad y se desactiva. LQM implementa una demora de modo que el enlace no rebote de un lado a otro.

La configuración **PPP *quality* 80**, que se muestra en la figura, establece una calidad mínima del 80%.

Utilice el verificador de sintaxis de la siguiente figura para configurar la encapsulación, la compresión y LQM de PPP en la interfaz Serial 0/0/1 del *router* R1.

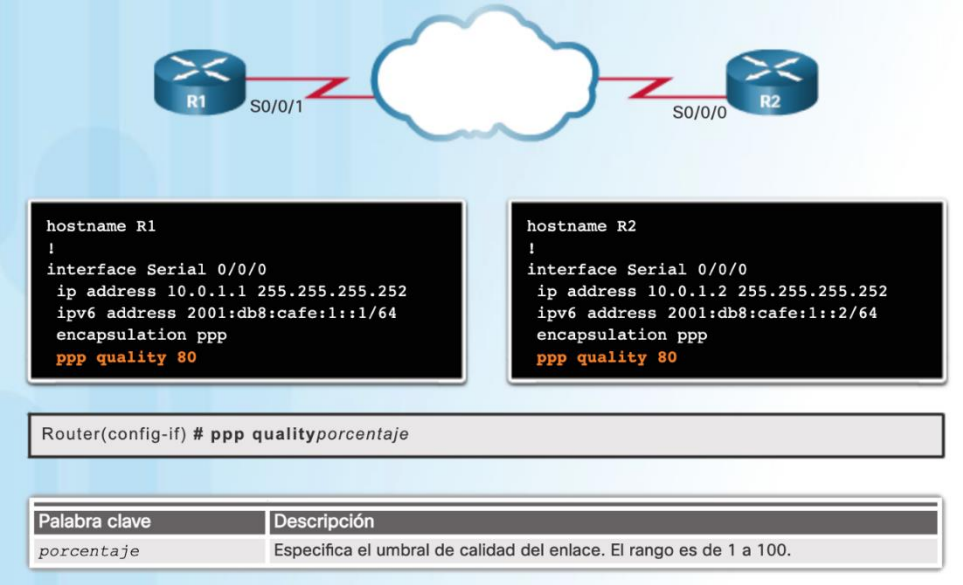


Figura 23: Control de calidad de enlace PPP.

Fuente: Cisco Networking Academy (2022).

2.11. Comandos de PPP multienlace

El protocolo PPP multienlace (también conocido como MP, MPPP, MLP o multienlace) proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos. Además, el protocolo PPP multienlace proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

MPPP permite fragmentar los paquetes y enviarlos simultáneamente a la misma dirección remota a través de varios enlaces punto a punto. Todos los enlaces físicos se activan en respuesta a un umbral de carga definido por el usuario. MPPP puede medir la carga solo en el tráfico entrante o solo en el tráfico saliente, pero no la carga combinada del tráfico entrante y saliente.

La configuración de MPPP requiere dos pasos, como se muestra en la siguiente figura.

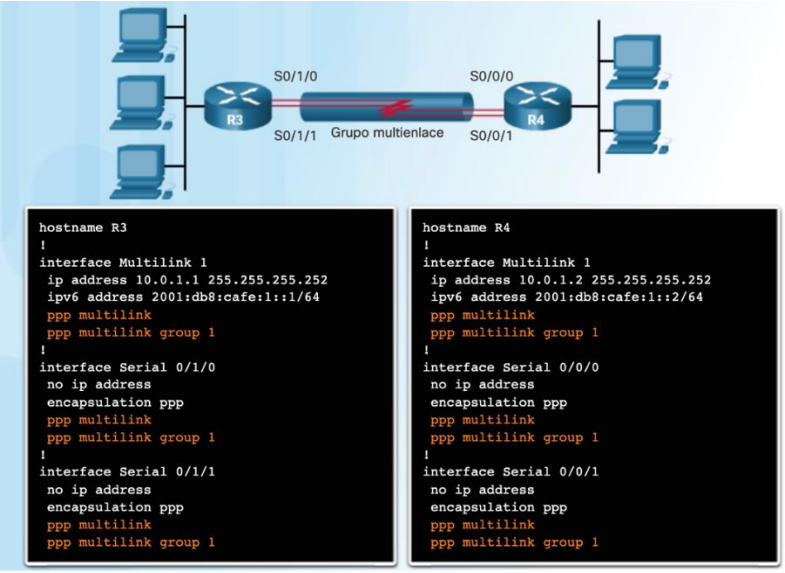


Figura 24: Protocolo PPP multienlace.

Fuente: Cisco Networking Academy (2022).

Paso 1. Cree un grupo multienlace.

- El comando *interface multilink* número crea la interfaz multienlace.
- En el modo de configuración de interfaz, se asigna una dirección IP a la interfaz de multienlace. En este ejemplo, se configuran direcciones IPv4 e IPv6 en los routers R3 y R4.
- La interfaz está habilitada para el protocolo PPP multienlace.
- Se asigna un número de grupo multienlace a la interfaz.

Paso 2. Asigne las interfaces al grupo multienlace.

Cada interfaz que forma parte del grupo multienlace tiene las siguientes características:

- Está habilitada para la encapsulación PPP.
- Está habilitada para el protocolo PPP multienlace.
- Está vinculada al paquete multienlace mediante el número de grupo multienlace configurado en el paso 1.

Para deshabilitar el multienlace PPP, use el comando no ppp multilink en cada una de las interfaces en paquete. Por ejemplo:

- R3(config)# interface s0/0/0.
- R3(config-if)# no ppp multilink.
- R3(config-if)# interface s0/0/1.
- R3(config-if)# no ppp multilink.

2.12. Verificación de la configuración de PPP

Utilice el *comando show interfaces serial* para verificar la configuración de la encapsulación PPP o HDLC. El resultado del comando en la siguiente figura muestra una configuración PPP.

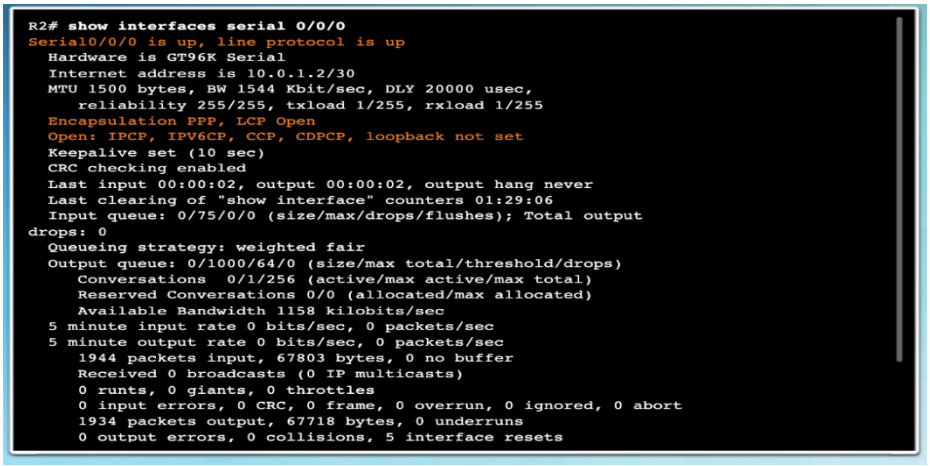


Figura 25: Verificación de la configuración de la encapsulación PPP serial.

Fuente: Cisco Networking Academy (2022)

Cuando configure HDLC, la salida del comando show interfaces serial debe mostrar *encapsulation* HDLC. Cuando se configura PPP, también se muestran los estados de LCP y NCP. Observe que los protocolos NCP IPCP e IPV6CP están abiertos para IPv4 e IPv6, ya que el R1 y el R2 se configuraron con direcciones IPv4 e IPv6.

En la siguiente figura, se resumen los comandos que se usan para verificar PPP.

Comando	Descripción
`show interfaces`	Muestra estadísticas de todas las interfaces configuradas en el router.
`show interfaces serial`	Muestra información sobre una interfaz serial.
`show ppp multilink`	Muestra información sobre una interfaz PPP multienlace.

Figura 26: Comandos de verificación de la configuración PPP.

Fuente: Cisco Networking Academy (2022).

El comando *show ppp multilink* verifica que el protocolo PPP multienlace esté habilitado en el R3, como se muestra en la siguiente figura. El resultado indica la interfaz Multilink 1, los nombres de host de las terminales locales y remotas, y las interfaces seriales asignadas al grupo multienlace.

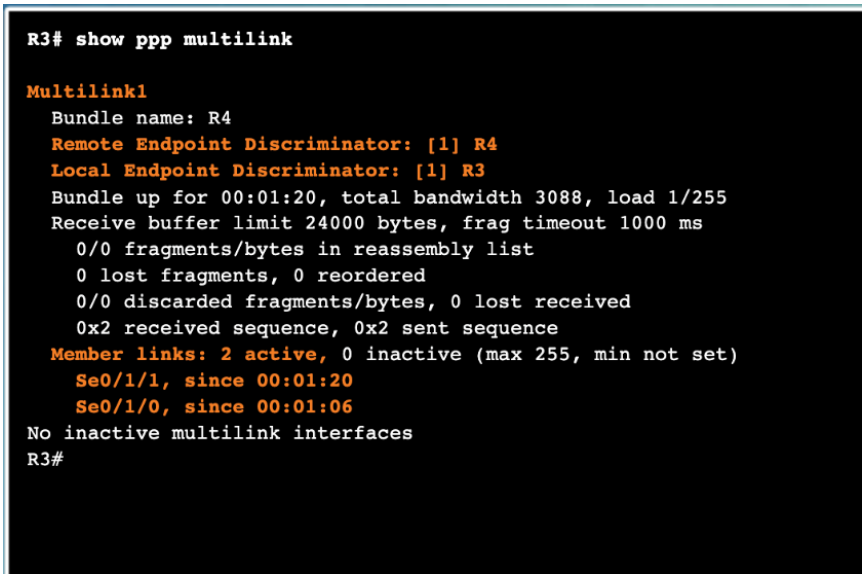


Figura 27: Verificación del protocolo PPP multienlace.

Fuente: Cisco Networking Academy (2022)

3. Protocolos de autenticación PPP

PPP define un protocolo LCP que permite la negociación de un protocolo de autenticación para autenticar a su par antes de permitir que los protocolos de capa de red transmitan por el enlace. RFC 1334, Protocolos de autenticación PPP, define dos protocolos para la autenticación, PAP y CHAP, como se muestra en la figura.

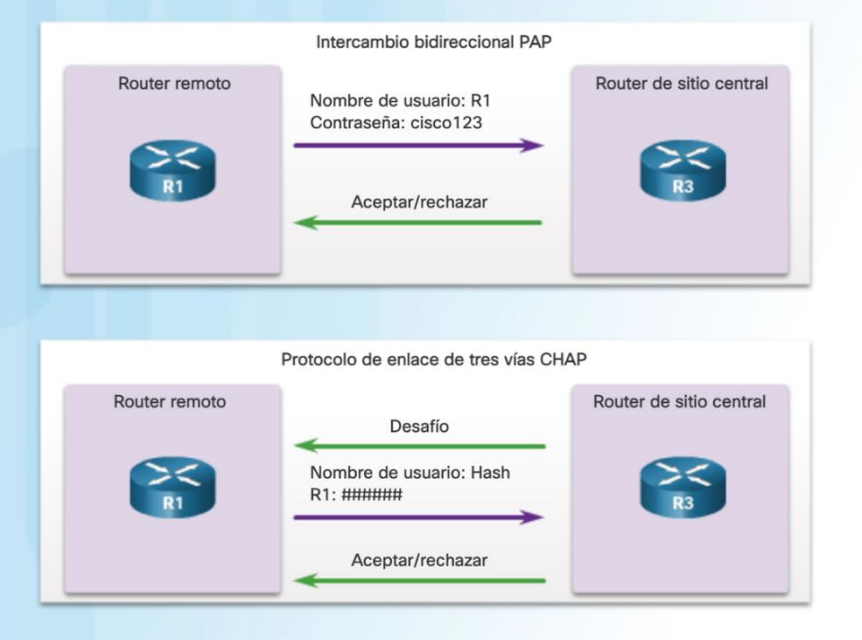


Figura 28: Protocolos de autenticación PPP.
Fuente: Cisco Networking Academy (2022).

PAP es un proceso bidireccional muy básico. No hay cifrado. El nombre de usuario y la contraseña se envían en texto no cifrado. Si se acepta, se permite la conexión. CHAP es más seguro que PAP. Implica un intercambio de tres vías de un secreto compartido.

La fase de autenticación de una sesión PPP es optativa. Si se utiliza, se autentica el peer después de que LCP establece el enlace y elige el protocolo

de autenticación. La autenticación ocurre antes de que comience la etapa de configuración del protocolo de capa de red.

Las opciones de autenticación requieren que la parte del enlace que llama introduzca la información de autenticación. Esto contribuye a asegurar que el usuario tenga permiso del administrador de red para realizar la llamada. Los routers pares intercambian mensajes de autenticación.

3.1. Protocolo de autenticación de contraseña (PAP)

PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante un protocolo de enlace bidireccional. PAP no es interactivo. Como se muestra en la siguiente figura, cuando se utiliza el comando ppp *Authentication pap*, se envía el nombre de usuario y la contraseña como un paquete de datos LCP, en lugar de que un dispositivo PPP envíe una solicitud de inicio de sesión y espere una respuesta, como en algunos mecanismos de autenticación.

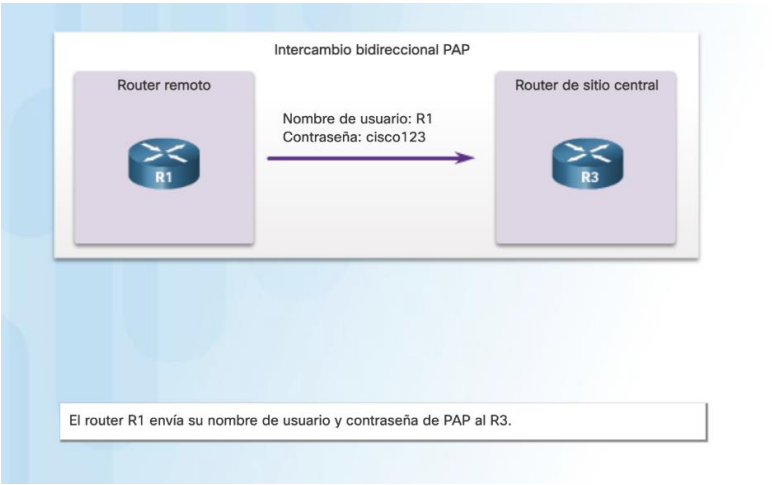


Figura 29: Inicio de PAP.

Fuente: Cisco Networking Academy (2022).

3.1.1. Proceso de PAP

Una vez que PPP completa la fase de establecimiento del enlace, el nodo remoto envía repetidamente un par de nombre de usuario y contraseña a través del enlace hasta que el nodo receptor lo confirma o finaliza la conexión.

En el nodo receptor, el dispositivo que ejecuta PPP verifica el nombre de usuario y la contraseña. Este dispositivo permite o deniega la conexión. Se devuelve un mensaje de aceptación o rechazo al solicitante, como se muestra en la figura.

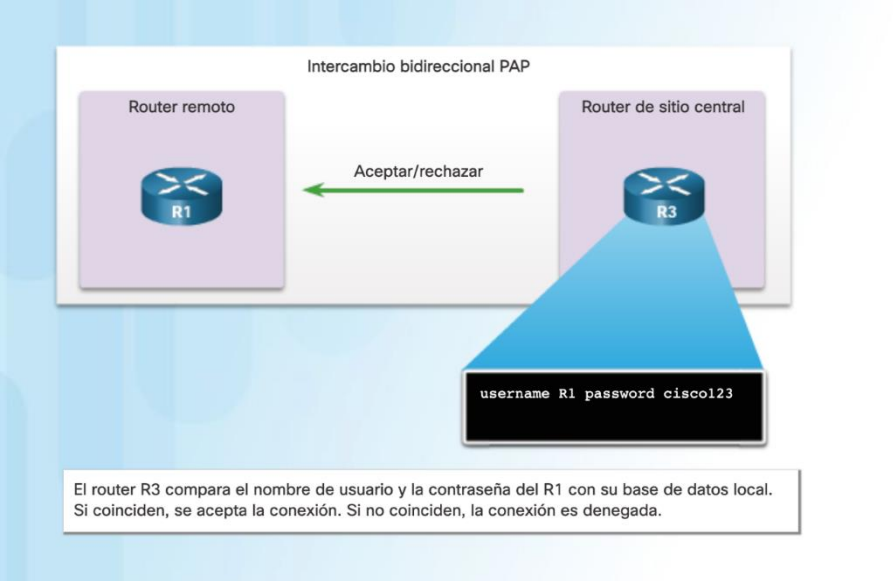


Figura 30: Finalización de PAP.

Fuente: Cisco Networking Academy (2022).

PAP no es un protocolo de autenticación seguro. Mediante PAP, las contraseñas se envían a través del enlace en texto no cifrado, y no existe protección contra los ataques de reproducción o los ataques repetidos de prueba y error. El nodo remoto tiene el control de la frecuencia y la temporización de los intentos de inicio de sesión.

No obstante, hay momentos en los que se justifica el uso de PAP. A pesar de sus limitaciones, PAP se puede utilizar en los siguientes entornos:

- Una gran base instalada de aplicaciones cliente que no admiten CHAP.
- Incompatibilidades entre las distintas implementaciones de CHAP de los proveedores.
- Situaciones en las que una contraseña de texto no cifrado debe estar disponible para simular un inicio de sesión en el host remoto.

Protocolo de autenticación de intercambio de señales (CHAP)

Una vez que se establece la autenticación con PAP, no se vuelve a autenticar. Esto deja la red vulnerable a los ataques. A diferencia de PAP, que autentica solo una vez, CHAP realiza desafíos periódicos para asegurar que el nodo remoto siga teniendo un valor de contraseña válido. El valor de contraseña varía y cambia de manera impredecible mientras existe el enlace. CHAP utiliza el comando ppp *Authentication chap*.

3.1.2. Proceso de CHAP

Una vez completa la fase de establecimiento del enlace PPP, el router local envía un mensaje de desafío al nodo remoto, como se muestra en la siguiente figura.

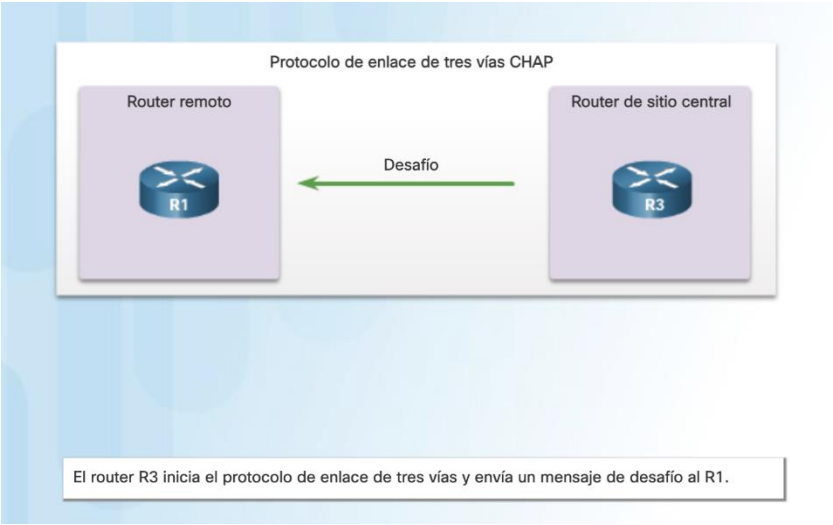


Figura 31: Inicio de CHAP.

Fuente: Cisco Networking Academy (2022).

El nodo remoto responde con un valor que se calcula mediante una función hash unidireccional. Generalmente es MD5 basado en la contraseña y el mensaje de desafío, como se muestra en la figura.

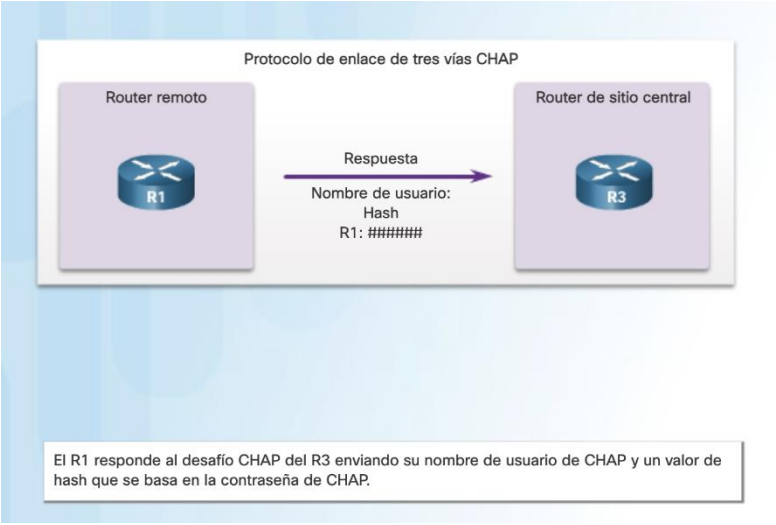


Figura 32: Respuesta de CHAP.

Fuente: Cisco Networking Academy (2022).

El *router* local compara la respuesta con su propio cálculo del valor de hash esperado. Si los valores coinciden, el nodo de inicio reconoce la autenticación, como se muestra en la siguiente figura. Si los valores no coinciden, el nodo de inicio finaliza la conexión de inmediato.

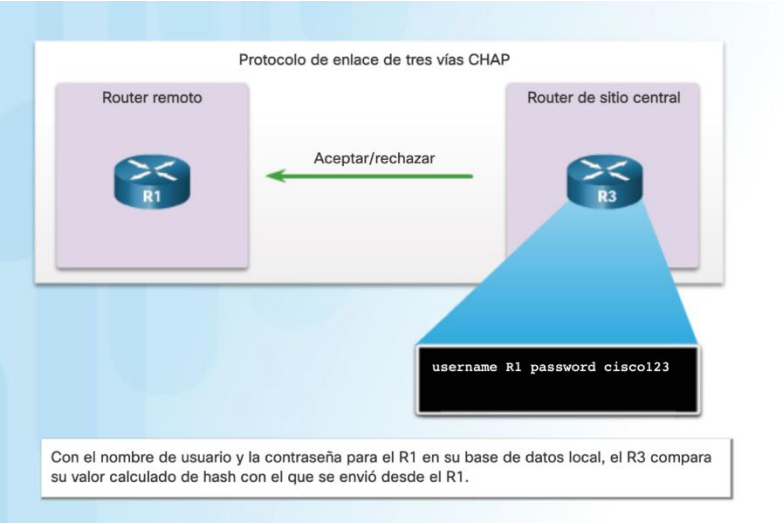


Figura 33: Finalización de CHAP.

Fuente: Cisco Networking Academy (2022).

CHAP proporciona protección contra los ataques de reproducción mediante el uso de un valor de desafío variable que es exclusivo e impredecible. Como la comprobación es única y aleatoria, el valor hash resultante también es único y aleatorio. El uso de comprobaciones reiteradas limita el tiempo de exposición ante cualquier ataque. El router local o un servidor de autenticación de terceros tiene el control de la frecuencia y la temporización de los desafíos.

3.2. Comando PPP *Authentication*

Para especificar el orden en que se solicitan los protocolos CHAP o PAP en la interfaz, utilice el comando de configuración de *interfaz ppp Authentication*, como se muestra en la figura. Utilice la versión no de este comando para deshabilitar esta autenticación

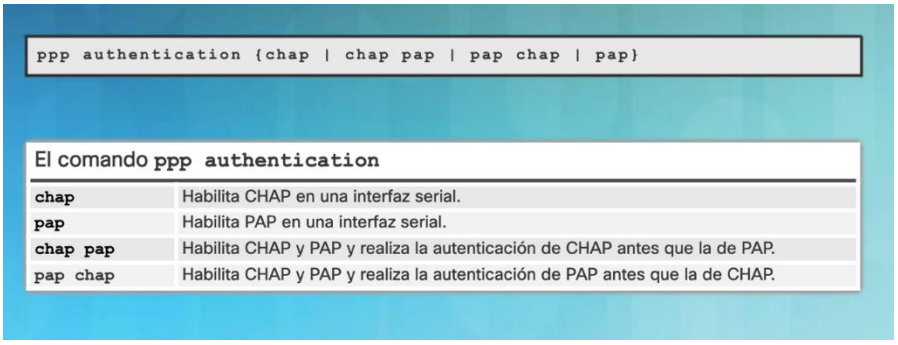


Figura 34: Comando PPP Authentication.

Fuente: Cisco Networking Academy (2022).

Se pueden habilitar PAP, CHAP, o ambos. Si ambos métodos están habilitados, se solicita el primer método especificado durante la negociación del enlace. Si el peer sugiere usar el segundo método o simplemente rechaza el primero, se debe probar con el segundo método. Algunos dispositivos remotos soportan sólo CHAP y algunos sólo PAP. El orden en que se especifican los métodos se basa en las preocupaciones sobre la capacidad del dispositivo remoto para negociar correctamente el método adecuado, así como la preocupación sobre la seguridad de la línea de datos.

3.3. Configuración de PPP con autenticación

El procedimiento descrito en la tabla explica cómo configurar la encapsulación PPP y los protocolos de autenticación PAP y CHAP. La configuración correcta es fundamental, ya que CHAP y PAP utilizan estos parámetros para autenticar.

3.3.1. Configuración de la autenticación PAP

En la siguiente figura, se muestra un ejemplo de configuración de autenticación PAP bidireccional. Ambos routers se autentican entre sí, por lo que los comandos de autenticación PAP se reflejan. El nombre de usuario y la contraseña PAP que cada router envía deben coincidir con los que se especificaron con el comando *username* nombre *Password* contraseña del otro *router*.

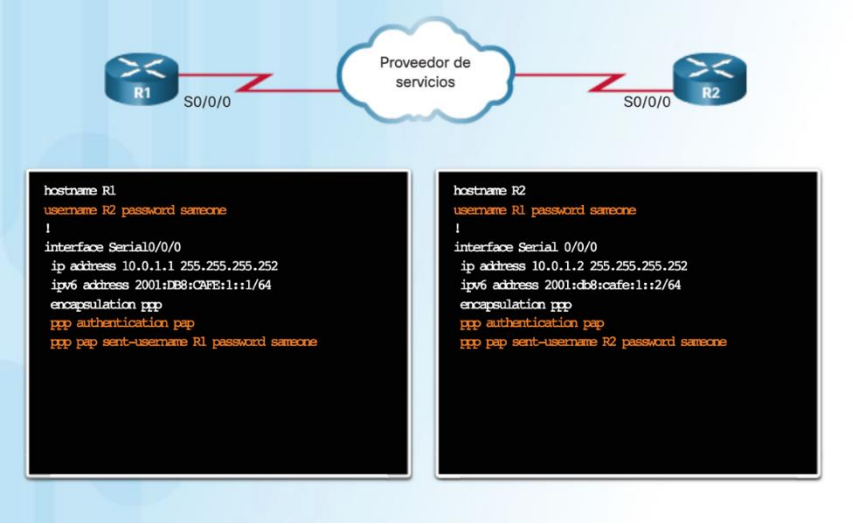


Figura 35: Configuración de autentificación PAP.

Fuente: Cisco Networking Academy (2022).

PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante un protocolo de enlace bidireccional. Esto se realiza solo en el establecimiento del enlace inicial. El nombre de host en un router debe coincidir con el nombre de usuario que el otro router configuró para PPP. Las contraseñas también deben coincidir. Para especificar los parámetros de nombre de usuario y contraseña, utilice el siguiente comando: ppp pap *sent-username* nombre *Password* contraseña.

3.3.2. Configuración de la autenticación CHAP

CHAP verifica periódicamente la identidad del nodo remoto mediante un protocolo de enlace de tres vías. El nombre de host en un router debe coincidir con el nombre de usuario que configuró el otro router. Las contraseñas también deben coincidir. Esto ocurre en el establecimiento del enlace inicial y se puede repetir en cualquier momento después de que se estableció el enlace. En la figura, se muestra un ejemplo de una configuración CHAP.

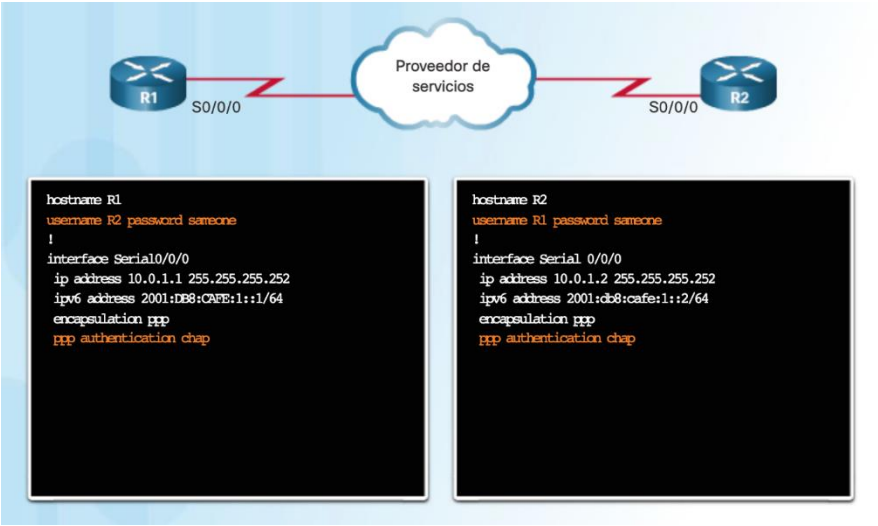
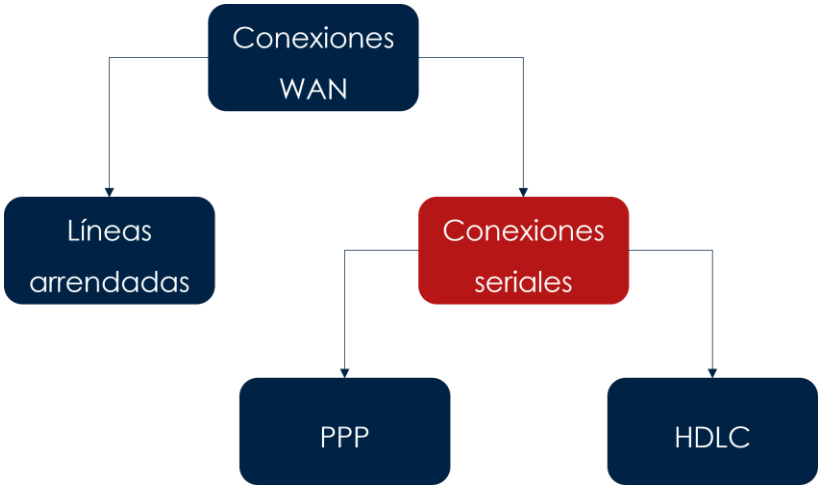


Figura 36: Configuración de autentificación CHAP.

Fuente: Cisco Networking Academy (2022).

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



Uno de los tipos de conexiones WAN más comunes, especialmente en las comunicaciones de larga distancia, son las conexiones punto a punto, que también se denominan "conexiones seriales" o "de líneas arrendadas ". Debido a que, en general, estas conexiones las proporciona una empresa prestadora de servicios, como una compañía telefónica, los límites entre lo que administra la prestadora y lo que administra el cliente se deben establecer con claridad.

En este capítulo, se abarcan los términos, la tecnología y los protocolos que se utilizan en las conexiones seriales. Se presentan los protocolos punto a punto (PPP) y HDLC. HDLC es el protocolo predeterminado en la interfaz serial de un router Cisco. PPP es un protocolo capaz de manejar la autenticación, la compresión y la detección de errores, de controlar la calidad de los enlaces, y de agrupar lógicamente varias conexiones seriales para compartir la carga.

Referencias bibliográficas

- *Cisco Networking Academy* (s/f). Recuperado en agosto del 2022, disponible en: www.netacad.com