CONEXIONES PUNTO A PUNTO

John Sebastián Luján Figueroa

1. Puertos serie y paralelos

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”.

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.

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).

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.

2. Enlaces de comunicación punto a punto

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.

3. 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).

Cisco desarrolló una extensión del protocolo HDLC para resolver la incapacidad de proporcionar compatibilidad multiprotocolo.

4. Estado de la interfaz en el router

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. “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).

5. ¿Qué es PPP (Protocolo Punto a Punto)?

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 ilustración. La encapsulación PPP se diseñó cuidadosamente para conservar la compatibilidad con el hardware más usado que la admite.

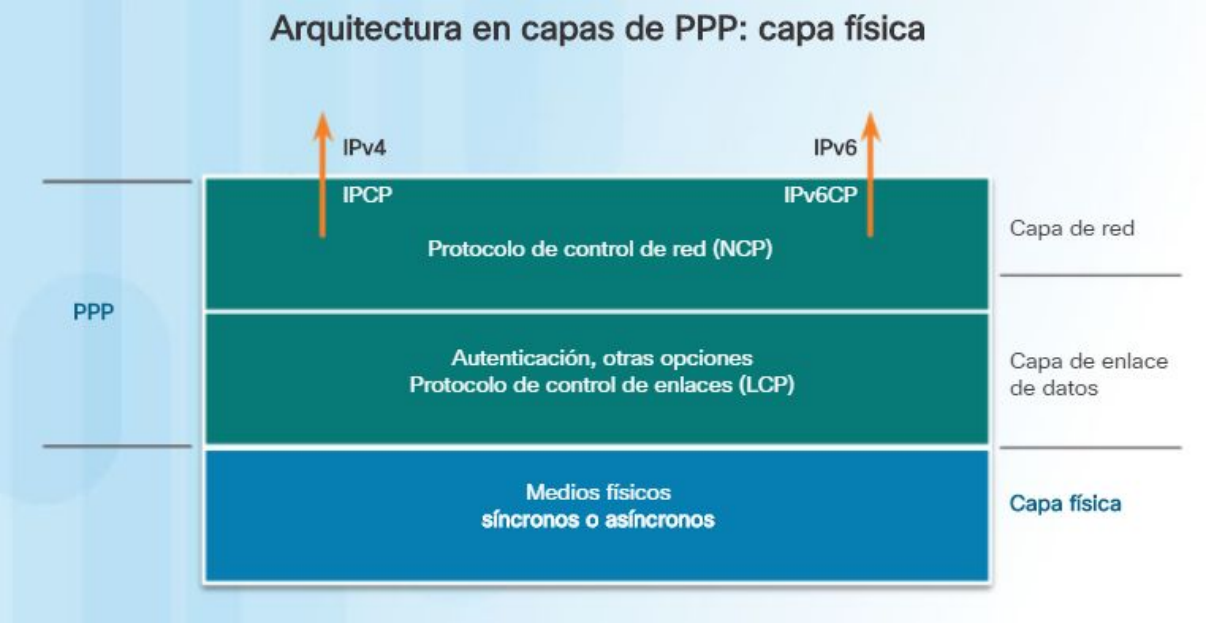
PPP encapsula tramas de datos para transmitirlas a través de enlaces físicos de capa 2. PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.

- 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.

6. Ventajas de PPP

- 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. Esta característica se explica y se práctica más adelante en otra sección.

7. **Arquitectura de capas PPP**



8. **LCP (Link Control Protocol):**

- Actúa en la **capa 2 OSI**.
- **Establecimiento** y **finalización** de la conexión.
- Determinación de cuándo un **enlace funciona** correctamente o cuándo falla.
- Acordar los formatos de **encapsulamiento**, **tamaños** de paquetes, la **autenticación**, la **compresión** y la detección de **errores**.

9. **NCP (Network Control Protocol):**

- **Encapsula** y **negocia** las opciones (compresión y dirección IPv4) para IPv4, IPv6 e IPX (**capa 2 OSI**).
- Administra paquetes de varios **protocolos de capa de red** (**capa 3 OSI**).

10. **Estructura de la trama PPP**

- **Indicador:** 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.

11. Establecimiento de una sesión PPP:

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.

12. Funcionamiento de PPP

- Las tramas de establecimiento de enlace establecen y configuran un enlace (solicitud de configuración, acuse de recibo de configuración, acuse de recibo negativo [NAK] de configuración y rechazo de configuración).
- Las tramas de mantenimiento de enlace administran y depuran un enlace (rechazo de código, rechazo de protocolo, solicitud de eco, respuesta de eco y solicitud de descarte).
- Las tramas de terminación de enlace terminan un enlace (solicitud de terminación y acuse de recibo de terminación).

Establecimiento del enlace

- Si las opciones no son aceptables o no se reconocen, el respondedor envía un mensaje de NAK de configuración o de rechazo de configuración. Si esto sucede y la negociación falla, el iniciador debe reiniciar el proceso con nuevas opciones.
- Si las opciones son aceptables, el respondedor responde con un mensaje de acuse de recibo de configuración, y el proceso pasa a la fase de autenticación. La operación del enlace se entrega a NCP.

Mantenimiento del enlace

- **Solicitud de eco, respuesta de eco y solicitud de descarte:** estas tramas se pueden utilizar para probar el enlace.
- **Rechazo de código y rechazo de protocolo**: estos tipos de trama brindan retroalimentación cuando un dispositivo recibe una trama válida. El dispositivo emisor vuelve a enviar el paquete.

Terminación del enlace

Una vez finalizada la transferencia de datos en la capa de red, LCP termina el enlace.. NCP solo termina el enlace NCP y de capa de red. El enlace permanece abierto hasta que LCP lo termina. Si LCP termina el enlace antes que NCP, también se termina la sesión NCP.

PPP puede terminar el enlace en cualquier momento cualquier tipo de pérdida de recurso o falla.

13. Explicación de NCP

Ejemplo de IPCP:

IPCP negocia dos opciones:

- **Compresión:** permite que los dispositivos negocien un algoritmo para comprimir encabezados TCP e IP, y ahorrar ancho de banda. La compresión de encabezados TCP/IP de Van Jacobson reduce los encabezados TCP/IP a un tamaño de hasta 3 bytes. Esto puede ser una mejora considerable en las líneas seriales lentas, en particular para el tráfico interactivo.
- **Dirección IPv4:** permite que el dispositivo de inicio especifique una dirección IPv4 para utilizar en el routing IP a través del enlace PPP, o para solicitar una dirección IPv4 para el respondedor. Antes de la llegada de las tecnologías de banda ancha como los servicios de DSL y de cable módem, los dispositivo de red de Internet por acceso telefónico normalmente usaban la opción de direcciones IPv4.

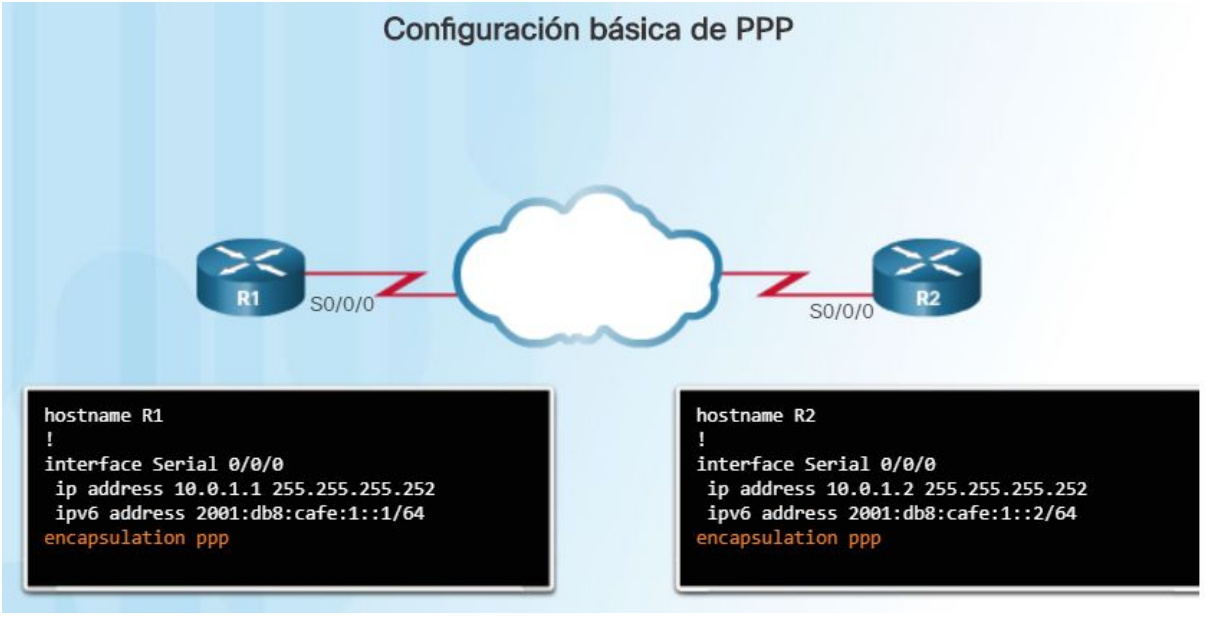
14. Opciones de configuración del PPP

Existen tres funciones opcionales:

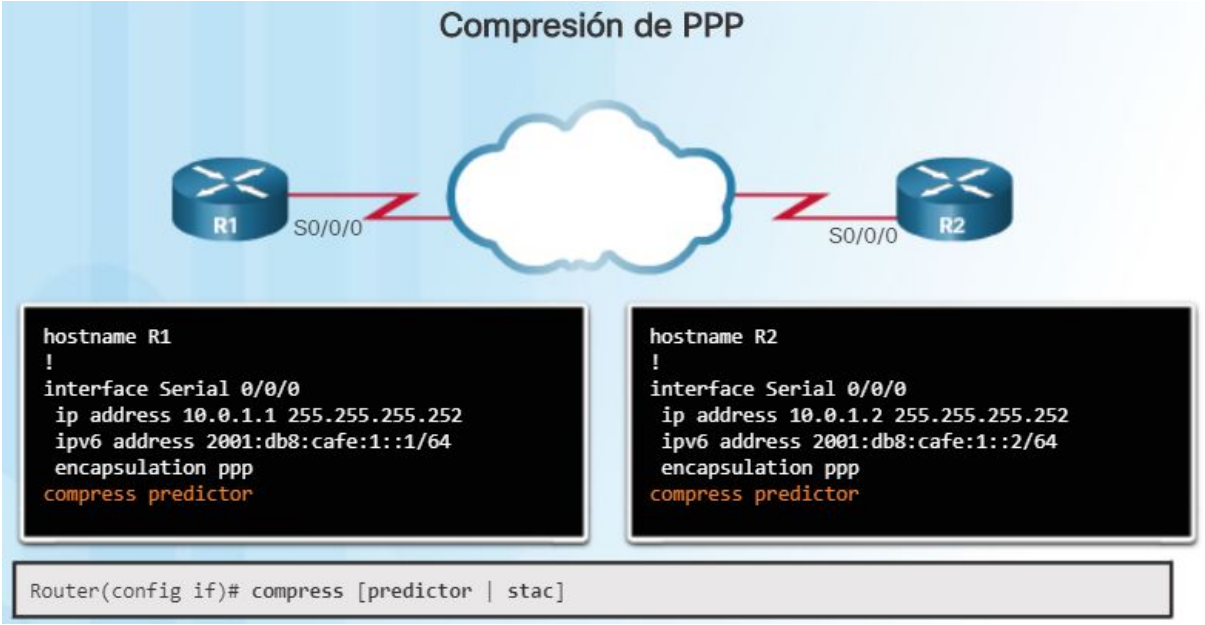
- **Autenticación:** los routers peers intercambian mensajes de autenticación. Las dos opciones de autenticación son: el protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) y el protocolo de autenticación de intercambio de señales (CHAP, Challenge Handshake Authentication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

- **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.

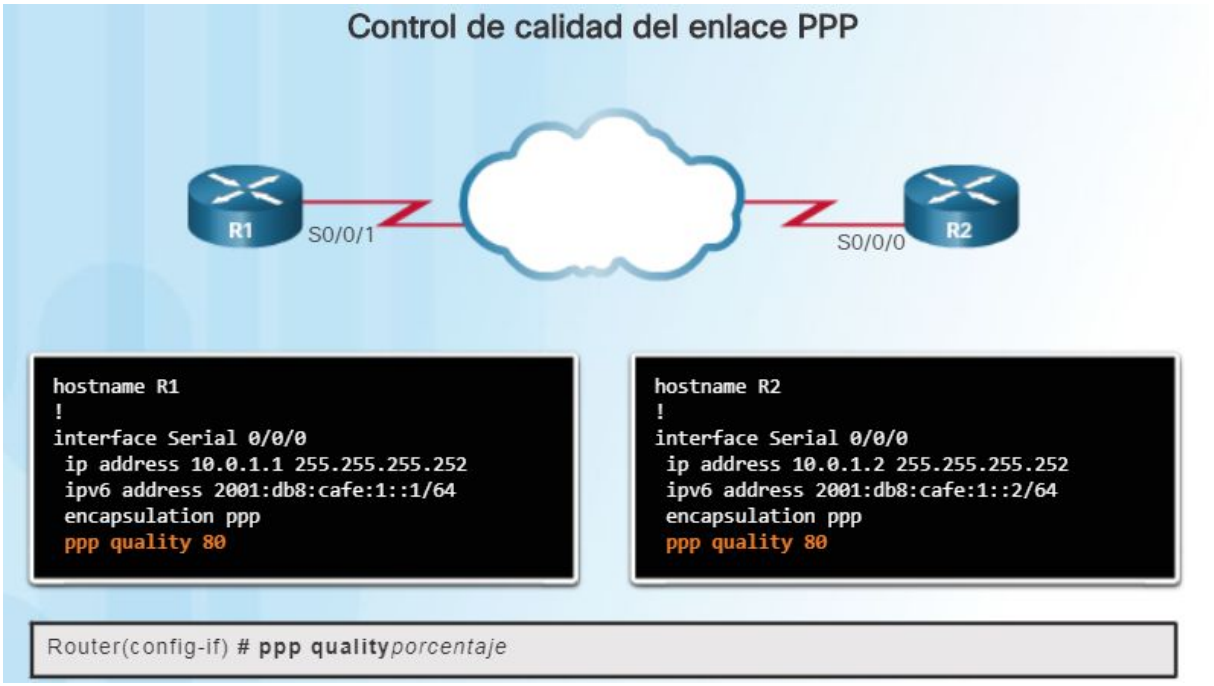
15. Comando de **configuración** básica de PPP



16. Comandos de compresión de PPP

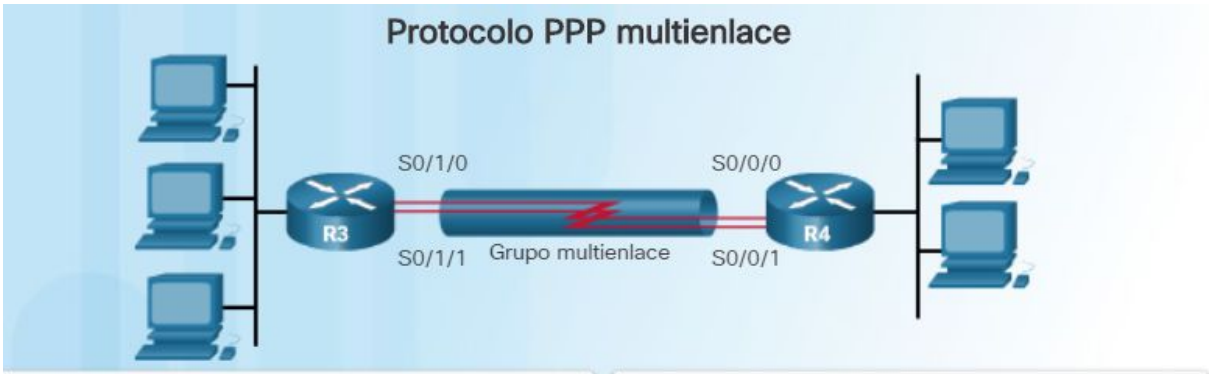


17. Comando de control de calidad del enlace PPP



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

18. Comandos de PPP multienlace




```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

19. Verificación de la configuración de PPP

Utilice el comando **show interfaces serial** para verificar la configuración de la encapsulación PPP o HDLC.

El comando **show ppp multilink** verifica que el protocolo PPP multienlace esté habilitado en el R3. 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.

20. Protocolos de autenticación PPP

Protocolo de autenticación de contraseña (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.

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.

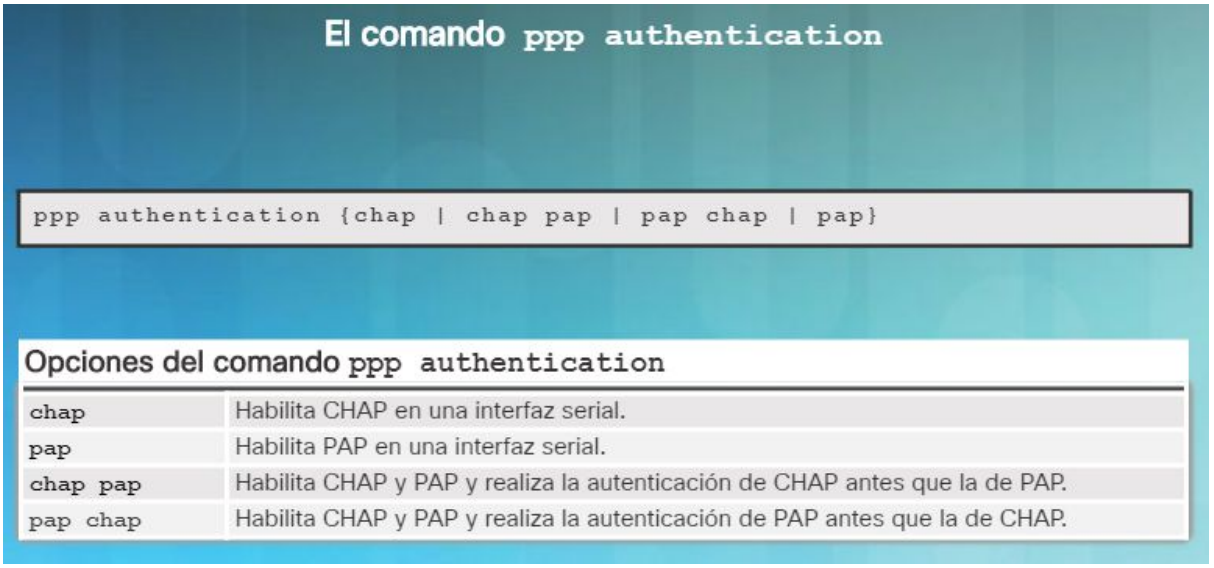
Protocolo de autenticación de intercambio de señales (CHAP)

Una vez completa la fase de establecimiento del enlace PPP, el router local envía un mensaje de desafío al nodo remoto.

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.

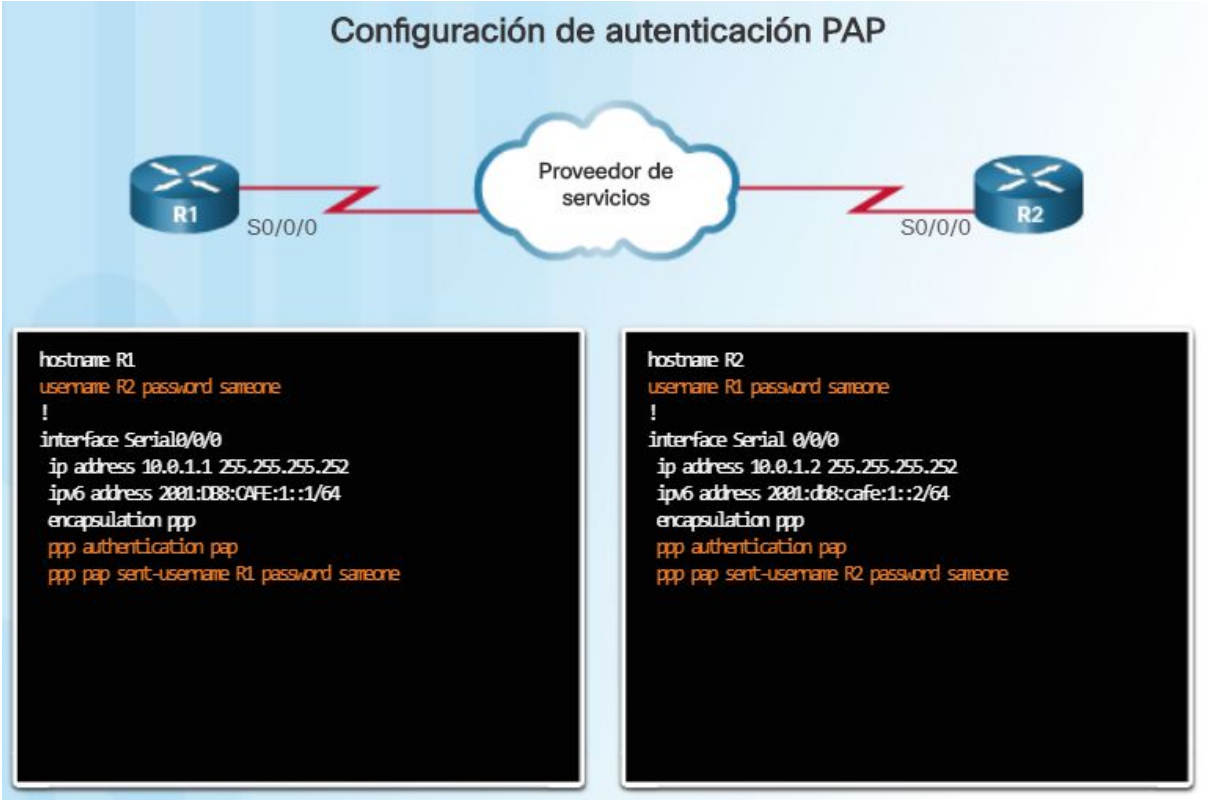
El router local compara la respuesta con su propio cálculo del valor de hash esperado. Si los valores coinciden, el nodo de inicio reconoce la autenticación. Si los valores no coinciden, el nodo de inicio finaliza la conexión de inmediato.

21. Comando PPP Authentication

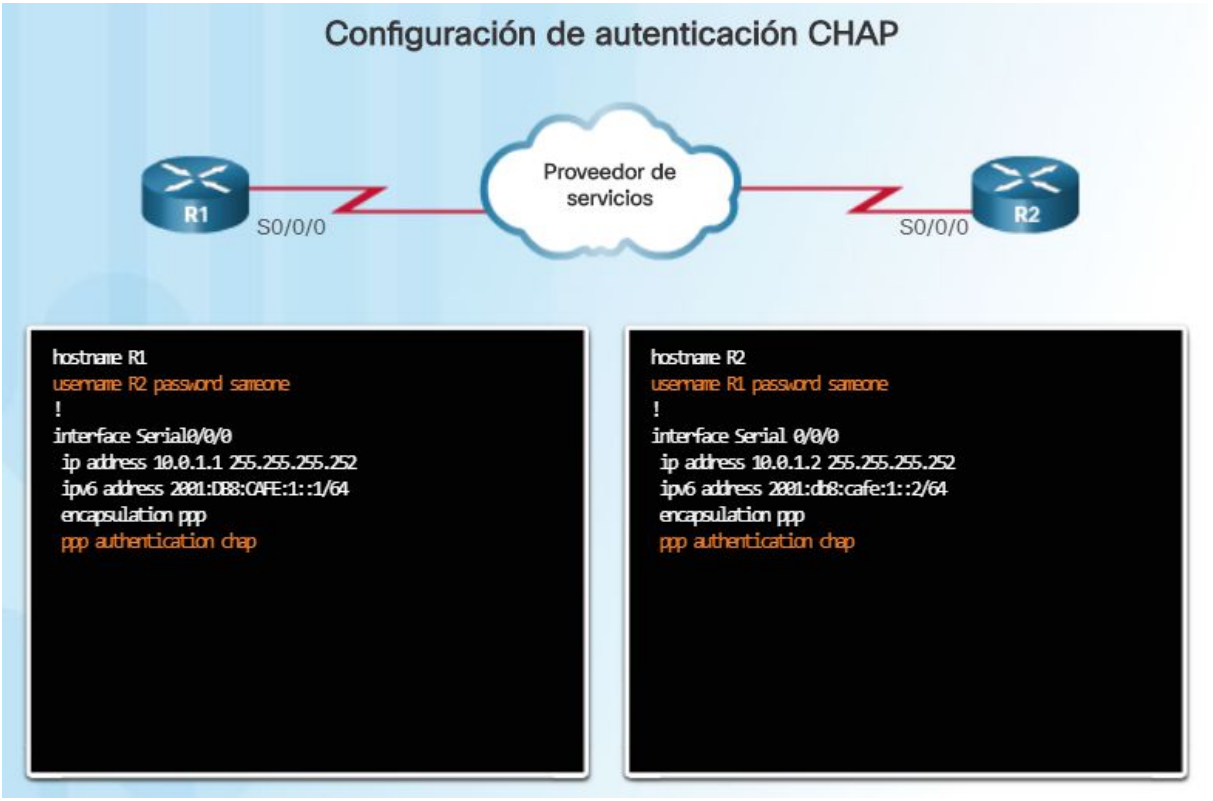


22. Configuración de PPP con autenticación

Configuración de la autenticación PAP



Configuración de la autenticación CHAP



23. **Resolución de problemas de la encapsulación PPP serial**

24. **Bibliografía**:

[1] Curso NETACAD (CISCO): Netacad.com

[2] Protocolo "punto a punto" (PPP):
http://www.ie.tec.ac.cr/einteriano/cisco/ccna4/Presentaciones/CCNA_Exploration_Accessing_the_WAN_-_Cap2.pdf

[3] Introduction to PPP(Point-to-Point Protocol):
https://www.youtube.com/watch?v=Oq0Si0WWHdM

[4] Funcionamiento de PPP: https://www.youtube.com/watch?v=JYpLvaeK2f4