Capítulo 2:
Protocolo Punto a Punto
Point-to-Point Protocol
(PPP)

CCNA Exploration 4 - Acceso a la WAN

Ricardo Chois

INSTITUTO TECNOLÓGICO DE SOLEDAD ATLÁNTICO - ITSA

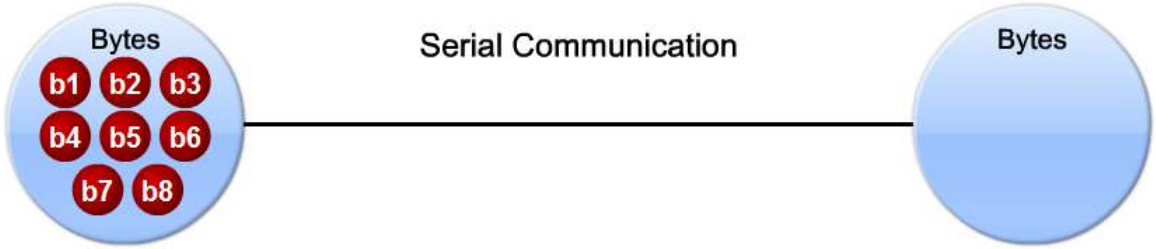
Version 4.0

Objetivos

- Describir los conceptos fundamentales de las comunicaciones seriales Punto a Punto incluyendo TDM, punto de demarcación, funciones de DTE y DCE, encapsulamiento HDLC y resolución de problemas con interfaces seriales.
- Describir los conceptos de PPP incluyendo la arquitectura por capas, la estructura de la trama, el establecimiento de sesión, el soporte multiprotocolo, el protocolo de control de enlace LCP, el Protocolo de control de red NCP, y el protocolo de control de IP (IPCP).
- Configurar PPP en una interfaz serial incluyendo la habilitación del encapsulamiento, verificación y resolución de problemas.
- Configurar la autenticación PPP incluyendo la comprensión de los protocolos PAP y CHAP, configuración autenticación usando PAP y CHAP y resolución de problemas de autenticación.

Comunicaciones Seriales

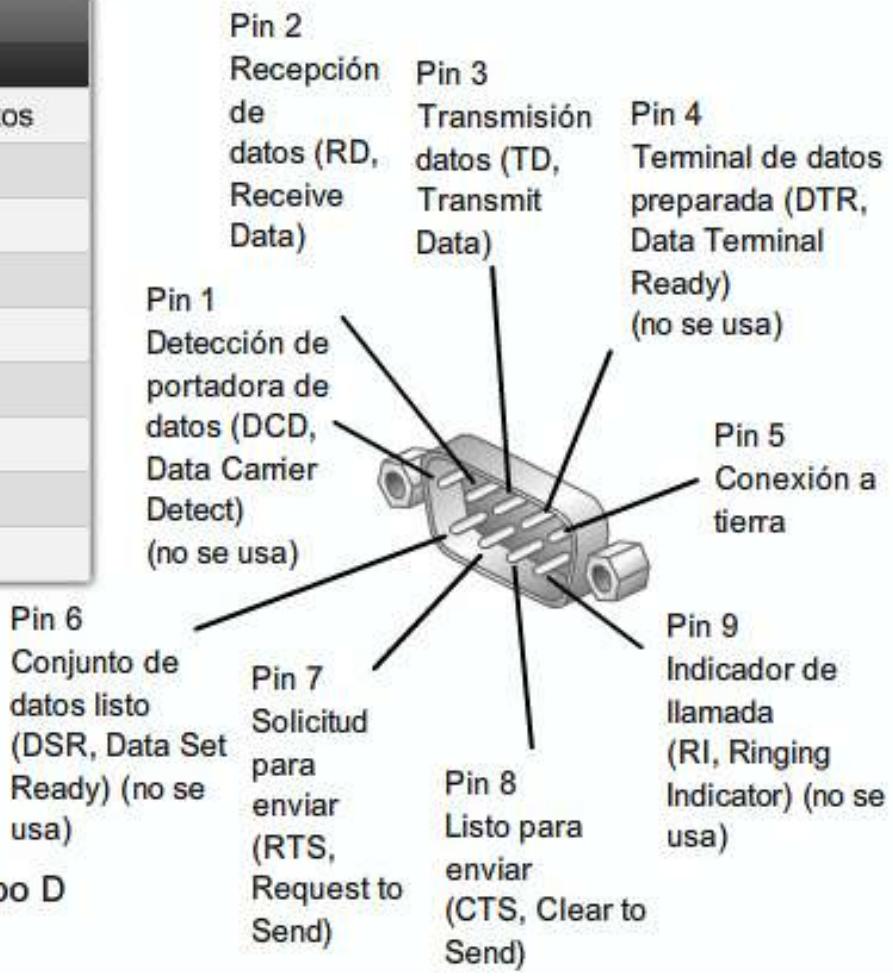
- Se envía un bit de datos a la vez a través del medio físico.
- En los PCs un conector de 9 pins emplea dos bucles, uno en cada dirección, para datos, y el resto para control de flujo de información.
- Las conexiones seriales son más económicas.
- Algunos de los estándares son:
  - HSSI (High Speed Serial Interface)
  - RS-232
  - V.35



Estándar RS-232

Conector RS-232 de 9 pins

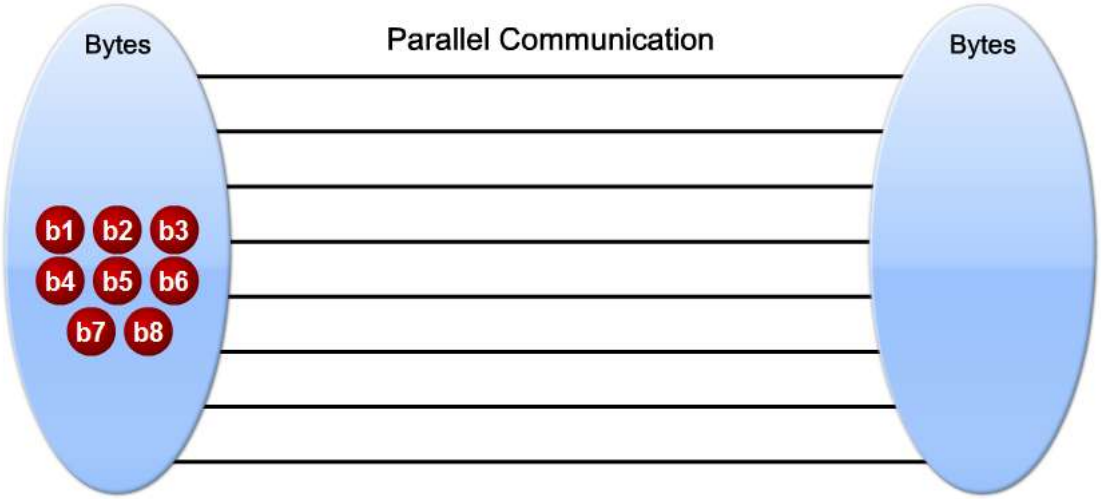
Número de pin	Señal	Descripción
1	DCD	Detección de portadora de datos
2	RxD	Recepción de datos
3	TxD	Transmisión de datos
4	DTR	Terminal de datos preparada
5	GND	Señal de conexión a tierra
6	DSR	Conjunto de datos listo
7	RTS	Preparado para enviar
8	CTS	Listo para enviar
9	RI	Indicador de llamada



Disposición de pines del conector serial RS-232 tipo D de 9 pins

Comunicaciones Paralelas

- Se envía los bits simultáneamente a través de más cables.
- En los PCs un conector de 25 pins, 8 para datos.
- Entonces, en teoría, es 8 veces más rápido que una conexión serial.



Comunicaciones Paralelas

Entonces…

¿Qué significa teóricamente más rápido?

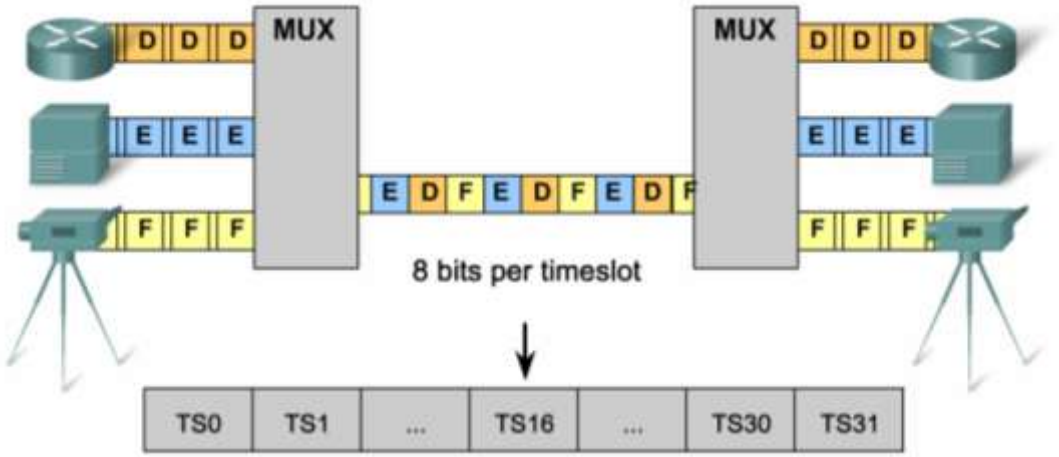
¿Es la más apropiada para realizar una conexión a una WAN?

Dos Factores que afectan las comunicaciones Paralelas

- Sesgo de Reloj
  - Significa que los algunos bits llegan más tarde que el resto al receptor.
  - El extremo receptor debe sincronizarse con el transmisor y, luego, esperar hasta que todos los bits hayan llegado.
  - La necesidad de temporización reduce la transmisión paralela mucho más de lo que, en teoría, se espera.
- Crosstalk
  - Significa que hay Ruido (interferencia) entre los hilos de cable adyacentes.
  - La posibilidad de crosstalk a través de los hilos implica más procesamiento, especialmente a frecuencias más altas.

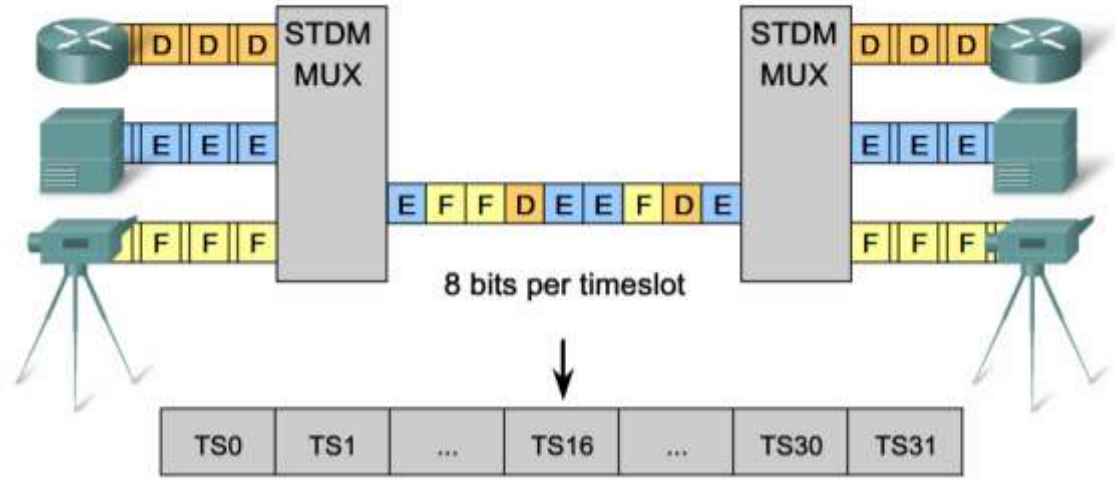
TDM – Multiplexación por división de tiempo

- Es la transmisión de muchas fuentes de información utilizando un canal común, o señal, y luego la reconstrucción del flujo original en el extremo remoto.
- Divide el ancho de banda de un solo enlace en canales separados o en periodos de tiempo.
- Transmite dos o más canales a través del mismo enlace mediante la asignación de diferentes intervalos de tiempo (periodo de tiempo) para la transmisión de cada canal.
- Las líneas telefónicas T1/E1 y RDSI(ISDN) son ejemplos comunes de TDM síncrona.



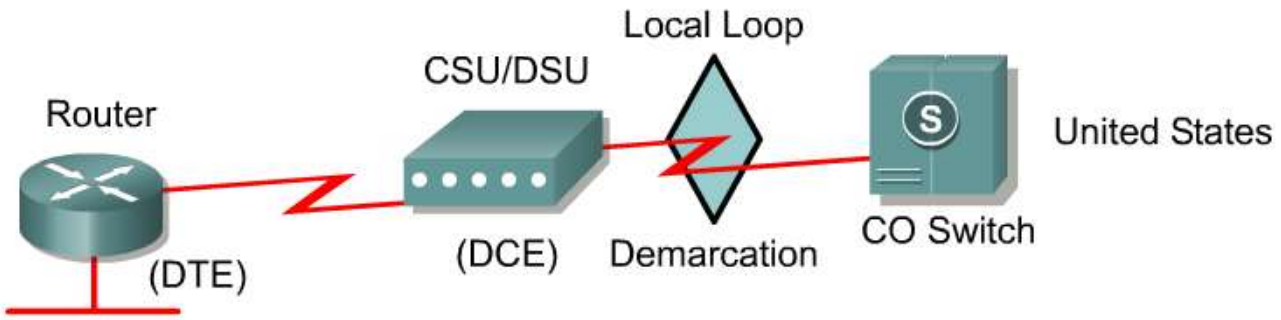
STDM – Multiplexación estadística por división de tiempo

- Utiliza una extensión variable para el periodo de tiempo, lo que permite que los canales compitan para obtener cualquier espacio libre del periodo.
- No desperdicia el tiempo de la línea de alta velocidad con canales inactivos con este esquema.
- Exige que cada transmisión transmita la información de identificación (un identificador de canal).



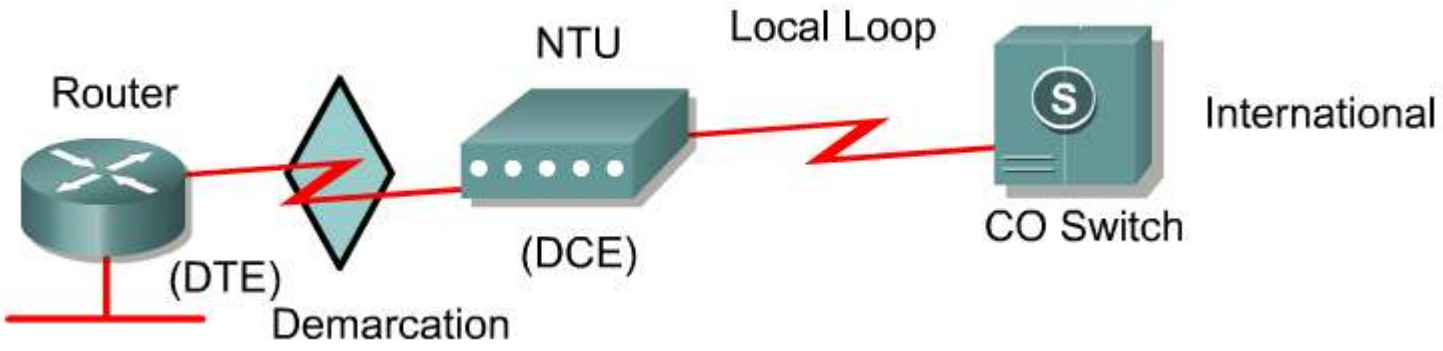
Punto de demarcación – Estados Unidos

- El **punto de demarcación o "demarc"**, es el punto de la red donde termina la responsabilidad del proveedor de servicios.
- El cliente provee los equipos activos tal como CSU/DSU en los cuales termina el loop local.
- El cliente es responsable de mantener, reemplazar y reparar los equipos



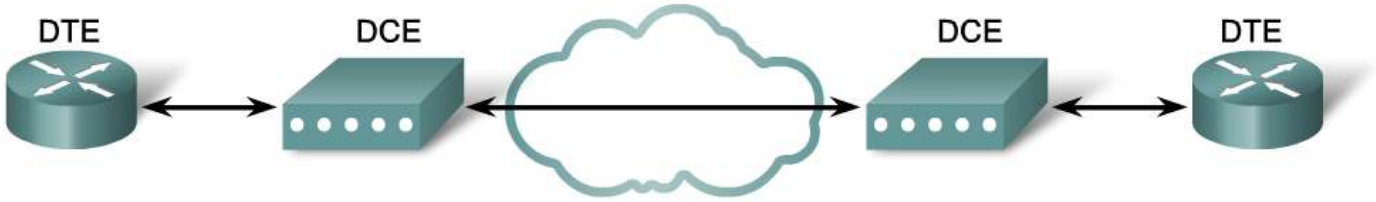
Punto de demarcación – Internacional

- El NTU (Networ Termination Unit) lo provee y administra el provedor de servicios.
- Le permite al proveedor administrar y resolver problemas con el loop local.
- El cliente conecta el CPE, router o dispositivo Frame Relay, al NTU utilizando una interfaz serial V.35 o RS-232



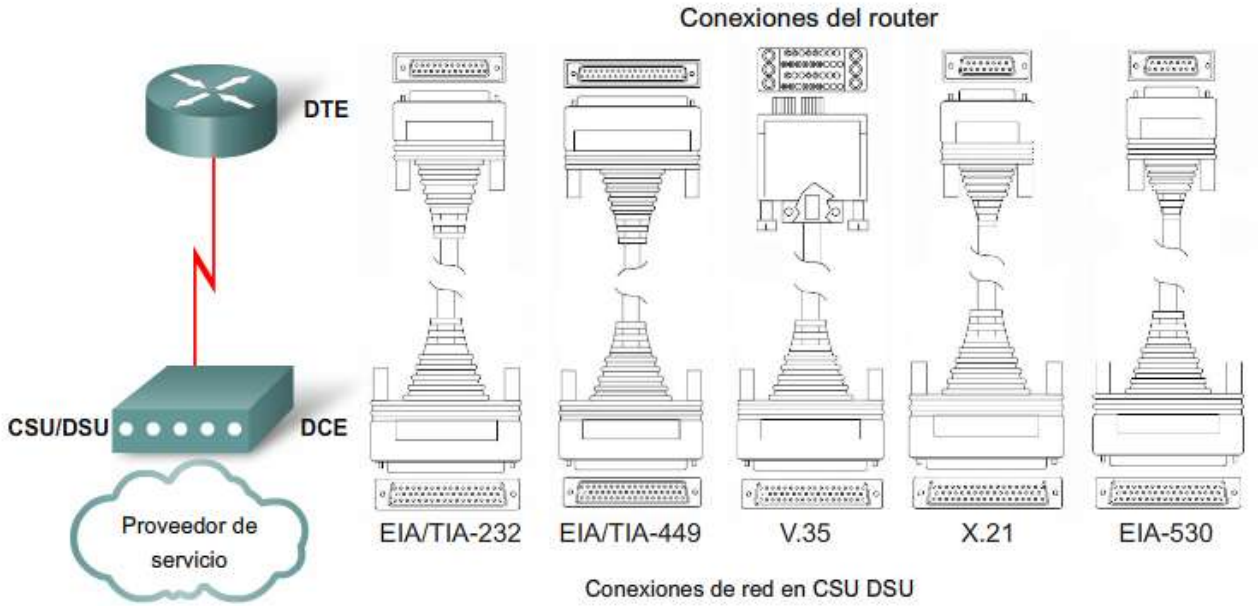
DTE-DCE

- DTE (Data Terminal Equipment)
  - Extremo del dispositivo del usuario.
  - CPE, por lo general un router.
- DCE (Data Communication Equipment)
  - Extremo de la instalación de comunicaciones del proveedor WAN.
  - Responsable de la temporización.
  - Por lo general un modem o CSU/DSU
- La EIA y la ITU-T han trabajado activamente en el desarrollo de los estándares.



DTE-DCE

- La interfaz DTE/DCE para un estándar en particular define las siguientes especificaciones:
  - **Mecánica/física:** número de pins y tipo de conector
  - **Eléctrica:** define los niveles de tensión para 0 y 1
  - **Funcional:** especifica las funciones que se ejecutan al asignar significados a cada una de las líneas de señalización de la interfaz
  - **Procedimental:** especifica la secuencia de eventos para la transmisión de los datos

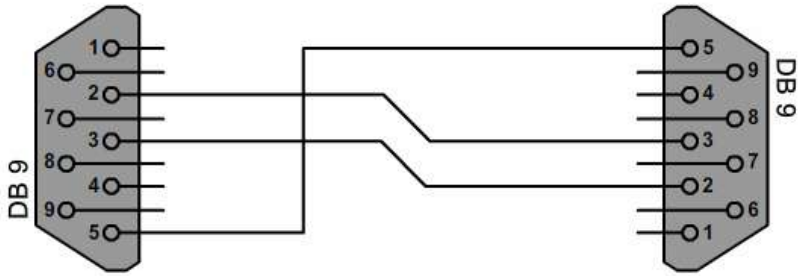


Conexiones de red en CSU DSU

DTE-DCE

- Si desea conectar dos DTE, como dos computadoras o dos routers en el laboratorio, se necesita un cable especial llamado módem nulo que reemplaza a un DCE.
- Para conexiones síncronas, donde se necesita una señal de reloj, un dispositivo externo o un DTE debe generar la señal de reloj.
- Para admitir mayores densidades en un factor de forma más pequeño, Cisco ha introducido el cable serial inteligente (Smart Serial).
- El extremo de la interfaz del router del cable serial inteligente es un conector de 26 pins mucho más compacto que el conector DB-60.

Módem nulo para conectar 2 DTE



Conector 1	Conector 2	Función
2	3	Rx ← Tx
3	2	Tx → Rx
5	5	Señal de conexión a tierra

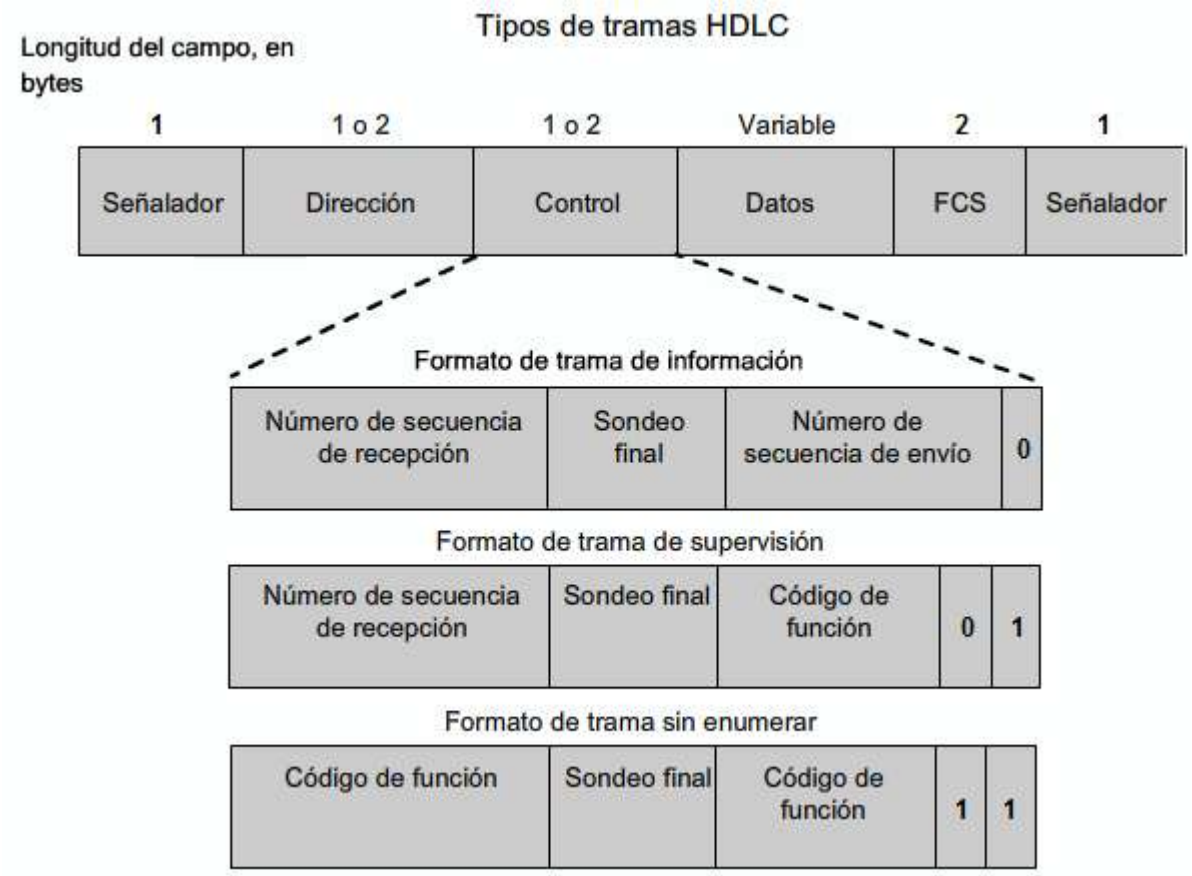
Observe los entrecruzamientos: Pin 2 a Pin 3 y Pin 3 a Pin 2

HDLC (High-level Data Link Control)

- Es el protocolo de capa de enlace de datos (Capa 2) por defecto en las interfaces seriales de routers cisco.
- Cisco desarrolló una extensión del protocolo HLDC para solucionar la incapacidad de brindar compatibilidad multiprotocolo. (cHDLC)

Tipos de tramas HDLC

- Tramas de Información(I) → Información de capa superior
- Tramas de Supervisión(S)→ Información de control
- Tramas sin enumerar(U) →Objetivos de control. No secuenciadas



Configuración de HDLC

- Utilice el HDLC de Cisco como un protocolo punto a punto en líneas arrendadas entre dos dispositivos de Cisco, si no, utilice PPP Síncrono.
- Esta configurado por defecto, si lo cambió, utilice el comando “encapsulation hdlc”, en el modo de configuración de interfaz o el comando “no encapsulation”.
- El comando “show interfaces serial 0/0/0”, muestra el estado de la línea y el tipo de encapsulamiento.

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

Veamos en Packet Tracer…

Resolución de problemas

- El resultado del comando ***show interfaces serial*** muestra información específica acerca de las interfaces seriales y podemos encontrar estas situaciones:

Estado de Línea	Estado de Protocolo	Razón/Capa
Administratively down	Down	Interface deshabilitada
Down	Down	Capa 1
Up	Down	Capa 2
Up	Up	Capa 3

- Cundo existen problemas de capa 2 verifique:
  - Que coincidan los tipos de encapsulamiento en los dos extremos del enlace.
  - La configuración de “keepalive”
  - Fallos en autenticación de capa 2 (PAP/CHAP)

Resolución de problemas

```
R1#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x62938244, driver data structure at 0x6293A608
wic_info 0x6293AC04
Physical Port 0, SCC Num 0
```

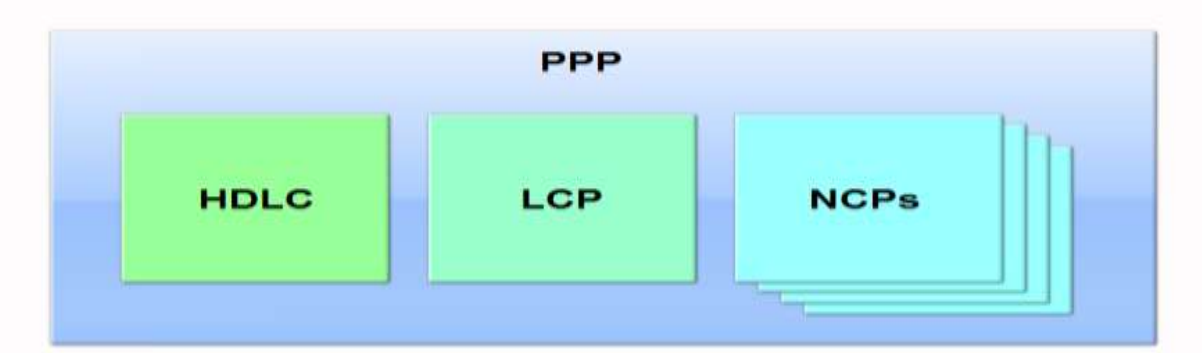
PPP (Point-to-Point Protocol)

- Es un protocolo de capa 2 que define características más allá de sólo ayudar a enviar datos sobre un enlace.
- Establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.
- Contiene 3 Componentes principales.

  HDLC → Para encapsulamiento de datagramas.

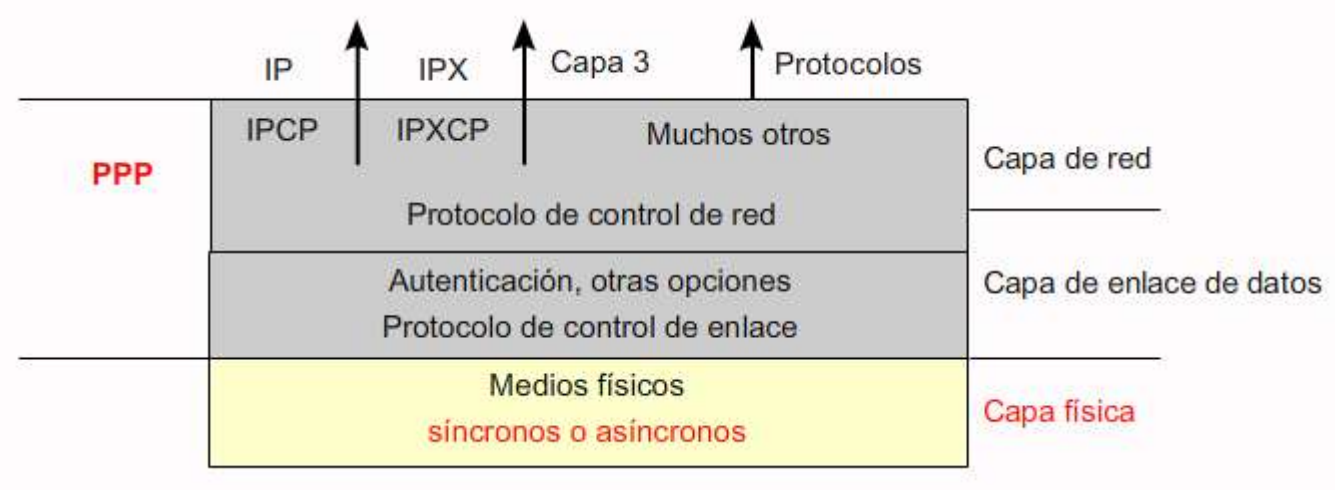
  LCP → Establecer, configurar y probarla conexión de enlace de datos.

  NPCs → Establecer y configurar distintos protocolos de capa de red.



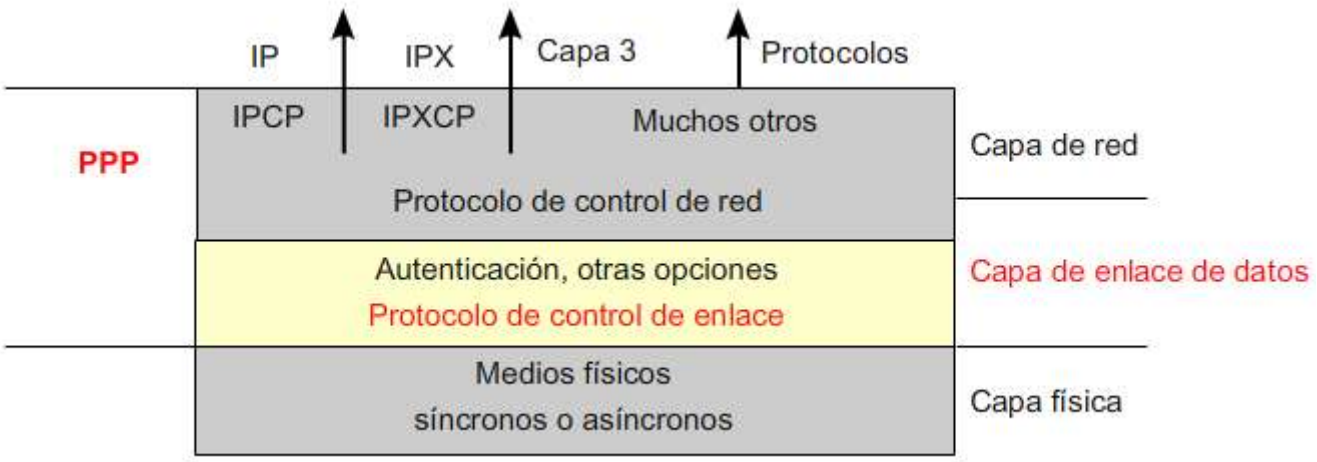
Arquitectura de capas de PPP

- **Capa Física.** PPP y OSI comparten la misma capa física. Se puede configurar PPP en una variedad de interfaces:
  - Serial Síncrona
  - Serial Asíncrona
  - HSSI
  - RDSI(ISDN)
- El único requisito absoluto impuesto por el PPP es un circuito duplex, dedicado o conmutado, que pueda funcionar en un modo serial de bits asíncrono o síncrono



Arquitectura de capas de PPP

- Capa LCP (Procolo de Control de Enlace)
- El LCP se ubica en la parte superior de la capa física
- Se utiliza para establecer, configurar y probar la conexión de enlace de datos.
- Se utiliza para acordar, de forma automática, acerca de formatos de encapsulación (autenticación, compresión, detección de errores) tan pronto como se establezca el enlace.



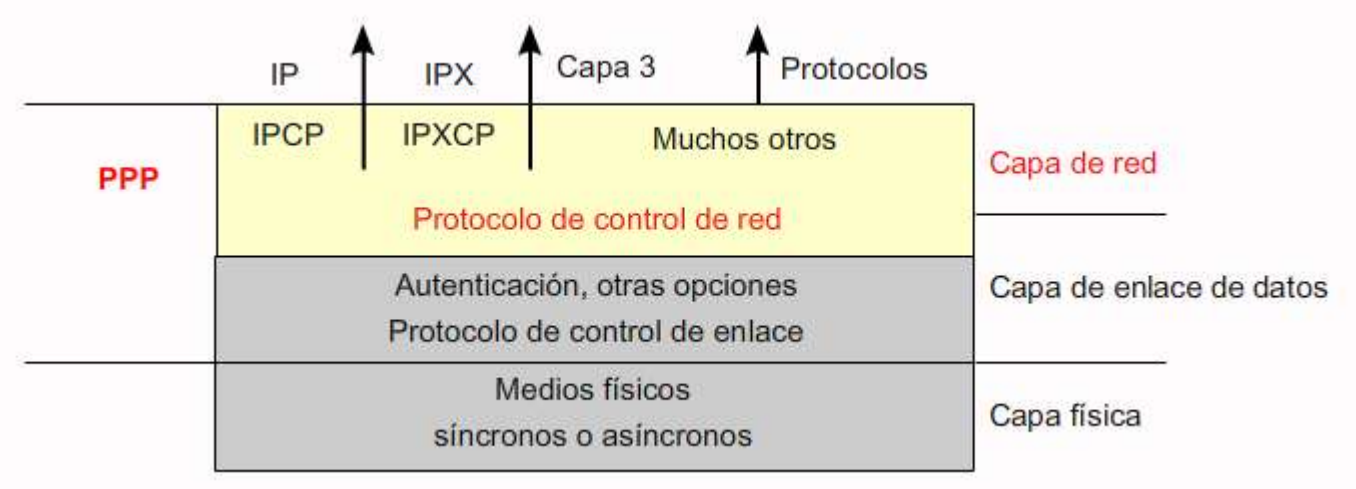
Arquitectura de capas de PPP

- Características de LCP

Función	Característica LCP	Descripción
Detección de loop en enlace	Número Mágico	Detecta si hay un loop en el enlace y deshabilita la interfaz, permitiendo re-enrutar por una mejor ruta.
Detección de errores	LQM (Link Quality Monitoring)	Deshabilita la interfaz que excede un margen de error, permitiendo re-enrutar por mejores rutas.
Soporte multienlace	Multilink PPP (MP)	Hace balanceo de tráfico sobre múltiples enlaces paralelos
Autenticación	PAP y CHAP	Intercambia usuarios y contraseñas para verificar la identidad de los dispositivos en cada extremo.
Compresión	Stacker, Predictor, TCP Header, MPPC	Comprime los datos en el origen y recupera los datos en el destino.

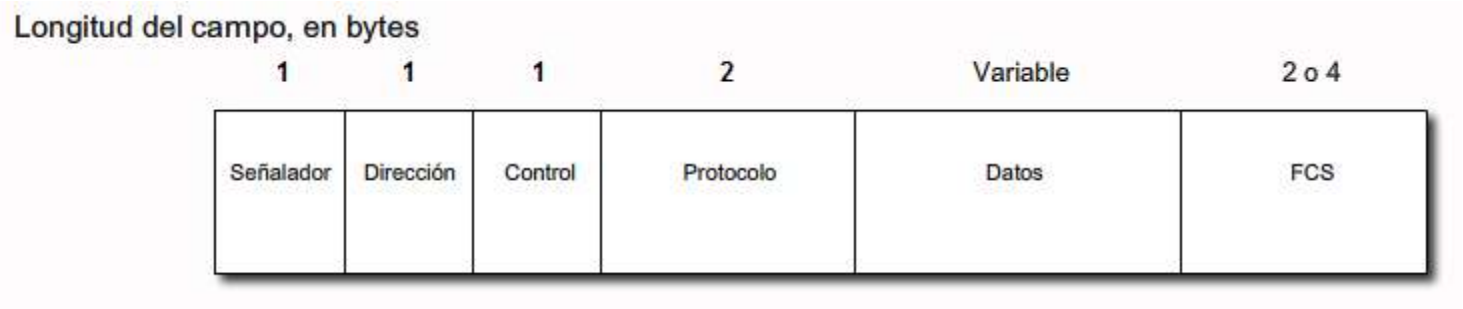
Arquitectura de capas de PPP

- Capa NCP (Procolo de Control de Red)
- Para cada protocolo de capa de red utilizado, el PPP utiliza un NCP distinto.



Valor (en hex)	Nombre del protocolo
8021	Protocolo de control del protocolo de Internet
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

Campos de la Trama PPP



- **Señalador** → Indica el comienzo o fin de una trama. Consiste en la secuencia 01111110 (0x7E).
- **Dirección** → Formada por la dirección de broadcast 11111111.
- **Control** → Secuencia 00000011, el cual requiere que la transmisión de datos se envíe en tramas no secuenciadas.
- **Protocolo** → Identifica el protocolo encapsulado en el campo de datos.
- **Datos** → Contiene el datagrama del protocolo especificado.
- **FCS** → Checksum de 16 bits para controlar errores en la trama.

Establecimiento de una Sesión PPP

- Se lleva a cabo en 3 Fases

Fase 1. Establecer el enlace: "Negociemos".

Fase 2. Determinar la calidad del enlace: "Quizás deberíamos analizar algunos detalles sobre la calidad. O quizás no ..."

Fase 3. Negociación del protocolo de red: "Está bien, dejaré a los NCP que analicen los detalles de nivel superior".

El LCP realiza toda la conversación.

Establecimiento de una Sesión PPP

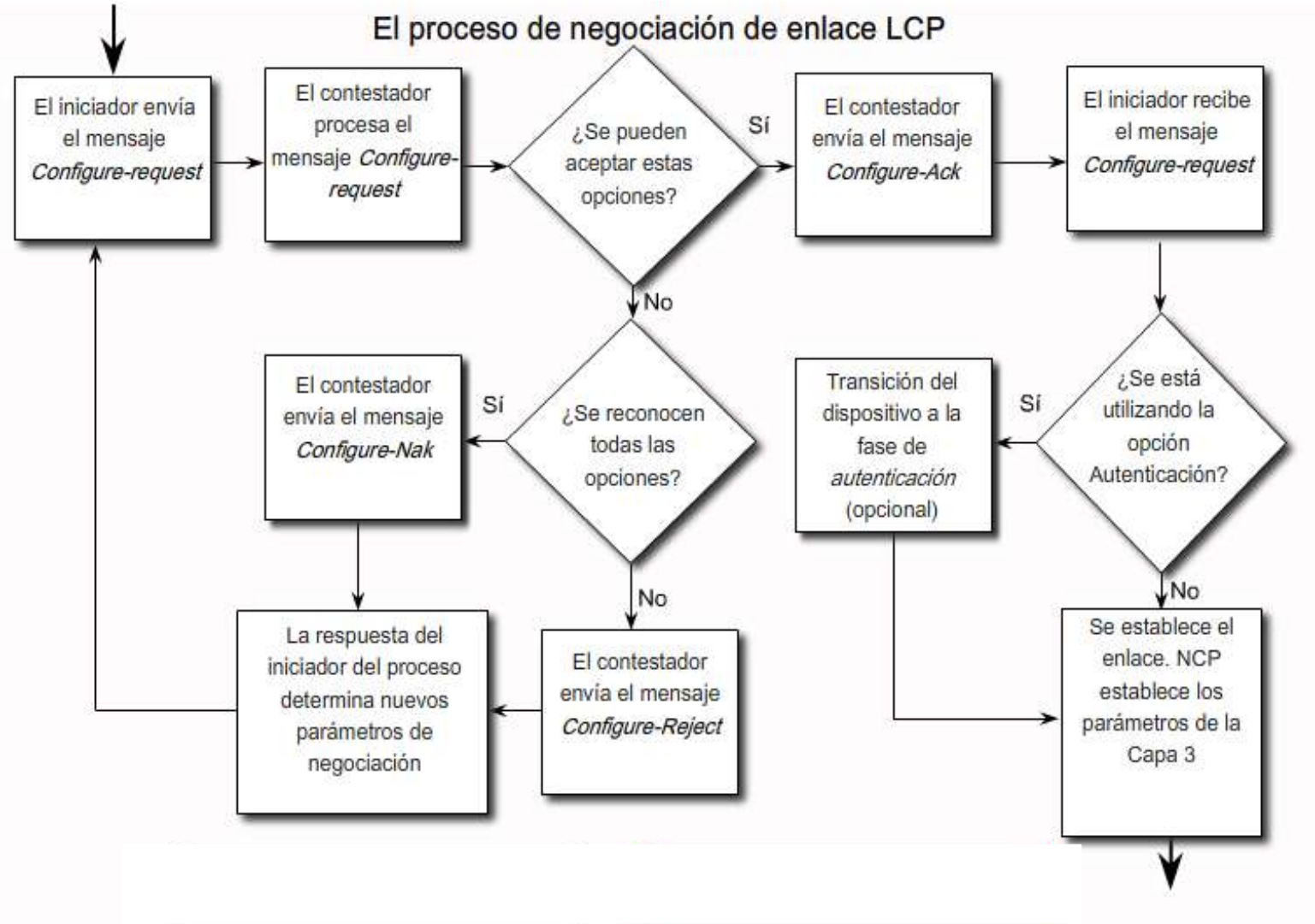
- **Fase 1: Establecimiento del enlace y negociación de la configuración.**

- Cada dispositivo envía tramas LCP para configurar y probar el enlace de datos.
- Las tramas LCP contienen un campo de “Opción” que le permite a los dispositivos negociar parámetros como:
  - MRU
  - Compresión
  - Protocolo de Autenticación
  - Multienlace
- Si en los paquetes LCP no se incluye una opción, el valor por defecto se asume. Por ejemplo, sin autenticación.
- Antes de intercambiar cualquier paquete de red, LCP primero debe abrir la conexión y negociar los parámetros de configuración .

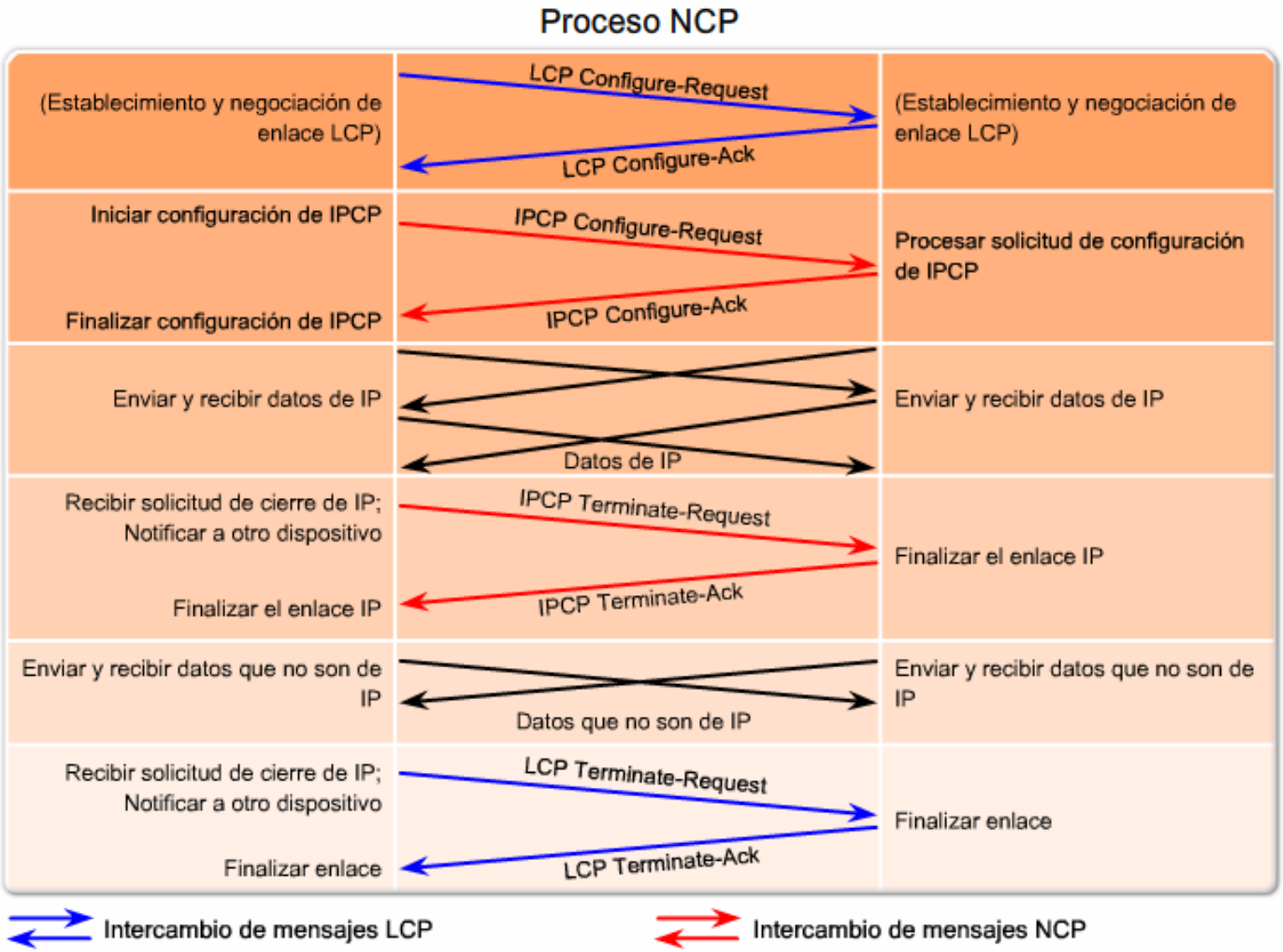
Establecimiento de una Sesión PPP

- Fase 2: Determinación de la calidad del enlace (Opcional)
  - LCP prueba el enlace para determinar si su calidad es suficiente para establecer los protocolos de capa de red.
  - LCP puede demorar la transmisión de la información del protocolo de capa de red hasta que esta fase se complete.
- Fase 3: Negociación del Protocolo de capa de Red.
  - Se envían paquetes NCP para escoger y configurar uno o más protocolos de capa de red, tal como IP.
  - Una vez que se han escogido los protocolos de red, los paquetes de cada protocolo pueden ser enviados.
  - Si LCP cierra la conexión, este informa a la capa de red para que esta tome las acciones apropiadas.

Proceso de negociación de enlace LCP

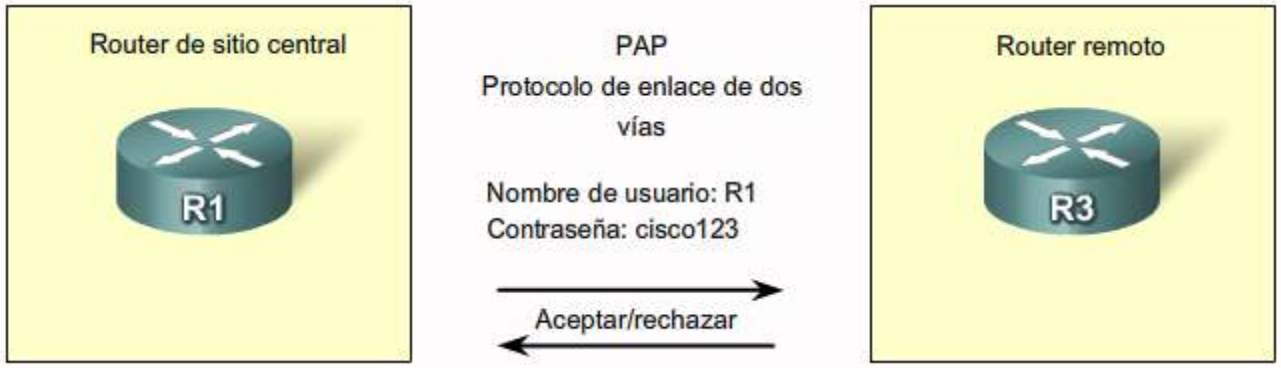


Proceso NCP



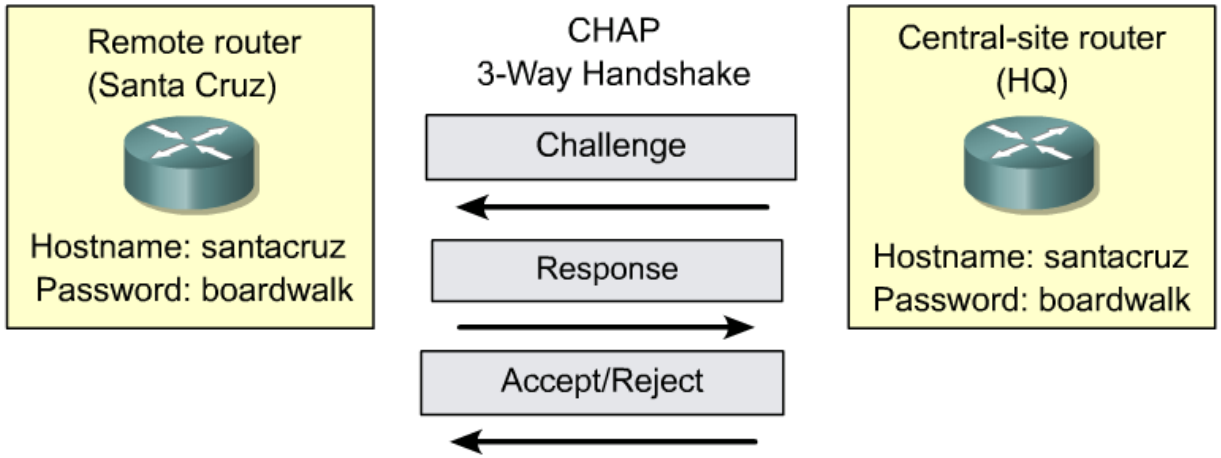
Protocolos de Autenticación de PPP

- **PAP (Password Authentication Protocol)**
  - Proceso de 2 vías para verificar la identidad.
  - Luego de la fase de establecimiento (Fase 1), el usuario y la contraseña se envían repetidamente hasta que se recibe un acuse de recibo o la conexión es terminada.
  - No hay cifrado. Usuario y contraseña se envían en texto plano y no hay método para prevenir ataques repetitivos de prueba y error.
  - **NO** es un protocolo seguro de autenticación.
  - El nodo remoto tiene el control de la frecuencia de los intentos de autenticación

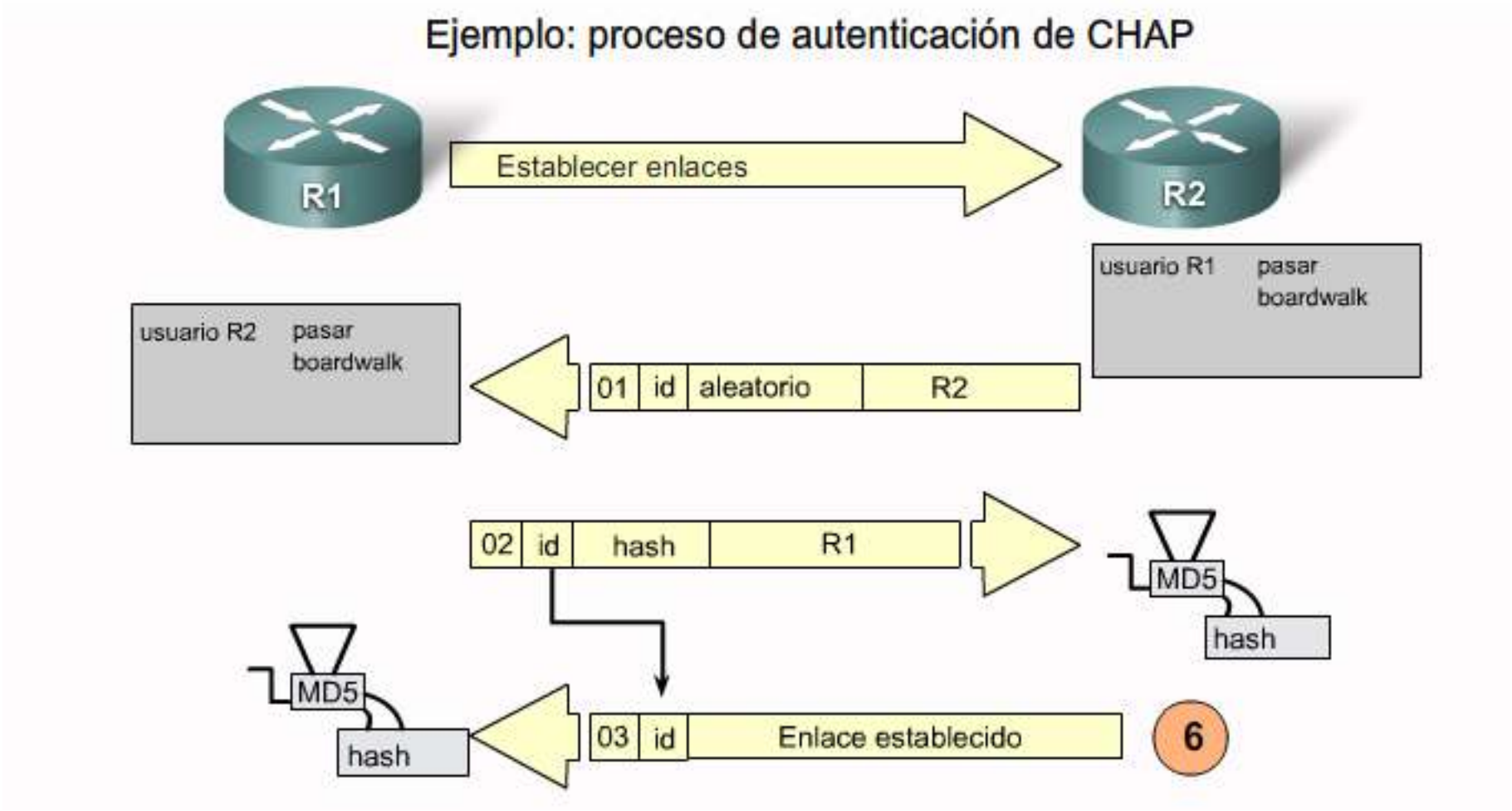


Protocolos de Autenticación de PPP

- **CHAP (Challenge Handshake Authentication Protocol)**
  - Es usado en la inicialización del enlace y periódicamente verifica la identidad del nodo remoto usando un intercambio de 3 vías.
  - Luego de la fase de establecimiento (Fase 1), el router local envía un mensaje de desafío (challenge) al host remoto.
  - El nodo remoto responde con un valor calculado con una función hash de una vía, normalmente Message Digest 5 (MD5).
  - La respuesta esta basada en la contraseña y el mensaje de desafío.
  - El router local revisa la respuesta contra su propio cálculo del valor hash esperado.
  - Si los valores concuerdan, hay acuse de recibo de la autenticación, de otra forma se termina inmediatamente la conexión.

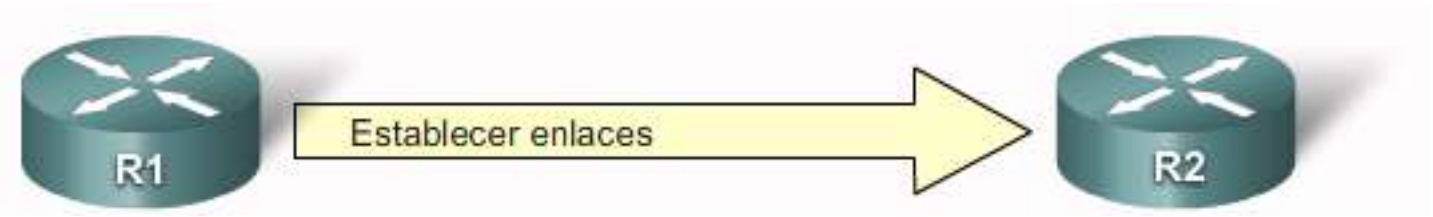


Operación de CHAP



LCP Establece y Negocia el enlace

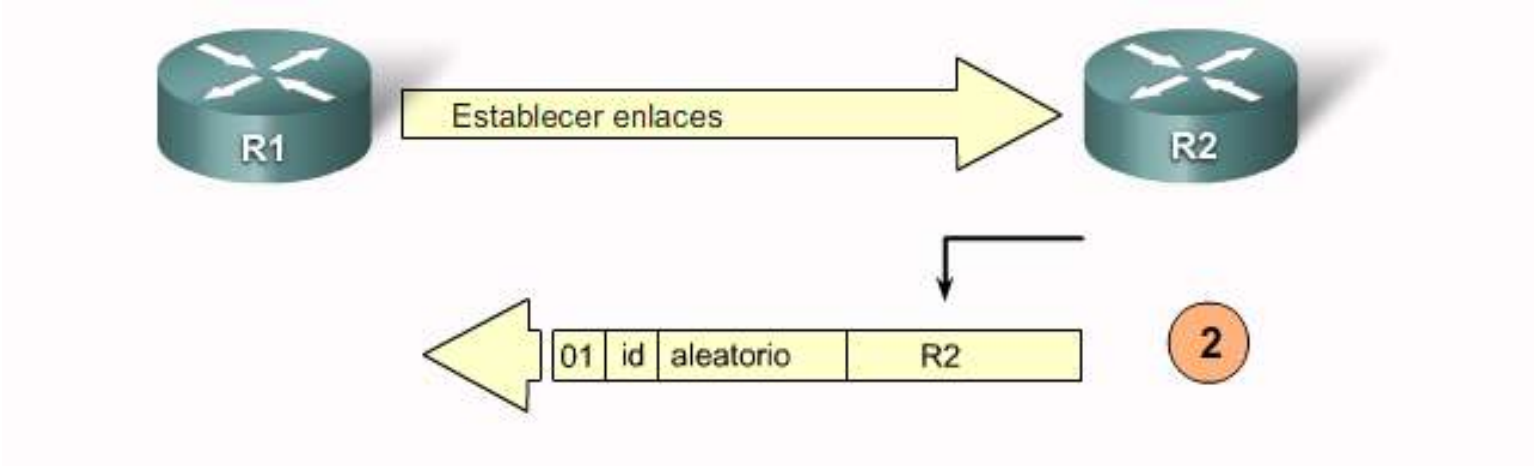
- La llamada entra R2. La interfaz entrante esta configurada con el comando *ppp authentication chap.*
- LCP negocia CHAP y MD5
- Un mensaje de desafio (Challenge) de R2 al router que llama es requerido en esta llamada



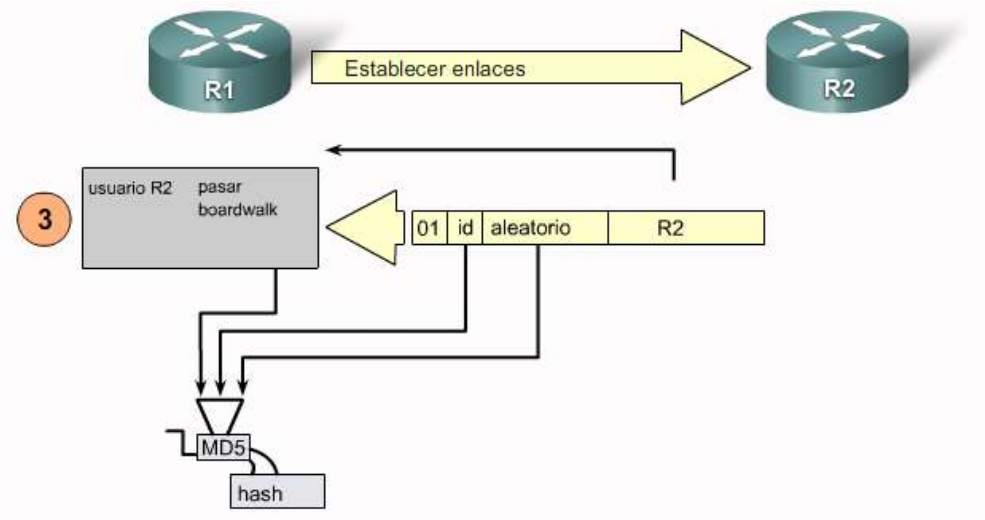
Desafío (Challenge) CHAP

- La figura ilustra lo siguiente:

1. Un paquete de desafío CHAP se crea con las siguientes caracteristicas:
   - 01 → Identificador del tipo de paquete de desafío.
   - id → Número secuencial que identifica el desafío.
   - aleatorio → Un número aleatorio generado por el router.
   - R2 → Nombre de autenticación del desafiador.
2. El id y aleatorio se guardan en el router al que llaman.
3. El paquete de desafío se envia al router que llama. Se mantiene una lista de los desafíos pendientes.



Recepción del mensaje de desafío (Challenge) CHAP



El router procesa el paquete de desafío entrante de la siguiente manera:

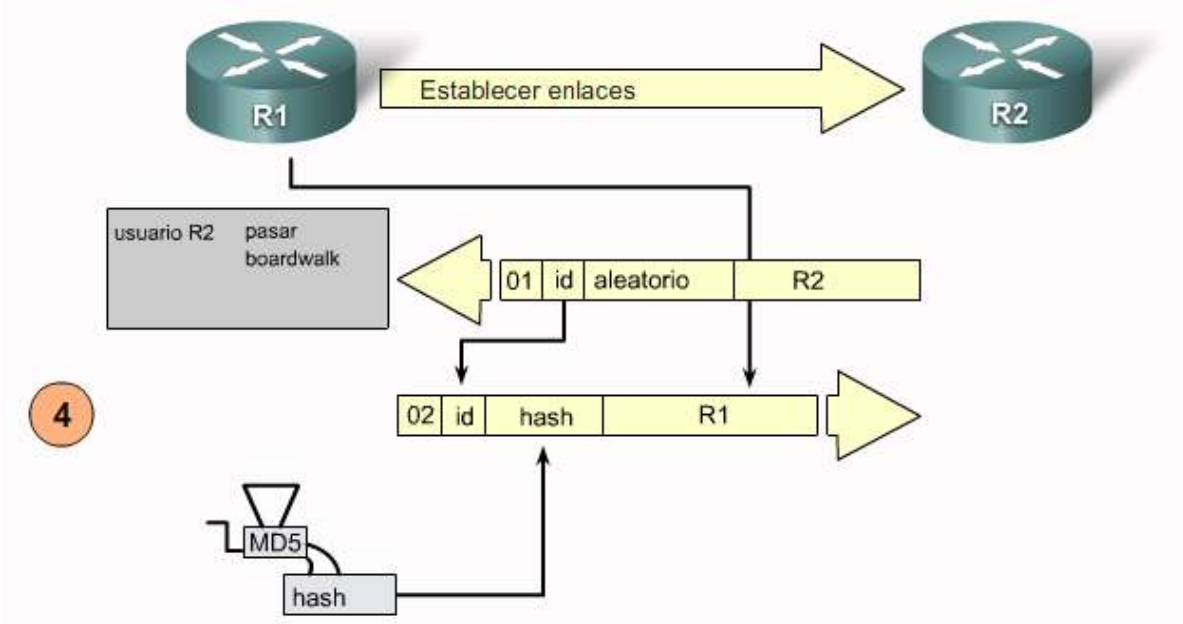
1. El valor de id se utiliza para alimentar el generador de hash MD5
2. El valor aleatorio se utiliza para alimentar el generador de hash MD5.
3. El nombre R2 se usa para buscar la contraseña. El router busca una entrada que coincida con el nombre de usuario del desafío. En el ejemplo busca por:

   username R2 password boardwalk
4. La contraseña se utiliza para alimentar el generador de hash MD5
5. El resultado es un valor hash MD5 que será enviado en la respuesta CHAP.

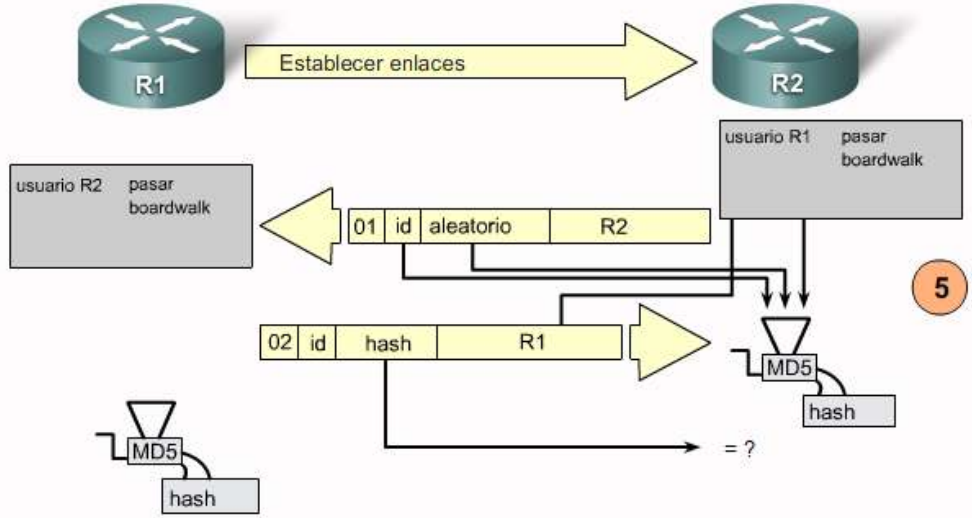
Respuesta (Response) CHAP

- La figura ilustra lo siguiente:

1. Un paquete de respuesta CHAP se crea con las siguientes caracteristicas:
   - 02 → Identificador del tipo de paquete de respuesta.
   - id → copiado del paquete de desafío.
   - hash → la salida del generador de hash MD5.
   - R1 → Nombre de autenticación del dispositivo. Necesario para que se pueda buscar la contraseña para verificar la identidad.
2. El paquete de respuesta se envía al desafiador.



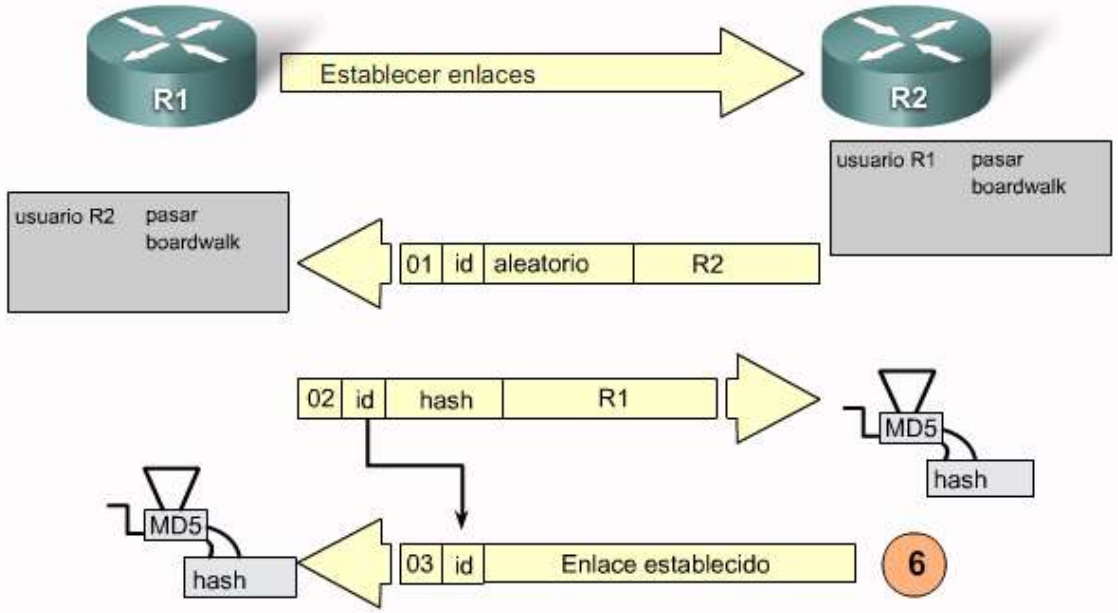
Recepción del mensaje de respuesta CHAP



El router procesa el paquete de desafío entrante de la siguiente manera:

1. El valor de id se utiliza para encontrar el paquete de desafío original.
2. El id alimenta el generador de hash MD5.
3. El valor original aleatorio se utiliza para alimentar el generador de hash MD5.
4. El nombre R1 se usa para buscar la contraseña en una de las siguientes fuentes:
   - Base de datos local de usuarios y contraseñas
     username R1 password boardwalk
   - Servidor RADIUS o TACACS+
5. La contraseña se utiliza para alimentar el generador de hash MD5
6. El valor de hash recibido se compara con el calculado a ver si son iguales.

Envío del mensaje de éxito/fallo CHAP



1. Si la autenticación fue exitosa, se crea un paquete CHAP de éxito con los siguientes componentes:
   - 03 → Identificador de tipo de mensaje de éxito
   - Id → copiado del paquete de respuesta
   - "Enlace establecido" → simplemente un mensaje legible
2. Si la autenticación falla, se crea un paquete CHAP de fallo con los siguientes componentes:
   - 04 → Identificador de tipo de mensaje de fallo
   - Id → copiado del paquete de respuesta
   - "Enlace fallido" → simplemente un mensaje legible
3. El paquete es enviado al router que llama.

Configuración de PPP

Configurar PPP en una Interfaz Serial

Comandos de configuración PPP

```
Router(config-if)#compress [predictor | stac]
```

Palabra clave	Descripción
Predictor	(Opcional) Especifica que se utilizará un algoritmo de compresión predictor.
Stac	(Opcional) Especifica que se utilizará un algoritmo de compresión Stacker (LZS).

```
Router(config-if)#ppp quality percentage
```

Palabra clave	Descripción
Porcentaje	Especifica el umbral de calidad del enlace. El rango es de 1 a 100.

Verificación de una configuración de encapsulación serial PPP

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:11
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
```

Configurar PPP en una Interfaz Serial

Práctica: Comandos de verificación y depuración

Descripción de	comandos
`show interfaces`	Muestra estadísticas para todas las interfaces configuradas en el router o servidor de acceso
`show interfaces serial`	Muestra información acerca de una interfaz serial
`debug ppp`	Depura PPP
`undebug all`	Desactiva todas las visualizaciones de depuración

Configurar PPP en una Interfaz Serial

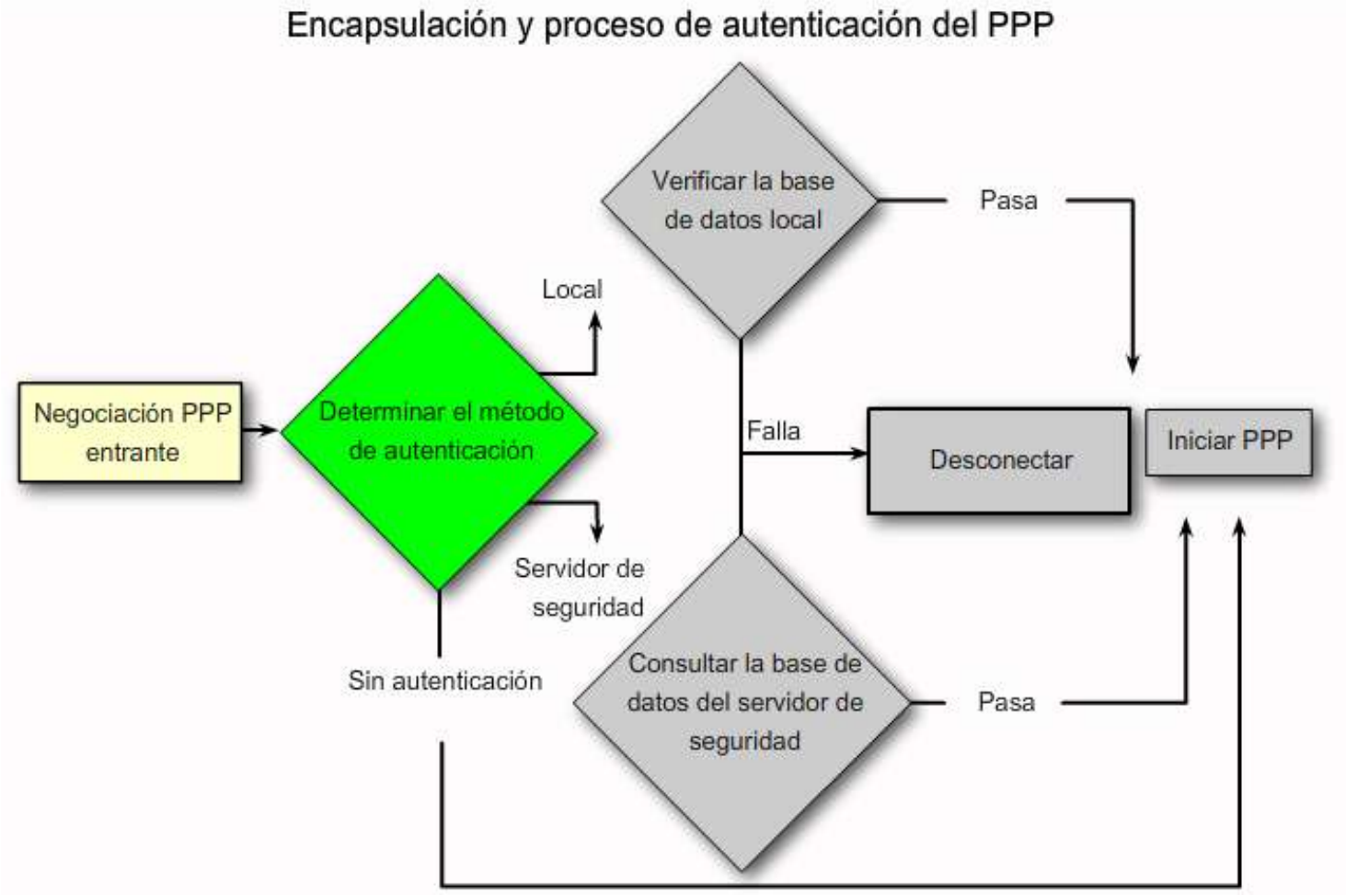
debug ppp Parámetros de comandos

```
debug ppp {packet | negotiation | error | authentication | compression |
           cbcp}
```

Parámetro	Uso
paquete	Muestra los paquetes PPP enviados y recibidos. (Este comando muestra las descargas de los paquetes de bajo nivel).
negociacin	Muestra los paquetes PPP enviados durante el inicio de PPP, cuando se negocian las opciones de PPP.
error	Muestra los errores de protocolo y las estadísticas de error relacionadas con la negociación y operación de la conexión PPP.
autenticacin	Muestra mensajes de protocolo de autenticación, incluidos los intercambios de paquetes del protocolo de autenticación de señales (CHAP, Challenge Authentication Protocol) y del protocolo de autenticación de contraseña (PAP, Password Authentication Protocol).
compresin	Muestra información específica para el intercambio de conexiones PPP mediante MPPC. Este comando es útil para obtener información sobre los números de secuencias de los paquetes incorrectos cuando la compresión MPPC se encuentra habilitada.
cbcp	Muestra los errores de protocolo y las estadísticas relacionadas con las negociaciones de conexión PPP mediante el uso de MSCB.

Configurar PPP con Autenticación

- Diagrama de flujo del proceso de autenticación



Configurar PPP con Autenticación

El comando `ppp authentication`

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

El comando ppp authentication	
chap	Habilita CHAP en una interfaz serial.
pap	Habilita PAP en una interfaz serial.
chap pap	Habilita CHAP y PAP y realiza la autenticación de CHAP antes que la de PAP.
pap chap	Habilita CHAP y PAP y realiza la autenticación de PAP antes que la de CHAP.
`if-needed` (opcional)	Usado con TACACS y XTACACS. No realice la autenticación CHAP o PAP si el usuario ya ha proporcionado la autenticación. Esta opción está disponible sólo en interfaces asíncronas.
`list-name` (opcional)	Usado con AAA/TACACS+. Especifica el nombre de una lista de métodos TACACS+ de nombre de lista auténtico, el sistema utiliza la opción predeterminada. Las listas se crean con el comando aaa **`authentication ppp`**.
`default` (opcional)	Usado con AAA/TACACS+. Creado con el comando **`aaa authentication ppp`**.
`callin`	Especifica la autenticación sólo en las llamadas entrantes (recibidas).

Configurar PPP con Autenticación

Resolución de problemas de una configuración PPP con autenticación

```
R2# debug ppp authentication

Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

Resumen

- PPP es un protocolo WAN utilizado ampliamente
- PPP provee conexiones LAN a WAN con múltiples protocolos
- Establecimiento de la sesión PPP – 4 fases

  Establecimiento del enlace

  Determinación de la calidad del enlace

  Negociación y configuración del protocolo de capa de red

  Terminación del enlace.
- Encapsulamiento WAN
  - HDLC (por defecto)
  - PPP

Resumen

- Autenticación PPP
  - PAP
    - Intercambio de 2 vías
  - CHAP
    - Intercambio de 3 vías
  - Use **debug ppp authentication** para confirmar la configuración de la autenticación
- Configuración de PPP
  - Se lleva a cabo en una interfaz serial
- Después de la configuración de PPP, use los comandos show de interfaces para mostrar:
  - Estado LCP
  - Estado NCP