TEMA 5

Protocolo de encapsulamiento punto a punto: PPP

Nivel de enlace en Internet

- El protocolo IP está diseñado para funcionar sobre casi cualquier medio físico (‘IP over everything’):

Medio	**RFC**	**Año**
X.25	877, 1356	1983
Ethernet	894	1984
802.x	1042	1988
FDDI	1188, 1390	1990
PPP	1171, 1663	1990
Frame Relay	1490	1993
ATM	1483, 1577	1994

PROTOCOLO PPP

- A finales de la década del ´80, el Protocolo Internet de enlace serial (SLIP) representaba una limitación para el crecimiento de Internet.
- PPP se creó para solucionar los problemas de conectividad remota de Internet.
- PPP era necesario para poder asignar direcciones IP de forma dinámica y permitir el uso de múltiples protocolos.
- PPP suministra conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos.

FUNCIONES OFRECIDAS POR PPP

- Control de la configuración del enlace de datos
- Proporciona asignación dinámica de direcciones IP
- Multiplexión de protocolo de red
- Configuración de enlace y verificación de la calidad del enlace
- Detección de errores
- Opciones de negociación para destrezas tales como negociación de la dirección de capa de red y negociaciones de compresión de datos

Funcionamiento de PPP

- Utiliza estructura de tramas tipo HDLC:

1	1	1	1 ó 2	Variable	2 ó 4	1
Delimitad. 01111110	Dirección 11111111	Control 00000011	Protocolo	Datos	CRC	Delimitad. 01111110

•La trama siempre tiene un número entero de bytes

•El campo dirección no se utiliza, siempre vale 11111111

•El campo control casi siempre vale 00000011, que especifica trama no numerada (funcionamiento sin ACK).

•Protocolo. Dos bytes que identifican el protocolo encapsulado en el campo de datos de la trama.

•Datos. Longitud máxima 1500 bytes. Contienen el datagrama del protocolo especificado en el campo protocolo.

•CRC. 2 bytes para control de errores.

•Generalmente en el inicio se negocia omitir los campos dirección y control

PPP (Point to Point Protocol)

- El protocolo de enlace ’característico’ de Internet es el PPP, que se utiliza en:
  - Líneas dedicadas punto a punto
  - Conexiones RTC analógicas o digitales (RDSI)
  - Conexiones de alta velocidad sobre enlaces SONET/SDH (redes ópticas)
- Puede funcionar de forma síncrona o asíncrona
- Es multiprotocolo, una comunicación soporta simultáneamente varios protocolos a nivel de red.

COMPONENTES BÁSICOS

PPP busca resolver los problemas de conectividad de Internet mediante tres componentes básicos:

1. Un **método para encapsular datagramas** a través de enlaces seriales. PPP utiliza el Control de enlace de datos de alto nivel (**HDLC**) como base para encapsular datagramas a través de enlaces punto a punto.
2. Un **Protocolo de control de enlace** (**LCP**) para establecer, configurar y probar la conexión de enlace de datos.
3. Una familia de **Protocolos de control de red** (**NCP**) para establecer y configurar distintos protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de capa de red. En la actualidad, PPP soporta otros protocolos además de IP, incluyendo Intercambio de paquetes de internetworking (IPX) y Appletalk. PPP utiliza su componente de NCP para encapsular múltiples protocolos.

LCP / NCP

LCP (Link Control Protocol) negocia parámetros del nivel de enlace en el inicio de la conexión para el establecimiento (supresión de campos dirección y control), configuración y chequeo (para determinar la calidad del enlace), mediante 3 clases de tramas:

a) Establecimiento para establecer y configurar el enlace

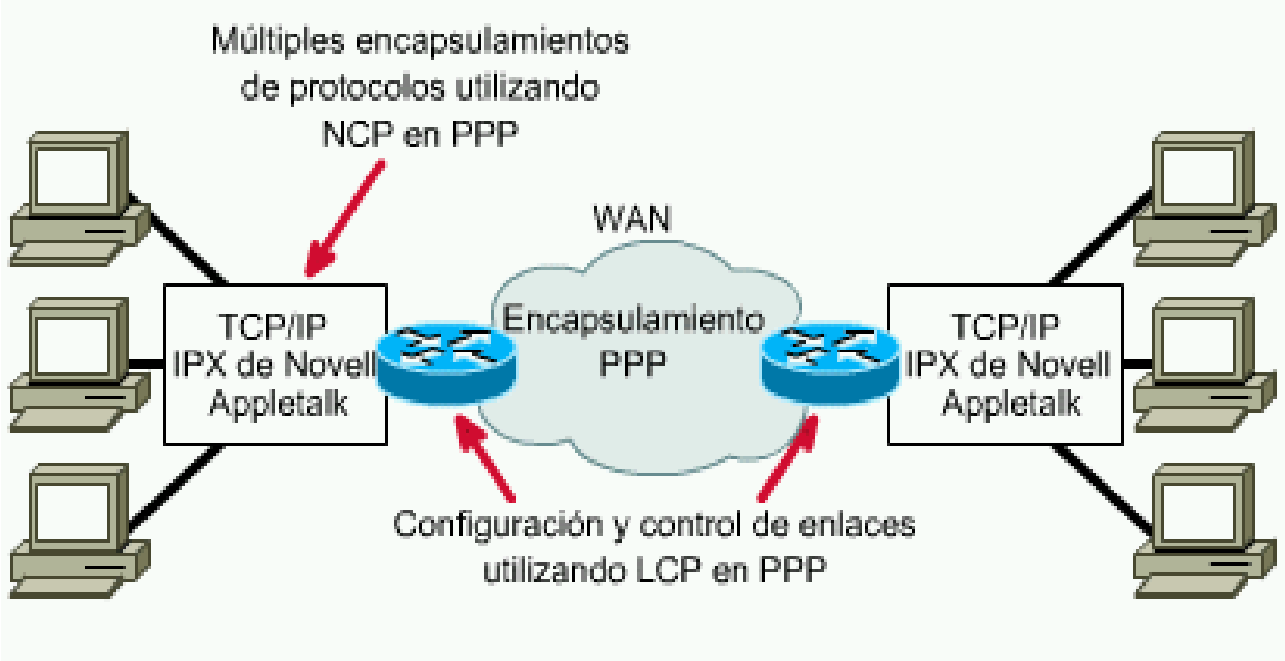
b) Finalización para finalización o cierre de conexión por Time Out, pérdida de portadora, etc

c) Mantenimiento del enlace, errores, etc (Testeo del enlace)

NCP (Network Control Protocol) que permite la negociación opcional de parámetros de configuración y opciones para encapsular multiprotocolos, permitiendo entre ellos la asignación dinámica de dirección IP

CLASES DE TRAMAS LCP

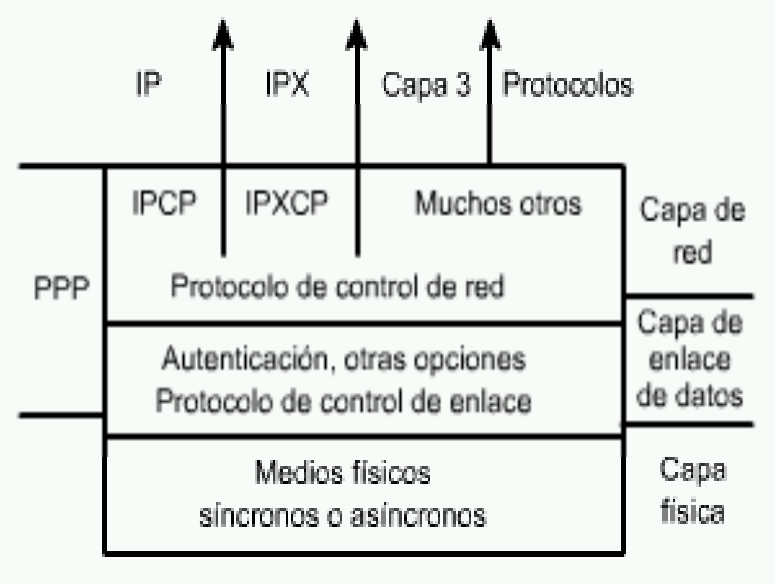
- Tramas de establecimiento de enlace: Se utilizan para establecer y configurar un enlace.
- Tramas de terminación del enlace: Se utilizan para terminar un enlace.
- Tramas de mantenimiento del enlace: Se utilizan para administrar y depurar un enlace.



- PPP puede transportar paquetes de varios protocolos
- PPP controla el ajuste de varias opciones de enlace

➔PPP proporciona confiabilidad en las conexiones

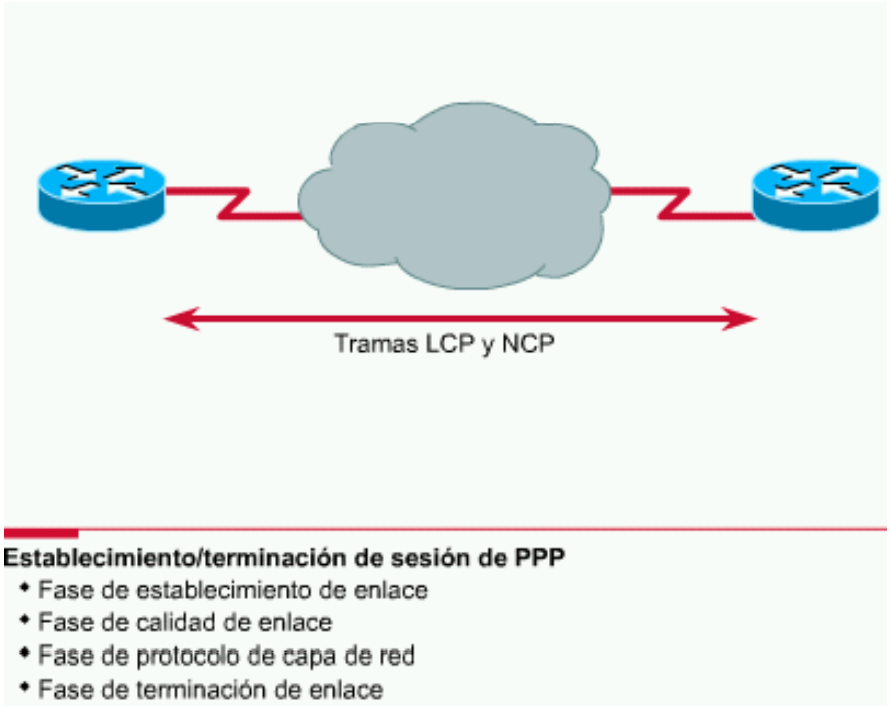
Funciones de capa PPP



PPP utiliza una arquitectura dividida en capas, como se indica en la figura.

- Con sus funciones de nivel inferior, PPP puede utilizar:
  - Medios físicos síncronos, como los que conectan las redes de la Red digital de servicios integrados (RDSI).
  - Medios físicos asíncronos, como los que utilizan el servicio telefónico básico para las conexiones de acceso telefónico del módem.
- Mediante sus funciones de nivel superior, PPP soporta o encapsula varios protocolos de capa de red con los NCP. Estos protocolos de nivel superior incluyen los siguientes:
  - BCP - Protocolo de control de puente
  - IPCP - Protocolo de control de protocolo Internet
  - IPXCP - Protocolo de control de intercambio de paquetes de internetworking

Negociación de los enlaces PPP



FASES

1.Establecimiento del enlace *(Abre conexión remota y negocia como se enviarán los datos a través de esa ruta: MTU (máxima unidad de transferencia), compresión de algunos campos de las tramas (como campos de dirección y control), protocolo de autentificación de enlace, etc)*

2.Chequeo del enlace para determinar la calidad (opcional)

3.Config. del protocolo capa red: IP, IPX. Datos.

4.Terminación *(Normal por LCP o por evento físico como pérdida de señal de portadora etc)*

NOTA: el proceso de negociación se observa con **show interfaces**

Fase 1: de establecimiento del enlace y negociación de la configuración

- En esta fase cada dispositivo PPP envía paquetes LCP para configurar y establecer el enlace de datos. Los paquetes LCP contienen un campo de opción de configuración que permite que los dispositivos negocien el uso de opciones, como la unidad máxima de transmisión (MTU), la compresión de determinados campos PPP y el protocolo de autenticación de enlace. Si no se incluye ninguna opción de configuración en un paquete LCP, se adopta el valor por defecto para esa configuración. Antes de que se pueda intercambiar cualquier datagrama de capa de red (por ejemplo, IP), LCP primero debe abrir la conexión y negociar los parámetros de configuración. Esta fase se completa cuando se ha enviado y recibido una trama de acuse de recibo de configuración.

Fase 2: Determinación de la calidad de enlace

- LCP permite una fase opcional de determinación de la calidad del enlace a continuación de la fase de establecimiento del enlace y negociación de la configuración. En la fase de determinación de la calidad del enlace, el enlace se prueba para determinar si la calidad del enlace es lo suficientemente buena como para establecer los protocolos de capa de red. Además, una vez que se ha establecido el enlace y que se ha elegido el protocolo de autentificación, se puede autentificar la estación de trabajo del cliente o usuario. La autentificación, en caso de que se utilice, se lleva a cabo antes de que comience la fase de configuración del protocolo de la capa de red. LCP puede retardar la transmisión de la información del protocolo de capa de red hasta que esta fase se haya completado.
- PPP soporta dos protocolos de autenticación: Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación de saludo (CHAP). Ambos protocolos se describen en detalle en RFC 1334, "Protocolos de autentificación PPP".

FASE 3: Negociación de la configuración del protocolo de la capa de red

- Cuando LCP finaliza la fase de determinación de la calidad del enlace, los protocolos de capa de red pueden ser configurados individualmente por el NCP adecuado y se pueden activar y desactivar en cualquier momento. En esta fase, los dispositivos PPP envían paquetes NCP para seleccionar y configurar uno o varios protocolos de capa de red (como IP). Cuando se ha configurado uno de los protocolos de capa de red elegidos, se pueden enviar datagramas desde cada uno de los protocolos de capa de red a través del enlace. Si LCP cierra el enlace, informa esto a los protocolos de la capa de red, para que puedan tomar las medidas adecuadas. Cuando PPP está configurado, puede verificar el estado de LCP y NCP mediante el comando **`show interfaces`**.

FASE 4: Terminación

- LCP puede terminar el enlace en cualquier momento. Esto generalmente se realiza a pedido del usuario, pero puede ocurrir debido a un suceso físico, como la pérdida de una portadora o la expiración de un límite de tiempo.

Mecanismos de autentificación: PAP y CHAP

Los dos protocolos que realizan tareas de autentificación de usuario son PAP y CHAP.

Mecanismos de autentificación: PAP

PAP(Password Authentication Protocol)

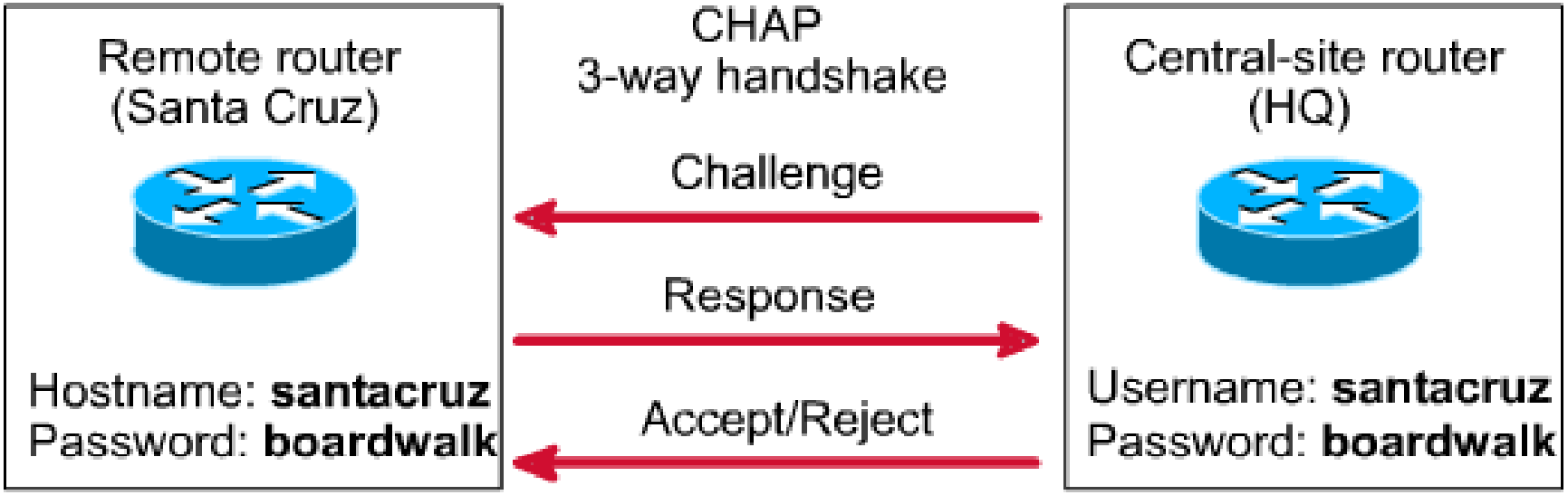
-Password/login se envían repetidamente hasta reconocerse.

-Texto claro

- No existe protección de la reproducción ni ataques repetidos de prueba y error
- El nodo remoto controla la frecuencia y el tiempo de los intentos de conexión

➔ **No constituye un método fuerte o rígido.**

Mecanismos de autentificación: CHAP



CHAP (Challenge Handshake Authentication Protocol):
R. local:envio mensaje "challenge" al nodo remoto.
Nodo remoto: responde con valor calculado con f. hash.
R. local:verifica la respuesta y compara con valor esperado. Coincidencia ➔ Autentificación confirmada.
-CHAP no permite al que realiza la llamada intentar la autenticación sin un desafío (challenge) previo
-El valor de "challenge" es único e impredecible, por lo que se proporciona protección frente a ataques
-Ofrece características como la verificación periódica para mejorar la seguridad (en PAP sólo se verifica una vez)
-El router local (o un servidor de autentificación) controla la frecuencia y la duración de los desafíos.

Ejemplo de configuración de PPP

(*ambos interfaces de la conexión serie deben tener el mismo encapsulamiento*)

En cada router, se define el nombre de usuario y la contraseña que espera el router remoto.

(config)# **username** *cliente* **password** *secreto*

!description, identifico el usuario a conectarse en el sistema remoto.

Ambos extremos tendrán la misma configuración.

cliente es el nombre de host del router remoto.

secreto debe de ser la misma en ambos routers.

(config)# int s0

(config-if)# **encapsulation ppp**

(config-if)# **ppp chap** password <secret>

!description: o se puede poner un ordenación de ellos:

(config-if)# **ppp authentication {pap|chap|pap chap|chap pap},** utilizando el orden preestablecido en su declaración y sujeto a negociación entre routers.

PAP esta desactivado por defecto por lo que para activarlo en la interfaz:

Router(config-if)# **ppp pap sent-username** *nombre-usuario* **password** *contraseña*

HDLC vs PPP

Ventajas de PPP:

1. mejor fiabilidad, por los mecanismos de mantenimiento del enlace, aunque ambos incorporen detección de errores con FCS (CRC)
2. es más estándar y puede utilizarse en todas las conexiones WAN, por ejemplo en T1, RDSI y conexiones de MODEM con enlace de datos síncronas y/o asíncronas. Además PPP es descrito en **RFC 1332 y RFC 1661**, mientras ***HDLC no***. Existe un campo de control en HDLC que difiere para cada fabricante, siendo por tanto propietario.
3. permite opcionalmente la seguridad y autentificación con los protocolos PAP (Password Authentication protocol, protocolo a 2 bandas en desuso) y/o CHAP en la parte del cliente (llamante)
4. por negociación de NCP permite múltiples protocolos como IP, con manejo de direcciones IP dinámicas e IPX. Permite la multiplexación por la identificación del campo de protocolo en las tramas PPP
5. implementa la negociación de compresión de datos

La única desventaja pueda ser un mayor uso de ancho de banda por temas administrativos, no para datos.