

U. T. N.
Facultad Regional La Plata

REDES DE INFORMACIÓN

Trabajo Final:

“PPP”
- Protocolo Punto a Punto -

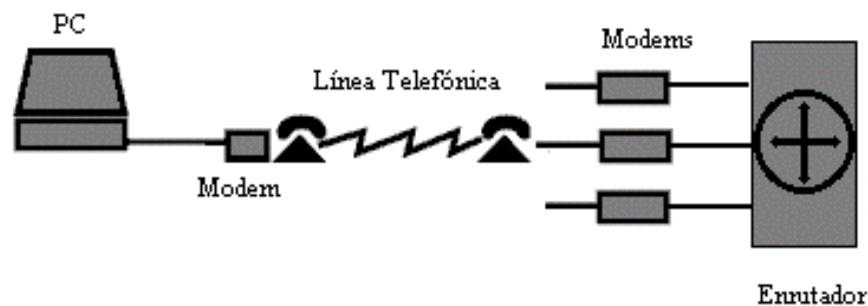
Noviembre de 1999

Autores: LÓPEZ, Oscar Raúl
SACCO, Antonio

INTRODUCCIÓN

La mayor parte de la infraestructura de redes de área extensa está construida a partir de líneas alquiladas punto a punto.

En la práctica, la comunicación punto a punto se utiliza de diferentes maneras. Actualmente, una de las formas más habituales de conectarse a Internet para un usuario común es a través de un módem y una línea telefónica. En general, la PC llama al *router* de su proveedor de Internet y así actúa como *host* de la Red. Este método de operación no es distinto a tener una línea arrendada entre la PC y el *router*, excepto que la conexión desaparece cuando el usuario termina la sesión. Este concepto se ilustra en la siguiente figura:



Tanto para la conexión por línea alquilada de *router* a *router* como para la conexión conmutada de *host* a *router* se requiere de un **protocolo** punto a punto de enlace de datos en la línea, para el manejo de marcos de control de errores y las demás funciones de la capa de enlace de datos.

Según nos acercamos al medio físico, la diversidad de los mismos provoca que existan varios protocolos a nivel de enlace de datos para adaptarse a las peculiaridades de cada medio físico.

Dos protocolos de este nivel utilizados ampliamente en Internet son **SLIP** (*Serial Line Internet Protocol*) y **PPP** (*Point to Point Protocol*).

Si bien el protocolo SLIP está específicamente diseñado para el transporte de tráfico TCP/IP, la tendencia actual es hacia el uso cada vez mayor del protocolo PPP, ya que también es apto para líneas telefónicas conmutadas, siempre que nuestro proveedor de Internet disponga de este protocolo para atender nuestra llamada.

Al utilizar SLIP, es necesario conocer tanto nuestra dirección IP como la de nuestro proveedor, lo que puede causarnos problemas en el caso de que este asigne dinámicamente las direcciones (algo muy común actualmente). Igualmente, existe la posibilidad de tener que configurar algunos parámetros como pueden ser la máxima unidad de transmisión (MTU), máxima unidad de recepción (MRU), el uso de cabeceras de compresión, etc.

El PPP fue desarrollado por el IETF (*Internet Engineering Task Force*) en 1993 para mejorar estas y algunas otras deficiencias, y crear un estándar internacional, por lo cual en este trabajo desarrollaremos principalmente el protocolo PPP, luego de lo que concluiremos con una breve comparación con su par (SLIP).

DESARROLLO

¿Para qué sirve el protocolo PPP?

El protocolo **PPP** proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos “pares” (a partir de aquí, y hasta el final de este trabajo, utilizaremos el término “par” para referirnos a cada una de las máquinas en los dos extremos del enlace -en inglés es *peer*-).

Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Tiene tres componentes:

1. Un mecanismo de enmarcado para encapsular datagramas multiprotocolo y manejar la detección de errores.
2. Un protocolo de control de enlace (**LCP**, *Link Control Protocol*) para establecer, configurar y probar la conexión de datos.
3. Una familia de protocolos de control de red (**NCPs**, *Network Control Protocols*) para establecer y configurar los distintos protocolos de nivel de red.

Funcionamiento general

Para dar un panorama inicial del funcionamiento de este protocolo en el caso comentado, en que un usuario de una PC quiera conectarse temporalmente a Internet, describiremos brevemente los pasos a seguir:

En primera instancia, la PC llama al *router* del **ISP** (*Internet Service Provider*, proveedor del servicio de Internet), a través de un módem conectado a la línea telefónica.

Una vez que el módem del *router* ha contestado el teléfono y se ha establecido una conexión física, la PC manda al *router* una serie de paquetes LCP en el campo de datos de uno o más marcos PPP (esto será explicado con mayor detalle más adelante). Estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.

Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.

Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.

En este momento la PC ya es un *host* de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP.

Luego se usa LCP para cancelar la conexión de la capa de enlace de datos.

Finalmente la computadora indica al módem que cuelgue el teléfono, liberando la conexión de la capa física.

PPP puede utilizarse no solo a través de líneas telefónicas de discado, sino que también pueden emplearse a través de SONET o de líneas HDLC orientadas a bits.

Configuración básica

Los enlaces PPP son fáciles de configurar. El estándar por defecto maneja todas las configuraciones simples. Se pueden especificar mejoras en la configuración por defecto, las cuales son automáticamente comunicadas al “par” sin la intervención del operador. Finalmente, el operador puede configurar explícitamente las opciones para el enlace, lo cual lo habilita para operar en ambientes donde de otra manera sería imposible.

Esta auto-configuración es implementada a través de un mecanismo de negociación de opciones extensible en el cual cada extremo del enlace describe al otro sus capacidades y requerimientos.

Entramado

La encapsulación PPP provee multiplexamiento de diferentes protocolos de la capa de red sobre el mismo enlace. Ha sido diseñada cuidadosamente para mantener compatibilidad con el hardware mayormente usado.

Sólo son necesarios 8 bytes adicionales para formar la encapsulación cuando se usa dentro del entramado por defecto. En ambientes con escaso ancho de banda, la encapsulación y el entramado pueden requerir menos bytes.

El formato de la trama completa es:

Indicador (1 byte)	Dirección (1 byte)	Control (1 byte)	Protocolo (1 o 2 bytes)	Información (variable)	Suma (2 o 4 bytes)	Indicador (1 byte)
-----------------------	-----------------------	---------------------	----------------------------	---------------------------	-----------------------	-----------------------

Todas las tramas comienzan con el byte **indicador** “01111110”. Luego viene el campo **dirección**, al que siempre se asigna el valor “11111111”. La dirección va seguida del campo de **control**, cuyo valor predeterminado es “00000011”. Este valor indica un marco sin número ya que PPP no proporciona por omisión transmisión confiable (usando números de secuencia y acuses) pero en ambientes ruidosos se puede usar un modo numerado para transmisión confiable. El anteúltimo campo es el de **suma de comprobación**, que normalmente es de 2 bytes, pero puede negociarse una suma de 4 bytes. La trama finaliza con otro byte **indicador** “01111110”.

Debido a que los campos indicados anteriormente son utilizados para encapsular la información fundamental del protocolo, desde ahora nos centraremos en el siguiente esquema:

Protocolo (1 o 2 bytes)	Información (y relleno) (variable)
----------------------------	---------------------------------------

Campo protocolo

Este campo es de 1 o 2 bytes y su valor identifica el contenido del datagrama en el campo de **información** del paquete (cuando hablamos de “paquete” nos estamos refiriendo al marco de la capa de enlace, que es en la que opera el PPP; no debe confundirse con los de la capa de red, manejados por IP). El bit menos significativo del byte menos significativo debe ser 1 y el bit menos significativo del byte más significativo debe ser 0. Los marcos recibidos que no cumplan con estas reglas deben ser tratados como irreconocibles.

Los valores en el campo de protocolo dentro del rango de 0_{hex} a 3_{hex} identifican el protocolo de capa de red de los paquetes específicos, y valores en el rango de 8_{hex} a B_{hex} identifican paquetes pertenecientes al protocolo de control de red asociado (NCPs). Los valores en el campo de protocolo dentro del rango de 4_{hex} a 7_{hex} son usados para protocolos con bajo volumen de tráfico, los cuales no tienen asociados NCP. Valores en el rango de C_{hex} a F_{hex} identifican paquetes de los protocolos de control de la capa de enlace (como LCP).

Campo **información**

Puede tener 0 o más bytes. Contiene el datagrama para el protocolo especificado en el campo protocolo. La máxima longitud para este campo, incluyendo el **relleno** pero no incluyendo el campo de **protocolo**, es determinada por la unidad máxima de recepción (MRU), la cual es de 1500 bytes por defecto. Mediante negociaciones, PPP puede usar otros valores para la MRU.

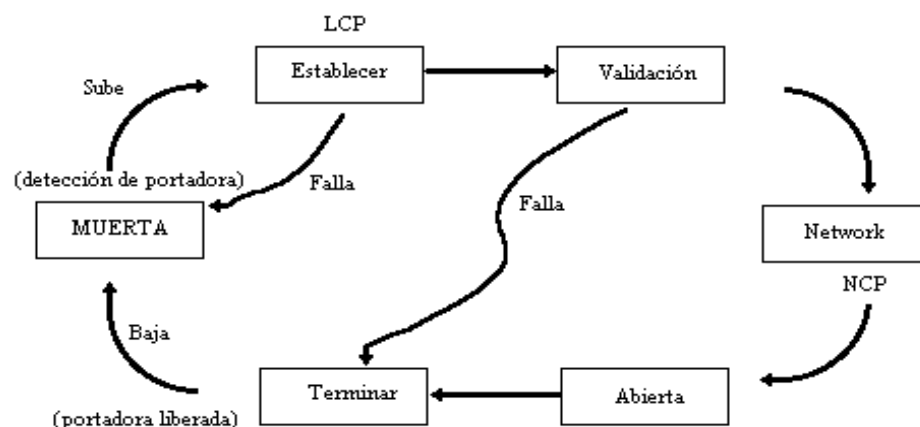
A la información se le puede agregar un **relleno**, con un número arbitrario de bytes, hasta llegar a la MRU.

Operación del PPP

Para establecer comunicaciones sobre un enlace punto a punto cada extremo del mismo debe enviar primero paquetes LCP para configurar y testear el enlace de datos. Después de que éste ha sido establecido, el “par” debe ser autenticado. Entonces, PPP debe enviar paquetes NCP para elegir y configurar uno o más protocolos de red. Una vez que han sido configurados cada uno de los protocolos de la capa de red elegidos, los datagramas de cada protocolo de capa de red pueden ser enviados a través del enlace. El enlace permanecerá configurado para la comunicación hasta que una serie de paquetes NCP o LCP cierren la conexión, o hasta que ocurra un evento externo (por ej., que un *timer* de inactividad expire o que se produzca una intervención del administrador de la red).

Fases de la operación

En la siguiente figura se muestran las fases por las que pasa una línea cuando es activada, usada y desactivada, a través del protocolo PPP. Esta secuencia se aplica tanto a las conexiones por módem como a las conexiones *router* a *router*.



Fase

El enlace comienza y termina necesariamente en esta fase. Cuando un evento externo (como una detección de portadora) indica que la capa física está lista para ser usada, PPP procederá con la fase de **establecimiento del enlace**.

Típicamente, si se utiliza un módem, el enlace volverá a esta fase automáticamente después de la desconexión del mismo. En el caso de un enlace *hard-wired* esta fase puede ser extremadamente corta, tan solo hasta detectar la presencia del dispositivo.

Fase de **establecimiento del enlace**

El protocolo de control de enlace (LCP) es usado para establecer la conexión a través de un intercambio de paquetes de configuración. Este intercambio está completo y se ingresa en el estado abierto de LCP una vez que un paquete de “reconocimiento de configuración” ha sido enviado y recibido por ambos.

Todas las opciones de configuración son asumidas con sus valores por defecto a menos que sean alteradas por un intercambio de paquetes de configuración.

Es importante notar que solo las opciones de configuración que son independientes de cada protocolo particular de capa de red son manejadas por el LCP. La configuración de los protocolos de capa de red individuales es manejada por separado por los protocolos de control de red (NCPs) durante la **fase de red**.

Cualquier paquete que no sea LCP recibido durante esta fase debe ser descartado.

Fase de **validación**

En algunos enlaces puede ser deseable solicitar al “par” que se autentifique a sí mismo antes de permitir el intercambio de paquetes del protocolo de capa de red.

Por defecto, la validación o autenticación no es obligatoria. Si una implementación desea que el “par” se autentifique con algún protocolo de validación específico, entonces ésta debe solicitar el uso del protocolo de autenticación durante la fase de **establecimiento del enlace**.

La autenticación debe tomar lugar tan pronto como sea posible después del **establecimiento del enlace**.

El progreso de la fase de autenticación a la fase de **red** no debe ocurrir hasta que la autenticación haya sido completada. Si ésta falla, el que realiza la autenticación debe proceder a la fase de **terminación del enlace**.

Durante esta fase, sólo son permitidos paquetes del protocolo de control de enlace, el protocolo de autenticación y el monitoreo de calidad de enlace. Cualquier otro paquete recibido debe ser descartado.

La autenticación debe proporcionar algún método de retransmisión, y se procederá a la fase de **terminación del enlace** sólo luego de que se ha excedido cierta cantidad de intentos de autenticación.

Fase de **red**

Una vez que el PPP finalizó las fases anteriores, cada protocolo de capa de red (como por ejemplo IP, IPX o AppleTalk) debe ser configurado separadamente por el protocolo de control de red (NCP) apropiado.

Cada NCP debe ser abierto y cerrado de a uno por vez.

Fase **abierta**

Una vez que un NCP ha alcanzado el estado abierto, PPP transportará los correspondientes paquetes del protocolo de capa de red. Cualquier paquete recibido mientras su NCP no esté en el estado abierto debe ser descartado.

Durante esta fase el tráfico del enlace consiste en cualquier combinación posible de paquetes LCP, NCP, y de protocolo de capa de red.

Fase de **terminación del enlace**

PPP puede terminar el enlace en cualquier momento. Esto puede ocurrir por la pérdida de la señal portadora, una falla de autenticación, una falla de la calidad del enlace, la expiración de un *timer*, o un cierre administrativo del enlace.

LCP es usado para cerrar el enlace a través de un intercambio de paquetes de “terminación”. Cuando el enlace ha sido cerrado, PPP informa a los protocolos de capa de red así ellos pueden tomar la acción apropiada.

Después del intercambio de paquetes de “terminación”, la implementación debe avisar a la capa física que desconecte la línea para forzar la terminación del enlace, particularmente en el caso de una falla de autenticación. El que envía una “solicitud de terminación” debe desconectarse después de recibir un “reconocimiento de terminación”, o después de que expire el *timer* correspondiente. El receptor de una “solicitud de terminación” debe esperar al “par” para desconectarse, y no lo debe hacer hasta que al menos haya pasado cierto tiempo de reiniciado después de enviar el “reconocimiento de terminación”. PPP procederá entonces con la fase de **enlace muerto**.

Cualquier paquete recibido durante esta fase que no sea LCP debe ser descartado. La clausura del enlace por LCP es suficiente. No es necesario que cada NCP envíe paquetes de terminación. A la inversa, el hecho de que un NCP sea cerrado no es razón suficiente para causar la terminación del enlace PPP, aún si ese NCP era el único actualmente en el estado abierto.

Negociación automática de opciones

La negociación de opciones es definida por eventos, acciones y transiciones de estados. Los eventos incluyen la recepción de comandos externos (como apertura y clausura), expiración de *timers*, y recepción de paquetes de un “par”. Las acciones incluyen el arranque de *timers* y la transmisión de paquetes al “par”.

Algunos tipos de paquetes (“no reconocimientos de configuración”, “rechazos de configuración”, “solicitudes de eco”, “respuestas de eco”, etc.) no son diferenciados aquí ya que producen siempre las mismas transiciones.

Estados

Algunos posibles estados son: “inicial” (la capa más baja no está disponible y no ha ocurrido una apertura), “*starting*” (ha sido iniciada una apertura pero la capa más baja aún no está disponible), “*closed*” (el enlace está disponible pero no ha ocurrido una apertura), etc.

Eventos

Las transiciones y las acciones en la negociación son causadas por eventos.

Algunos son: “*up*” (este evento ocurre cuando la capa más baja indica que está lista para transportar paquetes; típicamente es usado por los procesos de manejo y llamada de un módem, y también puede ser utilizado por el LCP para indicar a cada NCP que el enlace está entrando en la fase de red). Otro evento muy común es “*down*” (cuando la capa más baja indica que ya no está lista para transportar paquetes, este evento también es generalmente utilizado por un módem o por un LCP).

Acciones

Son causadas por eventos y habitualmente indican la transmisión de paquetes y/o el comienzo o parada de *timers*.

Algunas acciones son: “evento ilegal” (esto indica acerca de un evento que no puede ocurrir en una negociación implementada correctamente), “capa hacia arriba” (esta acción indica a las capas superiores que la negociación está entrando en estado “abierto”; típicamente es utilizada por el LCP para indicar el evento “*up*” a un NCP, por un protocolo de autenticación, o de calidad de enlace).

Prevención de ciclos

El PPP hace intento de evitar ciclos mientras se efectúa la negociación de opciones de configuración. De todas formas, el protocolo no garantiza que no ocurrirán ciclos. Como en cualquier negociación es posible configurar dos implementaciones PPP con políticas conflictivas que nunca converjan finalmente. También es posible configurar políticas que converjan, pero que se tomen un tiempo significativo para hacerlo.

Timers

Existen distintos tipos de *timers*. Por ejemplo, el “*timer* de reiniciado” es utilizado para controlar el tiempo de las transmisiones de solicitud de configuración y los paquetes de solicitud de terminación. La expiración de este *timer* causa un evento de “tiempo cumplido” y la retransmisión de la correspondiente “solicitud de configuración” o el paquete de “solicitud de terminación”. Este *timer* debe ser configurable, pero por defecto durará 3 segundos. Este tiempo está pensado para bajas velocidades, como las líneas telefónicas típicas.

Otro ejemplo de *timer* es el de “terminación máxima”, que es un contador de reiniciado requerido para las solicitudes de terminación. Indica el número de paquetes de “solicitudes de terminación” enviados sin recibir un “reconocimiento de terminación”. Debe ser configurable pero por defecto se establece en 2 transmisiones.

Protocolo de Control de Enlace (LCP)

El LCP es usado para acordar automáticamente las opciones del formato de encapsulación, los límites de manipulación de tamaño de paquete, detectar un enlace con ciclos, otros errores comunes por mala configuración, y terminar el enlace. Otras facilidades opcionales provistas son: autenticación de la identidad de los “pares” del

enlace, y determinación de cuándo el enlace está funcionando apropiadamente y cuándo está fallando.

Formato de los paquetes LCP

Hay tres clases de paquetes LCP:

1. Paquetes de configuración de enlace: usados para establecer y configurar el enlace (“solicitud de configuración”, “reconocimiento de configuración”, “no reconocimiento de configuración” y “rechazo de configuración”).
2. Paquetes de terminación de enlace: usados para terminar el enlace (“solicitud de terminación” y “reconocimiento de terminación”).
3. Paquetes de mantenimiento del enlace: usados para manejar y depurar el enlace (“rechazo de código”, “rechazo de protocolo”, “solicitud de eco”, “respuesta de eco”, “solicitud de descarte”).

Un paquete LCP es encapsulado en el campo de información PPP, donde el campo de protocolo PPP indica el tipo C021_{hex}.

Básicamente, el formato de un paquete del protocolo de control de enlace es el siguiente:

Código (1 byte)	Identificador (1 byte)	Longitud (2 bytes)	Datos (variable)
--------------------	---------------------------	-----------------------	---------------------

Campo **código**

Ocupa un byte y sirve para identificar el tipo de paquete LCP. Cuando se recibe un paquete con un campo de código desconocido, se transmite un paquete de “rechazo de código”.

Campo **identificador**

Es de un byte y ayuda en la comparación de las solicitudes y respuestas.

Campo **longitud**

Es de dos bytes e indica la longitud del paquete LCP, incluyendo los campos código, identificador, longitud y datos. La longitud no debe exceder la MRU del enlace. Los bytes fuera del rango del campo longitud son tratados como relleno e ignorados al ser recibidos.

Campo **datos**

Pueden ser 0 o más bytes, indicados por el campo longitud. El formato de los datos es determinado por el campo código.

A continuación describiremos brevemente los principales paquetes utilizados por el LCP:

Solicitud de configuración

Debe transmitirse para abrir una conexión. En el campo de datos se incluirán las opciones de configuración que el transmisor desee negociar (0 o más). Todas estas opciones son negociadas simultáneamente.

Reconocimiento de configuración

Si cada opción de configuración recibida en una “solicitud de configuración” es reconocible y sus valores son aceptables, la implementación receptora debe transmitir un paquete de “reconocimiento”. Estas opciones reconocidas no deberán ser modificadas luego. Las opciones reconocidas son enviadas en el área de datos del paquete simultáneamente.

No reconocimiento de configuración

Si cada opción de configuración es reconocible pero algunos valores no son aceptables, se debe transmitir un paquete de “no reconocimiento de configuración”. El campo de datos es completado sólo con las opciones no aceptadas de la “solicitud de configuración”.

Al recibir un paquete de “no reconocimiento”, el campo de identificación debe ser comparado con el de la última “solicitud de configuración”, y cuando se vuelva a enviar una “solicitud de configuración”, las opciones de la mismas deberán ser modificadas.

Rechazo de configuración

Este paquete será transmitido si se recibe una “solicitud de configuración” en la que algunas opciones no son reconocibles o aceptables para ser negociadas. El campo de datos es completado sólo con las opciones de configuración no aceptables.

Al recibir un “rechazo de configuración”, el campo identificador debe compararse con el de la última solicitud de configuración.

Solicitud de terminación y reconocimiento de terminación

Son utilizadas para terminar una conexión. Primero se debe transmitir una “solicitud de terminación”. Estas solicitudes se seguirán transmitiendo hasta recibir un “reconocimiento de terminación”, hasta que la capa inferior indique que se perdió la conexión, o hasta que se haya transmitido un cierto número de solicitudes al “par”.

El campo de datos puede contener 0 o más bytes, los cuales no son utilizados.

Rechazo de código

La recepción de un paquete LCP con un código desconocido indica que el “par” está operando con una versión diferente del protocolo. Esto debe ser reportado al transmisor del código desconocido por medio de un “rechazo de código”. Al recibir un paquete de este tipo acerca de un código que es fundamental para la versión utilizada del protocolo, se deberá reportar el problema y cesar la transmisión.

El campo de datos contiene una copia del paquete LCP que está siendo rechazado.

Rechazo de protocolo

La recepción de un paquete PPP con un campo de protocolo desconocido indica que el “par” está intentando usar un protocolo no soportado. Esto ocurre usualmente cuando el “par” intenta configurar un nuevo protocolo.

El campo de datos contiene en dos bytes el campo de protocolo PPP del paquete que está siendo rechazado y a continuación una copia del paquete rechazado.

Solicitud y respuesta de eco

Estos paquetes proveen al LCP de un mecanismo para detectar ciclos en la capa de enlace de datos, que puede ser utilizado en ambos sentidos. Es muy útil para ayudar en la depuración, la determinación de la calidad del enlace, de la performance y en varias funciones más.

Luego de recibir una “solicitud de eco” se debe transmitir la respuesta correspondiente.

El campo de datos contiene 4 bytes que son utilizados para enviar un número llamado “mágico”, que es utilizado para detectar enlaces con ciclos. A continuación puede ser transmitido cualquier valor binario elegido por el transmisor.

Solicitud de descarte

El LCP incluye estos paquetes para proveer un mecanismo de “hundimiento” de la capa de enlace de datos en el sentido desde el sitio local hacia el remoto. Este mecanismo se utiliza cuando se desea enviar paquetes para realizar alguna prueba, sin que el “par” realice ninguna acción en función de los mismos. Esto es útil para ayudar en la depuración, el testeo de performance y algunas otras funciones.

Los paquetes de “solicitudes de descarte” deben ser ignorados al ser recibidos.

Opciones de configuración de LCP

Estas opciones permiten la negociación o modificación de las características por defecto de un enlace punto a punto. Si no se incluyen opciones de configuración en un paquete de solicitud de configuración, se asumen los valores por defecto para las mismas. El permitir valores por defecto para cada opción otorga al enlace la capacidad de funcionar correctamente sin negociaciones, pero sin embargo sin alcanzar una performance óptima.

El formato de las opciones de configuración es el siguiente:

Tipo (1 byte)	Longitud (1 byte)	Datos (variable)
------------------	----------------------	---------------------

Campo tipo

Este campo es de 1 byte e indica el tipo de la opción de configuración.

Los valores posibles son: 0 (reservado), 1 (MRU), 3 (protocolo de autenticación), 4 (protocolo de calidad), 5 (número “mágico”), 7 (compresión del campo de protocolo) y 8 (compresión de los campos de dirección y control). Por supuesto, los valores que acabamos de indicar deben transmitirse en binario.

Campo *longitud*

Es de 1 byte e indica la longitud del paquete, incluyendo los campos tipo, longitud y datos.

Campo *datos*

Puede ser de 0 o más bytes, y contiene la información específica de cada opción a configurar. El formato y la longitud del campo de datos son determinados por los campos de tipo y longitud.

Protocolos de Control de Red (NCP)

Los enlaces punto a punto tienden a agravar muchos problemas con la familia actual de protocolos de red. Por ejemplo, la asignación y manejo de direcciones IP es especialmente difícil sobre circuitos conmutados de enlaces punto a punto (como los utilizados por los módems).

Estos problemas son manejados por una familia de protocolos de control de red (NCPs), cada uno de los cuales maneja las necesidades específicas requeridas por sus respectivos protocolos de la capa de red, por lo cual su definición detallada es tratada en forma separada de los documentos correspondientes al PPP.

COMPARACIÓN ENTRE PPP Y SLIP

Además de los aspectos comentados en la “Introducción” y las diferencias que se desprenden de la sección de “Desarrollo”, a continuación enumeraremos en una tabla, y a modo de resumen, algunas de las principales diferencias entre los protocolos PPP y SLIP.

SLIP	PPP
Fácil de implementar.	Más complejo.
Adiciona muy pocos bytes de <i>overhead</i>	Mayor <i>overhead</i>
No es un estándar aprobado de Internet	Estándar de facto
No efectúa detección ni corrección de errores.	Suma de verificación (CRC) en cada marco según entramado.
Solo reconoce IP	Múltiples protocolos
Debe conocerse la dirección IP de cada extremo.	Permite la asignación dinámica de direcciones IP.
No proporciona verificación de autenticidad	Proporciona verificación de autenticidad
Estático	Configurable a través de LCP.

BIBLIOGRAFÍA

- “The Point-to-Point Protocol (PPP)”, Request for Comments 1661, July 1994, W. Simpson.
- “PPP LCP Extensions”, Request for Comments 1570, January 1994, W. Simpson.
- “PPP LCP Internationalization Configuration Option”, Request for Comments 2484, January 1999, G. Zorn.
- “PPP white paper”, Morning Star Technologies.
- “Redes de computadores”, 1997, Tanenbaum, Andrew S.
- Diversos documentos obtenidos en Internet.

Nota: debido a que utilizamos documentos RFC originales, los mismos estaban en idioma inglés, por lo cual podría ser posible que hayamos cometido un pequeño error al escribir algún término técnico.