PPP

Protocolo Punto a Punto

Universidad Adventista
de Centro América

PPP

Telemática y Redes

Seth Villarreal

Impreso en Costa Rica
en los Talleres de Imprenta Grafos de
CETEBEDI, S. A.

Trabajo realizado el
22 noviembre del 2000

Indice

INTRODUCCIÓN

Protocolo de intercambio, en informática, como en las relaciones humanas, señal mediante la cual se reconoce que puede tener lugar la comunicación o la transferencia de información. Los protocolos de intercambio se pueden controlar tanto con *hardware* como con *software*. Un protocolo de intercambio de *hardware,* como el existente entre un ordenador o computadora con una impresora o con un módem, es un intercambio de señales, a través de cables específicos, en el que cada dispositivo señala su disposición para enviar o recibir datos. Un protocolo de *software*, normalmente el que se intercambia durante las comunicaciones del tipo módem a módem, consiste en una determinada información transmitida entre los dispositivos de envío y de recepción. Un protocolo de intercambio de *software* establece un acuerdo entre los dispositivos sobre los protocolos que ambos utilizarán al comunicarse. Un protocolo de intercambio de *hardware* es por tanto similar a dos personas que físicamente estrechan sus manos, mientras que un protocolo de intercambio de *software* es más parecido a dos grupos que deciden conversar en un lenguaje particular.

Comunicación de datos, intercambio de información entre computadoras. Sin apenas excepción alguna, los ordenadores modernos se basan en el concepto de dígitos binarios, denominados bits, que sólo pueden adoptar los valores 0 o 1. Todos los datos almacenados y procesados por una computadora tienen la forma de bits, por lo que la transferencia de datos entre máquinas implica enviar bits de un lado a otro. En principio resulta muy sencillo, ya que la señal está presente o ausente; por ejemplo, no existen los matices de tono y volumen que se aprecian en la comunicación de voz. En la práctica, sin embargo, las comunicaciones de datos son más complejas de lo que parecen. Una secuencia de dígitos enviados desde un ordenador debe volverse a transformar en una información significativa con independencia del retardo, ruido y corrupción que sufra en el trayecto.

Redes de datos

La comunicación entre computadoras siempre implica la transferencia de datos en bloques, en lugar de secuencias continuas de datos. Esto se traduce en que no hace falta una conexión permanente entre dos ordenadores o computadoras para intercambiar datos. A diferencia de las personas, pueden funcionar con un enlace que exista sólo de forma parcial durante el diálogo. Esto significa que hay alternativas para la comunicación de datos inviables en las llamadas normales de teléfono.

La comunicación de datos utiliza una técnica denominada conmutación de paquetes, que aprovecha la posibilidad de transferir bloques de datos entre terminales sin establecer una conexión punto a punto. Por el contrario, se transmiten de enlace a enlace, quedando almacenados temporalmente y en espera de ser transmitidos cuando se establece el correspondiente enlace. Las decisiones sobre su destino se toman basándose en la información de direccionamiento contenida en la "cabecera" que va al principio de cada bloque de datos. El término "paquete" abarca la cabecera más el bloque de datos. Este tipo de conexión suele ser más eficaz que un enlace punto a punto entre ambas partes, mantenida hasta el final de la comunicación. En la práctica, un mismo enlace físico puede ser compartido por más de un usuario, gracias a una técnica llamada multiplexación. El precio a pagar por el mayor rendimiento es el retraso que sufren algunos paquetes.

Protocolos

Son conjuntos de normas para el intercambio de información, consensuadas por las partes comunicantes. En términos informáticos, un protocolo es una normativa necesaria de actuación para que los datos enviados se reciban de forma adecuada.

Hay protocolos de muy diversos tipos. Unos se ocupan de aspectos bastantes primarios como por ejemplo, el de asegurar que el orden de los paquetes recibidos concuerda con el de emisión. A un nivel algo superior hay protocolos para garantizar que los datos enviados por una computadora se visualicen correctamente en el equipo receptor.

La informática moderna utiliza muchos protocolos distintos. La norma publicada por la International Standards Organization y conocida como "modelo de 7 niveles", recoge la estructura general común a todos ellos. La totalidad de los aspectos contemplados en la comunicación entre ordenadores queda clasificada en siete niveles. La idea es que los protocolos concretos desarrollados en cada uno de los niveles puedan entenderse para conseguir una comunicación eficaz. De forma resumida, la función de cada uno de los niveles es la siguiente:

Nivel 1: Físico

Se refiere a la forma de transmitir cada 0 y 1 que conforman toda información digital que viaja de un punto a otro. Esto incluye la definición de un 1 y un 0 en cuanto a señales eléctricas.

Nivel 2: Enlace

Describe la forma de transportar de manera fiable los bits desde un nodo a otro en una red conmutada. Define conceptos tales como tramas, detección y corrección de errores y control de flujo.

Nivel 3: Red

Se centra en el establecimiento de una conexión punto a punto entre cliente y servidor. Es el nivel en el que se trata, por ejemplo, el direccionamiento y encauzamiento global.

Nivel 4: Transporte

Es el primero de los niveles encargados del funcionamiento punto a punto. Se ocupa del formato y su misión es asegurar que una secuencia recibida de bits se transforme en datos significativos. Este nivel supone la existencia previa de una conexión fiable.

Nivel 5: Sesión

Es el encargado de la diferenciación y control del diálogo para las aplicaciones que lo precisan. En el caso de la mayoría de las modernas aplicaciones informáticas (que se hallan divididas en componentes cliente y servidor), este nivel constituye un elemento inherente del propio diseño.

Nivel 6: Presentación

Proporciona un mecanismo de negociación de los formatos de representación (conocidos como sintaxis de transferencia) para un determinado contenido del mensaje.

Nivel 7: Aplicación

Recoge el resto de las necesarias funciones dependientes de la aplicación.

Hay, en la práctica, otras muchas formas de estructurar y llevar a cabo las necesarias comprobaciones para que una computadora pueda dialogar con otra. El modelo de siete niveles constituye sin embargo un modelo útil y se utiliza con carácter general, especialmente en los niveles inferiores, cuyos protocolos son de normas más estables.

Errores

Las personas tienen una gran capacidad para compensar los errores sufridos por los datos transmitidos. Es posible mantener una conversación entre dos individuos aun cuando sólo llegue intacto un 30% de los datos. Los ordenadores están en el otro extremo del espectro. Un único error de transmisión puede echar por tierra todo un diálogo. Por tal razón, la comprobación y prevención de errores constituye un requisito básico de cualquier tipo de comunicación de datos.

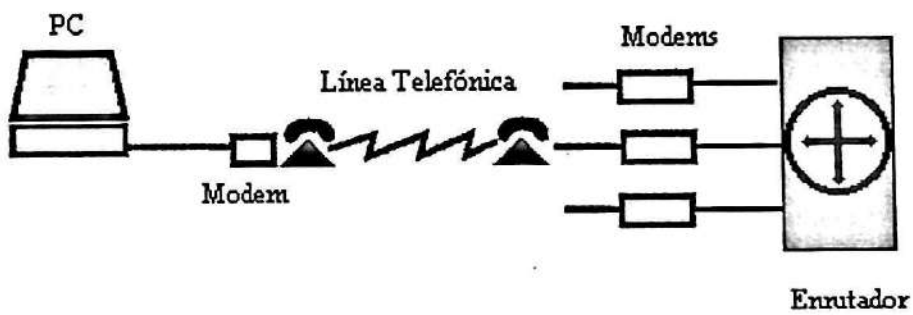
La protección contra los errores suele efectuarse añadiendo bits adicionales a los paquetes que contienen los datos a transferir. Alrededor del 4% de los bits en un paquete de datos se dedican a la detección de errores. El método más sencillo de aprovechar estos bits es fijar un bit de paridad, un

único dígito que se coloca para que la suma de una determinada secuencia de bits sea 1 o 0. Es una forma muy eficaz de detectar errores de bits aislados, pero no sirve cuando hay errores que afectan a 2 (o 4) bits.

Normalmente se utilizan otras técnicas más depuradas conocidas como sumas de control. Se fundamentan en complejos cálculos matemáticos y resultan eficaces para detectar diferentes tipos de errores. Más enrevesadas resultan las técnicas de corrección de errores, que suelen precisar un porcentaje mayor de bits, pero que son capaces de corregir realmente errores de transmisión eliminando la necesidad de retransmitir paquetes enteros por culpa de un único bit.[1]

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.

---

[1] "Comunicación de datos", *Enciclopedia Microsoft® Encarta® 99.* © 1993-1998 Microsoft Corporation. Reservados todos los derechos.

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).

¿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 0hex a 3hex identifican el protocolo de capa de red de los paquetes específicos, y valores en el rango de 8hex a Bhex identifican paquetes pertenecientes al protocolo de control de red asociado (NCPs). Los valores en el campo de protocolo dentro del rango de 4hex a 7hex son usados para protocolos con bajo volumen de tráfico, los cuales no tienen asociados NCP. Valores en el rango de Chex a Fhex 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.

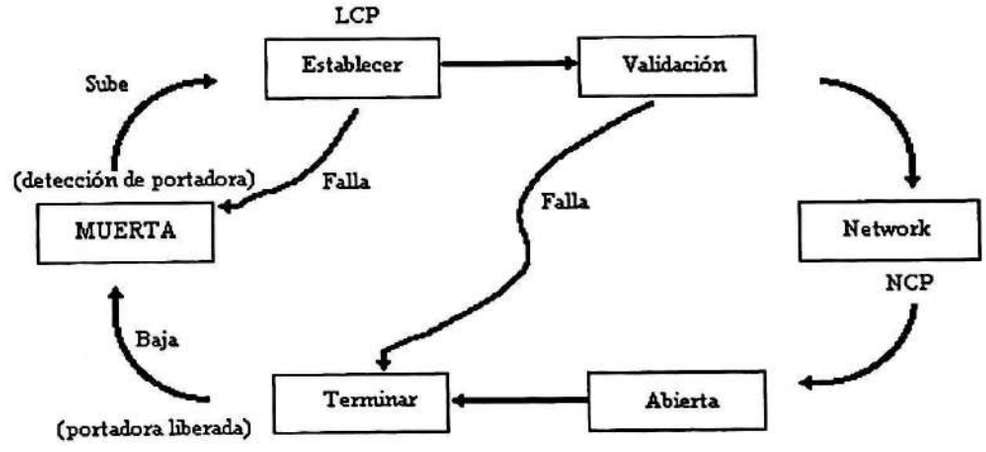
A la información se le puede agregar un **relleno**, con un número arbitrario de bytes, hasta llegar a la MRU.

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 autentificado. 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 de enlace muerto (capa física no lista)

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 intenta 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 C021hex.

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 dificultosa 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.

PPTP Protocolo Túnel Punto-a-punto

Estado de este Memorando

Este documento es un Internet-proyecto. Los Internet-proyectos están trabajando documentos del Internet Engineering la Fuerza de la Tarea (IETF), sus áreas, y sus grupos del funcionamiento. Note que ese otros grupos también pueden distribuir trabajando documentos como Internet-proyectos.

Los Internet-proyectos son documentos del proyecto válido para un máximo de seis meses y puede ponerse al día, reemplazó, o obsoleted por otros documentos a cualquiera tiempo. Es impropio usar Internet-proyectos como referencia material o para citarlos otra cosa que como "trabaje en marcha."

Lo abstracto

Este documento especifica un Protocolo Punto a Punto (PPP) para ser socavado a través de un IP red. PPTP no especifica ningún cambio al PPP protocolo sino describe un nuevo vehículo por llevar PPP. Una arquitectura del cliente-servidor se define en orden a la funciona que existe en Acceso de la Red actual Servidores (NAS) y apoyo las Redes Privadas Virtuales (VPNs).

El PPTP Red Servidor (PNS) se preve para correr adelante un sistema operativo del propósito general mientras el cliente, se refirió a como un Acceso de PPTP concentrador (PAC) opera en un dial acceda plataforma. PPTP especifica.

1. Introducción

PPTP permite existir Servidor de Acceso de Red (NAS) las funciones para ser separado usando una arquitectura del cliente-servidor.

Tradicionalmente, el las funciones siguientes son llevadas a cabo por un NAS:

1. La unión nativa física a PSTN o ISDN y mando de módems externos o adaptadores del término.

   Un NAS puede unir directamente a un teléfono el circuito analógico o digital o a una vía un módem externo o adaptador del término. Mando de un la conexión circuito-cambiada es cumplida con cualquier módem mando o DSS1 ISDN llaman protocolos del mando.

   El NAS, junto con el módem o adaptadores del término, puede realice adaptaciones la a proporción, analógico a la conversión digital,

sincronización al así conversión o varios otras alteraciones de arroyos de los datos.

2. La terminación lógica de un Punto-a-punto-protocolo (PPP) el Eslabón Protocolo del mando (LCP) la sesión.

3. La participación en PPP autenticación protocolos [3].

4. La agregación del cauce y dirección del bulto para PPP Protocolo. Mult. enlace

5. La terminación lógica de varios PPP conecta una red de computadoras protocolos del mando (NCP).

6. Multiprotocolo derrotando y ponteando entre las interfaces de NAS.

PPTP divide estas funciones entre el PAC y PNS. El PAC es responsable para funciona 1, 2, y posiblemente 3. El PNS puede ser responsable para función 3 y es responsable para funciona 4, 5, y 6. el protocolo llevaba PPP las unidades de los datos protocolares (PDUs) entre el PAC y PNS, así como llame mando y la dirección se dirige por PPTP.

El desarrollo de funciones de NAS ofrece estos beneficios:

IP flexibles se dirigen dirección. Dial-en usuarios puede mantener un solos IP se dirigen cuando ellos marcan en PACs diferente con tal de que ellos se sirve de un PNS comunes. Si un usos de red de empresa direcciones no registradas, un PNS asoció con la empresa asigna direcciones significante a la red privada.

Apoyo de no-IP los protocolos para las redes del dial detrás de las redes de IP.

Esto permite Appletalk y IPX, por ejemplo ser socavado a través de, un proveedor IP-único. La necesidad de PAC no es capaz de proceso estos protocolos.

Una solución al "fraccionamiento de cazar-grupo de Multilink" el problema. Multilink PPP, típicamente agregaba ISDN B encauza, requiere que todos los cauces que componen un bulto del Multilink son se agrupado a un solos NAS. Desde que un Multilink que el bulto de PPP puede ser manejado por un solos PNS, los cauces que comprenden el bulto pueden ser extienda por PACs múltiple.

1.3 Metas protocolares y Asunciones

El protocolo de PPTP sólo es llevado a cabo por el PAC y PNS. Ningún otro los sistemas necesitan ser consciente de PPTP. Las redes del dial pueden conectarse a un PAC sin ser consciente de PPTP. El PPP cliente software normal debe continúe operando en eslabones de PPP socavados.

Se prevé que habrá una muchos-a-muchos relación entre PACs y PNSs. Un PAC puede proporcionar servicio a muchos PNSs. Para ejemplo, un Internet servicio proveedor puede escoger apoyar PPTP para varios clientes de la red privados y crea VPNs para ellos. Cada uno la red privada puede operar uno o más PNSs. Un solo PNS puede asocie con muchos PACs para concentrarse tráfico de un número grande de geográficamente sitios diversos.

Mientras PPTP no se prevé para ser llevado a cabo en software de usuario de dial, esta aplicación no es evitada por el protocolo. PPTP usa un GRE-como la disciplina lleve al usuario los paquetes de PPP. Éstos los perfeccionamientos permiten congestión bajo-nivelada y mando de flujo para ser con tal de que en los túneles los datos del usuario llevaban entre PAC y PNS.

Este mecanismo permite uso eficaz del bandwidth disponible para los túneles y evita retransmisiones innecesario y pulidor desbordamientos. PPTP no dicta los algoritmos particulares a ser usados para este mando nivelado bajo pero define los parámetros que debe comunicarse para permitir tales algoritmos para trabajar.

1.2 Terminología

Canal analógico

Un camino de comunicación circuito-cambiado al que se piensa lleve 3.1 audio de Khz. en cada dirección.

Canal digital

Un camino de comunicación circuito-cambiado al que se piensa lleve información digital en cada dirección.

Llamada

Una conexión o intentó conexión entre dos término end points en un PSTN o ISDN--por ejemplo, una llamada telefónica entre dos módems.

Control de Conexión

Una conexión del mando se crea para cada PAC, PNS aparean y opera encima de TCP [4]. La conexión del mando gobierna aspectos del túnel y de sesiones asignadas al túnel.

Marque al Usuario

Un extremo-sistema o fresadora ataron a una en-demanda PSTN o ISDN qué o es el iniciador o destinatario de una llamada.

Servidor de Acceso de red (NAS)

Un dispositivo que proporciona temporal, acceso de red de en-demanda a usuarios. Este acceso es punto-a-punto que usa PSTN o líneas de ISDN.

PPTP Access Concentrator (PAC)

Un dispositivo ató a uno o más PSTN o ISDN línea capaz de Funcionamiento de PPP y de manejo el protocolo de PPTP. La necesidad de PAC sólo instrumento TCP/IP para pasaremos tráfico a uno o a más PNSs. Él también pueda socavar no-IP los protocolos.

PPTP Red de computadoras el Servidor (PNS)

Un PNS se prevé para operar en general-propósito plataformas del computing/server. El PNS maneja el lado del servidor de el protocolo de PPTP. Desde que PPTP confía en TCP/IP completamente y es independiente del hardware de la interfase, el PNS puede usar cualquiera la combinación de IP interfase hardware incluso LAN y LIVIDO dispositivos.

Sesión

PPTP se conexión-orienta. El PNS-PAC mantienen estado para cada usuario que se ata a un PAC. Una sesión se crea cuando extremo-a-extremo la conexión de PPP se intenta entre un usuario del dial y el PNS. Los data gramas relacionados a una sesión se envían encima del socave entre el PAC y PNS.

Túnel

Un túnel es definido por un par de PNS-PAC. El protocolo del túnel es definido por una versión modificada de GRE [1,2]. El túnel lleva Data gramas de PPP entre el PAC y el PNS. Muchas sesiones son múltiplex ión en un solo túnel. Un mando conexión operando encima de los mandos de TCP el establecimiento, suelte, y mantenimiento de sesiones y del propio túnel.

1.3 Apreciación global protocolar

Hay dos componentes paralelos de PPTP: 1) una Conexión del Mando entre cada uno PAC-PNS par que opera encima de TCP y 2) un túnel de IP operando entre el mismo PAC-PNS par que se usa para transportar GRE encapsuló paquetes de PPP para las sesiones del usuario entre el par.

1.3.1 Apreciación global de Conexión de mando

Antes del PPP socavar puede ocurrir entre un PAC y PNS, un mando, la conexión debe establecerse entre ellos. La conexión del mando es una sesión de TCP normal encima de la que PPTP llaman mando y dirección la información se pasa. La sesión del mando es lógicamente asociada con, pero separa de, las sesiones a socavándose a través de un PPTP, túnel. Para cada uno PAC-PNS el par un túnel y una conexión del mando exista. La conexión del mando es responsable para el establecimiento, dirección, y el descargo de sesiones llevó a cabo el túnel. Es los medios por los que un PNS se notifica de una llamada entrante a un PAC asociado, así como los medios por los que un PAC se instruye a ponga una llamada del dial saliente.

Una conexión del mando puede ser establecida por el PNS o el PAC. Siguiendo el establecimiento de la conexión de TCP requerida, el PNS, y PAC establece la conexión del mando que usa el Salida-mando - Conexión-demanda y mensajes de la -contestación. Estos mensajes también se usan para intercambiar información sobre las capacidades operando básicas del PAC y PNS. Una vez la conexión del mando se establece, el PAC o PNS pueda comenzar sesiones pidiendo llamadas que sale o respondiendo a demandas entrantes. La conexión del mando puede comunicar cambios en las características operando de una sesión del usuario individual con un Juego - Eslabón-Info el mensaje. Las sesiones individuales o pueden soltarse por el PAC o PNS, también a través de los mensajes de Conexión de Mando.

La propia conexión del mando es mantenida a través de eco guardar-vivo mensajes. Esto asegura que un fracaso del conectividad entre el PNS y el PAC puede descubrirse de una manera oportuna. Otros fracasos pueden ser informado vía el Lívido-error-notifique mensaje, también en el mando, conexión.

Se piensa que la conexión del mando también llevara dirección mensajes relacionados en el futuro, como un mensaje que permite el PNS a, pida el estado de un PAC dado; éstos que los tipos del mensaje no tienen todavía se definido.

1.3.2 Túnel la Apreciación global Protocolar

PPTP requiere el establecimiento de un túnel para cada uno comunicando par de PNS-PAC. Este túnel se usa para llevar toda la sesión del usuario PPP paquetes para sesiones que involucran un par de PNS-PAC dado. Una llave que es presente en el título de GRE indica qué sesión un PPP particulares el paquete pertenece a. De esta manera, los paquetes de PPP son múltiplex ión y de múltiplex ión encima de un solo túnel entre un par de PNS-PAC dado. El valore para usar en el campo importante es establecido por la llamada procedimiento del establecimiento que tiene lugar en la conexión del mando.

El título de GRE también contiene reconocimiento y secuencia de información que se usa para realizar algún nivel de congestión-mando y descu-brimiento del error encima del túnel. De nuevo la conexión del mando es determine la proporción y parámetros del buffering a los que son acostumbrados regule el flujo de paquetes de PPP para una sesión particular encima del túnel.

PPTP no especifica los algoritmos particulares para usar para congestión-mando y flujo-mando. Algoritmos sugeridos para el determinación de tiempo-exteriores adaptables para recuperar de los datos dejados caer o los reconocimientos en el túnel son incluido en Apéndice UN de esto documento.

1.4 Idioma de la especificación

En este documento, se usan varias palabras para significar los requisitos de la especificación. Estas palabras se capitalizan a menudo.

DEBA definición	Esta palabra, o el adjetivo "requirió", medios que la es un requisito absoluto de la especificación.
NO DEBA	Este medios de la frase que la definición es un prohibición absoluta de la especificación.
DEBA	Esta palabra, o el adjetivo "recomendó", medios que, en algunas circunstancias, válido las razones pueden existir para ignorar este artículo, pero el deben entenderse implicaciones llenas y cuidadosamente pesado antes de escoger un diferente curso. Los resultados inesperados pueden resultar por otra parte.
PUEDA	Esta palabra, o el adjetivo "optativo", medios que este

artículo es uno de un juego permitido de alternativas. Una aplicación que hace no incluya que esta opción debe prepararse a Inter.-operar con otra aplicación que incluya la opción.

Silenciosamente Deseche

La aplicación desecha el data gramas sin más allá proceso, y sin indicando un error al remitente. El la aplicación debe proporcionar la capacidad de anotar el error, incluso los volúmenes, del data gramas desechado, y debe grabar el evento en un contador de la estadística.

1.5 Formato del mensaje y Extensibility Protocolar

PPTP define un juego de mensajes enviado como datos de TCP en el mando conexión entre un PNS y un PAC dado. La sesión de TCP para el la conexión del mando es establecida comenzando una conexión de TCP a ponga a babor 5678. El puerto de la fuente se asigna a cualquier número del puerto sin usar.

Cada PPTP Mando Conexión mensaje empieza con un 8 octeto arreglado porción del título. Esto arregló que el título contiene a lo siguiente: el total la longitud del mensaje, el PPTP .Mensaje Tipo indicador, y un "la Magia Galleta."

Dos controles de conexión mensaje tipos son indicados por el PPTP campo de Tipo de mensaje:

1 - el Mensaje del mando
2 - el Mensaje de dirección

No se definen mensajes de dirección actualmente.

La Galleta Mágica siempre se envía como la constante 0x1A2B3C4D. Su el propósito básico es permitirle al receptor asegurar que es propiamente sincronizado con el TCP datos arroyo. No debe usarse como un medio para el resynchronizing de los datos de TCP vierten en el evento que un el transmisor emite un mensaje inadecuadamente estructurado. Pérdida de la sincronización debe producir cierre inmediato del mando la sesión de TCP de conexión.

Para claridad, todas las Mando Conexión mensaje plantillas en el próximo la sección incluye el PPTP Mando Conexión mensaje título entero. Números precedidos por 0x son valores del hexadecimal.

Los Mensajes del Mando actualmente definidos, se agrupados por función, son:

Controle de Mensaje	Código de Mensaje
(Dirección de Conexión de mando)	
Salida-mando-conexión-pida	1
Salida-mando-conexión-conteste	2
Detener-mando-conexión-pida	3
Detener-mando-conexión-conteste	4
Eco-pida	5
Eco-conteste	6

(Llame Dirección)

Saliente-llamar-pida	7
Saliente-llamar-conteste	8
Entrante-llamar-pida	9
Entrante-llamar-conteste	10
Entrante-llamar-conectado	11
Llamar-claro-pida	12
Llamar-desconectar-notifique	13

(Error que Informa)

Lívido-error-notifique	14

(PPP Sesión Mando)

Juego-eslabón-Información	15

La Salida-mando-conexión-demanda y mensajes de la -contestación determinan qué versión del protocolo de Conexión de Mando se usará. El campo de número de versión llevado en estos mensajes consiste en una versión numere en el octeto alto y un número de la revisión en el octeto bajo. El versión manejando se describe en Sección 3. El valor actual del el campo de número de versión es 0x0100 para versión 1, revisión 0.

El uso del GRE-como el título para el encapsulación de usuario de PPP
se especifican paquetes en Sección 4.

El MTU para los paquetes de datos de usuario encapsulados en GRE es 1532 octetos, no incluso los IP y títulos de GRE.

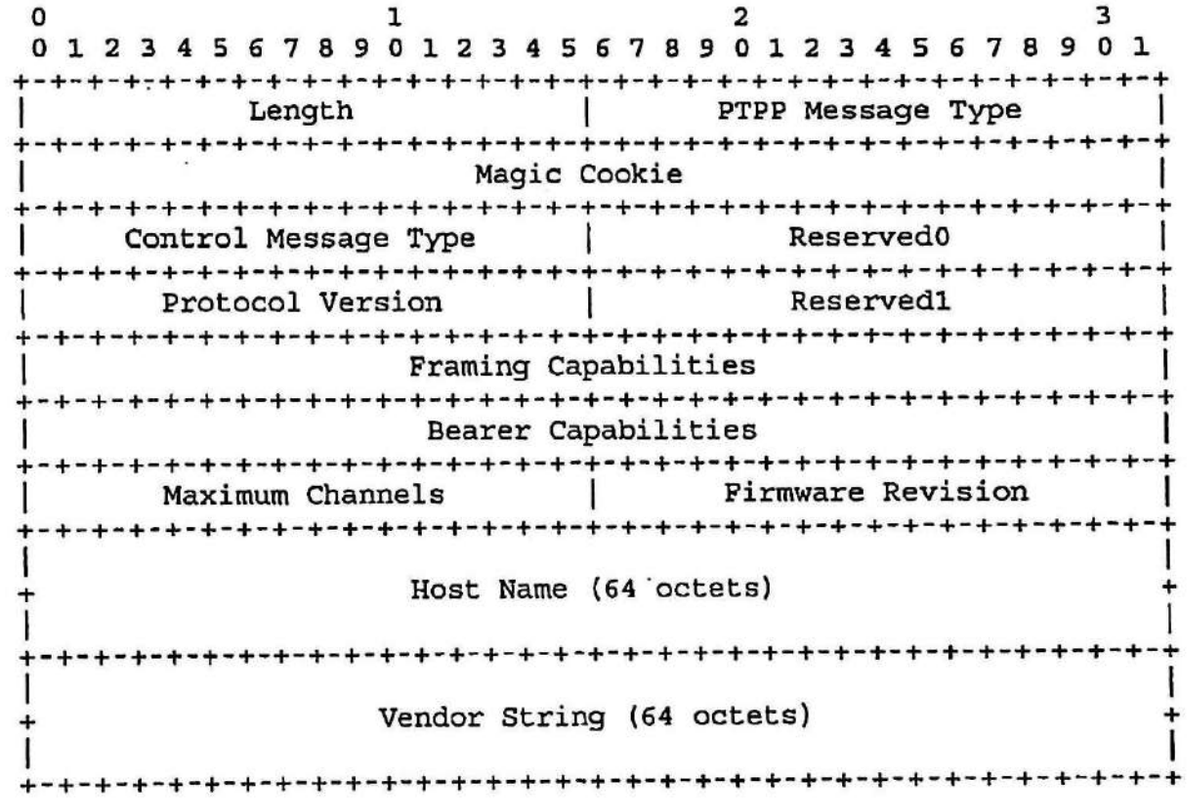
2.0 Conexión del mando la Especificación Protocolar

Controle se usan mensajes de Conexión para establecer y el usuario claro sesiones. El primero puesto de mensajes de Conexión de Mando se usa a mantenga la propia conexión del mando. La conexión del mando es comenzado por el PNS o PAC después de que ellos establecen el conexión de TCP subyacente. El procedimiento y configuración la información exigió determinar qué conexiones de TCP son establecido no es cubierto por este protocolo.

Los mensajes de Conexión de Mando siguientes son todos enviados como datos del usuario en la conexión de TCP establecida entre un par de PNS-PAC dado. Nota ese cuidado se ha tenido para asegurar que toda la palabra (2 octeto) y longword (4 octeto) los valores empiezan en límites apropiados. Todos los datos
se envía en orden de la red (octetos del orden altos primero). Cualquiera "reservado" deben enviarse campos como 0 valores para permitir extensibilidad protocolar.
El título de TCP es seguido por los campos de PPTP mostrados en lo siguiente:

2.1 salida-mando-conexión-demanda

La Salida-mando-conexión-demanda es un PPTP mando mensaje usado para establecer la conexión del mando entre un PNS y un PAC. Cada uno el par de PNS-PAC exige a una conexión del mando especializada ser establecido. Una conexión del mando debe establecerse antes de cualquiera pueden emitirse otros mensajes de PPTP. El establecimiento del mando la conexión puede ser comenzada por el PNS o PAC. Un procedimiento qué asas la ocurrencia de una colisión entre PNS y PAC Se describen salida-mando-conexión-demandas en Sección 3.



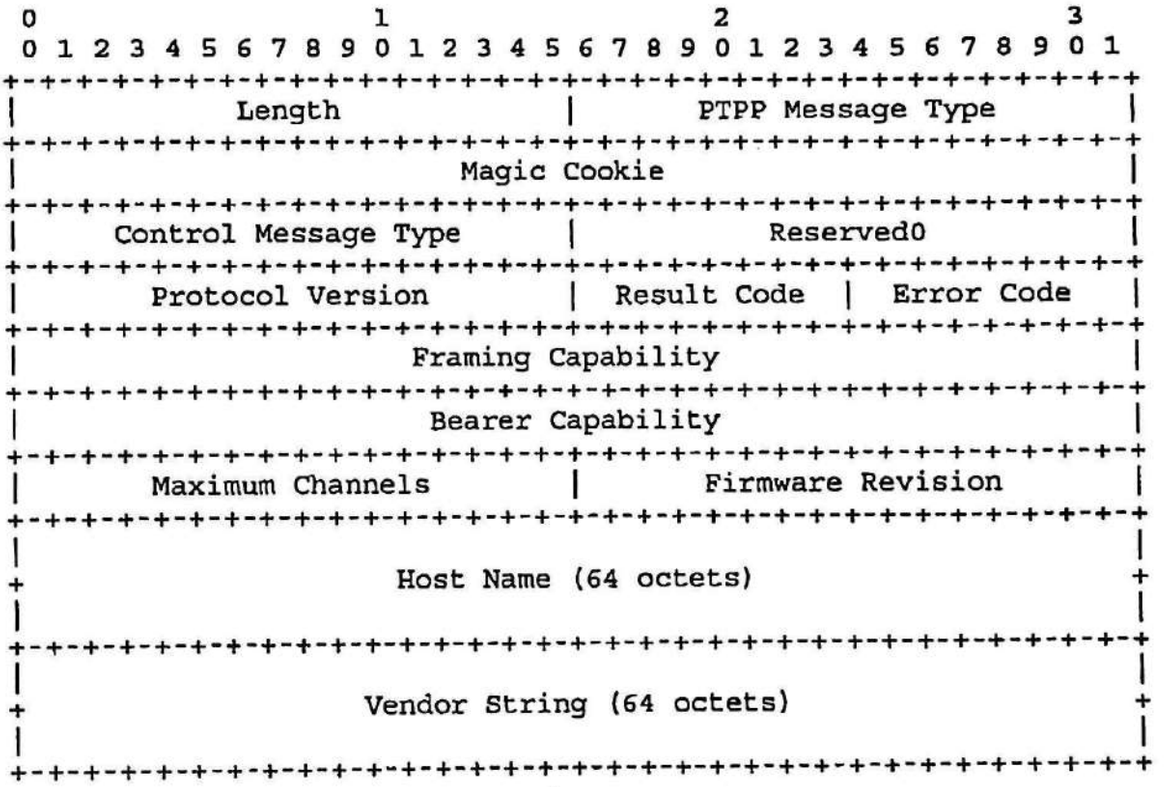
Longitud	La longitud total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo 1	Para el Mensaje del Mando.
Galleta mágica	0x1A2B3C4D este valor de la constante se usa como un cheque de sanidad en mensajes recibidos. (vea Sección 1.5).
Controle Mensaje Tipo 1	Para la Salida-mando-conexión-demanda.
Reservado 0	Este campo debe ser 0.

Versión protocolar	La versión del protocolo de PPTP que el remitente desea usar.
Reservado 1	Este campo debe ser 0.
Capacidades Ideando	Un juego de pedazos que indican el tipo de ideando que el remitente de este mensaje pueda proporcionar. El pedazo actualmente definido las escenas son: 1. Asíncronos soporte 2. Síncronos soporte
Capacidad Portadora	Un juego de pedazos que indican al portador capacidades que el remitente de esto el mensaje puede proporcionar. El actualmente las escenas del pedazo definidas son: 1- Soporte de acceso analógico 2- Soporte de acceso digital
Máximo Canal	El número total de PPP individual sesiones que este PAC puede apoyar. En Las salida-mando-conexión-demandas emitieron por el PNS, este valor debe ponerse a 0. debe ser ignorado por el PAC.
Revisión de Firmware	Este campo contiene la revisión del firmware número del PAC emisor, cuando emitió por el PAC, o la versión del PNS PPTP chófer si emitido por el PNS.
Nombre del Anfitrión	Un 64 campo del octeto que contiene el nombre de DNS del PAC emisor o PNS. Si menos de 64 octetos en longitud, el resto de este campo debe llenarse de octetos de valor 0.

Nombre Vendedor	Un 64 campo del octeto que contiene a un vendedor cordón específico que describe el tipo de PAC que se usa, o el tipo de PNS software que se usa si esta demanda es emitido por el PNS. Si menos de 64 octetos en longitud, el resto de esto el campo debe llenarse de octetos de valore 0.

2.2 Salida-mando-conexión-contestación

La Salida-mando-conexión-contestación es un PPTP mando mensaje enviado en conteste a un mensaje de la Salida-mando-conexión-demanda recibido. Esto el mensaje contiene un código del resultado que indica el resultado del mando esfuerzo de establecimiento de conexión.



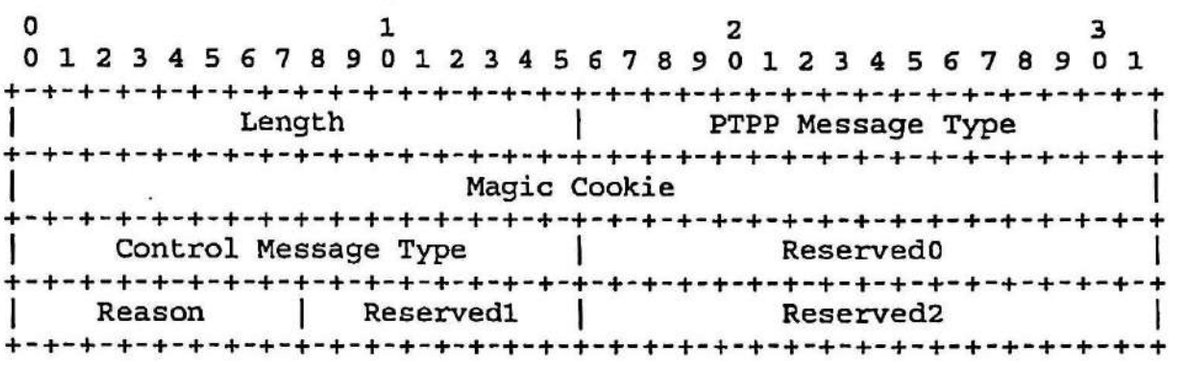
Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	2 para la Salida-mando-conexión-contestación.
Reserved0	Este campo debe ser 0.
Versión protocolar	La versión del protocolo de PPTP que el remitente desea usar.
El Código del resultado	Indica el resultado del orden encauce esfuerzo del establecimiento. Actual los

	valores de Código de Resultado válidos son: 1 - el establecimiento del cauce exitoso 2 - el error general--el Código del Error indica el problema 3 - el cauce del orden ya existe; 4 - Respuesta no es autorizado a establezca un cauce del orden 5 - la versión protocolar del resultado no se apoya
Código del error	Este campo se pone a 0 a menos que un "General Error" existe en que el Código de Resultado de caso póngase a 2 y este campo se pone al valor que corresponde al error general condicione como especificó en Sección 2.16.
Capacidades ideando	Un juego de pedazos que indican el tipo de ideando que el remitente de este mensaje pueda proporcionar. El pedazo actualmente definido las escenas son: 1 - los Ideando Asíncronos apoyaron 2 - los Ideando Síncronos apoyaron.
Portador capacidades	Un juego de pedazos que indican al portador capacidades que el remitente de esto el mensaje puede proporcionar. El actualmente las escenas del pedazo definidas son: 1 - el acceso analógico apoyó 2 - el acceso digital apoyó
El máximo canales	El número total de PPP individual sesiones que este PAC puede apoyar. En un Salida-mando-conexión-contestación emitida por el PNS, este valor debe ponerse a 0 y debe ser ignorado por el PAC. El PNS no debe acostumbrar este valor a intentar a rastree el número restante de PPP sesiones que el PAC permitirá.

Revisión de Firmware	Este campo contiene la revisión del firmware número del PAC emisor, o la versión del PNS chofer de PPTP si emitió por el PNS.
Nombre del anfitrión	Un 64 campo del octeto que contiene el nombre de DNS del PAC emisor o PNS. Si menos de 64 octetos en longitud, el resto de este campo debe llenarse de octetos de valor 0.
Nombre del Vendedor	Un 64 campo del octeto que contiene a un vendedor cordón específico que describe el tipo de PAC que se usa, o el tipo de PNS software que se usa si esta demanda es emitido por el PNS. Si menos de 64 octetos en longitud, el resto de esto el campo debe llenarse de octetos de valore 0.

2.3 Detener-mando-conexión-demanda

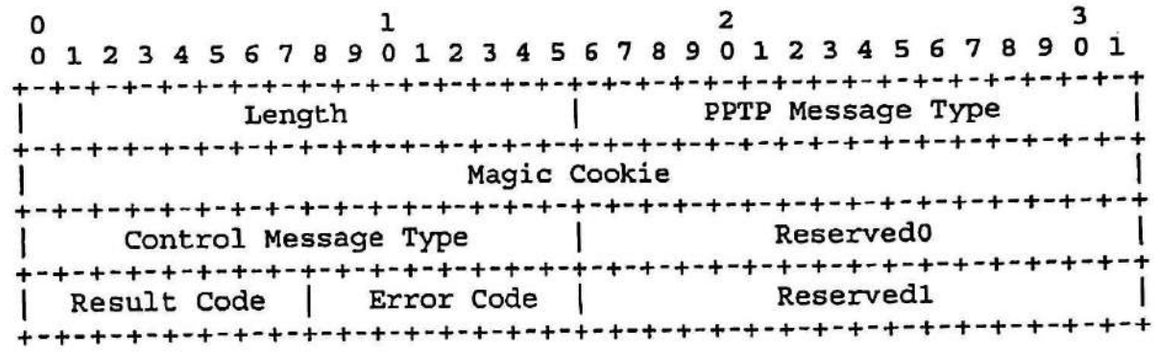
La Detener-mando-conexión-demanda es un PPTP mando mensaje enviado por un par de un PAC-PNS la conexión del mando para informar al otro par que la conexión del mando debe cerrarse. Además de cerrar la conexión del mando, todas las llamadas del usuario activas se aclaran implícitamente. La razón por emitir esta demanda se indica en el campo de la Razón.



Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Control Mensaje Tipo	3 para Detener-mando-conexión-demanda.
Reservado 0	Este campo debe ser 0.
La razón	Indica la razón para el mando conexión que está cerrado. Actual válido los valores de la razón son: 1 (ninguno) - General pide aclarar controle conexión. 2 (detener-protocolo) - no puede apoyar la versión de par del protocolo. 3. (detener-local-cierre) - Respuesta es estando abajo cerrado
Reserved1, Reserved2	Estos campos deben ser 0.

2.4 detener-mando-conexión-contestación

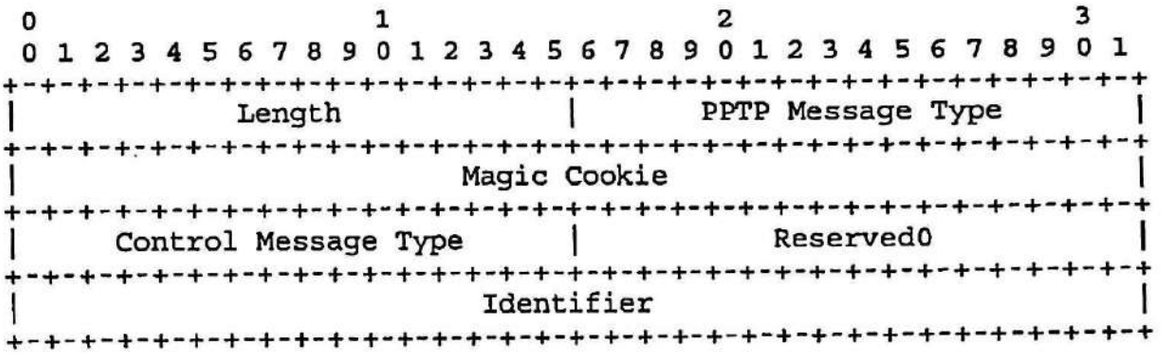
La Detener-mando-conexión-contestación es un PPTP mando mensaje enviado por un par de un PAC-PNS la conexión del mando en el recibo de una Parada - Mando-conexión-pida del otro par.



Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Control de Mensaje Tipo	4 para la Detener-mando-conexión-contestación.
Reservado 0	Este campo debe ser 0.
El Código del resultado	Indica el resultado del esfuerzo a cierre la conexión del mando. Actual los valores de Código de Resultado válidos son: 1 (OK) - la conexión del Mando cerró 2 (Error general) - la conexión del Mando no cerrado por razón indicada en Código del error
Código del error	Este campo se pone a 0 a menos que un "General Error" existe en que el Código de Resultado de caso póngase a 2 y este campo se pone al valor que corresponde al error general condicione como especificó en Sección 2.16.
Reservado 1	Este campo debe ser 0.

2.5 eco-demanda

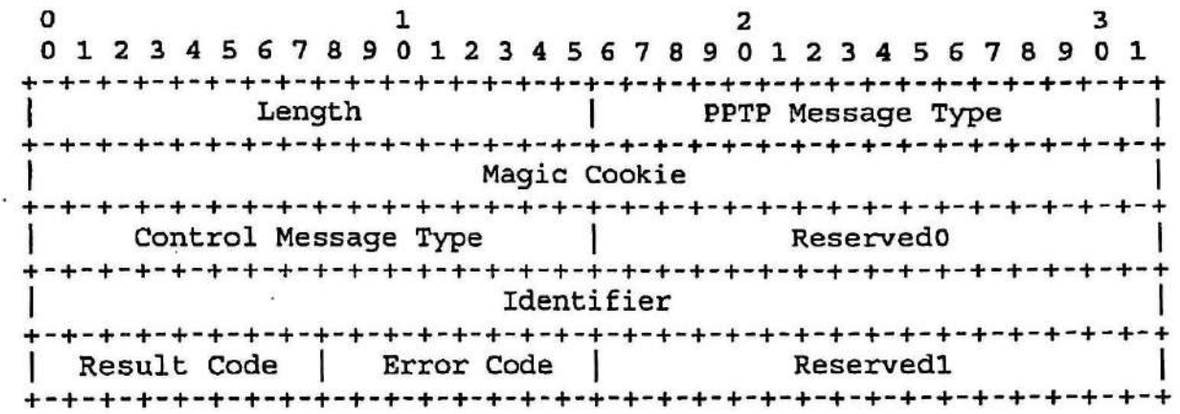
La Eco-demanda es un PPTP mando mensaje enviado por cualquier par de un PAC-PNS la conexión del mando. Este mensaje del mando se usa como un "guarde - Vivo" para la conexión del mando. Los problemas del par receptores un Eco-conteste a cada Eco-demanda recibida. Como especificó en Sección 3, si el remitente no recibe una Contestación de Eco en contestación a un Eco - Pida, aclarará la conexión del mando en el futuro.



Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica	0x1A2B3C4D.
Controle Mensaje Tipo	5 para la Eco-demanda.
Reserved0	este campo debe ser 0.
identificador	Un valor puesto por el remitente del Eco - Demanda que se usa para emparejar la contestación con la demanda correspondiente.

2.6 eco-contestación

La Eco-contestación es un PPTP mando mensaje enviado por cualquier par de un PAC-PNS la conexión del mando en contestación al recibo de un Eco - Demanda.

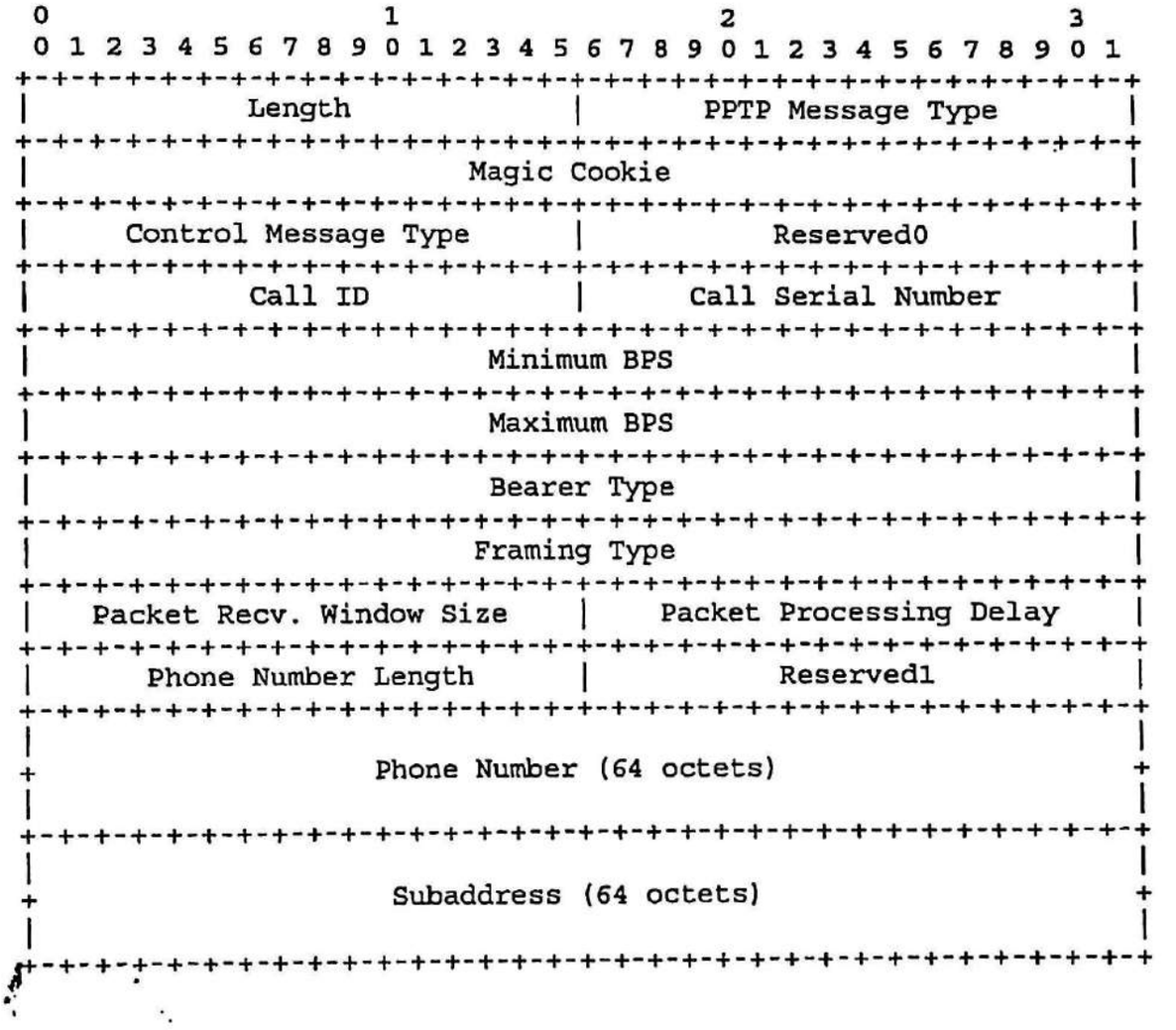


Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	6 para la Eco-contestación.
Reserved0	este campo debe ser 0.
Identifier	Los volúmenes del identifique campo de la Eco-demanda recibida se copia a este campo.
El Código del resultado demanda.	Indica el resultado del recibo de la Eco- Resultado válido actual Los valores del código son: 1 (OK) - La Eco-contestación es válida 2 (Error general) - la Eco-demanda no aceptado por la razón indicada en
Código del error	Código del error Este campo se pone a 0 a menos que un "General Error" la condición existe en que el caso El Código del resultado se pone a 2 y este campo es ponga al valor que corresponde al

	condición del error general como especificó en Sección 2.16.
Reserved1	este campo debe ser 0.

2.7 Saliente-llamar-demanda

La Saliente-llamar-demanda es un PPTP mando mensaje enviado por el PNS al PAC para indicar que una llamada que sale del PAC es ser establecido. Esta demanda le proporciona información requerida al PAC para hacer la llamada. También proporciona información al PAC que es regule la transmisión de datos al PNS para esta sesión una vez se establece.



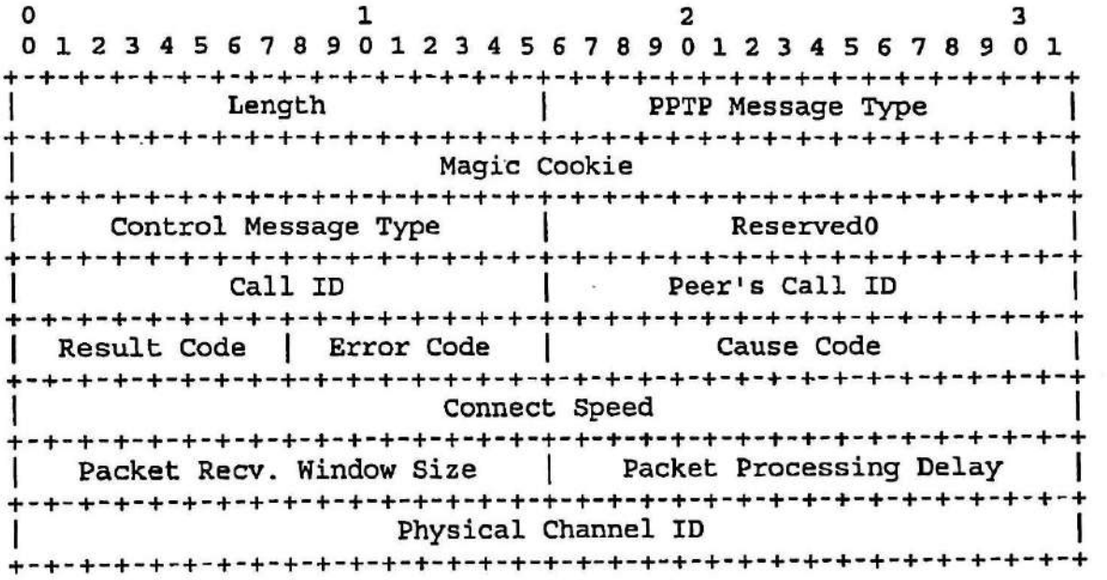
Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	7 para la Saliente-llamar-demanda.
Reserved0	Este campo debe ser 0.
Llame ID	Un únicos identificador, único a un

	particular PAC-PNS par asignado por el PNS a esta sesión. Se usa a multíplice y los datos del de múltiplex enviaron encima de el túnel entre el PNS y PAC involucrado en esta sesión.
Llame número de serie	Que un identificador asignados por el PNS a esto sesión con el propósito de identificar esta sesión del particular en sesión anotada información. Al contrario de la Llamada ID, ambos, el PNS y PAC asocian la misma Llamada Número de serie con una sesión dada. El combinación de dirección de IP y llamada de serie el número debe ser único.
BPS mínimo	La velocidad de la línea aceptable más baja (en bits/second) para esta sesión.
Máximo BPS	La velocidad de la línea aceptable más alta (en bits/second) para esta sesión.
Portador Type	Un valor que indica la capacidad del portador requerido para esta llamada de la salida. El los valores actualmente definidos son: 1 - llame para ser puesto adelante un analógico cauce 2 - llame para ser puesto adelante un digital cauce 3 - la llamada puede ponerse en cualquier tipo de cauce
Tipo ideando	Un valor que indica el tipo de PPP ideando para ser usado para esta salida llamada. 1 - llame para usar ideando Asíncrono 2 - llame para usar ideando Síncrono 3 - la llamada puede usar cualquier tipo de ideando

Paq. Recv Tamaño ventana	El número de paquetes de los datos recibidos el PNS lega pulidor para esta sesión.
Paquete que Procesa Retraso	UNA medida del paquete que procesa retraso eso podría imponerse en datos enviados al PNS del PAC. Este valor es especificado en unidades de 1/10 segundos. Para el PNS este número debe ser muy pequeño. Vea apéndice UN porque una descripción de cómo este valor es determinado y usado.
Longitud del número de teléfono	El número real de dedos válidos en el Campo del número de teléfono.
Reserved1	Este campo debe ser 0.
Número de teléfono	El número a ser marcado para establecer el sesión saliente. Para ISDN y analógico llamadas este campo es un cordón de ASCII. Si el número de teléfono está menos de 64 octetos en longitud, el resto de este campo está llenado de octetos de valor 0.
Sub.-dirección	Un 64 campo del octeto especificaba información marcando adicional. Si el sub.-dirección está menos de 64 octetos anhele, el resto de este campo está lleno con octetos de valor 0.

2.8 saliente-llamar-contestación

La Saliente-llamar-contestación es un PPTP mando mensaje enviado por el PAC a el PNS en contestación a un mensaje de la Saliente-llamar-demanda recibido. El la contestación indica el resultado del esfuerzo de la llamada saliente. Él también proporciona información al PNS sobre parámetros particulares usados para la llamada. Proporciona información para permitirle al PNS regular el la transmisión de datos al PAC para esta sesión.



Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	8 para la Saliente-llamar-contestación.
Reserved0	Este campo debe ser 0.
Llame ID	Un únicos identificador para el túnel, asignado por el PAC a esta sesión. Él se usa a multíplice y datos del de múltiplex enviado encima del túnel entre el PNS y PAC involucró en esta sesión.
La Llamada de par ID	Este campo se pone al valor recibido en la llamada el campo de ID del corresponder Mensaje de la saliente-llamar-demanda. Es usado por el PNS para emparejar la Salida -

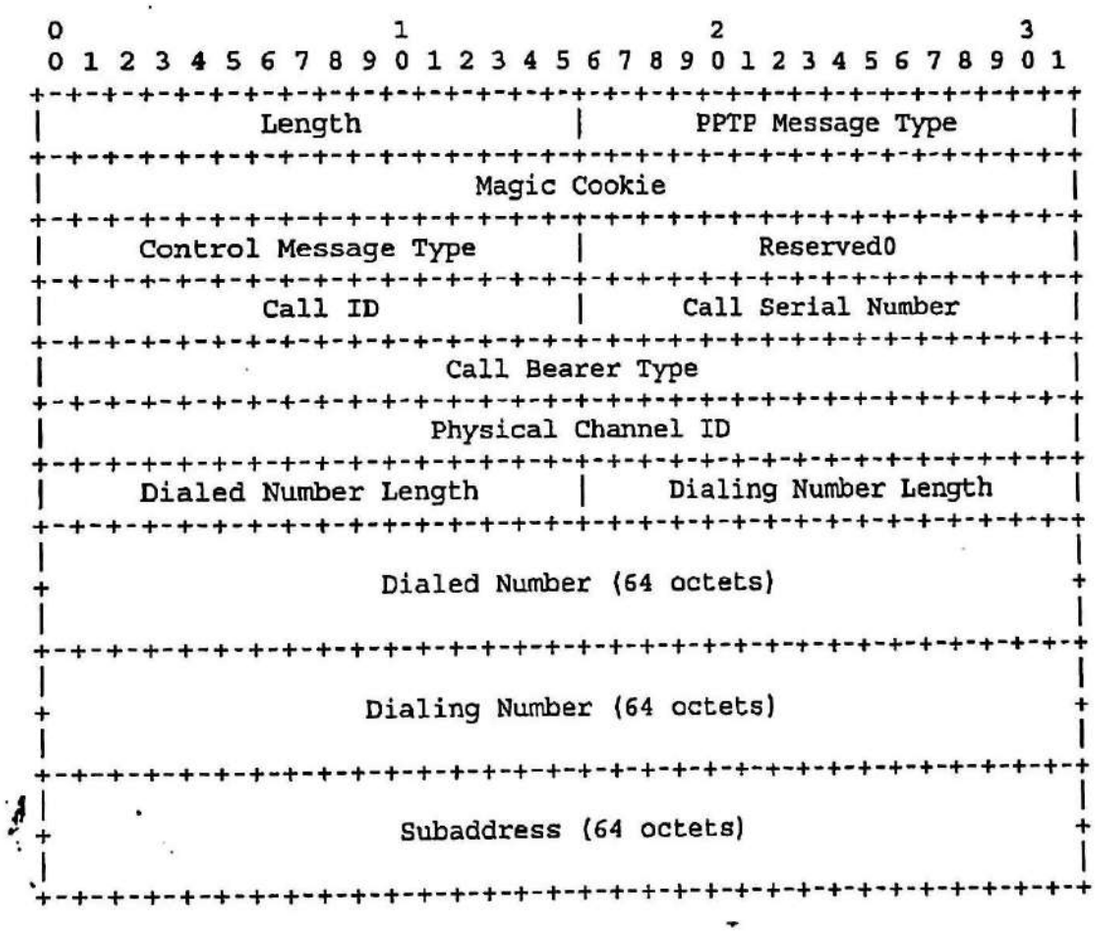
	Llamar-conteste con la Saliente-llamar-demanda emitió. También se usa como el valor enviado en el título de GRE para el mux/demuxing.
Código del resultado	Este valor indica el resultado del Esfuerzo de la saliente – llamar - demanda. Actualmente los valores válidos son: 1 (conectó) - la Llamada estableció con ningún error 2 (Error general) - la Llamada Saliente no establecido por la razón indicada en Código del Error 3 (ningún Portador) - la Llamada Saliente falló debido a ningún portador descubierto 4 (ocupado) - a la Llamada Saliente le faltó la deuda a descubrimiento de un signo ocupado 5 (ningún Tono del Dial) - la Llamada Saliente deuda fallada a la falta de un tono del dial 6 (Time-fuera) - la Llamada Saliente no era establecido dentro de tiempo repartido por PAC 7 (no Acepta) - la Llamada Saliente administrativamente prohibido
Código del error	Este campo se pone a 0 a menos que un "General Error" la condición existe en que el caso El Código del resultado se pone a 2 y este campo es ponga al valor que corresponde al condición del error general como especificó en Sección 2.16.
Código de la causa	Este campo da al fracaso adicional información. Su valor puede variar dependiendo en el tipo de llamada intentado. Para ISDN llame intenta es el Q.931 código de la causa.
Conecte Velocidad	La velocidad de conexión real usó, en bits/second.

Paquete Recv.	Tamaño de la ventana El número de paquetes de los datos recibidos el PAC lega pulidor para esta sesión.
Paquete Procesa Retraso	Una medida del paquete que procesa retraso eso podría imponerse en datos enviados al PAC del PNS. Este valor es especificado en unidades de 1/10 segundos. Para el PAC, este número se relaciona al el tamaño del pulidor sostenía paquetes para ser enviado al cliente y a la velocidad del eslabón al cliente. Este valor debe ponerse al retraso del máximo que normalmente pueda ocurrir entre el tiempo un el paquete llega al PAC y es entregado al cliente. Vea Apéndice un para un ejemplo de cómo este valor es determinado y usó.
Canal físico ID	Este campo es fijo por el PAC en un manera vendedor-específica al físico el número del cauce ponía esta llamada. Se usa por sólo anotar propósitos.

2.9 entrante-llamar-demanda

La Entrante-llamar-demanda es un PPTP mando mensaje enviado por el PAC al PNS para indicar que una llamada entrante será establecida de el PAC. Esta demanda le proporciona información del parámetro al PNS para la llamada entrante.

Este mensaje es el primero en el "apretón de manos del tres-manera" usado por PPTP por establecer llamadas entrantes. El PAC puede diferir contestando el llame hasta que haya recibido una Entrante-llamar-contestación del PNS indicando que la llamada debe establecerse. Este mecanismo permite el PNS para obtener información suficiente sobre la llamada antes de que sea contestó para determinar si la llamada debe contestarse o no.



Longitud la	Longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	8 para la Entrante-llamar-demanda.

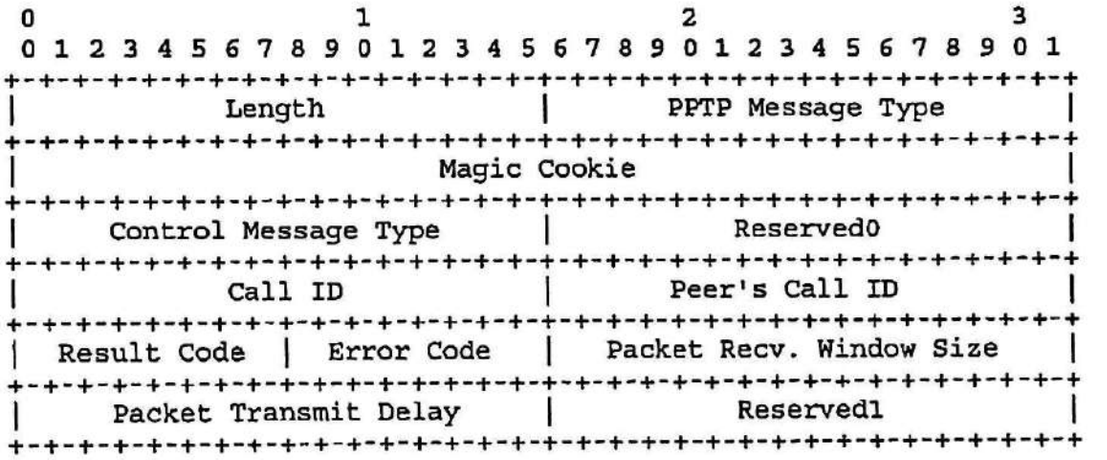
Reserved0	Este campo debe ser 0.
Llame ID	Un únicos identificador para este túnel, asignado por el PAC a esta sesión. Él se usa a multíplice y datos del de múltiplex enviado encima del túnel entre el PNS y PAC involucró en esta sesión.
Llame número de serie	Un identificador asignados por el PAC a esto sesión con el propósito de identificar esta sesión del particular en sesión anotada información. Al contrario de la Llamada ID, ambos, el PNS y PAC asocian la misma Llamada Número de serie a una sesión dada. El combinación de dirección de IP y llamada de serie el número debe ser único.
Tipo de portador	Un valor que indica la capacidad del portador usado para esta llamada entrante. Actualmente los valores definidos son: 1 - la llamada está en un cauce analógico 2 - la llamada está en un cauce digital
Canal físico ID	Este campo es fijo por el PAC en un manera vendedor-específica al número de el cauce físico que esta llamada llegó en.
Longitud del Número marcado	El número real de dedos válidos en el Campo del Número marcado.
Longitud del Número marcando	El número real de dedos válidos en el Campo del Número marcando.
Número marcado	El número que fue marcado por la visita. Para ISDN y las llamadas analógicas este campo es un cordón de ASCII. Si el Número Marcado es menos de 64 octetos en longitud, el resto de este campo está lleno con octetos de valor 0.
Número marcando	El número del que la llamada era puesto. Para ISDN y analógico llama esto el campo es un cordón de ASCII. Si el Marcando. El número está menos de 64 octetos en longitud, el resto de este campo está lleno con octetos de valor 0.

Sub Dirección	Un 64 campo del octeto especificaba información marcando adicional. Si el subaddress está menos de 64 octetos anhele, el resto de este campo está lleno con octetos de valor 0.

2.10 entrante-llamar-contestación

La Entrante-llamar-contestación es un PPTP mando mensaje enviado por el PNS a el PAC en contestación a un mensaje de la Entrante-llamar-demanda recibido. La contestación indica el resultado del esfuerzo de la llamada entrante. Él también proporciona información para permitirle al PAC regular la transmisión de datos al PNS para esta sesión.

Este mensaje es el segundo en el apretón de manos del tres-manera usado por PPTP por establecer llamadas entrantes. Indica al PAC si la llamada debe contestarse o no.



Longitud	La longitud Total en octetos de este PPTP mensaje, incluso el PPTP entero, título.
Mensaje de PTPP Tipo	1 para el Mensaje del Mando.
Galleta mágica.	0x1A2B3C4D
Controle Mensaje Tipo	10 para la Entrante-llamar-contestación.
Reserved0	Este campo debe ser 0.
Llame ID	Un únicos identificador para este túnel asignado por el PAC a esta sesión. Él se usa a multíplice y datos del de múltiplex enviado encima del túnel entre el PNS y PAC involucró en esta sesión.
La Llamada de par ID	Este campo se pone al valor recibido en la Llamada el campo de ID del corresponder Mensaje de la entrante-llamar-demanda. Se usa por el PAC para emparejar el Entrante-llamada - Conteste con la Entrante-llamar-demanda él emitido. Este valor es incluido

	en el GRE título de paquetes de los datos transmitidos para esta sesión.
Código del resultado	Este valor indica el resultado del Esfuerzo la entrante-llamar-demanda. Actual los valores de Código de Resultado válidos son: 1 (conecte) - El PAC debe contestar la llamada entrante 2 (Error general) - La Llamada Entrante no debe establecerse deuda la razón indicó en Código del Error. 3 (no Acepta) - El PAC no debe acepte la llamada entrante. Debe cuelgue o emita una indicación ocupada
Código del error	Este campo se pone a 0 a menos que un "General Error" la condición existe en que el caso.
El Código del resultado	Se pone a 2 y este campo es ponga al valor que corresponde al condición del error general como especificó en Sección 2.16.
Paq. Recv. Tamaño Ventana	El número de paquetes de los datos recibidos el PAC lega pulidor para esta sesión.
El paquete Transmite Retraso	Una medida del paquete que procesa retraso eso podría imponerse en datos enviados al PAC del PNS. Este valor es especificado en unidades de 1/10 segundos. Vea Apéndice UN porque una descripción de cómo esto el valor es determinado y usado.
Reserved1	Este campo debe ser 0.

2.16 Error general Codifica

Los códigos del error generales pertenecen a los tipos de errores que no son específicos a cualquier PPTP particular pide, sino a protocolo o mensaje estructure errores. Si una contestación de PPTP indica en su. Código del Resultado que un el error general ocurrió, el valor del Error General debe examinarse a determinado lo que el error era. El Error General actualmente definido los códigos y sus significados son:

0 (ninguno)	- Ningún error general
1 (no-conectó)	- Ninguna conexión del mando existe todavía para esto PAC-PNS el par
2 (malo-formato)	- la Longitud es el valor de la Galleta malo o Mágico es incorrecto
3 (malo-valor)	- Uno de los valores del campo estaba fuera de rango o el campo reservado era no-ceros
4 (ningún-recurso)	- los recursos Insuficientes para manejar este orden ahora
5 (malo-llame ID)	- La Llamada ID es inválido en este contexto
6 (PAC-error)	- UN error vendedor-específico genérico ocurrió en el PAC

3.0 Conexión del mando el Funcionamiento Protocolar

Esta sección describe el funcionamiento de varios mando de PPTP la conexión funciona y los mensajes de Conexión de Mando que son apóyelos. El funcionamiento protocolar del mando la conexión se simplifica porque TCP es acostumbrado a proporcionar un fiable transporte mecanismo.

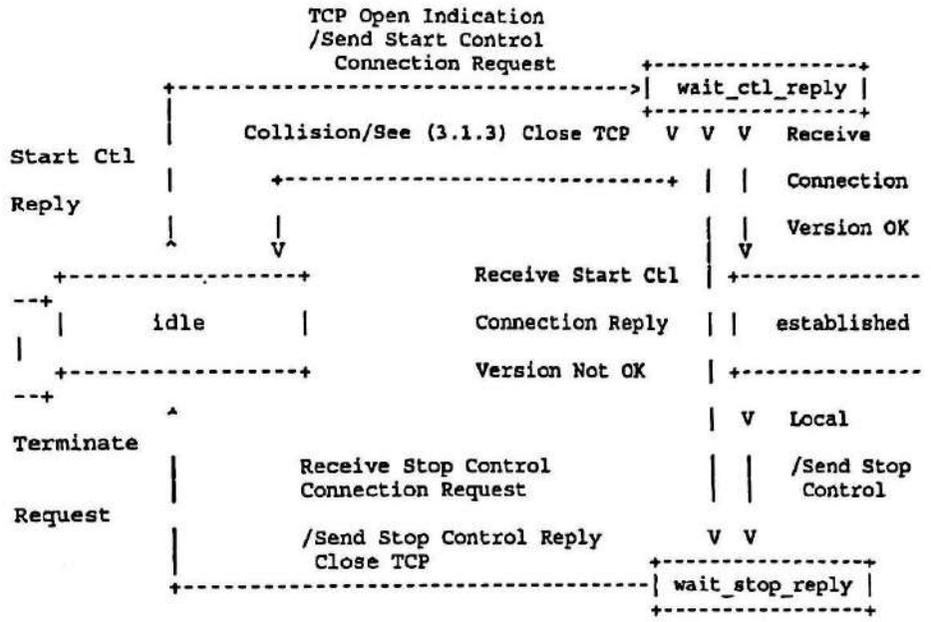
Pidiendo y el retransmisión de mensajes no está una preocupación en esto nivel. La propia conexión de TCP, sin embargo, puede cerrar en cualquier momento y un mecanismo de recuperación de error apropiado debe proporcionarse para manejar este caso. Algunos procedimientos de recuperación de error son comunes a todos los estados del controle conexión. Si una contestación esperada no llega dentro de 60 segundos, la conexión del mando está cerrada, a menos que por otra parte especificado. Los anotando apropiados deben llevarse a cabo para fácil la determinación de los problemas y las razones por cerrar el mando conexión.

El recibo de un inválido o malformed Controla que el mensaje de conexión debe se anotado apropiadamente, y la conexión del mando debe cerrarse y reinició para asegurar recuperación en un estado conocido.

3.1 Conexión del mando Estados

La conexión del mando cuenta en una conexión de TCP normal para su servicio. Los PPTP controlan que el protocolo de conexión no es discernible entre el PNS y PAC, pero es discernible entre el creador y receptor. El par originando es el uno que primero esfuerzos que los TCP abren. Desde que o PAC o PNS pueden originar un conexión, es posible para una colisión de TCP ocurrir. Vea Sección 3.1.3 para una descripción de esta situación.

3.1.1 Creador de Conexión de mando (puede ser PAC o PNS)



Ocioso

El creador de conexión de mando intenta abrir una conexión de TCP al par durante el estado ocioso. Cuando la conexión de TCP está abierta, el el creador transmite un envía Salida-mando-conexión-demanda y entonces entra en wait_ctl_reply state.

wait_ctl_reply

El creador verifica para ver si otra conexión de TCP ha sido pedido del mismo par, y en ese caso, asas la colisión la situación describió en Sección 3.1.3.

Cuando una Salida-mando-conexión-contestación se recibe, se examina para una versión compatible. Si la versión de la contestación es más bajo que el la versión envió en la demanda, el más viejo (baje) la versión debe usarse con tal de que se apoya. Si la versión en la contestación es más temprana y apoyado, el creador mueve al estado establecido. Si el la versión es más temprana y apoyada, un Detener-mando-conexión - La demanda debe enviarse al par y el creador mueve en el los wait_stop_reply declaran.

Establecido

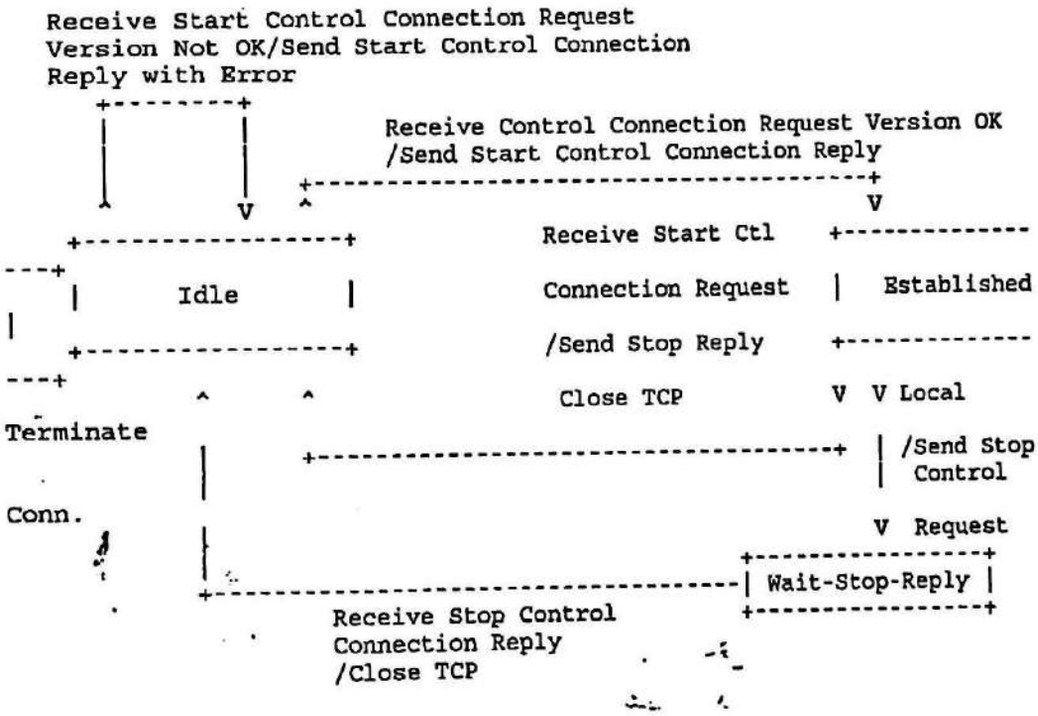
Una conexión establecida o puede terminarse por un local condición o el recibo de una Detener-mando-conexión-demanda. En el evento de una terminación local, el creador debe enviar una Parada - Mando-conexión-demanda y entra en el estado del wait_stop_reply.

Si el creador recibe una Detener-mando-conexión-demanda él Deba enviar una Detener-mando-conexión-contestación y deba cerrar el TCP conexión que se asegura que la información de TCP final ha sido "empujó" propiamente.

wait_stop_reply

Si una Detener-mando-conexión-contestación se recibe, la conexión de TCP debe cerrarse y la conexión del mando se pone ociosa.

3.1.2 Receptor de conexión de mando (puede ser PAC o PNS)



Ocioso

El receptor de conexión de mando espera por un TCP abra esfuerzo en puerto 5678. Cuando notificó de una conexión de TCP abierta, debe preparar a reciba mensajes de PPTP. Cuando una Salida-mando-conexión-demanda es recibido que su campo de la versión debe examinarse. Si la versión es antes que la versión del receptor y la versión más temprana puede ser apoyado por el receptor, el receptor debe enviar un Salida-mando - Conexión-contestación. Si la versión es más temprana que el receptor no pueden apoyarse versión y la versión, el receptor debe enviar una Salida - el mensaje de la Conexión-contestación, cierre la conexión de TCP y

permanezca en el estado ocioso. Si la versión del receptor es igual que antes que el par, el receptor debe enviar un Salida-mando - Conexión-conteste con la versión del receptor y entre el estado establecido.

Establecido

Una conexión establecida o puede terminarse por un local condición o la recepción de una Detener-mando-conexión-demanda. En el evento de una terminación local, el creador debe enviar una Parada - Mando-conexión-demanda y entra en el estado del wait_stop_reply.

Si el creador recibe una Detener-mando-conexión-demanda él Deba enviar una Detener-mando-conexión-contestación y deba cerrar el TCP conexión, asegurándose que la información de TCP final ha sido "empujó" propiamente.

wait_stop_reply

Si una Detener-mando-conexión-contestación se recibe, la conexión de TCP debe cerrarse y la conexión del mando se pone ociosa.

3.1.3 salida Mando Conexión Iniciación Demanda Colisión

Un PAC y PNS deben tener sólo una conexión del mando entre ellos es posible, sin embargo, para un PNS y un PAC a simultáneamente esfuerzo para establecer una conexión del mando a nosotros. Cuando una Salida - La mando-conexión-demanda se recibe en una conexión de TCP y otra Salida-mando-conexión-demanda ya se ha enviado adelante otra conexión de TCP al mismo par, una colisión ha ocurrido.

El "ganador" de la raza de la iniciación es el par con el IP más alto dirección (comparó como 32 pedazo los valores sin firmar, número de la red más significante). por ejemplo, si los pares 192.33.45.17 y 192.33.45.89 choque, el último se declarará el ganador.

El perdedor cerrará la conexión de TCP que comenzó inmediatamente, sin enviar cualquier PPTP extenso los mensajes controlan en él y testamento responda a la demanda del ganador con una Salida-mando-conexión-contestación mensaje. El ganador esperará por la Salida-mando-conexión-contestación en la conexión comenzó y también espera por una terminación de TCP indicación en la conexión el perdedor abrió. El ganador no DEBE envíe cualquier mensaje en la conexión que el perdedor comenzó.

3.1.3 Manteniéndolas en línea y cronómetros

Una conexión del mando debe ser cerrada cerrando el TCP subyacente conexión bajo las circunstancias siguientes:

1.si una conexión del mando no está en el estado establecido (es decir, Salida-mando-conexión-demanda y Salida-mando-conexión - La contestación no se ha intercambiado), una conexión del mando debe ser cerrado después de 60 segundos por un par que espera por un Salida-mando - Conexión-demanda o mensaje de la Salida-mando-conexión-contestación.

2. si la conexión del mando de un par está en el estado establecido y tiene no recibido un mensaje del mando durante 60 segundos, debe enviar un Mensaje de la eco-demanda. Si una Eco-contestación no se recibe 60 segundos después de la transmisión de mensaje de Eco-demanda, el mando la conexión debe cerrarse.

3.2 llamada Estados

3.2.1 consideraciones cronometrando

Debido a la naturaleza del real-tiempo de señalización del teléfono, ambos los PNS y PAC debe llevarse a cabo con arquitecturas multi-enhebradas tal no se fabrican en serie ese mensajes relacionados a las llamadas múltiples y bloqueado. El retraso del tránsito entre el PAC y PNS no debe exceder un segundo. La llamada y conexión que las figuras estatales no especifican excepciones causadas por cronómetros. La asunción implícita es ese desde que la conexión del mando TCP-basado está verificándose con guardar-alives, hay menos necesidad de mantener cronómetros estrictos para el mando de la llamada mensajes.

Llamadas internacionales que sale estableciendo, incluso el módem, entrenando y sucesiones de la negociación, puede tomar más de así 1 minuto el uso de cronómetros cortos se descorazona.

Si una transición estatal no ocurre dentro de 1 minuto (salvo conexiones en el ocioso o estableció estados), la integridad del el proceso protocolar entre los pares es sospechoso y el ENTERO La CONEXION del MANDO debe cerrarse y debe reiniciarse. Todos Llaman que IDs son lógicamente soltó siempre que una conexión del mando se empiece. Esto presumiblemente también los auxilios previniendo peaje llaman de ser "perdido" y nunca aclarado.

3.2.2 llamada los valores de ID

Cada par asigna una Llamada que ID valoran a cada sesión del usuario pide o acepta. Esta Llamada el valor de ID debe ser único para el túnel entre el PNS y PAC a los que pertenece. Los túneles a otros pares pueden usar el misma Llamada ID numeran al receptor de un paquete así en un túnel necesita a asocie una sesión del usuario con un túnel particular y Llame ID. Es sugerido que el número de Llamada potencial que ID valora para cada túnel sea por lo menos dos veces tan grande como el número del máximo de llamadas esperadas adelante un túnel dado.

Una sesión es definida por el triple (PAC, PNS, Llama ID).

3.2.3 llamadas entrantes

Un mensaje de la Entrante-llamar-demanda es generado por el PAC cuando un anillos de línea de teléfono asociados. El PAC selecciona una Llamada ID y folletín número y indica el tipo de portador de llamada. Los módems siempre deben indique tipo de la llamada analógico. Las llamadas de ISDN deben indicar digital cuando servicio digital sin restricción o el adaptación de la proporción se usa y analógico si los módems digitales están envueltos. Número marcando, número marcado, y los sub. direcciones pueden ser incluidos en el mensaje si ellos están disponibles de la red del teléfono.

Una vez el PAC envía la Entrante-llamar-demanda, espera por una contestación del PNS pero no contesta la llamada de la red del teléfono. El PNS puede escoger no aceptar la llamada si:

- Ningún recurso está disponible manejar más sesiones

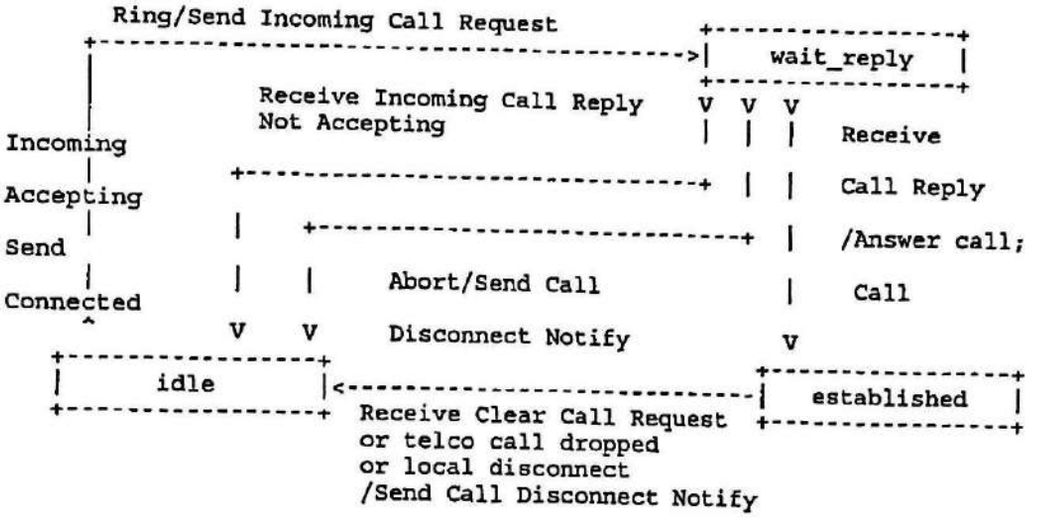
- Los marcaron, marcando, o los campos del sub direcciones no son indicativos de un usuario autorizado.

- El servicio del portador no es autorizado o se apoya

Si el PNS escoge aceptar la llamada, responde con una Salida - Llamar-contestación que también indica ventana clasifica según tamaño (vea Apéndice B). Cuando el PAC recibe la Saliente-llamar-contestación, intenta conectar el llame, asumiendo la fiesta de la profesión no ha colgado. Una llamada final el mensaje conectado del PAC al PNS indica que la llamada estados para el PAC y el PNS debe entrar en los establecieron estado.

Cuando el marcar-en caídas del cliente a, la llamada normalmente se aclara y el PAC envía un Llamar-desconectar-notifique mensaje. Si el PNS desea a aclare una llamada, envía un mensaje de la Llamar-claro-demanda y entonces las esperas para un Llamar-desconectar-notifique.

3.2.3.1 PAC la Llamada Entrante Estados



Los estados asociados con el PAC para las llamadas entrantes son:

Ocioso

El PAC descubre una llamada entrante encendida de sus interfaces del telco. Típicamente esto significa una línea analógica está cercando o un ISDN TE tiene descubierto un Q.931 mensaje del ARREGLO entrante. El PAC envía un Entrante - El mensaje de la llamar-demanda y movimientos al estado del wait_reply.

Wait_reply

El PAC recibe un mensaje de la Entrante-llamar-contestación que indica no - buena gana para aceptar la llamada (error general o no acepta) y movimientos atrás en el estado ocioso. Si el mensaje de la contestación indica eso la llamada se acepta, el PAC envía un Entrante-llamar-conectó mensaje y entra en el estado establecido.

Establecido

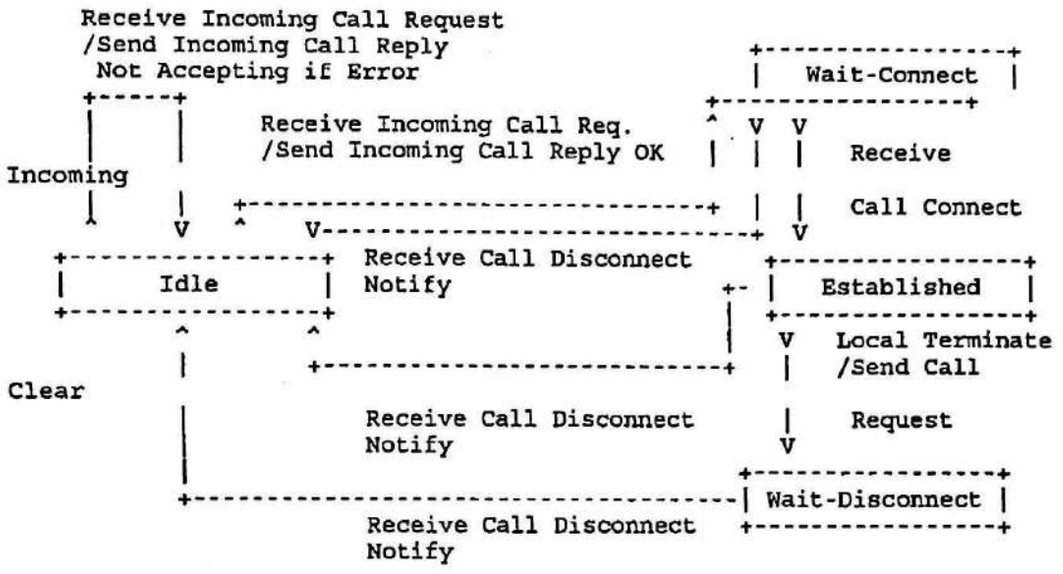
El datos se intercambia encima del túnel. La llamada que sigue puede aclararse:

Un evento en la conexión del telco. El PAC envía una Llamada - Desconectar-notifique mensaje

Recibo de una Llamar-claro-demanda. El PAC envía un Llamar-desconecte - Notifique mensaje

Una razón local. El PAC envía un Llamar-desconectar-notifique mensaje.

3.2.3.2 PNS la Llamada Entrante Estados



Los estados asociados con el PNS para las llamadas entrantes son:

Ocioso

Un mensaje de la Entrante-llamar-demanda se recibe. Si la demanda no es aceptable, una Entrante-llamar-contestación se envía atrás al PAC y el PNS permanece en el estado ocioso. Si el mensaje de la Entrante-llamar-demanda es aceptable, una Entrante-llamar-contestación que indica se envía acepte en el código del resultado. La sesión mueve al estado del wait_connect.

Wait_connect

Si la sesión se conecta en el PAC, el PAC envía un entrante llame conecte mensaje al PNS al que entonces pasa estableció estado. El PAC puede enviar un Llamar-desconectar-notifique para indicar que el la visita entrante no podría conectarse. Esto podría pasar, para ejemplo, si un accidente de usuario de teléfono pone una llamada de la voz normal a un PAC que produce un fracaso del apretón de manos en el módem llamado.

Establecido

La sesión o es terminada por recibo de un Llamar-desconecte - Notifique mensaje del PAC o enviando una Llamar-claro-demanda. Una vez una Llamar-claro-demanda se ha enviado, la sesión entra el los wait_disconnect declaran.

Wait_disconnect

Una vez un Llamar-desconectar-notifique se recibe los movimientos de la sesión atrás a el estado ocioso.

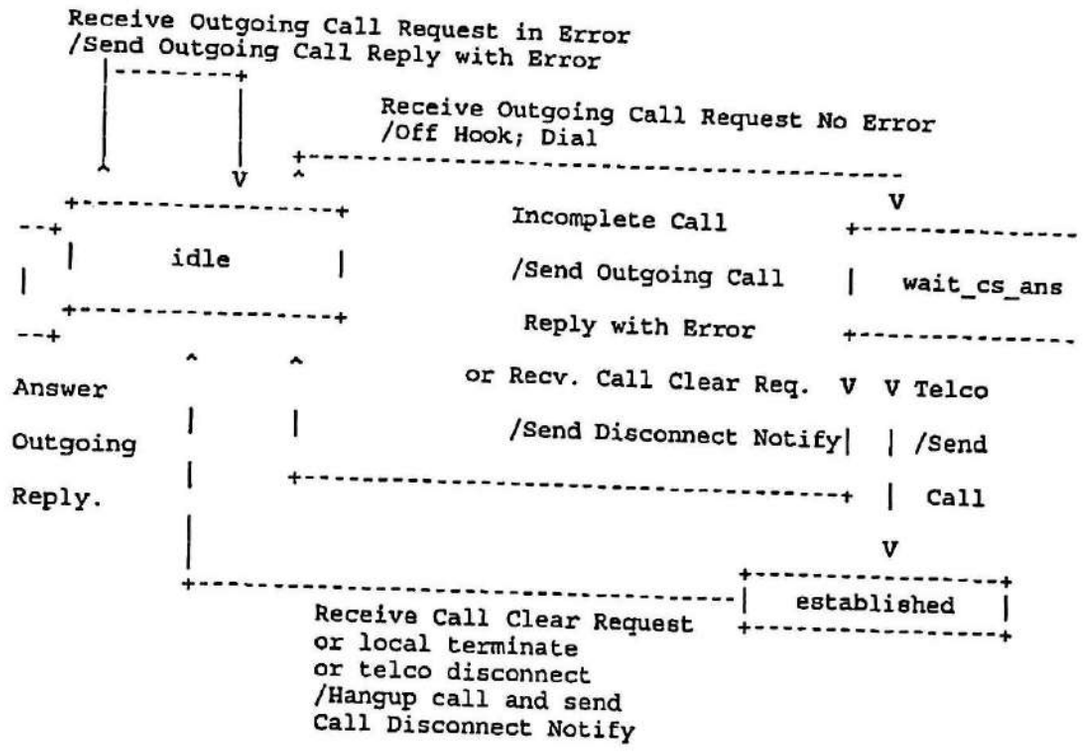
3.2.4 salida llama

Los mensajes salientes son comenzados por un PNS y le dicen a un PAC que ponga una llamada en una interfase del telco. Hay sólo dos mensajes para la salida llamadas: Saliente-llamar-demanda y Saliente-llamar-contestación. El PNS envía una Saliente-llamar-demanda que especifica el número de teléfono de la fiesta marcado y sub direcciones así como la velocidad y parámetros de la ventana. El PAC MUST responda al mensaje de la Saliente-llamar-demanda con un Saliente-llamada - Mensaje de la contestación una vez el PAC determina eso:

La llamada se ha conectado con éxito

Un fracaso de la llamada ha ocurrido por las razones como: ninguna interfase es disponible para dial-fuera, la fiesta llamada está ocupada o no hace conteste, o ningún tono del dial se descubre en la interfase escogida para marcando.

3.2.4.1 PAC Salida Llamada Estados



Los estados asociados con el PAC para las llamadas salientes son:

Ocioso

Saliente-llamar-demanda recibida. Si esto se recibe en error, responda con una Saliente-llamar-contestación con juego de condición de error. Por otra parte, asigne cauce físico para marcar adelante. Ponga la llamada que sale, espera, para una conexión, y mueve al estado del wait_cs_ans.

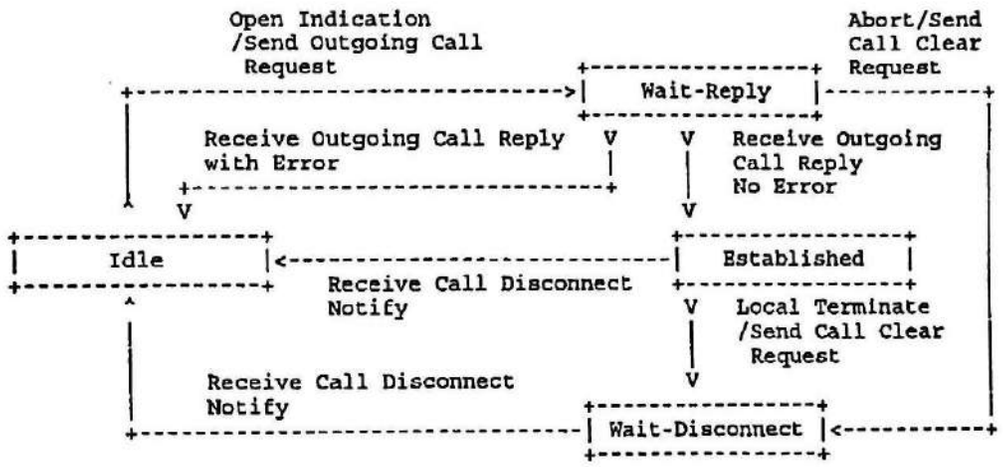
Wait_cs_ans

Si la llamada está incompleta, envía una Saliente-llamar-contestación con un no - ponga a cero Código del Error. Si un cronómetro expira en una llamada que sale, envía atrás un Saliente-llamar-conteste con un no-cero Código del Error. Si un circuito cambiara la conexión se establece, envíe un Saliente-llamar-contestación indicar éxito.

Establecido

Si una Llamar-claro-demanda se recibe, la llamada del telco debe ser soltado vía los mecanismos apropiados y un Llamar-desconectar-notifique el mensaje debe enviarse al PNS. Si la llamada está desconectada por el cliente o por la interfase del telco, un Llamar-desconectar-notifique mensaje debe enviarse al PNS.

3.2.4.2 PNS Salida Llamada Estados



Los estados asociados con el PNS para las llamadas salientes son:

Ocioso

Un mensaje de la Saliente-llamar-demanda se envía al PAC y la sesión movimientos en el estado del wait_reply.

Wait_reply

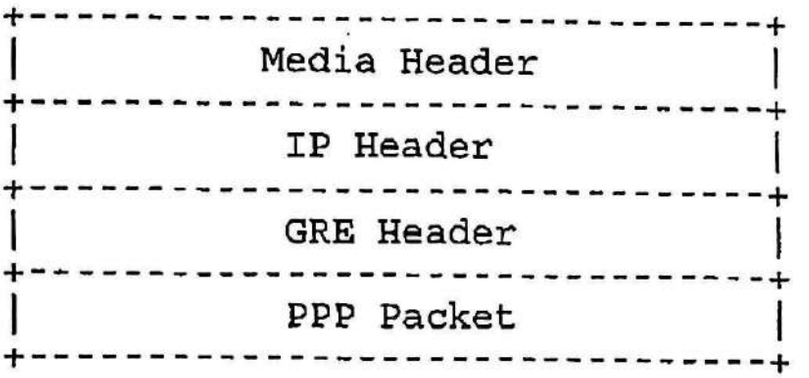
Una Saliente-llamar-contestación se recibe qué indica un error. El la sesión vuelve para estar ocioso estado. Ninguna llamada del telco es activa. Si el La saliente-llamar-contestación no indica un error, la llamada del telco es conectado y la sesión mueve al estado establecido. Establecido Si un Llamar-desconectar-notifique se recibe, la llamada del telco ha sido terminado por la razón indicada en el Resultado y Códigos de la Causa. Los movimientos de la sesión atrás al estado ocioso. Si el PNS escoge a termine la sesión, le envía una Llamar-claro-demanda al PAC y entonces entra en el estado del wait_disconnect.

Wait_disconnect

Un desconexión de la sesión está esperando ser confirmado por el PAC. Una vez el PNS recibe el Llamar-desconectar-notifique mensaje, la sesión, entra en estado ocioso.

4.0 túnel el Funcionamiento Protocolar

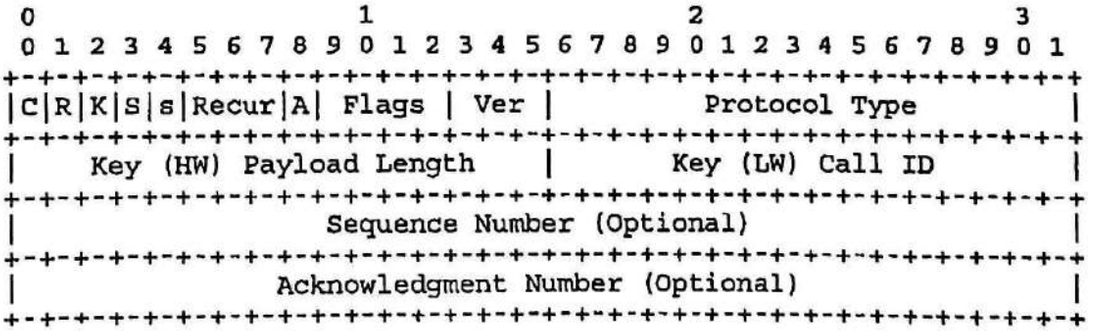
Los datos del usuario llevados por el protocolo de PPTP son PPP datos paquetes. PPP se llevan paquetes entre el PAC y PNS, encapsulados en GRE, paquetes que a su vez se llevan encima de IP. El PPP encapsulado los paquetes son esencialmente PPP datos paquetes menos cualquier medios de comunicación específico elementos ideando. Ningún HDLC marca, inserción del pedazo, caracteres del mando, o los escapes de carácter de mando son incluido. Ningún CRCs se envía a través de el túnel. Los paquetes de IP transmitieron encima de los túneles entre un PAC y PNS tiene la estructura general siguiente:



4.1 título de GRE reforzado

El título de GRE usado en PPTP se refuerza ligeramente de eso especificado en el GRE actual la especificación protocolar [1,2]. La diferencia principal involucra la definición de un nuevo campo de Número de Reconocimiento, usada a, determine si un paquete de GRE particular o juego de paquetes han llegado a el extremo remoto del túnel. Esta capacidad del Reconocimiento no es usado junto con cualquier retransmisión de paquetes de datos de usuario. Él se usa para determinar la proporción en la que los paquetes de datos de usuario están en cambio para ser transmitido encima del túnel para una sesión del usuario dada.

El formato del título de GRE reforzado es como sigue:



C	(Pedazo 0) el Presente de Checksum. Ponga para poner a cero (0).
R	(Pedazo 1) Derrotando Presente. Ponga para poner a cero (0).
K	(Pedazo 2) el Presente Importante. Ponga a uno (1).
S	(Pedazo 3) el Presente de Número de Sucesión. Ponga a uno (1) si un payload (datos) el paquete es presente. Ponga para poner a cero (0) si el payload es no el presente (el paquete de GRE es un Reconocimiento sólo).
S	(Pedazo 4) el presente de ruta de fuente Estricto. Juego para poner a cero (0).
Repítase	(Pedazos 5-7) el mando de Recursion. Ponga a ceros (0).
Un	(Pedazo 8) el número de sucesión de Reconocimiento presente. Ponga a uno (1) si el paquete contiene Número del Reconocimiento ser usado por reconocer previamente transmitió datos.
Banderas	(Pedazos 9-12) debe ponerse para poner a cero (0).
Ver	(Pedazos 13-15) debe contener 1 (reforzó GRE).
El Tipo protocolar	Contiene el ID protocolar para PPTP [6].
Llave	El Uso importante del campo Importante está despierto al aplicación. PPTP lo usa como sigue: Longitud de carga paga (2 octetos altos de Llave) el Tamaño del carga pagada, no incluso el título de GRE, Llame ID (2 octetos bajos) Contiene al Par Llame ID para la sesión a que esto el paquete pertenece.
El Número de la sucesión	Contiene el número de la sucesión del carga pagada Presente si S mordiera (Pedazo 3) es uno (1).

El Número del reconocimiento — Contiene el número de la sucesión del paquete de GRE numerado más alto recibido por el par enviando para esta sesión del usuario. Presente si UN pedazo (Pedazo 8) es uno (1).

La sección del payload contiene un PPP datos paquete sin cualquier medios de comunicación elementos ideando específicos.

Los números de la sucesión involucrados están por los números de sucesión de paquete. El el número de la sucesión para cada sesión del usuario se pone para poner a cero a la sesión startup. Cada paquete envió para una sesión del usuario dada que contiene un payload (y tiene el S mordió (Pedazo 3) ponga a uno) se asigna el próximo número de la sucesión consecutivo para esa sesión.

Este protocolo permite llevar los reconocimientos con los datos y hechuras el protocolo global más eficaz, qué a su vez requiere menos buffering de paquetes.

4.2 Protocolo de la Ventana corredizo

El protocolo de la ventana corredizo usado en el PPTP datos camino se usa para mando de flujo por cada lado del intercambio de los datos. El GRE reforzado el protocolo permite reconocimientos del paquete para ser piggybacked en datos paquetes. También pueden enviarse separadamente reconocimientos de los datos paquetes. De nuevo, el propósito principal del protocolo de la ventana corredizo es para el mando de flujo--los retransmisiones no son realizados por el túnel pares.

4.3 Múltiple Reconocimiento del Paquete

Un rasgo del PPTP que el protocolo de la ventana corredizo es que permite el reconocimiento de paquetes múltiples con un solo reconocimiento. Todos los paquetes excelentes con un número de la sucesión bajan o igualan al número del reconocimiento es considerado reconocido. Time-fuera se realizan cálculos usando el tiempo el paquete que corresponde a el número de la sucesión más alto a reconociéndose fue transmitido.

Adaptable tiempo-fuera los cálculos sólo se realiza cuando un el reconocimiento se recibe. Cuando los reconocimientos del multi-paquete son usado, el arriba del adaptable tiempo-fuera el algoritmo está reducido. El PAC no se exige transmitir reconocimientos del multi-paquete; puede en cambio reconoce cada paquete individualmente cuando se entrega a el cliente de PPP.

4.4 Paquetes de la fuera-de-sucesión

De vez en cuando los paquetes pierden su sequencing por un complicado intered. Diga, por ejemplo que un PNS envía 0 a 5 a los paquetes a un PAC. Debido al redireccionamiento en la interred, paquete 4 llega a el PAC antes de paquete 3. El PAC reconoce paquete 4, y puede asuma que paquete 3 está perdido. Este reconocimiento concede crédito de la ventana más allá de paquete 4.

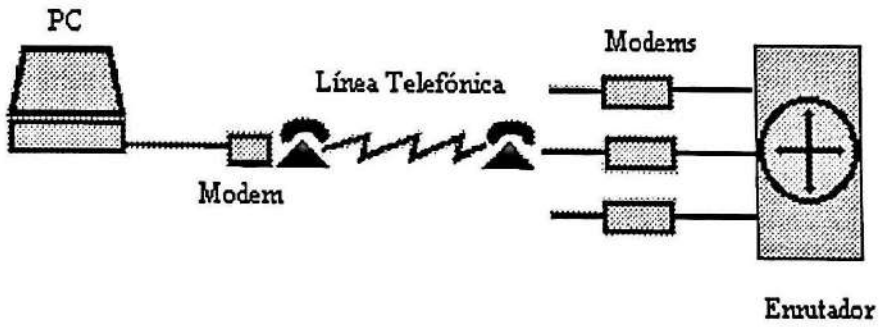
Cuando el PAC recibe paquete 3, no debe intentar transmitir el cliente de PPP correspondiente. Hacer podrían causar problemas así, como PPP apropiado el funcionamiento protocolar se establece como premisas en los paquetes receptores en sucesión. PPP se trata propiamente de la pérdida de paquetes, pero no con pedir de nuevo así fuera de paquetes de la sucesión entre el PNS y PAC debe desecharse silenciosamente, o ellos pueden pedirse de nuevo por el receptor. Cuando paquete 5 entra, es reconocido por el PAC desde que tiene un número de la sucesión más alto que 4 que fueron el último paquete más alto reconocido por el PAC. Paquetes con duplicado los números de la sucesión nunca deben ocurrir subsecuentemente nunca el PAC y PNS retransmite los paquetes de GRE. Una aplicación robusta quiere silenciosamente desecho los paquetes de GRE dobles, si debe recibir cualquiera.

5.0 Consideraciones de seguridad

No se dirigen problemas de seguridad en este documento. Acabe para acabar la seguridad se es dirigida por PPP. Más allá las consideraciones de seguridad serán se dirigido por la próxima versión de PPTP.

COMPARACIÓN ENTRE PPP Y SLIP

SLIP y PPP son dos protocolos de nivel 2 ampliamente utilizados; en especial para realizar conexiones caseras entre un PC y el proveedor de acceso a Internet; donde se requiere un protocolo punto a punto de enlace de datos. Son sencillos y pequeños; pensando tal vez en su fácil implementación; y en la baja velocidad de los enlaces telefónicos.



SLIP

SLIP viene de Serial Line IP; es una forma muy simple de encapsulación para datagramas IP en lineas seriales; diseñado en 1984 por Rick Adams para conectar estaciones de trabajo SUN a Internet a travésde una línea de discado usando un Modem.

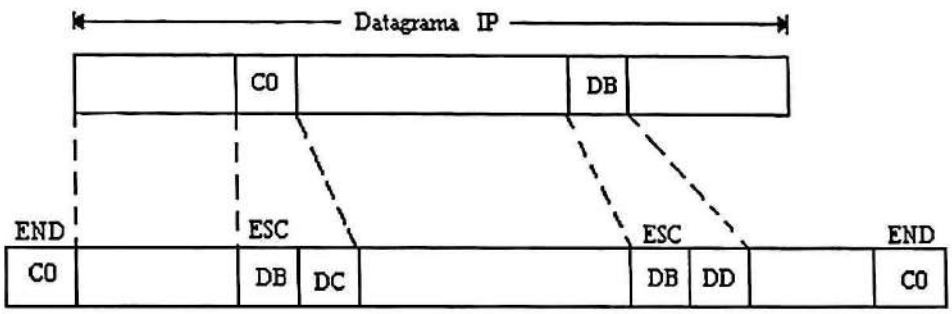
Se ha vuelto muy popular para conectar sistemas caseros a Internet. a través del puerto serial RS-232 que se encuentra en casi todos los computadores y modems.

Formato:

1. Cada datagrama IP es terminado por el carácter especial C0. Para prevenir ruido de línea se acostumbra mandar uno al principio también; de modo que se de por terminada cualquier tipo de conexión errónea anterior.

2. Si el carácter C0 se presenta en el contenido del datagrama; se utiliza la secuencia de dos bytes DB, DC el carácter DB es el carácter de escape de SLIP (distinto al valor ASCII de ESC –1B--).

3. Si en el contenido se presenta el carácter de escape; se reemplaza por la secuencia DB, DD.



SLIP deja a las capas superiores la detección y recuperación de marcos perdidos.

CSLIP

Teniendo en cuenta el gran tamaño del header de IP y TCP, aun para enviar muy poca información, se creó una nueva versión de SLIP llamada CSLIP (compressed SLIP). Este reduce el header típico de 40 bytes a 3 o 5 bytes, ayudándose del hecho de que muchos de los campos del header no varían durante una conexión.

PPP

El PPP es el producto del grupo de trabajo IETF (Internet Engineering Task Force), y es básicamente un protocolo de enlace de datos para líneas punto a punto.

PPP provee un protocolo de encapsulación tanto sobre enlaces sincrónicos orientados a bits, como sobre enlaces asincrónicos con 8 bits de datos sin paridad.

PPP puede operar a través de cualquier interfaz DTE/DCE. Estos enlaces deben ser Full-Duplex pero pueden ser dedicados, o de circuitos conmutados.

Lo conforman básicamente 3 aspectos:

1. Un método de encapsulado sin ambigüedades que identifica claramente el inicio de un datagrama y el final del anterior.

2. Un protocolo de control de enlace, para activar y probar líneas; negociar opciones y desactivar el enlace ordenadamente cuando ya no es necesario.

3. Una familia de NCPs (Network Control Protocols) para negociar opciones de la capa de red con independencia del protocolo de red usado.

El procedimiento típico de conexión es el siguiente:

· El PC llama al enrutador del proveedor a través de un modem.

· El modem del enrutador contesta y establece una conexión física.

· El PC y el enrutador intercambian una serie de paquete LCP para seleccionar los parámetros PPP por usar.

· Se envía una serie de paquetes NCP para configurar la capa de red.

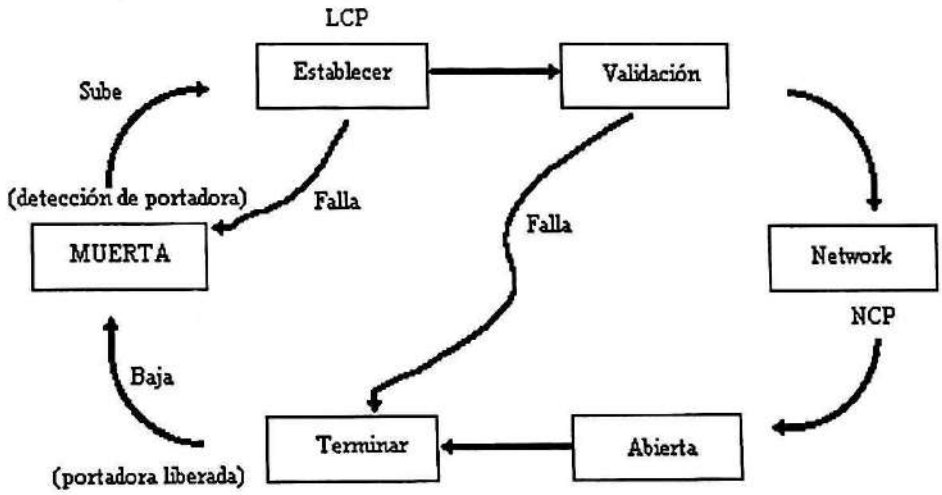
· Se asigna al PC una dirección IP a través de NCP para IP.

· El enlace continua configurado para comunicaciones, hasta que LCP, NCP , o algún evento externo lo tumbe.

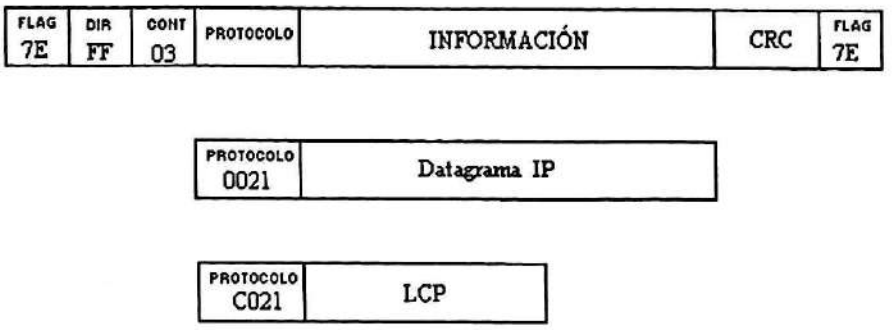
· Se usa NCP para desmantelar la conexión en la capa de red y liberar la dirección IP.

· Se usa LCP para eliminar la conexión a nivel de enlace.

· El modem cuelga liberando la capa física.



El formato de un marco de PPP es muy similar al formato de marco de HDLC; con la diferencia que PPP es orientado a caracteres y no a bits; todos los marcos tienen un número entero de bytes.



Cada marco comienza y termina con un byte "bandera" 7E; para evitar que la aparición de este byte en los campos de información cause confusiones; se utiliza bit stuffing si el enlace es sincrónico. Si el enlace es asincrónico se utiliza el carácter 7D como carácter de escape. Cada vez que este carácter aparece en un marco PPP indica que el siguiente carácter tiene su sexto bit complementado.

Si en el campo de información se presenta un byte 7E; sería transmitido como 7D 5E; y el escape del carácter de escape sería 7D 5D .

Por defecto cualquier valor que corresponda a un carácter ASCII de control es escapado, ya que en algunos casos estos caracteres son interpretados de manera especial por los modems.

Es posible determinar por LCP cuales de los 32 caracteres de control son escapados; por defecto todos lo son.

Luego viene el campo de dirección que siempre vale FF; indicando a todas las estaciones que deben aceptar el marco, de este modo se evita tener que asignar direcciones a nivel de enlace.

Viene después el campo de control; con valor predeterminado 03, que indica que es un marco no-numerado.

Por omisión PPP no proporciona transmisión confiable usando números de secuencia y acuses; pero puede ser implementada en ambientes particularmente ruidosos.

El siguiente campo es el de protocolo; que indica que tipo de carga está en el campo de información. Se definen valores válidos por ejemplo para LCP,NCP, IP, IPX y Appletalk.

Este byte siempre es impar, el bit menos significativo siempre es 1. Si el bit mas significativo del marco es un cero, se trata de un protocolo de nivel de red (IP, IPX, OSI CLNP, XNS); el primer bit en uno indica otros protocolos como LCP y un NCP particular para cada protocolo de nivel 3 admitido. Los desarrolladores de nuevos protocolos deben obtener un número válido del IANA (Internet Assigned Numbers Authority)

La longitud de este campo (2 bytes) puede reducirse a través de LCP.

Los valores asignados (para 1992) son los siguientes:

Valor (en hexa)	Protocolo
0001 a 001f	reserved (transparency inefficient)
0021	Internet Protocol
0023	OSI Network Layer
0025	Xerox NS IDP
0027	DECnet Phase IV
0029	Appletalk
002b	Novell IPX
002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
0031	Bridging PDU
0033	Stream Protocol (ST-II)
0035	Banyan Vines
0037	reserved (until 1993)
00ff	reserved (compression inefficient)
0201	802.1d Hello Packets
0231	Luxcom
0233	Sigma Network Systems
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8025	Xerox NS IDP Control Protocol
8027	DECnet Phase IV Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
802d	Reserved
802f	Reserved
8031	Bridging NCP
8033	Stream Protocol Control Protocol
8035	Banyan Vines Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c223	Challenge Handshake Authentication Protocol

El campo de información es de longitud variable, con un máximo predeterminado de 1500 bytes pero alterable también a través de LCP.

Luego viene el campo para CRC (suma de comprobación) que permite identificar errores a nivel de enlace.

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 *overhead*	Mayor *overhead*
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

1. "The Point-to-Point Protocol (PPP)", Request for Comments 1661, July 1994, W. Simpson.
2. "PPP LCP Extensions", Request for Comments 1570, January 1994, W. Simpson.
3. "PPP LCP Internationalization Configuration Option", Request for Comments 2484, January 1999, G. Zorn.
4. "PPP white paper", Morning Star Technologies.
5. "Redes de computadores", 1997, Tanenbaum, Andrew S.
6. www.monografias.com
7. Redes de computadores. Tanenbaum, Andrew S.
8. TCP/IP illustrated Volume 1. Stevens, W.Richard.
9. RFC 1331, Network Working Group, Simpson, W.
10. RFC 1055, Network Working Group, Romkey, J.

Nota: debido a que utilicé documentos RFC originales, los mismos estaban en idioma inglés, por lo cual podría ser posible que haya cometido unos pequeños errores al escribir algún término técnico.

http://www.incredimail.com/english/download.html