Introducción al resultado de debug ppp negotiation

Contenido

Introducción

En las aplicaciones relacionadas con el marcado, PPP es el tipo de encapsulación más utilizado. El PPP permite que dos equipos en un link de comunicación punto a punto puedan negociar varios parámetros para la autenticación, compresión y los protocolos de Capa 3 (L3), tales como IP. Una falla en la negociación PPP entre dos routers imposibilita establecer la conexión.

El comando **debug ppp negotiation** le permite ver las transacciones de negociación PPP, identificar el problema o la etapa en la que se produce el error, y desarrollar una solución. No obstante, es fundamental que comprenda la salida del comando **debug ppp negotiation**. Este documento proporciona un método amplio para leer los resultados del comando debug ppp negotiation.

prerrequisitos

Requisitos

Quienes lean este documento deben asegurarse de que se cumplan las siguientes condiciones:

- PPP debe estar habilitado en las interfaces de ambos routers. Para esto, ejecute el comando **encapsulation ppp**.
- Ejecute el siguiente comando para activar los sellos de fecha y hora en milisegundos en el router:`Router(config)# service timestamp debug datetime msec` Para obtener más información sobre los comandos de debug, consulte Información Importante sobre Comandos Debug.

Nota: La negociación PPP entre dos pares no puede comenzar a menos que funcione la capa inferior (ISDN, interfaz física, línea de marcado manual, y así sucesivamente) bajo el PPP perfectamente. Por ejemplo, si usted quiere ejecutar el PPP over ISDN, después todas las capas ISDN deben estar para arriba; si no el PPP no comienza.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

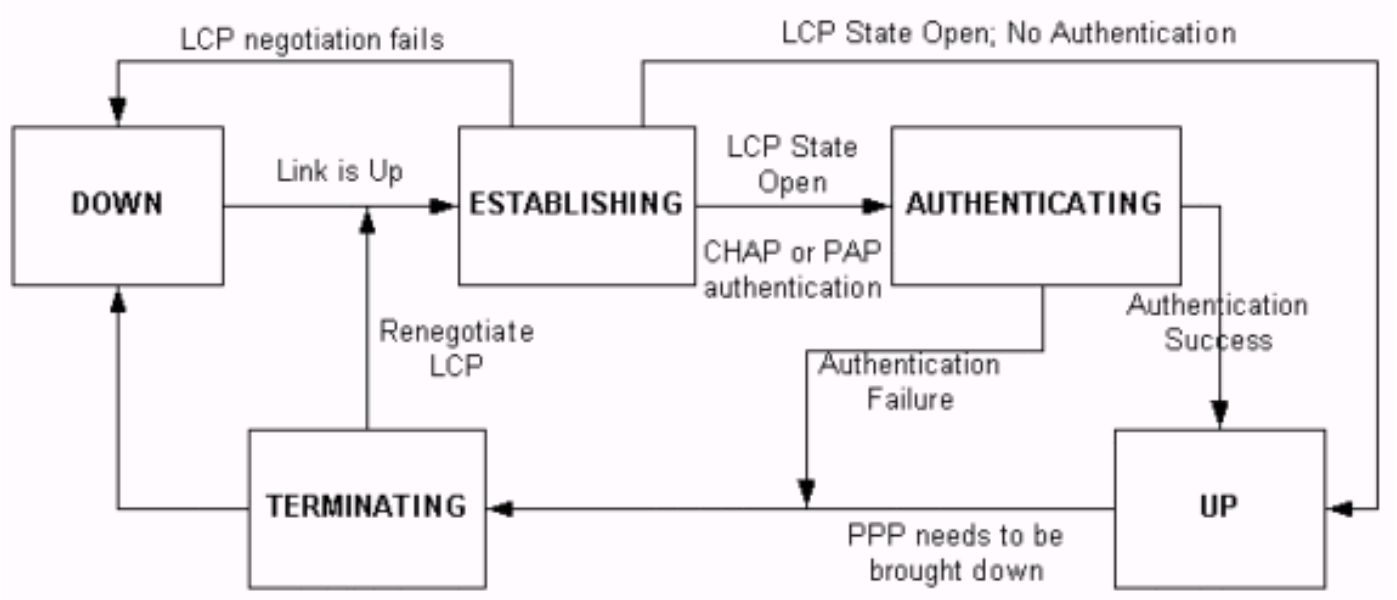
Etapas de la negociación PPP

El enlace pasa a través de varias fases en el proceso de negociación PPP, como se muestra en esta tabla. El resultado final es que PPP está activo o inactivo.

Fase	Descripción
DOWN (INACTIVO)	En esta fase, el PPP está inactivo. Este mensaje se puede ver luego de que el link y PPP estén completamente inactivos: `*Mar 3 23:32:50.296: BR0:1 PPP: Phase is DOWN`
ESTABLECIMIENTO	Las transiciones PPP a esta fase cuando recibe una indicación de que la capa física está activa y lista para ser utilizada. En esta fase tiene lugar la negociación LCP1. `*Mar 3 23:32:06.884: BR0:1 PPP: Phase is ESTABLISHING`
AUTHENTICATING (En proceso de autenticación)	Si se requiere la autenticación del PPP (CHAP2 o PAP3) en el enlace, el PPP pasa a esta fase. Recuerde que la autenticación del PPP es opcional. `*Mar 3 23:32:06.952: BR0:1 PPP: Phase is AUTHENTICATING`
EN FUNCIONAMIENTO	Una vez realizada la autenticación, el PPP pasa a la fase UP (Activo). En esta fase tiene lugar la negociación NCP4. `*Mar 3 23:42:53.412: BR0:1 PPP: Phase is UP`
TERMINATING	En esta fase, el PPP se cierra. `*Mar 3 23:43:23.256: BR0:1 PPP: Phase is TERMINATING`

1. LCP = Link Control Protocol
2. GRIETA = Challenge Handshake Authentication Protocol
3. PAP = protocolo password authentication
4. NCP = protocolo network control

Este diagrama muestra la transición del PPP a las diversas fases:



Paquetes de Negociación PPP: Descripción

Esta tabla incluye una descripción de los paquetes de negociación PPP que se utilizan en la negociación LCP y NCP.

Paquete	Código	Descripción
CONFREQ	Configure-Request	Para abrir una conexión al par, el dispositivo transmite este mensaje junto con las opciones de configuración y los valores que el remitente desea que el par admita. Todas las opciones y los valores se negocian simultáneamente. Si el par responde con un mensaje CONFREJ o CONFNAK, entonces el router envía otro mensaje CONFREQ con otra serie de opciones y valores.
CONFREJ	Configure-Reject	Si alguna opción de configuración recibida en el mensaje CONFREQ no es aceptable o reconocible, el router responde con un mensaje CONFREJ. Se incluye la opción no aceptada (del mensaje CONFREQ) en el mensaje CONFREJ.

CONFNAK	Configure-NAK1	Si la opción de configuración recibida es reconocible y aceptable, pero alguno de los valores no es aceptable, el router transmite el mensaje CONFNAK. El router agrega la opción y el valor que puede aceptar en el mensaje CONFNAK para que el par pueda incluir esa opción en el mensaje CONFREQ siguiente.
CONFACK	Configure-ACK2	Si todas las opciones en el mensaje CONFREQ son reconocibles y todos los valores aceptables, entonces el router transmite el mensaje CONFACK.
TERMREQ	Terminate-Request (Pedido de finalización)	Este mensaje se usa para iniciar un cierre LCP.
TERMACK	Terminate-ACK	Este mensaje es transmitido en respuesta al mensaje TERMREQ.

1. NAK = reconocimiento negativo

2. El ACK = reconoce

Nota: Cada par puede enviar los CONFREQ con la opción o valorarla quisiera que el par soportara. Por consiguiente, las opciones negociadas en cada dirección pueden ser diferentes. Por ejemplo, un lado puede desear autenticar al par y el otro no.

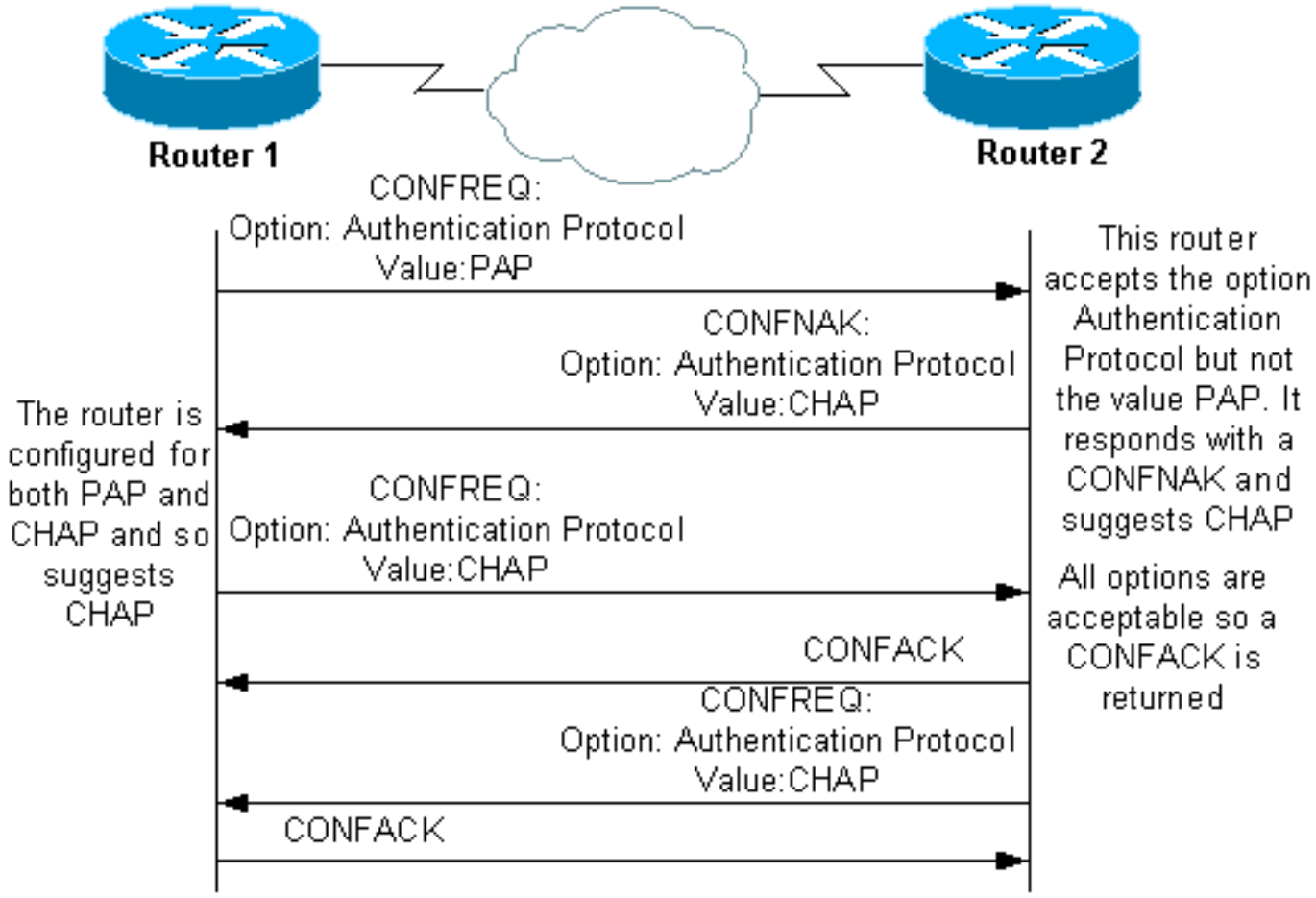
LCP, Autenticación y Etapa NCP

En algunas de las fases del PPP descritas previamente, éste también pasa por etapas específicas tales como la negociación LCP, la autenticación y la negociación NCP. Para más información, refiera al RFC 1548 y al RFC 1661 .

LCP (Fase Obligatoria)

LCP es una fase en la que se negocian los parámetros para establecer, configurar y probar la conexión de enlace de datos. El estado abierto del LCP significa que el LCP se completó con éxito, mientras que el estado cerrado indica que falló.

Este diagrama proporciona una vista conceptual de una entrada en contacto del LCP:



La negociación LCP también utiliza un parámetro llamado MagicNumber, que se utiliza para determinar si el link posee un loopback. Se envía una cadena aleatoria a través del enlace y si se devuelve el mismo valor, entonces el router determina que el enlace posee un bucle de retorno.

Autenticación (Fase Opcional Predeterminada)

En esta etapa, la autenticación se realiza con acuerdo del protocolo de autenticación (CHAP o PAP) durante la negociación LCP. Para obtener información relacionada con el PAP, consulte Configuración y Solución de Problemas del Password Authentication Protocol (PAP) del PPP.

Para obtener información relacionada con el CHAP, consulte Introducción y Configuración de Autenticación del CHAP del PPP.

Nota: La autenticación es opcional y el PPP ingresa solamente esta etapa si necesita autenticar.

NCP (Fase Obligatoria)

Esta fase se utiliza para establecer y configurar diferentes protocolos de capa de red. El protocolo L3 negociado más común es IP. Los routers intercambian mensajes de IP Control Protocol (IPCP) para negociar opciones específicas del protocolo (en este ejemplo, IP).

El RFC 1332 dice que el IPCP negocia dos opciones: compresión y asignaciones de direcciones IP. Sin embargo, el IPCP también se utiliza para pasar información relacionada con la red, tal como los servidores primario y de respaldo, Servicio de Nombres de Windows (WINS) y Sistema de Nombres de Dominio (DNS).

La negociación se realiza mediante el uso de mensajes CONF, como se describe en la sección Paquetes de Negociación PPP: Descripción de este documento.

Solución de Problemas con la Salida del Comando debug ppp negotiation

Cuando lea la salida del comando **debug ppp negotiation** a fin de solucionar problemas, siga estas instrucciones:

1. Identifique las transiciones de fase en la salida del comando **debug**. Determine la última fase que alcanzó la conexión, tales como UP (Activo) o AUTHENTICATING (En proceso de autenticación). Esto podrá ayudarlo a identificar la fase en la que falló la conexión. Para obtener más información sobre las fases, consulte la sección Fases de la Negociación PPP.
2. En la fase en la que se produjo la falla, busque mensajes que indiquen que el LCP, la autenticación o el NCP (según corresponda) se ejecutaron con éxito:El estado del LCP debería ser abierto. También es posible ver los últimos mensajes CONFACK entrantes y salientes para verificar que los parámetros que requiere han sido negociados.La autenticación debe finalizar con éxito. Si utiliza una autenticación bidireccional, entonces cada transacción debe ejecutarse con éxito. Para obtener más información sobre la solución de problemas de fallas en la autenticación del PPP, consulte Solución de Problemas de Autenticación del PPP (CHAP o PAP).El estado IPCP debería estar abierto. Verifique que el direccionamiento sea correcto y que haya instalada una ruta hacia el par.

Lectura de la Salida del Comando debug ppp negotiation

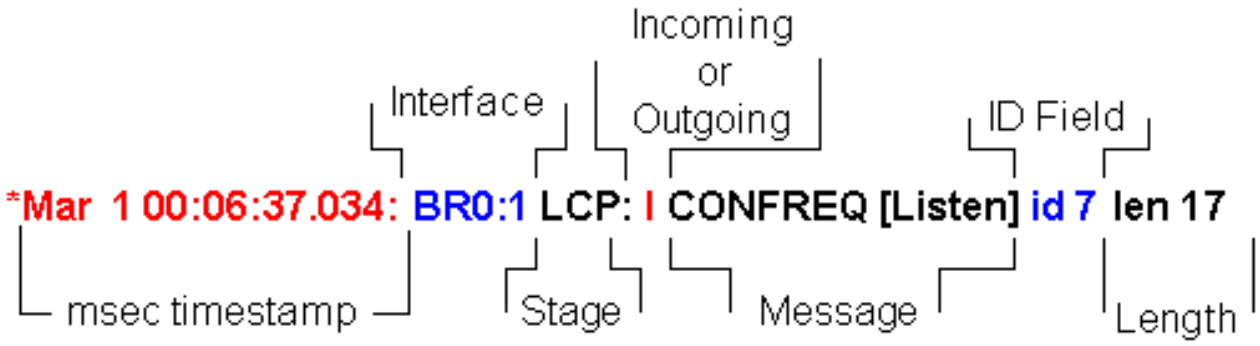
La mayoría de las líneas en la salida del comando **debug ppp negotiation** se caracterizan por:

1. Los sellos de fecha y hora en milisegundos son útiles. Consulte la sección Prerrequisitos de este documento para obtener más información.
2. **Interfaz y Número de interfaz**: Este campo es útil cuando las conexiones de debug utilizan múltiples conexiones o cuando la conexión pasa a través de diversas interfaces. Por ejemplo, determinadas conexiones (como las llamadas de enlaces múltiples) son controladas por la interfaz física al comienzo y luego por la interfaz del marcador o la interfaz de acceso virtual.
3. **Tipo de mensaje del PPP**: Este campo indica si la línea es un mensaje general del PPP, LCP, CHAP, PAP o IPCP.
4. **Dirección del mensaje**: La **I** indica un paquete entrante y la **O** indica un paquete saliente. Este campo puede utilizarse para determinar si el mensaje fue generado o recibido por el router.
5. **Mensaje**: Este campo incluye la transacción particular en la negociación.
6. **ID** — Este campo se utiliza para hacer juego y para coordinar los mensajes request a los mensajes de respuesta apropiados. Usted puede utilizar el campo ID para asociar una respuesta con un mensaje entrante. Esta opción es especialmente útil cuando un mensaje entrante y su respuesta están muy apartados uno de otra en la salida de debug.
7. **Longitud**: El campo longitud define la extensión del campo de información. Este campo no es importante para la solución general de problemas.

Nota: Los campos 4 a 7 pueden no aparecer en todos los mensajes PPP, dependiendo del

propósito del mensaje.

Nota: Este ejemplo ilustra los campos:



Salida de debug ppp negotiation de muestra

La siguiente es una descripción comentada de la salida del comando **debug ppp negotiation**:

```
maui-soho-01#debug ppp negotiation PPP protocol negotiation debugging is on maui-soho-01# *Mar 1
00:06:36.645: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up !--- The Physical Layer (BRI
Interface) is up. Only now can PPP !--- negotiation begin. *Mar 1 00:06:36.661: BR0:1 PPP:
Treating connection as a callin *Mar 1 00:06:36.665: BR0:1 PPP: Phase is ESTABLISHING, Passive
Open [0 sess, 0 load] !--- The PPP Phase is ESTABLISHING. LCP negotiation now occurs. *Mar 1
00:06:36.669: BR0:1 LCP: State is Listen *Mar 1 00:06:37.034: BR0:1 LCP: I CONFREQ [Listen] id 7
len 17 !--- This is the incoming CONFREQ. The ID field is 7. *Mar 1 00:06:37.038: BR0:1 LCP:
AuthProto PAP (0x0304C023) *Mar 1 00:06:37.042: BR0:1 LCP: MagicNumber 0x507A214D
(0x0506507A214D) *Mar 1 00:06:37.046: BR0:1 LCP: Callback 0 (0x0D0300) !--- The peer has
requested: !--- Option: Authentication Protocol, Value: PAP !--- Option: MagicNumber (This is
used to detect loopbacks and is always sent.) !--- Option: Callback, Value: 0 (This is for PPP
Callback; MS Callback uses 6.) *Mar 1 00:06:37.054: BR0:1 LCP: O CONFREQ [Listen] id 4 len 15 !-
-- This is an outgoing CONFREQ, with parameters for the peer to implement. !--- Note that the ID
Field is 4, so this is not related to the previous !--- CONFREQ message. *Mar 1 00:06:37.058:
BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:06:37.062: BR0:1 LCP: MagicNumber 0x1081E7E1
(0x05061081E7E1) !--- This router requests: !--- Option: Authentication Protocol, Value: CHAP !-
-- Option: MagicNumber (This is used to detect loopbacks and is always sent.) *Mar 1
00:06:37.066: BR0:1 LCP: O CONFREJ [Listen] id 7 len 7 !--- This is an outgoing CONFREJ for
message with Field ID 7. !--- This is the response to the CONFREQ received first. *Mar 1
00:06:37.070: BR0:1 LCP: Callback 0 (0x0D0300) !--- The option that this router rejects is
Callback. !--- If the router wanted to do MS Callback rather than PPP Callback, it !--- would
have sent a CONFNAK message instead. *Mar 1 00:06:37.098: BR0:1 LCP: I CONFACK [REQsent] id 4
len 15 !--- This is an incoming CONFACK for a message with Field ID 4. *Mar 1 00:06:37.102:
BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:06:37.106: BR0:1 LCP: MagicNumber 0x1081E7E1
(0x05061081E7E1) !--- The peer can support all requested parameters. *Mar 1 00:06:37.114: BR0:1
LCP: I CONFREQ [ACKrcvd] id 8 len 14 !--- This is an incoming CONFREQ message; the ID field is
8. !--- This is a new CONFREQ message from the peer in response to the CONFREJ id:7. *Mar 1
00:06:37.117: BR0:1 LCP: AuthProto PAP (0x0304C023) *Mar 1 00:06:37.121: BR0:1 LCP: MagicNumber
0x507A214D (0x0506507A214D) !--- The peer has requested: !--- Option: Authentication Protocol,
Value: PAP !--- Option: MagicNumber (This is used to detect loopbacks and is always sent.) *Mar
1 00:06:37.125: BR0:1 LCP: O CONFNAK [ACKrcvd] id 8 len 9 !--- This is an outgoing CONFNACK for
a message with Field ID 8. *Mar 1 00:06:37.129: BR0:1 LCP: AuthProto CHAP (0x0305C22305) !---
This router recognizes the option Authentication Protocol, !--- but does not accept the value
PAP. In the CONFNAK message, !--- it suggests CHAP instead. *Mar 1 00:06:37.165: BR0:1 LCP: I
CONFREQ [ACKrcvd] id 9 len 15 !--- This is an incoming CONFREQ message with Field ID 9. *Mar 1
00:06:37.169: BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1 00:06:37.173: BR0:1 LCP:
MagicNumber 0x507A214D (0x0506507A214D) !--- CHAP authentication is requested. *Mar 1
00:06:37.177: BR0:1 LCP: O CONFACK [ACKrcvd] id 9 len 15 !--- This is an outgoing CONFACK for a
message with Field ID 9. *Mar 1 00:06:37.181: BR0:1 LCP: AuthProto CHAP (0x0305C22305) *Mar 1
00:06:37.185: BR0:1 LCP: MagicNumber 0x507A214D (0x0506507A214D) *Mar 1 00:06:37.189: BR0:1 LCP:
```

State is Open *!--- This indicates that the LCP state is Open.* *Mar 1 00:06:37.193: BR0:1 **PPP: Phase is AUTHENTICATING, by both** [0 sess, 0 load] *!--- The PPP Phase is AUTHENTICATING. PPP Authentication occurs now. !--- Two-way authentication is now performed (indicated by the both keyword).* *Mar 1 00:06:37.201: BR0:1 **CHAP: O CHALLENGE id 4** len 33 from "maui-soho-01" *!--- This is the outgoing CHAP Challenge. !--- In LCP the routers had agreed upon CHAP as the authentication protocol.* *Mar 1 00:06:37.225: BR0:1 **CHAP: I CHALLENGE id 3** len 33 from "maui-soho-03" *!--- This is an incoming Challenge message from the peer.* *Mar 1 00:06:37.229: BR0:1 CHAP: Waiting for peer to authenticate first *Mar 1 00:06:37.237: BR0:1 **CHAP: I RESPONSE id 4** len 33 from "maui-soho-03" *!--- This is an incoming response from the peer.* *Mar 1 00:06:37.244: BR0:1 **CHAP: O SUCCESS id 4** len 4 *!--- This router has successfully authenticated the peer.* *Mar 1 00:06:37.248: BR0:1 CHAP: Processing saved Challenge, id 3 *Mar 1 00:06:37.260: BR0:1 CHAP: O RESPONSE id 3 len 33 from "maui-soho-01" *Mar 1 00:06:37.292: BR0:1 CHAP: **I SUCCESS id 3** len 4 *!--- This is an incoming Success message. Each side has !--- successfully authenticated the other.* *Mar 1 00:06:37.296: BR0:1 **PPP: Phase is UP** [0 sess, 0 load] *!--- The PPP status is now UP. NCP (IPCP) negotiation begins.* *Mar 1 00:06:37.304: BR0:1 IPCP: **O CONFREQ** [Closed] id 4 len 10 *Mar 1 00:06:37.308: BR0:1 IPCP: Address 172.22.1.1 (0x0306AC160101) *!--- This is an outgoing CONFREQ message. It indicates that !--- the local machine address is 172.22.1.1.* *Mar 1 00:06:37.312: BR0:1 CDPCP: O CONFREQ [Closed] id 4 len 4 *Mar 1 00:06:37.320: BR0:1 CDPCP: I CONFREQ [REQsent] id 4 len 4 *Mar 1 00:06:37.324: BR0:1 **CDPCP**: O CONFACK [REQsent] id 4 len 4 *!--- These messages are for CDP Control Protocol (CDPCP).* *Mar 1 00:06:37.332: BR0:1 IPCP: I CONFREQ [REQsent] id 4 len 10 *Mar 1 00:06:37.336: BR0:1 IPCP: Address 172.22.1.2 (0x0306AC160102) *!--- This is an incoming CONFREQ message that indicates that the peer !--- address is 172.22.1.2. An address of 0.0.0.0 indicates that the peer !--- does not have an address and requests the local router to provide it !--- with an address in IPCP negotiation.* *Mar 1 00:06:37.344: BR0:1 IPCP: O CONFACK [REQsent] id 4 len 10 *Mar 1 00:06:37.348: BR0:1 IPCP: Address 172.22.1.2 (0x0306AC160102) *Mar 1 00:06:37.356: BR0:1 IPCP: I CONFACK [ACKsent] id 4 len 10 *Mar 1 00:06:37.360: BR0:1 IPCP: Address 172.22.1.1 (0x0306AC160101) *Mar 1 00:06:37.363: BR0:1 IPCP: State is Open *!--- The IPCP state is Open. Note that in the IPCP negotiation, each side !--- accepted the IP address of the peer, and one was assigned to the peer.* *Mar 1 00:06:37.371: BR0:1 CDPCP: I CONFACK [ACKsent] id 4 len 4 *Mar 1 00:06:37.375: BR0:1 **CDPCP: State is Open** *!--- This indicates that the CDPCP state is Open.* *Mar 1 00:06:37.387: BR0 **IPCP: Install route to 172.22.1.2** *!--- A route to the peer is installed.* *Mar 1 00:06:38.288: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed state to up *Mar 1 00:06:42.609: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to maui-soho-03

Glosario y mensajes comunes

General

CONFREQ (Solicitud de Configuración):

Una vez que la capa inferior está disponible (Up [Activo]), se envía un mensaje CONFREQ para iniciar la primera fase del PPP (fase LCP). Se utiliza en las fases del LCP y NCP como un intento de configurar la conexión. Para abrir una conexión al par, el dispositivo transmite este mensaje junto con las opciones de configuración y los valores que el remitente desea que el par admita. Todas las opciones y los valores se negocian simultáneamente. Si el par responde con un mensaje CONFREJ o CONFNAK, entonces el router envía otro mensaje CONFREQ con otra serie de opciones y valores.

CONFACK (Configure-Acknowledge [Reconocimiento de Configuración]):

Si todas las opciones en el mensaje CONFREQ son reconocibles y todos los valores aceptables, entonces el router transmite el mensaje CONFACK.

CONFREJ (Configure Reject [Rechazo de Configuración]):

Si alguna opción de configuración recibida en el mensaje CONFREQ no es aceptable o

reconocible, el router responde con un mensaje CONFREJ. Se incluye la opción inaceptable (del CONFREQ) en el mensaje CONFREJ.

CONFACK (Configure Negative Acknowledge [Reconocimiento Negativo de Configuración]):

Si la opción de configuración recibida es reconocible y aceptable, pero alguno de los valores no es aceptable, el router transmite el mensaje CONFNAK. El router agrega la opción y el valor que puede aceptar en el mensaje CONFNAK para que el par pueda incluir esa opción en el mensaje CONFREQ siguiente.

ECHOREQ (Echo Request [Solicitud de Eco]) y ECHOREP (Echo Reply [Respuesta de Eco]):

El PPP utiliza señales de mantenimiento para mantener la integridad de la conexión. Estas señales de mantenimiento constituyen la trama del mensaje ECHOREQ que se envía al par PPP remoto y éste debe responder con una trama ECHOREP al recibir aquélla. De forma predeterminada, si el router pierde cinco tramas de mensaje ECHOREP, el enlace se considera inhabilitado y el PPP se cierra.

TERMREQ (Petición de terminación):

Esta trama indica que el par PPP que envió esta trama finaliza la conexión PPP.

TERMACK (Reconocimiento de finalización):

Este mensaje es transmitido en respuesta al mensaje TERMREQ. Esto termina la conexión PPP.

TERMINATING

Este mensaje indica que la conexión PPP ha sido cerrada. Una conexión LCP o NCP puede interrumpirse:

- en el caso de un cierre administrativo (sólo LCP).
- cuando el nivel más bajo queda fuera de servicio (línea de marcado manual, ISDN y otros).
- cuando las negociaciones no se concretan.
- detección de loops en línea.

LCP (Protocolo de control de enlace)

ACCM (Asynchronous Control Character Map [Mapa de Caracteres de Control Asíncronos]):

Ésta es una de las opciones negociadas de LCP dentro de la trama CONFREQ. El ACCM establece las secuencias de escape de caracteres. Indica al puerto que ignore caracteres de control especificados, incluidos en el flujo de datos. Si el router al otro extremo de la conexión no admite la negociación ACCM, el puerto se ve forzado a utilizar FFFFFFFF. En ese caso, ejecute este comando:

```
ppp accm match 000a000
```

ACFC (Address and Control Field Compression [Compresión de los Campos Control y Dirección]):

La ACFC es una opción de LCP que permite a los puntos finales enviar mensajes hacia adelante y atrás con mayor eficacia.

AuthProto (Authentication Protocol [Protocolo de Autenticación]):

AuthProto es el tipo de protocolo de autenticación negociado en la trama CONFREQ entre los pares de conexión PPP, para utilizarlo en la fase de autenticación. Si no se configura una autenticación PPP, no se visualizará la salida en los parámetros negociados de la trama CONFREQ. Los valores posibles son CHAP o PAP.

Callback "#" (Devolución de llamadas "n.º"):

Este mensaje indica que la opción "devolución de llamadas" está siendo negociada. El número que figura después de "devolución de llamadas" indica qué opción de devolución de llamadas se está negociando. El número 0 representa la devolución de llamadas de PPP normal mientras que el número 6 indica la opción de devolución de llamadas de Microsoft (que está automáticamente disponible en la versión 11.3(2)T de Cisco IOS® Software o versiones posteriores).

CHAP (Challenge Handshake Authentication Protocol [Protocolo de Confirmación de Aceptación de la Autenticación]):

Este mensaje indica que el protocolo de autenticación que está siendo negociado es CHAP.

EndpointDisc (End Point Discriminator [Discriminador de Punto Final]):

Esta es una opción de LCP utilizada para identificar un par PPP en una conexión links múltiples PPP. Para obtener más información, consulte Criterios para la Denominación de Grupos PPP de Enlaces Múltiples.

LCP: El estado está abierto

Este mensaje indica que la negociación LCP ha finalizado con éxito.

LQM (Link Quality Monitoring [Control de Calidad del Enlace])

El LQM está disponible en todas las interfaces seriales que ejecutan el PPP. El LQM controla la calidad del enlace y lo cierra cuando la calidad está por debajo del porcentaje configurado. Los porcentajes se calculan para las direcciones entrantes y salientes. La calidad de salida se calcula mediante la comparación del número total de paquetes y bytes enviados con el número total de paquetes y bytes recibidos por el par. La calidad de entrada se calcula mediante la comparación del número total de paquetes y bytes recibidos con el número total de paquetes y bytes enviados por el par.

Cuando el LQM está habilitado, se envían Informes de Calidad del Enlace (LQR) en cada período de mantenimiento. Los LQR se envían en lugar de las señales de mantenimiento. Todas las señales de mantenimiento entrantes se responden como es debido. Si no se configura el LQM, las señales de mantenimiento se envían cada período de mantenimiento y todos los LQR entrantes se responden con un LQR.

MagicNumber

El soporte de Magic Number está disponible en todas las interfaces seriales. El PPP siempre intenta negociar los Magic Numbers, que se utilizan para detectar redes con bucles de retorno. Se envía una cadena aleatoria a través del link y si se devuelve el mismo valor, entonces el router determina que el enlace posee un bucle de retorno.

El link pudo o no se pudo tomar abajo sobre la detección del circuito hecho atrás; depende del uso del comando down-when-looped.

PAP (Password Authentication Protocol [Protocolo de Autenticación de Contraseña])

Este mensaje indica que el protocolo de autenticación que se está negociando para ser utilizado por los pares PPP es el PAP. Para obtener más información sobre el PAP, consulte Configuración y Solución de Problemas del Password Authentication Protocol (PAP) del PPP.

PFC (Protocol Field Compression [Compresión de Campos del Protocolo])

Esta opción activa y desactiva la función de compresión para los campos del protocolo.

MRRU (Max Receive Reconstructed Unit [Unidad Reconstruida de Recepción Máxima])

Ésta es una opción de LCP negociada en el proceso de configuración de LCP de enlaces múltiples PPP. Esta opción determina el número máximo de bytes que pueden constituir una trama. Si no se negocia la MRRU en el LCP, entonces no puede ejecutarse el PPP de Enlaces Múltiples (MPPP) en el enlace.

MRU (Maximum Received Unit [Unidad Máxima Recibida])

La MRU es una opción de LCP negociada en la trama CONFREQ para negociar el tamaño de los paquetes intercambiados.

Autenticación

AUTH-REQ (Authentication Request [Solicitud de Autenticación])

Esta trama es enviada desde el par PPP local (en el que la autenticación está habilitada) al par remoto. Solicita al par remoto que envíe un nombre de usuario y una contraseña válidos para la autenticación de la conexión PPP. Esta trama sólo es utilizada por el PAP.

AUTH-ACK (Authentication Acknowledge [Reconocimiento de Autenticación])

Esta trama se envía desde el par PPP autenticado al par PPP que autentica. Esta trama lleva el par válido de nombre de usuario y contraseña. Y se implementa sólo cuando se utiliza el PAP para la autenticación de la conexión PPP.

AUTH-NAK o FAILURE (Autenticación No Reconocida o Falla)

Esta trama es enviada desde el par PPP que autentica cuando la autenticación falló en dicho par.

DESAFÍO

Esta es la trama de desafío CHAP que se envía desde la entidad par PPP que autentica hacia la entidad par PPP autenticada. La trama de desafío consiste en un ID, un número aleatorio y el nombre del host del servidor de comunicación local o el nombre del usuario en el dispositivo remoto. Esta trama se implementa sólo cuando se utiliza el CHAP para la autenticación de la conexión PPP.

RESPUESTA

Esta trama es la respuesta CHAP enviada desde el par PPP autenticado al par PPP que autentica.

La respuesta requerida consta de dos partes:

- Una salida hash MD5 del secreto compartido.
- El nombre del host del dispositivo remoto o el nombre del usuario en el dispositivo remoto.

Esta trama se implementa sólo cuando se utiliza el CHAP para la autenticación de la conexión PPP.

NCP

Address a.b.c.d (Dirección a.b.c.d)

- En un mensaje CONFREQ saliente, este valor indica la dirección IP que el router local desea utilizar. Si la dirección incluida es 0.0.0.0, la máquina local solicita al par que le proporcione una dirección IP que pueda utilizar.
- En un mensaje CONFREQ de entrada, este valor indica la dirección IP que el par desea utilizar. Si la dirección incluida es 0.0.0.0, el par solicita a la máquina local que le proporcione una dirección IP que pueda utilizar.
- En un mensaje CONFNAK de salida, este valor indica la dirección IP que el par debería usar en lugar de la que el par sugirió en el mensaje CONFREQ.
- En un mensaje CONFNAK entrante, este valor indica la dirección IP que debe utilizar la máquina local, en lugar de la dirección sugerida en el mensaje CONFREQ anterior.
- En un mensaje CONFACK saliente, este valor indica que la dirección IP solicitada por el par es aceptable para la máquina local.
- En un mensaje CONFACK de entrada, este valor indica que la dirección IP solicitada por la máquina local es aceptable para el par.

CCP (Compression Control Protocol [Protocolo de Control de Compresión])

Este mensaje indica que se está negociando un protocolo de compresión entre ambos pares PPP. Cisco IOS Software admite que estos protocolos de compresión se negocien en una conexión PPP:

- Compresión Punto a Punto de Microsoft (MS-PPC)

- stacker
- predictor

CDPCP (Cisco Discovery Protocol Control Protocol [Protocolo de Control del Protocolo Cisco Discovery])

Este mensaje indica que la negociación CDP ocurre en la fase NCP. Para desactivar el CDP en el router, ejecute el comando **no cdp run**.

CODEREJ (Code Reject [Rechazo de Código])

Se envía un paquete CODEREJ al recibir un paquete indescifrable del par PPP remoto.

Install route to a.b.c.d (Instalar ruta hacia a.b.c.d)

Una vez que el router finaliza el IPCP (fase NCP para el protocolo IP de L3), debe instalar la dirección IP dada hacia el par PPP remoto en la tabla de ruteo y debe visualizarse como una ruta conectada en dicha tabla. Si no ve este mensaje, verifique que el comando **no peer neighbor-route** no esté configurado.

IPCP (IP Control Protocol [Protocolo de Control IP])

Este valor indica que IP es la capa de red que se está negociando en la fase NCP.

IPCP State is Open (El Estado del IPCP es Abierto)

Este mensaje indica que el IPCP (fase NCP para el protocolo IP de L3) se completó con éxito.

PROTREJ (Protocol Reject [Rechazo del Protocolo])

El par PPP, al recibir un paquete PPP con un campo de protocolo desconocido, utiliza el mensaje PROTREJ para indicar que el par ha intentado utilizar un protocolo no admitido. Cuando un dispositivo PPP recibe un mensaje PROTREJ, debe suspender el envío de paquetes del protocolo indicado cuanto antes.

Información Relacionada

- Configuración y resolución de problemas del Protocolo de autenticación de contraseñas (PAP, por sus siglas en inglés) de PPP
- Autenticación de PPP utilizando los comandos ppp chap hostname y ppp authentication chap callin
- Cómo funciona y se configura la autenticación PPP CHAP
- Resolución de problemas de autenticación de PPP (CHAP o PAP)
- Páginas de soporte de la tecnología de marcación
- Soporte Técnico - Cisco Systems