Tecnología de marcación manual: Técnicas de resolución de problemas

Contenido

Introducción

Dialup es simplemente la aplicación de la Red de Telefonía Pública Conmutada (PSTN) que transporta datos en nombre del usuario final. Implica un dispositivo Customer Premises Equipment (CPE) que envía al switch de teléfono un número de teléfono al cual dirigir una conexión. Cisco3600, AS5200, AS5300 y AS5800 son todos ejemplos de routers que tienen la capacidad de ejecutar un PRI junto con bancos de módems digitales. El AS2511, por otra parte, es un ejemplo de router que se comunica con módems externos.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de lo siguiente:

El mercado de los operadores ha crecido significativamente y el mercado exige ahora mayores densidades de módem. La respuesta a esta necesidad es un mayor grado de interoperación con el equipo de la compañía telefónica y el desarrollo del módem digital. Se trata de un módem capaz de acceder directamente a la red PSTN. Como resultado, se han desarrollado módems CPE más rápidos que aprovechan la claridad de la señal que disfrutan los módems digitales. El hecho de que los módems digitales que se conectan a la PSTN a través de una PRI o BRI puedan transmitir datos a más de 53k usando el estándar de comunicación V.90, da fe del éxito de la idea.

Los primeros servidores de acceso fueron Cisco2509 y Cisco2511. El AS2509 podría soportar 8 conexiones entrantes usando módems externos, y el AS2511 podría soportar 16. El AS5200 se introdujo con 2 PRI y podía admitir 48 usuarios usando módems digitales, y representaba un gran avance en tecnología. Las densidades de los módems han aumentado constantemente con el AS5300 que admite 4 y luego 8 PRI. Por último, el AS5800 se introdujo para cubrir las necesidades de las instalaciones de clase de operador que necesitaban gestionar decenas de T1 entrantes y cientos de conexiones de usuario.

Un par de tecnologías obsoletas merecen mención en un debate histórico sobre la tecnología del marcador. 56Kflex es un estándar de módem de 56k más antiguo (anterior a V.90) propuesto por Rockwell. Cisco admite la versión 1.1 del estándar 56Kflex en sus módems internos, pero recomienda migrar los módems CPE a V.90 lo antes posible. Otra tecnología obsoleta es el AS5100. El AS5100 fue una empresa conjunta entre Cisco y un fabricante de módem. El AS5100 se creó como una manera de aumentar la densidad del módem mediante el uso de tarjetas de cuatro módems. Se trataba de un grupo de AS2511s construido como tarjetas que se insertaban en una placa de interconexiones compartida por tarjetas de cuatro módems y una tarjeta T1 dual.

Componentes Utilizados

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

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Resolución de problemas de llamadas entrantes

La resolución de problemas de una llamada entrante comienza en la parte inferior y funciona en su sentido ascendente. El flujo general de razonamiento busca lo siguiente:

1. ¿Vemos llegar la llamada? (La respuesta *afirmativa* avanza a la siguiente pregunta)
2. ¿El extremo receptor contesta la llamada?
3. ¿Se ha completado la llamada?
4. ¿Los datos pasan a través del enlace?
5. ¿Se ha establecido el período de sesiones? (PPP o terminal)

Para las conexiones del módem, una llamada de datos se ve igual que una sesión de terminal que llega hasta el final donde la llamada de datos va a negociar PPP.

En el caso de las llamadas entrantes que involucran módems digitales, asegúrese primero de que la ISDN o CAS subyacentes estén recibiendo la llamada. Si se utiliza un módem externo, se pueden omitir las secciones de grupos ISDN y CAS.

Resolución de problemas de llamadas ISDN entrantes

Utilice el comando **debug isdn q931**. Este es un ejemplo de resultado de una conexión exitosa:

```
Router# debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
 Bearer Capability i = 0x8890
 Channel ID i = 0x89
 Calling Party Number i = 0x0083, `5551234'
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

El mensaje de configuración indica que el extremo remoto está iniciando una conexión. Los números de referencia de llamada se mantienen como un par. En este caso, el número de referencia de llamada para el lado entrante de la conexión es 0x06 y el número de referencia de llamada del lado saliente de la conexión es 0x86. La función portadora (a menudo denominada portadora) indica al router qué tipo de llamada entra. En este caso, la conexión es de tipo 0x8890. Ese valor indica "Velocidad ISDN 64 Kb/s". Si el portador hubiera sido 0x8090A2, habría indicado "llamada u-law de voz/voz".

Si no aparece ningún mensaje de configuración, debe verificar el número correcto llamándolo manualmente, si se ha aprovisionado la voz. También debe verificar el estado de la interfaz ISDN (consulte Uso del Comando **show isdn status** para Troubleshooting de BRI). Si todo esto se desprotege, asegúrese de que el autor de la llamada realiza la llamada correcta. Esto se puede hacer poniéndose en contacto con la compañía telefónica. El originador de la llamada puede rastrear la llamada para ver dónde se envía. Si la conexión es de larga distancia, intente una portadora de larga distancia diferente usando un código de larga distancia 1010.

Si la llamada entrante es una llamada de módem asincrónica, asegúrese de que la línea esté aprovisionada para permitir llamadas de voz.

Nota: La llamada de módem asíncrono BRI es una función de los 3600 routers que ejecutan 12.0(3)T o posterior. Requiere una revisión reciente del hardware del módulo de red de la interfaz BRI. Los módulos WIC no admiten llamadas de módem asíncronas.

Si la llamada ha llegado pero no ha finalizado, busque un código de causa (consulte la tabla 17-10). Una finalización correcta se indica mediante la conexión de retorno.

Si se trata de una llamada de módem asíncrono, vaya a la sección "Resolución de problemas de llamadas del módem entrante".

En este momento, la llamada ISDN está conectada, pero no se ha visto ningún dato en el link. Utilice el comando **debug ppp negotiation** para ver si hay tráfico PPP que atraviesa la línea. Si no ve tráfico, puede haber una discordancia de velocidad. Para determinar si este es el caso, utilice el comando **show running-config privileged exec** para ver la configuración del router. Verifique las entradas del comando de configuración de la interfaz **dialer map** en el router local y remoto. Estas

entradas deben ser similares a las siguientes:

```
dialer map ip 131.108.2.5 speed 56 name C4000
```

Para los perfiles de marcador, se debe definir una clase de mapa para establecer la velocidad. Tenga en cuenta que, de forma predeterminada, las interfaces ISDN intentan utilizar velocidades de comunicaciones de 64K en cada canal.

Para obtener información detallada sobre la configuración de mapas y perfiles de marcador, refiérase a la *Guía de Configuración de Soluciones de Marcado de Cisco IOS*, la *Referencia de Comandos de Soluciones de Marcado* y la *Guía de Configuración Rápida de Soluciones de Marcado*.

Si recibe paquetes PPP válidos, el link está activo y funcionando. En este momento debe continuar con la sección "Resolución de problemas de PPP".

Solución de problemas de llamadas CAS entrantes

Para resolver problemas del grupo CAS que atiende la conectividad a los módems, utilice los comandos **debug modem**, **debug modem csm** y **debug cas**.

Nota: El comando **debug cas** apareció por primera vez en 12.0(7)T para AS5200 y AS5300. Las versiones anteriores de IOS utilizan el servicio de comando de configuración de nivel del sistema interno junto con el comando exec **modem-mgmt debug rbs**. La depuración de esta información en un AS5800 requiere la conexión a la propia tarjeta de línea troncal.

En primer lugar, determine si el switch de la compañía telefónica se "descolgó" para indicar la llamada entrante. Si no lo hizo, verifique el número al que se llama. Para ello, conecte un teléfono a la línea telefónica del lado de origen y llame al número. Si la llamada entra correctamente, el problema se encuentra en el CPE de origen. Si la llamada todavía no aparece en el CAS, verifique el T1 (capítulo 15).En este caso, utilice el comando **debug serial interfaces**.

A continuación se muestra una buena conexión usando **debug modem CSM**:

```
Router# debug modem csm
CSM_MODEM_ALLOCATE: slot 1 and port 0 is allocated.
MODEM_REPORT(0001): DEV_INCALL at slot 1 and port 0
CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 0
CSM_RING_INDICATION_PROC: RI is on
CSM_RING_INDICATION_PROC: RI is off
CSM_PROC_IC1_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
MODEM_REPORT(0001): DEV_CONNECTED at slot 1 and port 0
CSM_PROC_IC2_WAIT_FOR_CARRIER: CSM_EVENT_ISDN_CONNECTED at slot 1, port 0
```

En este ejemplo, la llamada se dirigió a un módem. Si la llamada se dirigió a un módem, vaya a la sección "Resolución de problemas de llamadas del módem entrante", a continuación.

Solución de problemas de llamadas de módem entrantes

Utilice los siguientes comandos debug cuando resuelva las llamadas del módem entrante:

- **debug modem**
- **debug modem csm** (para módems digitales integrados)

Utilice los siguientes comandos debug junto con para indicar la nueva llamada entrante:

- **debug isdn q931**
- **debug cas**

Suponiendo que la llamada llegue al módem, el módem necesita atender la llamada.

Consejos para depurar módems externos

Para facilitar la depuración en un módem externo conectado a una línea TTY, aumente el volumen del altavoz. Esto ayuda a hacer que algunos problemas sean más evidentes.

Cuando el módem de origen llama, ¿suena el módem de recepción? Si no es así, verifique el número e intente realizar una llamada manual desde el sitio remoto. Intente utilizar un teléfono normal también en el extremo receptor. Sustituya los cables y el hardware según sea necesario.

Captura de llamada de módem asíncrono

Si un módem externo no responde, verifique el cableado entre el módem y el servidor de acceso o router. Confirme que el módem está conectado al puerto TTY o auxiliar del router con un cable RJ-45 enrollado y un adaptador MMOD DB-25. Cisco recomienda y admite esta configuración de cable para los puertos RJ-45. Tenga en cuenta que estos conectores suelen estar etiquetados: *Módem.*

El cableado RJ-45 viene en algunos tipos: recto, enrollado y cruzado. Puede determinar el tipo de cableado manteniendo los dos extremos de un cable RJ-45 lado a lado. Verán ocho tiras coloreadas, o pines, en cada extremo.

- Si el orden de los pines coloreados es igual en cada extremo, el cable es de conexión directa.
- Si el orden de los colores es opuesto en cada extremo, el cable es enrollado.
- El cable es un cable de cruce si los colores indican lo siguiente:

Cable de cruce de RJ45 a RJ45:

```
RJ45                    RJ45
          5 ------------------ 2
          2 ------------------ 5
          4 ------------------ 1
          1 ------------------ 4
```

Para asegurarse de que la señalización es correcta, utilice el comando **show line** descrito en el capítulo 16.

Dejando a un lado los problemas de cableado, un módem externo debe inicializarse para contestar automáticamente. Verifique el módem remoto para ver si está configurado como respuesta automática. Por lo general, se enciende una luz indicadora AA cuando se establece la respuesta automática. Establezca el módem remoto en respuesta automática si aún no está configurado. Para obtener información sobre cómo verificar y cambiar los parámetros del módem, consulte la documentación del módem. Utilice un telnet inverso para inicializar el módem (consulte el capítulo 16).

Captura de llamada de módem digital (integrado)

En un módem externo está claro si la llamada se está contestando, pero los módems internos requieren una llamada manual al número receptor. Escuche el tono de respuesta (ABT). Si no oye un ABT, verifique la configuración para las dos cosas siguientes:

1. Asegúrese de que el comando **isdn incoming-voice modem** exista bajo cualquier interfaz ISDN que maneje conexiones de módem entrante.
2. Bajo la configuración de línea para el TTY del módem, asegúrese de que el comando **modem inout** exista.

También es posible que el Módulo de conmutación de llamadas (CSM) no haya asignado un módem interno para manejar la llamada entrante. Este problema puede deberse a que el módem o los conjuntos de recursos se están configurando para muy pocas conexiones entrantes. También puede significar que el servidor de acceso simplemente esté fuera de los módems. Verifique la disponibilidad de los módems y ajuste la configuración del agrupamiento de módems o del administrador de recursos apropiadamente. Si se asignó un módem y la configuración muestra **modem inout**, recopile debugs y comuníquese con Cisco para obtener ayuda.

Formación del módem

Si el módem receptor eleva el DSR, la preparación se realizó correctamente. Las fallas de la formación pueden indicar un problema de circuito o incompatibilidad del módem.

Para llegar a la parte inferior de un problema de módem individual, vaya al mensaje AT en el módem de origen mientras está conectado a la línea de interés POTS. Si llama a un módem digital en un servidor de acceso de Cisco, prepárese para grabar un archivo .wav de la música de preparación o de la secuencia de aprendizaje de deterioro digital (DIL). La DIL es la puntuación musical (secuencia PCM) que el módem analógico V.90 de origen indica al módem digital de recepción que se reproduzca. La secuencia permite que el módem analógico detecte cualquier deterioro digital en el circuito; como múltiples conversiones D/A, una ley/u-law, bits robados o pads digitales. Si no oye el DIL, los módems no negociaron V.90 en V.8/V.8bis (es decir, un problema de compatibilidad del módem). Si oye el DIL y un nuevo tren en V.34, el módem analógico decidió (en base a la reproducción DIL) que V.90 era inviable.

¿La música tiene ruido? Si es así, limpie el circuito.

¿El cliente se rinde rápidamente, sin ejecutar la formación V.34? Por ejemplo, quizás no sabe qué hacer cuando escucha el V.8bis. En este caso, debería intentar desactivar V.8bis (por lo tanto, K56Flex) en el servidor (si es aceptable). Debe obtener el nuevo firmware del cliente o intercambiar el módem del cliente. Como alternativa, el extremo de marcación podría insertar cinco comas al final de la cadena de marcado. Esto retrasa la escucha del módem que llama y hará que el tono V.8bis del servidor receptor se agote sin afectar al módem del cliente. Cinco comas en la cadena de marcado es una directriz general y puede que sea necesario ajustar para permitir las condiciones locales.

Establecimiento de sesión

En este punto de la secuencia, los módems están conectados y entrenados. Ahora es el momento de averiguar si se está produciendo algún tráfico correctamente.

Si la línea que recibe la llamada se configura con **autoselect ppp** y la interfaz asíncrona se configura con el **modo asíncrono interactivo**, utilice el comando **debug modem** para verificar el proceso de autoselección. A medida que el tráfico entra en el link asíncrono, el servidor de acceso

examinará el tráfico para determinar si el tráfico se basa en caracteres o en paquetes. Según la determinación, el servidor de acceso iniciará una sesión PPP o no irá más allá de tener una sesión exec en la línea.

Secuencia de autoselect normal con paquetes PPP LCP entrantes:

```
*Mar  1 21:34:56.958: TTY1: DSR came up
*Mar  1 21:34:56.962: tty1: Modem: IDLE->READY
*Mar  1 21:34:56.970: TTY1: EXEC creation
*Mar  1 21:34:56.978: TTY1: set timer type 10, 30 seconds
*Mar  1 21:34:59.722: TTY1: Autoselect(2) sample 7E
 !--- The inbound traffic is displayed in hexadecimal format. This is based on the !--- bits
coming in over the line, regardless of whether the bits are ASCII !--- characters or elements of
a packet. The bits represented in this example are !--- correct for a LCP packet. Anything
different would be either a malformed packet !--- or character traffic. *Mar 1 21:34:59.726:
TTY1: Autoselect(2) sample 7EFF *Mar 1 21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D *Mar 1
21:34:59.730: TTY1: Autoselect(2) sample 7EFF7D23 *Mar 1 21:34:59.734: TTY1 Autoselect cmd: ppp
negotiate !--- Having determined that the inbound traffic is actually an LCP packet, the access
!--- server triggers the PPP negotiation process. *Mar 1 21:34:59.746: TTY1: EXEC creation *Mar
1 21:34:59.746: TTY1: create timer type 1, 600 seconds *Mar 1 21:34:59.794: TTY1: destroy timer
type 1 (OK) *Mar 1 21:34:59.794: TTY1: destroy timer type 0 *Mar 1 21:35:01.798: %LINK-3-UPDOWN:
Interface Async1, changed state to up !--- The async interface changes state to up, and the PPP
negotiation (not shown) !--- commences.
```

Si la llamada es una sesión PPP y si el **modo asíncrono dedicado** está configurado en la interfaz asíncrona, utilice el comando **debug ppp negotiation** para ver si algún paquete de solicitud de configuración viene del extremo remoto. Los debugs muestran estos como CONFREQ. Si observa tanto los paquetes PPP entrantes como los salientes, continúe con "Troubleshooting PPP". De lo contrario, conéctese desde el extremo de origen de la llamada con una sesión en modo de carácter (o "exec") (es decir, una sesión que no es PPP).

Nota: Si el extremo receptor muestra **módem asíncrono dedicado** bajo la interfaz asíncrona, un dial-in exec sólo muestra lo que parece ser basura ASCII aleatoria. Para permitir una sesión de terminal y aún tener capacidad PPP, utilice el comando de configuración de interfaz asíncrona **async mode Interactive**. Bajo la configuración de la línea asociada, utilice el comando **autoselect ppp**.

El módem no puede enviar ni recibir datos

Si los módems se conectan con una sesión de terminal y no se encuentra ningún dato, verifique las siguientes causas posibles y los cursos de acción sugeridos:

- **La configuración de velocidad del módem no está bloqueada**Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe indicar las velocidades Tx y Rx configuradas actualmente.Para obtener una explicación del resultado del comando **show line**, vea la sección "Uso de Comandos Debug" en el capítulo 15.Si la línea no está configurada a la velocidad correcta, utilice el comando de configuración de línea **speed** para establecer la velocidad de línea en el servidor de acceso o la línea del router. Establezca el valor en la velocidad más alta común entre el módem y el servidor de acceso o puerto del router. Para establecer la velocidad en baudios de terminal, utilice el comando de configuración de línea **speed**. Este comando establece las velocidades de transmisión (a terminal) y recepción (desde terminal).Sintaxis:**velocidad** *bps*Descripción de la Sintaxis:*bps*: velocidad en baudios en bits por segundo (bps). El valor predeterminado es 9600 bps.El siguiente ejemplo establece las líneas 1 y 2 en un servidor de acceso Cisco 2509 en 115200

bps:

```
line 1 2
speed 115200
```

Nota: Si, por alguna razón, no puede utilizar el control de flujo, limite la velocidad de línea a 9600 bps. Es probable que las velocidades más rápidas conduzcan a la pérdida de datos.Utilice el comando **show line** exec de nuevo y confirme que la velocidad de línea está establecida en el valor deseado.Cuando esté seguro de que el servidor de acceso o la línea del router están configurados para la velocidad deseada, inicie una sesión Telnet inversa al módem a través de esa línea. Para obtener más información, consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" del capítulo 16.Utilice una cadena de comandos del módem que incluya el comando "lock DTE speed" para el módem. Consulte la documentación del módem para obtener la sintaxis exacta del comando de configuración.**Nota:** El comando lock DTE speed, al que también se podría llamar *port rate adjust* o *buffered mode*, a menudo está relacionado con la manera en que el módem maneja la corrección de errores. Este comando varía ampliamente de un módem a otro.El bloqueo de la velocidad del módem garantiza que el módem siempre se comunica con el servidor de acceso o router de Cisco a la velocidad configurada en el puerto auxiliar de Cisco. Si no se utiliza este comando, el módem vuelve a la velocidad del link de datos (la línea telefónica), en lugar de comunicarse a la velocidad configurada en el servidor de acceso.

- **Control de flujo de hardware no configurado en un módem o router local o remoto**Utilice el comando **show line** ***aux-line-number*** exec y busque lo siguiente en el campo Capacidades:

  ```
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
  ```

  Para obtener más información, consulte Interpretación de la Salida de Mostrar Línea en el Capítulo 16.Si no se menciona el control de flujo de hardware en este campo, el control de flujo de hardware no está habilitado en la línea. Se recomienda el control de flujo de hardware para las conexiones de servidor a módem de acceso.Para obtener una explicación del resultado del comando **show line**, vea la sección "Uso de Comandos Debug" en el capítulo 15.Configure el control de flujo de hardware en la línea mediante el comando de configuración de línea de hardware flowcontrol.Para establecer el método de control de flujo de datos entre el terminal u otro dispositivo serial y el router, utilice el comando de configuración de línea **flowcontrol**. Utilice la forma no de este comando para inhabilitar el control de flujo.Sintaxis:**flowcontrol {none | software [lock] [in | out] | hardware [in | out]}**Descripción de la Sintaxis:**none**: desactiva el control de flujo.**software**: establece el control de flujo de software. Una palabra clave opcional especifica la dirección: **in** hace que el software Cisco IOS escuche el control de flujo desde el dispositivo conectado, y **out** hace que el software envíe información de control de flujo al dispositivo conectado. Si no especifica una dirección, se asumen ambas.**lock** - Hace imposible apagar el control de flujo del host remoto cuando el dispositivo conectado necesita control de flujo de software. Esta opción se aplica a las conexiones que utilizan los protocolos Telnet o rlogin.**hardware**: establece el control de flujo de hardware. Una palabra clave opcional especifica la dirección: **in** hace que el software escuche el control de flujo desde el dispositivo conectado y **out** hace que el software envíe información de control de flujo al dispositivo conectado. Si no especifica una dirección, se asumen ambas. Para obtener más información sobre el control de flujo de hardware, consulte el manual de hardware que se envió con el router.Ejemplo:El siguiente ejemplo establece el control de flujo de hardware en la línea 7:

  ```
  line 7
  flowcontrol hardware
  ```

  Nota: Si por alguna razón no puede utilizar el control de flujo, limite la velocidad de línea a 9600 bps. Es probable que las velocidades más rápidas conduzcan a la pérdida de

datos.Después de habilitar el control de flujo de hardware en el servidor de acceso o la línea del router, inicie una sesión Telnet inversa al módem a través de esa línea. Para obtener más información, consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" del capítulo 16.Utilice una cadena de comandos del módem que incluya el comando **RTS/CTS Flow** para su módem. Este comando asegura que el módem esté utilizando el mismo método de control de flujo (es decir, control de flujo de hardware) que el servidor de acceso o router de Cisco. Consulte la documentación del módem para obtener la sintaxis exacta del comando de configuración.

- **Comandos mal configurados dialer map**Utilice el comando **show running-config privileged** exec para ver la configuración del router. Verifique las entradas del comando **dialer map** para ver si se especifica la palabra clave **broadcast**.Si falta la palabra clave, agréguela a la configuración.Sintaxis:**dialer map** ***protocol next-hop-address*** **[name** ***hostname*****] [broadcast] [*****dial-string*****]**Descripción de la Sintaxis:*protocol* - El protocolo sujeto a la asignación. Entre las opciones se incluyen IP, IPX, bridge y Snapshots.*next-hop-address* - La dirección del protocolo de la interfaz asíncrona del sitio opuesto.**name** ***hostname*** : parámetro requerido utilizado en la autenticación PPP. Es el nombre del sitio remoto para el cual se crea el mapa del marcador. El nombre distingue entre mayúsculas y minúsculas y debe coincidir con el nombre de host del router remoto.**broadcast**: palabra clave opcional que transmite paquetes (por ejemplo, IP RIP o IPX RIP/SAP updates) que se reenvían al destino remoto. En las configuraciones de ejemplo de ruteo estático, no se desean actualizaciones de ruteo y se omite la palabra clave **broadcast**.*dial-string*: el número de teléfono del sitio remoto. Se deben incluir todos los códigos de acceso (por ejemplo, 9 para salir de una oficina, códigos de marcación internacionales, códigos de área).Asegúrese de que los comandos **dialer map** especifican las direcciones de salto siguiente correctas.Si la dirección del salto siguiente es incorrecta, cámbiela usando el comando **dialer map**.Asegúrese de que todas las demás opciones de los comandos dialer map estén correctamente especificadas para el protocolo que está utilizando.Para obtener información detallada sobre la configuración de mapas de marcador, refiérase a la *Guía de Configuración de Networking de Área Amplia de Cisco IOS* y a la *Referencia de Comandos de Networking de Área Amplia*.
- **Problema con la marcación del módem**Asegúrese de que el módem de marcación esté operativo y conectado correctamente al puerto correcto. Determine si otro módem funciona cuando está conectado al mismo puerto.

La depuración de una sesión de exec entrante suele dividirse en algunas categorías principales:

- El cliente de marcación recibe No Exec Prompt
- Sesión de marcado "basura"
- Sesión de marcación abierta en una sesión existente
- El Módem De Recepción De Marcación No Se Desconecta Correctamente

El cliente de marcado recibe mensaje sin exec

- **La selección automática está activada en la línea**Intente acceder al modo exec pulsando Intro.
- **La línea se configura con el comando no exec**Utilice el comando **show line** exec para ver el estado de la línea apropiada.Verifique el campo Capacidades para ver si dice "exec suppress". Si este es el caso, el comando de configuración de línea **no exec** está habilitado.Configure el comando de configuración de línea **exec** en la línea para permitir que

se inicien las sesiones exec. Este comando no tiene argumentos ni palabras clave.El siguiente ejemplo activa el exec en la línea 7:

```
line 7
exec
```

- **El control de flujo no está habilitado.orEl control de flujo se habilita sólo en un dispositivo (DTE o DCE).orEl control de flujo está mal configurado.**Utilice el comando **show line** *aux-line-number* exec y busque lo siguiente en el campo Capacidades:

```
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
```

Para obtener más información, consulte Interpretación de la Salida de Mostrar Línea en el Capítulo 16.Si no se menciona el control de flujo de hardware en este campo, el control de flujo de hardware no está habilitado en la línea. Se recomienda el control de flujo de hardware para las conexiones de servidor a módem de acceso.Para obtener una explicación del resultado del comando show line, consulte la sección "Uso de comandos de depuración" del capítulo 15.Configure el control de flujo de hardware en la línea mediante el comando de configuración de línea **flowcontrol hardware**. El siguiente ejemplo establece el control de flujo de hardware en la línea 7:

```
line 7
flowcontrol hardware
```

Nota: Si por alguna razón no puede utilizar el control de flujo, limite la velocidad de línea a 9600 bps. Es probable que las velocidades más rápidas conduzcan a la pérdida de datos.Después de habilitar el control de flujo de hardware en el servidor de acceso o la línea del router, inicie una sesión Telnet inversa al módem a través de esa línea. Para obtener más información, consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" del capítulo 16.Utilice una cadena de comandos del módem que incluya el comando RTS/CTS Flow para el módem. Este comando asegura que el módem esté utilizando el mismo método de control de flujo (es decir, control de flujo de hardware) que el servidor de acceso o router de Cisco. Consulte la documentación del módem para obtener la sintaxis exacta del comando de configuración.

- **La configuración de velocidad del módem no está bloqueada**Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe indicar las velocidades Tx y Rx configuradas actualmente.Para obtener una explicación del resultado del comando show line, vea la sección "Uso de comandos de depuración" del capítulo 15.Si la línea no está configurada a la velocidad correcta, utilice el comando de configuración de la línea de velocidad para establecer la velocidad de línea en el servidor de acceso o la línea del router. Establezca el valor en la velocidad más alta común entre el módem y el servidor de acceso o puerto del router. Para establecer la velocidad en baudios de terminal, utilice el comando speed line configuration. Este comando establece las velocidades de transmisión (a terminal) y recepción (desde terminal).Sintaxis:**velocidad** *bps*Descripción de la Sintaxis:*bps*: velocidad en baudios en bits por segundo (bps). El valor predeterminado es 9600 bps.Ejemplo:El siguiente ejemplo establece las líneas 1 y 2 en un servidor de acceso Cisco 2509 en 115200 bps:

```
line 1 2
speed 115200
```

Nota: Si por alguna razón no puede utilizar el control de flujo, limite la velocidad de línea a 9600 bps. Es probable que las velocidades más rápidas conduzcan a la pérdida de datos.Utilice el comando **show line** exec de nuevo y confirme que la velocidad de línea está establecida en el valor deseado.Cuando esté seguro de que el servidor de acceso o la línea del router están configurados para la velocidad deseada, inicie una sesión Telnet inversa al

módem a través de esa línea. Para obtener más información, consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" del capítulo 16.Utilice una cadena de comandos del módem que incluya el comando **lock** DTE speed para el módem. Consulte la documentación del módem para obtener la sintaxis exacta del comando de configuración.**Nota:** El comando de velocidad **lock** DTE, que también podría denominarse modo de ajuste de velocidad de puerto o modo almacenado en búfer, se relaciona a menudo con la manera en que el módem maneja la corrección de errores. Este comando varía ampliamente de un módem a otro.El bloqueo de la velocidad del módem garantiza que el módem siempre se comunica con el servidor de acceso o router de Cisco a la velocidad configurada en el puerto auxiliar de Cisco. Si no se utiliza este comando, el módem vuelve a la velocidad del link de datos (la línea telefónica) en lugar de comunicarse a la velocidad configurada en el servidor de acceso.

Las sesiones de marcado ven "basura"

- **La configuración de velocidad del módem no está bloqueada**Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe indicar las velocidades Tx y Rx configuradas actualmente.Para obtener una explicación del resultado del comando **show line**, vea la sección "Uso de Comandos Debug" en el capítulo 15.Si la línea no está configurada a la velocidad correcta, utilice el comando de configuración de línea **speed** para establecer la velocidad de línea en el servidor de acceso o la línea del router. Establezca el valor en la velocidad más alta común entre el módem y el servidor de acceso o puerto del router.Para establecer la velocidad en baudios de terminal, utilice el comando de configuración de línea **speed**. Este comando establece las velocidades de transmisión (a terminal) y recepción (desde terminal).Sintaxis:*bps* ***de velocidad***Descripción de la Sintaxis:Velocidad en baudios de bps en bits por segundo (bps). El valor predeterminado es 9600 bps.Ejemplo:El siguiente ejemplo establece las líneas 1 y 2 en un servidor de acceso Cisco 2509 en 115200 bps:line 1 2velocidad 115200**Nota:** Si por alguna razón no puede utilizar el control de flujo, limite la velocidad de línea a 9600 bps. Es probable que las velocidades más rápidas conduzcan a la pérdida de datos.Utilice el comando **show line** exec de nuevo y confirme que la velocidad de línea está establecida en el valor deseado.Cuando esté seguro de que el servidor de acceso o la línea del router están configurados para la velocidad deseada, inicie una sesión Telnet inversa al módem a través de esa línea. Para obtener más información, consulte la sección "Establecimiento de una sesión Telnet inversa a un módem" del capítulo 16.Utilice una cadena de comandos del módem que incluya el comando **lock** DTE speed para el módem. Consulte la documentación del módem para obtener la sintaxis exacta del comando de configuración.**Nota:** El comando **lock** DTE speed, que también se podría denominar *port rate adjust* **o** *buffered mode***, a menudo está relacionado con la manera en que el módem maneja la corrección de errores.** Este comando varía ampliamente de un módem a otro.El bloqueo de la velocidad del módem garantiza que el módem siempre se comunica con el servidor de acceso o router de Cisco a la velocidad configurada en el puerto auxiliar de Cisco. Si no se utiliza este comando, el módem vuelve a la velocidad del link de datos (la línea telefónica) en lugar de comunicarse a la velocidad configurada en el servidor de acceso.

Síntoma: La sesión de marcado remoto se abre en una sesión ya existente iniciada por otro usuario. Es decir, en lugar de obtener un mensaje de inicio de sesión, un usuario de marcado ve una sesión establecida por otro usuario (que puede ser un símbolo del sistema UNIX, una sesión de editor de texto, etc.).

Sesión de marcación abierta en una sesión existente

- **Módem configurado para DCD siempre alto**El módem se debe reconfigurar para que tenga DCD alto solamente en CD. Esto se logra generalmente usando la cadena de comando **&C1** del módem, pero verifique la documentación del módem para ver la sintaxis exacta para su módem.Es posible que tenga que configurar la línea de servidor de acceso a la que está conectado el módem con el comando de configuración de línea **no exec**. Borre la línea con el comando **clear line privileged exec**, inicie una sesión Telnet inversa con el módem y reconfigure el módem para que DCD sólo esté alto en el CD.Para finalizar la sesión Telnet, introduzca **disconnect** y reconfigure la línea del servidor de acceso con el **comando exec** line configuration
- **El control del módem no está activado en el servidor de acceso o en el router**Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe mostrarse **inout** o **RIisCD** en la columna Módem. Esto indica que el control del módem está habilitado en la línea del servidor de acceso o del router.Para obtener una explicación de la salida **show line**, vea la sección "Uso de Comandos Debug" en el capítulo 15.Configure la línea para el control del módem mediante el comando de configuración de línea **modem inout**. El control del módem está ahora habilitado en el servidor de acceso.**Nota:** Asegúrese de utilizar el comando **modem inout** en lugar del comando **modem dialin** mientras la conectividad del módem está en cuestión. Este último comando permite a la línea aceptar sólo llamadas entrantes. Se rechazarán las llamadas salientes, lo que hace imposible establecer una sesión Telnet con el módem para configurarla. Si desea habilitar el comando **modem dialin**, hágalo sólo después de estar seguro de que el módem funciona correctamente.
- **Cableado incorrecto**Verifique el cableado entre el módem y el servidor de acceso o router. Confirme que el módem está conectado al puerto auxiliar del servidor de acceso o router con un cable RJ-45 enrollado y un adaptador MMOD DB-25. Cisco recomienda y admite esta configuración de cableado para puertos RJ-45. Estos conectores suelen estar etiquetados: Módem.Hay dos tipos de cableado RJ-45: recto y enrollado. Si mantiene los dos extremos de un cable RJ-45 lado a lado, verá ocho tiras de colores, o pines, en cada extremo. Si el orden de los pines de color es el mismo en cada extremo, el cable está derecho. Si se invierte el orden de los colores en cada extremo, entonces se enrolla el cable.El cable enrollado (CAB-500RJ) es estándar con el 2500/CS500 de Cisco.Utilice el comando **show line** exec para verificar que el cableado es correcto. Vea la explicación del resultado del comando **show line** en la sección "Uso de Comandos Debug" en este capítulo 15.

El Módem De Recepción De Marcación No Se Desconecta Correctamente

- **El módem no detecta DTR**Ingrese la cadena de comando **Hangup DTR modem**. Este comando indica al módem que descarte la portadora cuando la señal DTR ya no se recibe.En un módem compatible con Hayes, la cadena **&D3** se utiliza comúnmente para configurar **Hangup DTR** en el módem. Para obtener la sintaxis exacta de este comando, consulte la documentación del módem.
- **El control del módem no está activado en el router o en el servidor de acceso**Utilice el comando **show line** exec en el servidor de acceso o el router. La salida para el puerto auxiliar debe mostrar **inout** o **RIisCD** en la columna Módem. Esto indica que el control del módem está habilitado en la línea del servidor de acceso o del router.Para obtener una explicación del resultado de show line, vea la sección "Uso de comandos de depuración" del capítulo

15.Configure la línea para el control del módem mediante el comando modem inout line configuration. El control del módem está ahora habilitado en el servidor de acceso.**Nota:** Asegúrese de utilizar el comando **modem inout** en lugar del comando **modem dialin** mientras la conectividad del módem está en cuestión. Este último comando permite a la línea aceptar sólo llamadas entrantes. Se rechazarán las llamadas salientes, lo que hace imposible establecer una sesión Telnet con el módem para configurarla. Si desea habilitar el comando **modem dialin**, hágalo sólo después de estar seguro de que el módem funciona correctamente.

Resolución de problemas de llamadas salientes

Mientras que el enfoque de solución de problemas para las llamadas entrantes comienza en la parte inferior, la resolución de problemas de una conexión saliente comienza en la parte superior. El flujo general de razonamiento busca lo siguiente:

1. ¿El enrutamiento de marcado a petición (DDR) inicia una llamada? (Una respuesta afirmativa avanza a la siguiente pregunta)
2. Si se trata de un módem asincrónico, ¿los scripts de chat emiten los comandos esperados?
3. ¿La llamada llega a PSTN?
4. ¿El extremo remoto contesta la llamada?
5. ¿Se ha completado la llamada?
6. ¿Pasan los datos por el enlace?
7. ¿Se ha establecido el período de sesiones? (PPP o Terminal)

Verificación del funcionamiento del marcador

Para ver si el marcador está tratando de hacer una llamada a su destino remoto, utilice el comando **debug dialer events**. Se puede obtener información más detallada de **debug dialer packet**, pero el comando **debug dialer packet** hace un uso intensivo de recursos y no se debe utilizar en un sistema ocupado que tiene varias interfaces de marcador funcionando.

La siguiente línea de salida de eventos de debug dialer para un paquete IP enumera el nombre de la interfaz DDR y las direcciones de origen y destino del paquete:

```
Dialing cause: Async1: ip (s=172.16.1.111 d=172.16.2.22)
```

Si el tráfico no inicia un intento de marcado, la razón más común es una configuración incorrecta (cualquiera de las definiciones de tráfico interesante, el estado de la interfaz del marcador o el ruteo).

El tráfico no inicia un intento de marcado

- **Falta o no hay definiciones de "tráfico interesante"**Con el comando **show running-config**, asegúrese de que la interfaz esté configurada con un **dialer-group** y de que haya un **dialer-list** de nivel global configurado con un número coincidente.Asegúrese de que el comando **dialer-list** esté configurado para permitir un protocolo completo o para permitir el tráfico que coincida con una lista de accesoVerifique que la lista de acceso declare que los paquetes que cruzan el link son interesantes. Una prueba útil es utilizar el comando exec privilegiado **debug ip**

packet [list number] usando el número de la lista de acceso pertinente. A continuación, intente hacer ping o enviar tráfico de otro modo a través del link. Si los filtros de tráfico interesantes se han definido correctamente, verá los paquetes en el resultado de la depuración. Si no hay salida de depuración de esta prueba, la lista de acceso no coincide con los paquetes.

- **Estado de la interfaz**Utilice el comando **show interfaces [*interface name*]** para asegurarse de que la interfaz se encuentre en el estado "up/up (spoofing)".Interfaz en modo "en espera"Se ha configurado otra interfaz (principal) en el router para utilizar la interfaz del marcador como interfaz de respaldo. Además, la interfaz primaria no se encuentra en estado "down/down", lo que se requiere para sacar la interfaz del marcador del modo de espera. Además, un *retraso de respaldo* debe configurarse en la interfaz primaria, o el **comando backup interface** nunca se aplicará.Para verificar que la interfaz del marcador cambiará de "standby" a "up/up (spoofing)", generalmente es necesario extraer el cable de la interfaz primaria. Simplemente apagar la interfaz primaria con el comando de configuración **shutdown** no pondrá la interfaz primaria en "down/down", sino que la pondrá en "administrativamente down", no lo mismo.Además, si la conexión principal es a través de Frame Relay, la configuración de Frame Relay se debe realizar en una subinterfaz serial punto a punto, y la compañía telefónica debe pasar el bit "activo". Esta práctica también se conoce como "LMI integral".La interfaz está "administrativamente inactiva"La interfaz del marcador se ha configurado con el comando **shutdown**. Este es también el estado predeterminado de cualquier interfaz cuando se inicia un router Cisco por primera vez. Utilice el comando de configuración de interfaz **no shutdown** para eliminar este impedimento.
- **Routing incorrecto**Ejecute el comando exec **show ip route [*a.b.c.d*]**, donde *a.b.c.d* es la dirección de la interfaz del marcador del router remoto. Si **ip unnumbered** se utiliza en el router remoto, utilice la dirección de la interfaz enumerada en el comando **ip unnumbered**.El resultado debe mostrar una ruta a la dirección remota a través de la interfaz del marcador. Si no hay ruta, asegúrese de que se hayan configurado rutas estáticas o flotantes examinando el resultado de show running-config.Si hay una ruta a través de una interfaz que no sea la interfaz del marcador, la implicancia es que DDR se está usando como respaldo. Examine la configuración del router para asegurarse de que se hayan configurado rutas estáticas estáticas o flotantes. La manera más segura de probar el ruteo, en este caso, es inhabilitar la conexión primaria y ejecutar el comando **show ip route [*a.b.c.d*]** para verificar que la ruta adecuada se haya instalado en la tabla de ruteo.**Nota:** Si lo intenta durante las operaciones de red en directo, se puede activar un evento de marcado. Este tipo de pruebas se realiza mejor durante los ciclos de mantenimiento programados.

Colocación de llamada

Si el enrutamiento y los filtros de tráfico interesantes son correctos, se debe iniciar una llamada. Esto se puede ver usando **eventos debug dialer**:

```
Async1 DDR: Dialing cause ip (s=10.0.0.1, d=10.0.0.2)
Async1 DDR: Attempting to dial 5551212
```

Si se ve la causa de marcación pero no se intenta marcar, la razón habitual es un mapa de marcador o perfil de marcador mal configurado.

Llamada no realizada

A continuación se enumeran algunos posibles problemas y acciones sugeridas:

- **Mapa de marcador mal configurado**Utilice el comando **show running-config** para asegurarse de que la interfaz de marcado esté configurada con al menos una *sentencia de mapa de marcador* que apunte a la dirección del protocolo y al número llamado del sitio remoto.
- **Perfil de marcador mal configurado**Utilice el comando **show running-config** para asegurarse de que la interfaz del marcador esté configurada con un **comando dialer pool X** y que una interfaz del marcador en el router esté configurada con un *dialer pool-member X* coincidente. Si los perfiles de marcador no están correctamente configurados, es posible que vea un mensaje de depuración como:
  ```
  Dialer1: Can't place call, no dialer pool set
  ```
  Asegúrese de que una **cadena de marcador** esté configurada.

Llamada saliente asíncrona - Verificación del funcionamiento del script de conversación

Si la llamada saliente es una llamada de módem, se debe ejecutar una secuencia de comandos de conversación para que la llamada continúe. Para el DDR basado en mapa del marcador, el script de chat es invocado por el parámetro modem-script en un comando dialer map. Si DDR se basa en el perfil del marcador, esto se logra mediante el comando **script dialer**, configurado en la línea TTY. Ambos usuarios se basan en un script de chat existente en la configuración global del router, por ejemplo:

```
chat-script callout AT OK atdt\T TIMEOUT 60 CONNECT \c
```

En cualquier caso, el comando para ver la actividad del script de chat es **debug chat**. Si la cadena de marcado (es decir, número de teléfono) utilizada en el comando **dialer map** o **dialer string** fueran 5551212, el resultado de la depuración sería similar al siguiente:

```
CHAT1: Attempting async line dialer script

CHAT1: Dialing using Modem script: callout & System script: none
CHAT1: process started
CHAT1: Asserting DTR
CHAT1: Chat script callout started
CHAT1: Sending string: AT
CHAT1: Expecting string: OK
CHAT1: Completed match for expect: OK
CHAT1: Sending string: atdt5551212
CHAT1: Expecting string: CONNECT
CHAT1: Completed match for expect: CONNECT
CHAT1: Chat script callout finished, status = Success
```

Los problemas del script de conversación se pueden dividir en tres categorías:

- Error de configuración
- Falla del módem
- Falla de conexión

Fallo de secuencia de comandos de conversación

Esta lista muestra los posibles resultados de debug chat muestra y sugiere acciones:

- **no se ha encontrado ninguna secuencia de comandos de conversación coincidente para [number]**No se ha configurado un script de conversación. Agregue uno.
- **Se ha finalizado el marcado de salida del script de conversación, estado = se ha agotado el tiempo de espera de la conexión; el host remoto no responde**El módem no responde al script de chat. Verifique la comunicación con el módem (consulte la Tabla 16-2 en el Capítulo 16).
- **Tiempo de espera: CONNECT(conectar)***Posibilidad 1*: El módem local no está realizando la llamada. Verifique que el módem pueda realizar una llamada realizando una Telnet inversa al módem e iniciando manualmente una marcación.*Posibilidad 2*: El módem remoto no responde. Pruebe esto marcando el módem remoto con un teléfono POTS normal.*Posibilidad 3*: El número marcado es incorrecto. Verifique el número marcándolo manualmente. Corrija la configuración, si es necesario.*Posibilidad 4*: La preparación del módem tarda demasiado o el valor de TIMEOUT es demasiado bajo. Si el módem local es externo, encienda el volumen del altavoz del módem y escuche los tonos de formación. Si la formación se corta de forma repentina, intente aumentar el valor de TIMEOUT en el comando **chat-script**. Si el TIEMPO DE ESPERA ya es de 60 segundos o más, vea la sección Formación del módem.

Llamada saliente ISDN

Ante la primera sospecha de una falla ISDN, ya sea en un BRI o en un PRI, siempre verifique la salida del **estado show isdn**. Los aspectos clave a tener en cuenta son que la Capa 1 debe estar activa y la Capa 2 debe estar en un estado de *MULTIPLE_FRAME_ESTABLISHED*. Consulte la sección "Interpretación del resultado de show ISDN Status" en el Capítulo 16 para obtener información sobre la lectura de este resultado, así como para las medidas correctivas.

Para las llamadas ISDN salientes, **debug isdn q931** y **debug isdn events** son las mejores herramientas para usar. Afortunadamente, la depuración de llamadas salientes es muy similar a la depuración de llamadas entrantes. Una llamada normal exitosa podría verse de la siguiente manera:

```
*Mar 20 21:07:45.025: ISDN BR0: Event: Call to 5553759 at 64 Kb/s
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
*Mar 20 21:07:45.141: ISDN BR0: RX <-  CALL_PROC pd = 8  callref = 0xAC
*Mar 20 21:07:45.145:         Channel ID i = 0x89
*Mar 20 21:07:45.157: ISDN BR0: received HOST_PROCEEDING
        Channel ID i = 0x0101
*Mar 20 21:07:45.161:   -------------------
        Channel ID i = 0x89
*Mar 20 21:07:45.313: ISDN BR0: RX <-  CONNECT pd = 8  callref = 0xAC
*Mar 20 21:07:45.325: ISDN BR0: received HOST_CONNECT
 !--- The CONNECT message is the key indicator of success. If a CONNECT is not received, !---
you may see a DISCONNECT or a RELEASE_COMP (release complete) message followed by !--- a cause
code (see below) *Mar 20 22:11:03.212: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0x8F *Mar
20 22:11:03.216: Cause i = 0x8295 - Call rejected
```

El valor de la causa indica dos cosas.

- El segundo byte del valor de 4 o 6 bytes indica desde dónde en la trayectoria de llamada de extremo a extremo se recibió DISCONNECT o RELEASE_COMP. Esto puede ayudarle a localizar el problema.
- Los bytes tercero y cuarto indican la razón real de la falla. Vea las tablas siguientes para los

significados de los diferentes valores.

Nota: La siguiente impresión generalmente indica una falla de protocolo superior:

```
Cause i = 0x8090 - Normal call clearing
```

La falla de autenticación PPP es una razón típica. Active **debug ppp negotiation** y **debug ppp authentication** antes de asumir que la falla de conexión es necesariamente un problema ISDN

Campos de código de causa

La tabla 17-9 enumera los campos de código de causa ISDN que se muestran en el siguiente formato dentro de los comandos debug:

```
i=0x y1 y2 z1 z2 [a1 a2]
```

Campos de Código de Causa ISDN

Campo	Descripción del valor
0x	Los valores que siguen están en hexadecimal.
y1	8: codificación estándar ITU-T.
y2	0—Usuario 1—Red privada que presta servicios a usuarios locales 2—Red pública que presta servicios a usuarios locales 3—Red de tránsito 4—Red pública que presta servicios a usuarios remotos 5—Red privada que presta servicios a usuarios remotos 7—Red internacional A—Red más allá de los puntos de conexión entre redes
z1	Clase (el número hexadecimal más significativo) del valor de causa. Consulte la siguiente tabla para obtener información detallada sobre los posibles valores.
z2	Valor (el número hexadecimal menos significativo) del valor de causa. Consulte la siguiente tabla para obtener información detallada sobre los posibles valores.
a1	(Opcional) Campo de diagnóstico que siempre es 8.
a2	(Opcional) Campo de diagnóstico que es uno de los siguientes valores: 0: desconocido 1: permanente 2: transitorio

Valores de causa ISDN

La tabla siguiente muestra descripciones de algunos de los valores de causa más frecuentes del elemento de información de causa: los bytes tercero y cuarto del código de causa. Para obtener información más completa sobre los códigos y valores de ISDN, refiérase a Comprensión de **debug isdn q931** Códigos de Causa de Desconexión.

Valor hex	Causa	Explicación
81	Número no asignado (no asignado)	El número ISDN se envió al switch en el formato correcto; sin embargo, el número no se asigna a ningún equipo de destino.
90	Verificación normal de llamadas	Se ha producido una compensación de llamada normal.
91	Usuario ocupado	El sistema llamado reconoce la solicitud de conexión pero no puede aceptar la llamada porque todos los canales B están en uso.
92	Sin respuesta de usuarios	No se puede completar la conexión porque el destino no responde a la llamada.
93	No hay respuesta del usuario (se alerta al usuario)	El destino responde al pedido de conexión pero no puede completar la conexión en el tiempo prescrito. El problema está en el extremo remoto de la conexión.
95	Llamada rechazada	El destino es capaz de aceptar la llamada pero la rechazó por una razón desconocida.
9C	El formato del número no es válido	No se pudo establecer la conexión porque la dirección de destino se presentó en un formato irreconocible o porque la dirección de destino estaba incompleta.
9F	Normal, sin especificar	Informa si ocurrió un evento normal que no haya sido consecuencia de una causa estándar. No se requiere acción
A2	No hay circuito/canal disponible	No se puede establecer la conexión porque no hay ningún canal adecuado disponible para realizar la llamada.

A6	Red no disponible	No se puede alcanzar el destino porque la red no funciona correctamente y la condición puede durar un período de tiempo prolongado. Un intento de reconexión inmediata probablemente no sea exitoso.
AC	El circuito/canal solicitado no está disponible	El equipo remoto no puede brindar el canal solicitado por un motivo desconocido. Esto podría ser un problema temporal.
B2	Prestación solicitada no disponibe (requiere suscripción)	El equipo remoto admite el servicio suplementario solicitado sólo mediante suscripción. A menudo se trata de una referencia al servicio de larga distancia.
B9	Capacidad portadora no autorizada	El usuario solicitó una capacidad portadora que proporciona la red, pero no está autorizado a utilizarla. Esto podría ser un problema de suscripción.
D8	Destino incompatible	Indica que se intentó conectarse a equipos que no son ISDN. Por ejemplo, a una línea analógica.
E0	Falta el elemento de información obligatorio	El equipo receptor recibió un mensaje que no incluía uno de los elementos de información obligatorios. Por lo general, esto se debe a un error en el canal D. Si este error ocurre sistemáticamente, notifíquelo a su proveedor de servicios ISDN.
E4	Contenido del elemento de información no válido	El equipo remoto recibió un mensaje que incluye información no válida en el elemento information. Por lo general, esto se debe a un error en el canal D.

Llamada saliente CAS

Para las llamadas salientes a través de CAS T1 o E1 y módems digitales integrados, gran parte de la resolución de problemas es similar a otros troubleshooting DDR. Lo mismo se aplica a las llamadas de módem integrado saliente a través de una línea PRI. Las características únicas involucradas en la realización de una llamada de esta manera requieren un debugging especial

en caso de una falla de llamada.

En cuanto a otras situaciones de DDR, debe asegurarse de que se requiera un intento de llamada. Use **debug dialer events** para este propósito. Consulte Verificación de la Operación del Marcador.

Antes de realizar una llamada, se debe asignar un módem a la llamada. Para ver este proceso y la llamada subsiguiente, utilice los siguientes comandos debug:

- **debug modem**
- **debug modem csm**
- **debug cas**

Nota: El comando **debug cas** apareció por primera vez en la versión 12.0(7)T del IOS para AS5200 y AS5300. Las versiones anteriores de IOS utilizan un comando de configuración de nivel del sistema **service internal** junto con el comando exec **modem-mgmt debug rbs**:

Activación de los depuradores

```
router#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#service internal
router(config)#^Z

router#modem-mgmt csm ?
  debug-rbs     enable rbs debugging
  no-debug-rbs  disable rbs debugging

router#modem-mgmt csm debug-rbs
router#
neat msg at slot 0: debug-rbs is on
neat msg at slot 0: special debug-rbs is on
```

Desactivación de los depuradores

```
router#
router#modem-mgmt csm no-debug-rbs
neat msg at slot 0: debug-rbs is off
```

Nota: La depuración de esta información en un AS5800 requiere la conexión a la tarjeta troncal. El siguiente es un ejemplo de una llamada saliente normal sobre un CAS T1 que se aprovisiona y configura para FXS-Ground-Start:

```
Mica Modem(1/0): Rcvd Dial String(5551111) [Modem receives digits from chat script]
CSM_PROC_IDLE: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_LOCK at slot 1 and port 0
CSM_PROC_OC4_DIALING: CSM_EVENT_DSX0_BCHAN_ASSIGNED at slot 1, port 0
Mica Modem(1/0): Configure(0x1)
Mica Modem(1/0): Configure(0x2)
Mica Modem(1/0): Configure(0x5)
Mica Modem(1/0): Call Setup
neat msg at slot 0: (0/2): Tx RING_GROUND
Mica Modem(1/0): State Transition to Call Setup
neat msg at slot 0: (0/2): Rx TIP_GROUND_NORING [Telco switch goes OFFHOOK]
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_START_TX_TONE at slot 1 and port 0
```

```
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_START_TX_TONE at slot 1, port 0
neat msg at slot 0: (0/2): Tx LOOP_CLOSURE [Now the router goes OFFHOOK]
Mica Modem(1/0): Rcvd Tone detected(2)
Mica Modem(1/0): Generate digits:called_party_num=5551111 len=8
Mica Modem(1/0): Rcvd Digits Generated
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_ADDR_INFO_COLLECTED at slot 1, port 0
CSM_RX_CAS_EVENT_FROM_NEAT:(A003):  EVENT_CHANNEL_CONNECTED at slot 1 and port 0
CSM_PROC_OC5_WAIT_FOR_CARRIER: CSM_EVENT_DSX0_CONNECTED at slot 1, port 0
Mica Modem(1/0): Link Initiate
Mica Modem(1/0): State Transition to Connect
Mica Modem(1/0): State Transition to Link
Mica Modem(1/0): State Transition to Trainup
Mica Modem(1/0): State Transition to EC Negotiating
Mica Modem(1/0): State Transition to Steady State
Mica Modem(1/0): State Transition to Steady State Speedshifting
Mica Modem(1/0): State Transition to Steady State
```

Las depuraciones para T1s y E1s con otros tipos de señalización son similares.

Llegar a este punto en la depuración indica que los módems de llamada y de respuesta se han entrenado y conectado, y que los protocolos de capa superior pueden comenzar a negociar. Si un módem se asigna correctamente para la llamada saliente pero la conexión no llega hasta aquí, se debe examinar la T1. Consulte el Capítulo 15 para obtener información sobre Troubleshooting de T1.

Resolución de problemas de PPP

La resolución de problemas de la parte PPP de una conexión comienza cuando se sabe que la conexión de marcado, ISDN o asíncrona, se establece correctamente.

Es importante comprender cómo se ve una secuencia PPP de depuración exitosa antes de resolver problemas de negociación PPP. De esta manera, al comparar una sesión de depuración PPP defectuosa con una secuencia PPP de depuración completada correctamente, se ahorra tiempo y esfuerzo.

A continuación se muestra un ejemplo de una secuencia PPP exitosa. Consulte Detalles de la Negociación LCP PPP para obtener una descripción detallada de los campos de salida.

```
Montecito#
Mar 13 10:57:13.415: %LINK-3-UPDOWN: Interface Async1, changed state to up
Mar 13 10:57:15.415: As1 LCP: O CONFREQ [ACKrcvd] id 2 len 25
Mar 13 10:57:15.415: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.415: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.415: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.415: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.415: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:15.543: As1 LCP: I CONFACK [REQsent] id 2 len 25
Mar 13 10:57:15.543: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:15.543: As1 LCP:    AuthProto CHAP (0x0305C22305)
Mar 13 10:57:15.543: As1 LCP:    MagicNumber 0x1084F0A2 (0x05061084F0A2)
Mar 13 10:57:15.543: As1 LCP:    PFC (0x0702)
Mar 13 10:57:15.547: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP: I CONFREQ [ACKrcvd] id 4 len 23
Mar 13 10:57:16.919: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:16.919: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:16.919: As1 LCP:    PFC (0x0702)
Mar 13 10:57:16.919: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
```

```
Mar 13 10:57:16.919: As1 LCP: O CONFREJ [ACKrcvd] id 4 len 7
Mar 13 10:57:16.919: As1 LCP:    Callback 6  (0x0D0306)
Mar 13 10:57:17.047: As1 LCP: I CONFREQ [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: O CONFACK [ACKrcvd] id 5 len 20
Mar 13 10:57:17.047: As1 LCP:    ACCM 0x000A0000 (0x0206000A0000)
Mar 13 10:57:17.047: As1 LCP:    MagicNumber 0x001327B0 (0x0506001327B0)
Mar 13 10:57:17.047: As1 LCP:    PFC (0x0702)
Mar 13 10:57:17.047: As1 LCP:    ACFC (0x0802)
Mar 13 10:57:17.047: As1 LCP: State is Open
Mar 13 10:57:17.047: As1 PPP: Phase is AUTHENTICATING, by this end
Mar 13 10:57:17.047: As1 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 10:57:17.191: As1 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 10:57:17.191: As1 CHAP: O SUCCESS id 1 len 4
Mar 13 10:57:17.191: As1 PPP: Phase is UP
Mar 13 10:57:17.191: As1 IPCP: O CONFREQ [Closed] id 1 len 10
Mar 13 10:57:17.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:17.303: As1 IPCP: I CONFREQ [REQsent] id 1 len 40
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.303: As1 IPCP: O CONFREJ [REQsent] id 1 len 22
Mar 13 10:57:17.303: As1 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
Mar 13 10:57:17.303: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:17.303: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:17.319: As1 CCP: I CONFREQ [Not negotiated] id 1 len 15
Mar 13 10:57:17.319: As1 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
Mar 13 10:57:17.319: As1 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
Mar 13 10:57:17.319: As1 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
Mar 13 10:57:17.319: As1 LCP:  (0x80FD0101000F12060000000111050001)
Mar 13 10:57:17.319: As1 LCP:  (0x04)
Mar 13 10:57:17.319: As1 IPCP: I CONFACK [REQsent] id 1 len 10
Mar 13 10:57:17.319: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:18.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
 changed state to up
Mar 13 10:57:19.191: As1 IPCP: TIMEout: State ACKrcvd
Mar 13 10:57:19.191: As1 IPCP: O CONFREQ [ACKrcvd] id 2 len 10
Mar 13 10:57:19.191: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:19.315: As1 IPCP: I CONFACK [REQsent] id 2 len 10
Mar 13 10:57:19.315: As1 IPCP:    Address 172.22.66.23 (0x0306AC164217)
Mar 13 10:57:20.307: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 34
Mar 13 10:57:20.307: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.307: As1 IPCP: O CONFREJ [ACKrcvd] id 2 len 16
Mar 13 10:57:20.307: As1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
Mar 13 10:57:20.307: As1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
Mar 13 10:57:20.419: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 0.0.0.0 (0x030600000000)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
Mar 13 10:57:20.419: As1 IPCP: O CONFNAK [ACKrcvd] id 3 len 22
Mar 13 10:57:20.419: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.419: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
```

```
Mar 13 10:57:20.419: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.543: As1 IPCP: I CONFREQ [ACKrcvd] id 4 len 22
Mar 13 10:57:20.543: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: O CONFACK [ACKrcvd] id 4 len 22
Mar 13 10:57:20.547: As1 IPCP:    Address 10.1.1.1 (0x03060A010101)
Mar 13 10:57:20.547: As1 IPCP:    PrimaryDNS 171.68.10.70 (0x8106AB440A46)
Mar 13 10:57:20.547: As1 IPCP:    SecondaryDNS 171.68.10.140 (0x8306AB440A8C)
Mar 13 10:57:20.547: As1 IPCP: State is Open
Mar 13 10:57:20.551: As1 IPCP: Install route to 10.1.1.1
```

Nota: Es posible que sus depuraciones aparezcan en un formato diferente. Este ejemplo muestra el formato de salida de depuración PPP más nuevo que se modificó en la versión 11.2(8) del IOS. Consulte el Capítulo 16 para ver un ejemplo de depuración PPP con las versiones anteriores de IOS.

Detalles de la negociación PPP LCP

Marca de tiempo	Descripción
10:57:15.415	Solicitud de configuración saliente (O CONFREQ). El NAS envía un paquete de solicitud de configuración PPP saliente al cliente.
10:57:15.543	Reconocimiento de configuración entrante (CONFACK). El cliente acepta la solicitud PPP de Montecito.
10:57:16.919	Solicitud de configuración entrante (I CONFREQ). El cliente desea negociar el protocolo de devolución de llamada.
10:57:16.919	Rechazo de configuración saliente (O CONFREJ). El NAS rechaza la opción de devolución de llamada.
10:57:17.047	Solicitud de configuración entrante (I CONFREQ). El cliente solicita un nuevo conjunto de opciones. Observe que esta vez no se solicita la devolución de llamada de Microsoft.
10:57:17.047	Reconocimiento de configuración saliente (O CONFACK). El NAS acepta el nuevo conjunto de opciones.
10:57:17.047	La negociación PPP LCP se ha completado correctamente. El estado de LCP es "Abierto". Ambos lados han reconocido (CONFACK) la solicitud de configuración del otro lado (CONFREQ).
10:57:17.047 hasta las 10:57:17.19	La autenticación PPP se ha completado correctamente. Después de que el LCP negocie, se inicia la autenticación. La autenticación debe tener lugar antes de que se entreguen los protocolos de red, como IP. Ambos lados se autentican con el método negociado durante LCP. Montecito está autenticando al cliente

1	usando CHAP.
10:57:20.551	El estado está abierto para IP Control Protocol (IPCP). Se negocia e instala una ruta para el peer IPCP, al que se asigna la dirección IP 1.1.1.1.

Protocolo de control de link

Se suelen encontrar dos tipos de problemas durante la negociación LCP.

La primera ocurre cuando un par realiza solicitudes de configuración que el otro par no puede o no reconocerá. Aunque esto ocurre con frecuencia, puede ser un problema si el solicitante insiste en el parámetro. Un ejemplo típico es la negociación de AUTHTYPE (también conocido como "AuthProto"). Por ejemplo, muchos servidores de acceso están configurados para aceptar solamente CHAP para la autenticación. Si la persona que llama está configurada para hacer solamente la autenticación PAP, las CONFREQ y CONFNAK se intercambiarán hasta que un par o el otro descarte la conexión.

```
BR0:1 LCP: I CONFREQ [ACKrcvd] id 66 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 66 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 67 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 67 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
BR0:1 LCP: I CONFREQ [ACKrcvd] id 68 len 14
BR0:1 LCP:    AuthProto PAP (0x0304C023)
BR0:1 LCP:    MagicNumber 0xBC6B9F91 (0x0506BC6B9F91)
BR0:1 LCP: O CONFNAK [ACKrcvd] id 68 len 9
BR0:1 LCP:    AuthProto CHAP (0x0305C22305)
...
...
```

El segundo tipo de problema en LCP es cuando sólo se ven CONFREQ salientes en uno o ambos peers como en el ejemplo siguiente. Esto es generalmente el resultado de lo que se conoce como una *discordancia de velocidad* en la capa inferior. Esta condición puede ocurrir en DDR asíncrono o ISDN

```
Jun 10 19:57:59.768: As5 PPP: Phase is ESTABLISHING, Active Open
Jun 10 19:57:59.768: As5 LCP: O CONFREQ [Closed] id 64 len 25
Jun 10 19:57:59.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:57:59.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:57:59.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:57:59.768: As5 LCP: PFC (0x0702)
Jun 10 19:57:59.768: As5 LCP: ACFC (0x0802)
Jun 10 19:58:01.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:01.768: As5 LCP: O CONFREQ [REQsent] id 65 len 25
Jun 10 19:58:01.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:01.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:01.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:01.768: As5 LCP: PFC (0x0702)
Jun 10 19:58:01.768: As5 LCP: ACFC (0x0802).
Jun 10 19:58:03.768: As5 LCP: TIMEout: State REQsent
```

```
Jun 10 19:58:03.768: As5 LCP: O CONFREQ [REQsent] id 66 len 25
Jun 10 19:58:03.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000)
Jun 10 19:58:03.768: As5 LCP: AuthProto CHAP (0x0305C22305)
Jun 10 19:58:03.768: As5 LCP: MagicNumber 0x5779D9D2 (0x05065779D9D2)
Jun 10 19:58:03.768: As5 LCP: PFC (0x0702)
Jun 10 19:58:03.768: As5 LCP: ACF.C (0x0802)
Jun 10 19:58:05.768: As5 LCP: TIMEout: State REQsent
Jun 10 19:58:05.768: As5 LCP: O CONFREQ [REQsent] id 67 len 25
!--- This repeats every two seconds until: Jun 10 19:58:19.768: As5 LCP: O CONFREQ [REQsent] id
74 len 25 Jun 10 19:58:19.768: As5 LCP: ACCM 0x000A0000 (0x0206000A0000) Jun 10 19:58:19.768:
As5 LCP: AuthProto CHAP (0x0305C22305) Jun 10 19:58:19.768: As5 LCP: MagicNumber 0x5779D9D2
(0x05065779D9D2) Jun 10 19:58:19.768: As5 LCP: PFC (0x0702) Jun 10 19:58:19.768: As5 LCP: ACFC
(0x0802) Jun 10 19:58:21.768: As5 LCP: TIMEout: State REQsent Jun 10 19:58:21.768: TTY5: Async
Int reset: Dropping DTR
```

Si la conexión es asíncrona, la causa probable es una discordancia de velocidad entre el router y su módem. Esto suele deberse a que no se pudo bloquear la velocidad DTE del módem a la velocidad configurada de la línea TTY. El problema se puede encontrar en cualquiera de los pares o en ambos, así que verifique ambos. Consulte El módem no puede enviar ni recibir datos anteriormente en este capítulo.

Si se observan los síntomas cuando la conexión se realiza sobre ISDN, es probable que el problema sea que un par se conecte a 56K mientras que el otro a 64K. Aunque esta condición es rara, sí ocurre. El problema podría ser uno o ambos pares, o posiblemente la compañía telefónica. Utilice **debug isdn q931** y examine los mensajes SETUP en cada uno de los pares. La capacidad portadora enviada desde un par debe coincidir con la capacidad portadora que se ve en el mensaje SETUP recibido en el otro par. Como solución posible, configure la velocidad de marcado, 56K o 64K, en el comando interface level **dialer map** o en el comando **dialer isdn speed** configurado bajo una clase map.

```
*Mar 20 21:07:45.033: ISDN BR0: TX ->  SETUP pd = 8  callref = 0x2C
*Mar 20 21:07:45.037:         Bearer Capability i = 0x8890
*Mar 20 21:07:45.041:         Channel ID i = 0x83
*Mar 20 21:07:45.041:         Keypad Facility i = 0x35353533373539
```

Esta situación puede justificar una llamada al TAC de Cisco. Recopile los siguientes resultados de ambos pares antes de llamar al TAC:

- **show running-config**
- **show version**
- **debug isdn q931**
- **debug isdn events**
- **debug ppp negotiation**

Autenticación

La autenticación fallida es la única razón más común para una falla PPP. Los nombres de usuario y las contraseñas mal configurados o no coincidentes crean mensajes de error en el resultado de la depuración.

El siguiente ejemplo muestra que el nombre de usuario Goleta no tiene permiso para marcar en el NAS, que no tiene un nombre de usuario local configurado para este usuario. Para solucionar el problema, utilice el comando **username** *name* **password** *password* para agregar el nombre de usuario "Goleta" a la base de datos AAA local del NAS:

```
Mar 13 11:01:42.399: As2 LCP: State is Open
Mar 13 11:01:42.399: As2 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:01:42.399: As2 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 11:01:42.539: As2 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:01:42.539: As2 CHAP: Unable to validate Response.  Username Goleta not found
Mar 13 11:01:42.539: As2 CHAP: O FAILURE id 1 len 26 msg is "Authentication failure"
Mar 13 11:01:42.539: As2 PPP: Phase is TERMINATING
```

El siguiente ejemplo muestra que el nombre de usuario "Goleta" está configurado en el NAS. Sin embargo, la comparación de contraseñas falló. Para solucionar este problema, utilice el comando **username *name* password *password*** para especificar la contraseña de inicio de sesión correcta para Goleta:

```
Mar 13 11:04:06.843: As3 LCP: State is Open
Mar 13 11:04:06.843: As3 PPP: Phase is AUTHENTICATING, by this end
Mar 13 11:04:06.843: As3 CHAP: O CHALLENGE id 1 len 28 from "Montecito"
Mar 13 11:04:06.987: As3 CHAP: I RESPONSE id 1 len 30 from "Goleta"
Mar 13 11:04:06.987: As3 CHAP: O FAILURE id 1 len 25 msg is "MD/DES compare failed"
Mar 13 11:04:06.987: As3 PPP: Phase is TERMINATING
```

Para obtener más información sobre la autenticación PAP, consulte Configuración y resolución de problemas del protocolo de autenticación de contraseña PPP (PAP).

Protocolo de control de red

Después de que los peers hayan realizado correctamente la autenticación necesaria, la negociación pasa a la fase NCP. Si ambos peers están correctamente configurados, la negociación NCP podría verse como el siguiente ejemplo que muestra un equipo cliente marcando y negociando con un NAS:

```
solvang# show debug
Generic IP:
IP peer address activity debugging is on
PPP:
PPP protocol negotiation debugging is on

*Mar  1 21:35:04.186: As4 PPP: Phase is UP
*Mar  1 21:35:04.190: As4 IPCP: O CONFREQ [Not negotiated] id 1 len 10
*Mar  1 21:35:04.194: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:04.282: As4 IPCP: I CONFREQ [REQsent] id 1 len 28
*Mar  1 21:35:04.282: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.286: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:04.290: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:04.298: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:04.306: As4 IPCP: O CONFREJ [REQsent] id 1 len 10
*Mar  1 21:35:04.310: As4 IPCP:    CompressType VJ 15 slots CompressSlotID
 (0x0206002D0F01)
*Mar  1 21:35:04.314: As4 CCP: I CONFREQ [Not negotiated] id 1 len 15
*Mar  1 21:35:04.318: As4 CCP:    MS-PPC supported bits 0x00000001 (0x120600000001)
*Mar  1 21:35:04.318: As4 CCP:    Stacker history 1 check mode EXTENDED (0x1105000104)
*Mar  1 21:35:04.322: As4 LCP: O PROTREJ [Open] id 3 len 21 protocol CCP
*Mar  1 21:35:04.326: As4 LCP:  (0x80FD0101000F12060000000111050001)
*Mar  1 21:35:04.330: As4 LCP:  (0x04)
*Mar  1 21:35:04.334: As4 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar  1 21:35:04.338: As4 IPCP:    Address 10.1.2.1 (0x03060A010201)
*Mar  1 21:35:05.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async4,
 changed state to up
*Mar  1 21:35:07.274: As4 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
```

```
*Mar  1 21:35:07.278: As4 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  1 21:35:07.282: As4 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  1 21:35:07.286: As4 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  1 21:35:07.294: As4 IPCP: O CONFNAK [ACKrcvd] id 2 len 22
*Mar  1 21:35:07.298: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.302: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.310: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.426: As4 IPCP: I CONFREQ [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.430: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.434: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.442: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.446: ip_get_pool: As4: validate address = 10.1.2.2
*Mar  1 21:35:07.450: ip_get_pool: As4: using pool default
*Mar  1 21:35:07.450: ip_get_pool: As4: returning address = 10.1.2.2
*Mar  1 21:35:07.454: set_ip_peer_addr: As4: address = 10.1.2.2 (3) is redundant
*Mar  1 21:35:07.458: As4 IPCP: O CONFACK [ACKrcvd] id 3 len 22
*Mar  1 21:35:07.462: As4 IPCP:    Address 10.1.2.2 (0x03060A010202)
*Mar  1 21:35:07.466: As4 IPCP:    PrimaryDNS 10.2.2.3 (0x81060A020203)
*Mar  1 21:35:07.474: As4 IPCP:    SecondaryDNS 10.2.3.1 (0x83060A020301)
*Mar  1 21:35:07.478: As4 IPCP: State is Open
*Mar  1 21:35:07.490: As4 IPCP: Install route to 10.1.2.2
```

[Detalles de la negociación PPP NCP]

Marca de tiempo	Descripción
21:35:04.190	Solicitud de configuración saliente (O CONFREQ). El NAS envía un paquete de solicitud de configuración PPP saliente que contiene su dirección IP al par.
21:35:04.282	CONFREQ entrante. El par solicita hacer la compresión del encabezado VJ. Necesita una dirección IP para sí misma, así como las direcciones de los servidores DNS primario y secundario.
21:35:04.306	Rechazo de configuración saliente (CONFREJ). Se rechaza la compresión del encabezado VJ.
21:35:04.314 hasta las 21:35:04.330	El par envía una solicitud para hacer el Protocolo de control de compresión; el NAS rechaza todo el protocolo mediante un mensaje PROTREJ. El par no debe intentar (y no lo hace) reintentar CCP.
21:35:04.334	El par reconoce la dirección IP del NAS con un CONFACK.
21:35:07.274	CONFREQ entrante. El par ya no solicita hacer la compresión de encabezado VJ, pero aún necesita una dirección IP para sí mismo, así como las direcciones de los servidores DNS primario y secundario.
21:35:07.294	El NAS envía un CONFNAK que contiene la dirección que desea que el par utilice y las direcciones de los servidores DNS primario y secundario.

21:35:07.426	El par envía las direcciones nuevamente al NAS; intento de confirmar que las direcciones fueron recibidas correctamente.
21:35:07.458	El NAS reconoce las direcciones con un CONFACK.
21:35:07.478	Cada lado de la conexión que ha emitido un CONFACK, la negociación finaliza. El comando **show interfaces Async4** en el NAS muestra "IPCP: Abrir".
21:35:07.490	Una ruta de host al par remoto se instala en la tabla de ruteo de NAS.

Es posible que los pares negocien simultáneamente más de un protocolo de Capa 3. Por ejemplo, es frecuente ver que se negocian IP e IPX. También es posible que un protocolo negocie con éxito mientras que el otro no lo hace.

Resolución de problemas de NCP

Los problemas que se producen durante la negociación del NCP pueden atribuirse normalmente a las configuraciones de los pares negociadores. Si la negociación PPP falla durante la fase NCP, consulte los siguientes pasos:

1. Verificar la configuración del protocolo de interfazExamine el resultado del comando exec privilegiado **show running-config**. Verifique que la interfaz esté configurada para soportar el protocolo que desea ejecutar sobre la conexión.
2. Verificar dirección de interfazConfirme que la interfaz en cuestión tenga configurada una dirección. Si utiliza **ip unnumbered [***interface-name***]** o **ipx ppp-client loopback [**number**]**, asegúrese de que la interfaz a la que se hace referencia esté configurada con una dirección.
3. Verificar la disponibilidad de la dirección del clienteSi se supone que el NAS debe emitir una dirección IP para la persona que llama, asegúrese de que dicha dirección esté disponible. La dirección IP que se enviará a la persona que llama se puede obtener a través de uno de los siguientes métodos:Configuración local en la interfaz. Verifique la configuración de la interfaz para el comando **peer default ip address a.b.c.d**. En la práctica, este método sólo se debe utilizar en interfaces que acepten conexiones de un único llamador, como en una interfaz asíncrona (*no* asíncrona).Conjunto de direcciones configurado localmente en el NAS. La interfaz debe tener el comando **peer default ip address pool [***pool-name***]**. Además, el conjunto debe definirse en el nivel del sistema con el comando **ip local pool [***pool-name***] [***first-address***] [***last-address***]** . El rango de direcciones definido en el conjunto debe ser lo suficientemente grande como para alojar a tantos llamantes conectados simultáneamente como el NAS sea capaz.Servidor DHCP. La interfaz NAS se debe configurar con el comando **peer default ip address dhcp**. Además, el NAS se debe configurar para apuntar a un servidor DHCP con el comando de configuración global **ip dhcp-server [***address***]**.AAA. Si utiliza TACACS+ o RADIUS para la autorización, el servidor AAA se puede configurar para entregar una dirección IP específica a una persona que llama cada vez que se conecta la persona que llama. Consulte el capítulo 16 para obtener más información.
4. Verificar la configuración de la dirección del servidorPara devolver las direcciones configuradas de los servidores de nombres de dominio o de Windows NT en respuesta a las solicitudes BOOTP, asegúrese de que los comandos de nivel global **async-bootp dns-server**

[*address*] y **async-bootp nbns-server [*address*]** estén configurados.**Nota:** Mientras que el comando **async-bootp subnet-mask [*mask*]** se puede configurar en el NAS, la máscara de subred **no se negociará entre el NAS y un equipo cliente de marcado PPP.** Debido a la naturaleza de las conexiones punto a punto, el cliente utiliza automáticamente la dirección IP del NAS (aprendida durante la negociación IPCP) como gateway predeterminado. La máscara de subred no es necesaria en ese entorno punto a punto. La PC sabe que si la dirección de destino no coincide con la dirección local, el paquete debe reenviarse al gateway predeterminado (NAS) al que siempre se accede a través del enlace PPP.

Antes de llamar al equipo del TAC de Cisco Systems

Antes de llamar al centro de asistencia técnica Cisco Systems Technical Assistance Center (TAC), asegúrese de leer este capítulo y completar las acciones sugeridas para el problema del sistema.

Además, haga lo que se describe a continuación y documente los resultados para que podamos proporcionarle una mejor asistencia:

Para todos los problemas, recopile el resultado de **show running-config** y **show version**. Asegúrese de que el comando **service timestamps debug datetime msec** esté en la configuración.

Para los problemas de DDR, recopile lo siguiente:

- **show dialer map**
- **debug dialer**
- **debug ppp negotiation**
- **debug ppp authentication**

Si está involucrado ISDN, recopile:

- **mostrar estado isdn**
- **debug isdn q931**
- **debug isdn events**

Si hay módems involucrados, recopile:

- **show lines**
- **show line [x]**
- **show modem** (si hay módems integrados involucrados)
- **show modem version** (si hay módems integrados involucrados)
- **debug modem**
- **debug modem** csm (si hay módems integrados involucrados)
- **debug chat** (si se trata de un escenario DDR)

Si hay T1s o PRIs involucrados, recopile:

- **show controller t1**

Información Relacionada

- Página de Troubleshooting de T1/E1

- Guía de soluciones de marcado de Cisco IOS
- Supervisión y mantenimiento de la interfaz T1/E1
- Solución de problemas de negociación PPP
- Resolución de problemas de módems
- Comandos Debug del Módem
- Resolución de problemas de ISDN
- Diagnóstico de T1 PRI
- Soporte Técnico y Documentación - Cisco Systems