Tecnologia dialup: Técnicas para Troubleshooting

Contents

Introduction

A discagem é simplesmente a aplicação da rede telefônica pública comutada (PSTN) que transporta dados em nome do usuário final. Ele envolve um dispositivo CPE (Customer Premises Equipment, equipamento das instalações do cliente) que envia ao switch telefônico um número de telefone para o qual direcionar uma conexão. O Cisco3600, AS5200, AS5300 e AS5800 são exemplos de roteadores que têm a capacidade de executar uma PRI junto com bancos de modems digitais. O AS2511, por outro lado, é um exemplo de um roteador que se comunica com modems externos.

Prerequisites

Requirements

Os leitores deste documento devem estar cientes da seguinte informação:

O mercado de operadoras cresceu significativamente, e o mercado agora exige maiores densidades de modem. A resposta para essa necessidade é um grau maior de interoperação com o equipamento da companhia telefônica e o desenvolvimento do modem digital. Esse é um modem capaz de acessar diretamente a PSTN. Como resultado, já foram desenvolvidos modems CPE mais rápidos que aproveitam a clareza do sinal que os modems digitais desfrutam. O fato de que os modems digitais que se conectam à PSTN através de uma PRI ou BRI podem transmitir dados a mais de 53 k usando o padrão de comunicação V.90 atesta o sucesso da ideia.

Os primeiros servidores de acesso foram o Cisco2509 e o Cisco2511. O AS2509 poderia suportar 8 conexões de entrada usando modems externos, e o AS2511 poderia suportar 16. O AS5200 foi introduzido com 2 PRIs e poderia suportar 48 usuários usando modems digitais, e representou um grande salto em tecnologia. As densidades do modem aumentaram continuamente com o AS5300 suportando 4 e depois 8 PRIs. Finalmente, o AS5800 foi introduzido para atender às necessidades das instalações de classe de operadora que precisam lidar com dezenas de T1s de entrada e centenas de conexões de usuário.

Algumas tecnologias desatualizadas têm sido mencionadas em uma discussão histórica sobre a tecnologia do discador. 56Kflex é um padrão de modem de 56k mais antigo (pré-V.90) proposto pela Rockwell. A Cisco suporta a versão 1.1 do padrão 56Kflex em seus modems internos, mas recomenda a migração dos modems CPE para V.90 o mais rápido possível. Outra tecnologia desatualizada é o AS5100. O AS5100 era uma joint venture entre a Cisco e um fabricante de modem. O AS5100 foi criado como uma forma de aumentar a densidade do modem através do uso de placas de modem quádruplo. Ele envolveu um grupo de AS2511s construídos como placas inseridas em um backplane compartilhado por placas de modem quádruplo e uma placa T1 dupla.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

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

Troubleshooting de Chamadas Recebidas

A identificação e solução de problemas de uma chamada recebida começa na parte inferior e funciona completamente para cima. O fluxo geral de raciocínio procura o seguinte:

1. Vemos a chamada chegar? (Uma resposta *sim* avança para a próxima pergunta)
2. O receptor atende a chamada?
3. A chamada é concluída?
4. Os dados estão passando pelo link?

5. A sessão está estabelecida? (PPP ou terminal)

Para conexões de modem, uma chamada de dados parece a mesma que uma sessão de terminal entrando até o final onde a chamada de dados vai para negociar o PPP.

Para chamadas recebidas envolvendo modems digitais, primeiro verifique se o ISDN ou CAS subjacente está recebendo a chamada. Se estiver usando um modem externo, as seções do grupo ISDN e CAS podem ser ignoradas.

Troubleshooting de Chamada ISDN Recebida

Use o comando **debug isdn q931**. Aqui está um exemplo de saída de uma conexão bem-sucedida:

```
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
```

A mensagem de configuração indica que uma conexão está sendo iniciada pela extremidade remota. Os números de referência da chamada são mantidos como um par. Nesse caso, o número de referência da chamada do lado de entrada da conexão é 0x06 e o número de referência da chamada do lado de saída da conexão é 0x86. O recurso do portador (geralmente conhecido como bearercap) informa ao roteador que tipo de chamada está entrando. Nesse caso, a conexão é do tipo 0x8890. Esse valor indica "Velocidade ISDN de 64 Kb/s". Se a tampa frontal fosse 0x8090A2, ela teria indicado "Speech/voice call u-law".

Se nenhuma mensagem de configuração for recebida, você deverá verificar o número correto ligando manualmente para ele, se ele for provisionado por voz. Você também deve verificar o status da interface ISDN (consulte Using the **show isdn status** Command for BRI Troubleshooting). Se tudo isso for verificado, verifique se o originador da chamada está fazendo a chamada correta. Isso pode ser feito entrando em contato com a companhia telefônica. O originador da chamada pode rastrear a chamada para ver onde ela está sendo enviada. Se a conexão for de longa distância, tente uma portadora de longa distância diferente usando um código de longa distância 1010.

Se a chamada recebida for uma chamada de modem assíncrona, verifique se a linha está provisionada para permitir chamadas de voz.

Observação: a chamada de modem assíncrono BRI é um recurso de 3600 roteadores executando 12.0(3)T ou posterior. Requer uma revisão de hardware recente do módulo de rede da interface BRI. Os módulos WIC não suportam chamada de modem assíncrona.

Se a chamada chegou, mas não foi concluída, procure um código de causa (consulte a Tabela 17-10). Uma conclusão bem-sucedida é indicada pelo connect-ack.

Se esta for uma chamada de modem assíncrona, avance para a seção "Troubleshooting de Chamada de Modem de Entrada".

Nesse ponto, a chamada ISDN está conectada, mas não foi visto nenhum dado atravessando o link. Use o comando **debug ppp negotiation** para ver se algum tráfego PPP está cruzando a linha.

Se você não vir o tráfego, pode haver uma incompatibilidade de velocidade. Para determinar se esse é o caso, use o comando **show running-config privileged exec** para exibir a configuração do roteador. Verifique as entradas do comando de configuração de interface **dialer map** no roteador local e remoto. Essas entradas devem ser semelhantes às seguintes:

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

Para perfis de discador, é necessário definir uma classe de mapa para definir a velocidade. Observe que, por padrão, as interfaces ISDN tentam usar velocidades de comunicação de 64K em cada canal.

Para obter informações detalhadas sobre como configurar mapas e perfis de discador, consulte o *Guia de Configuração de Soluções de Discagem do Cisco IOS*, a *Referência de Comandos de Soluções de Discagem* e o *Guia de Configuração Rápida de Soluções de Discagem*.

Se você receber pacotes PPP válidos, o link estará ativo e funcionando. Você deve prosseguir para a seção "Solução de problemas de PPP" neste momento.

Troubleshooting de Chamada CAS Recebida

Para solucionar problemas de conectividade do grupo CAS com os modems, use os comandos **debug modem**, **debug modem csm** e **debug cas**.

Observação: o comando **debug cas** apareceu primeiro em 12.0(7)T para o AS5200 e o AS5300. As versões anteriores do IOS usam o serviço interno de comando de configuração de nível de sistema juntamente com o comando exec **modem-mgmt debug rbs**. A depuração dessas informações em um AS5800 exige a conexão com a própria placa de tronco.

Primeiro, determine se o switch da companhia telefônica ficou "fora do gancho" para sinalizar a chamada recebida. Caso contrário, verifique o número chamado. Faça isso conectando um telefone à linha telefônica do lado de origem e ligando para o número. Se a chamada entrar corretamente, o problema está no CPE de origem. Se a chamada ainda não for exibida no CAS, verifique o T1 (capítulo 15). Nesse caso, use o comando **debug serial interfaces**.

O seguinte mostra uma boa conexão 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
```

Neste exemplo, a chamada foi direcionada para um modem. Se a chamada foi direcionada para um modem, vá para a seção "Troubleshooting de Chamada de Modem de Entrada", abaixo.

Troubleshooting de Chamada de Modem Recebida

Utilize os seguintes comandos debug ao Troubleshoot chamadas de modem recebidas:

- **debug modem**
- **debug modem csm** (para modems digitais integrados)

Use os seguintes comandos debug em conjunto para indicar a entrada da nova chamada:

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

Supondo que a chamada chegue ao modem, o modem precisa atender a chamada.

Dicas para depurar modems externos

Para facilitar a depuração em um modem externo conectado a uma linha TTY, aumente o volume do alto-falante. Isso ajuda a tornar alguns problemas mais aparentes.

Quando o modem de origem chama, o modem receptor toca? Caso contrário, verifique o número e tente uma chamada manual do site remoto. Tente usar um telefone regular na extremidade de recebimento também. Substitua os cabos e o hardware conforme necessário.

Atendimento de chamada de modem assíncrono

Se um modem externo não estiver respondendo, verifique o cabeamento entre o modem e o servidor de acesso ou roteador. Confirme se o modem está conectado à porta TTY ou auxiliar no roteador com um cabo RJ-45 enrolado e um adaptador MMOD DB-25. A Cisco recomenda e suporta essa configuração de cabo para portas RJ-45. Observe que esses conectores normalmente são rotulados: *Modem.*

O cabeamento RJ-45 vem em alguns tipos: reto, laminado e cruzado. Você pode determinar o tipo de cabeamento segurando as duas extremidades de um cabo RJ-45 lado a lado. Você verá oito tiras coloridas, ou pinos, em cada extremidade.

- Se a ordem dos pinos coloridos for a mesma em cada extremidade, o cabo será reto.
- Se a ordem das cores for invertida em cada extremidade, o cabo será rolado.
- O cabo é um cabo cruzado se as cores indicarem o seguinte:

Cabo crossover RJ45 para RJ45:

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

Para verificar se a sinalização está OK, use o comando **show line** descrito no capítulo 16.

Problemas de cabeamento à parte, um modem externo precisa ser inicializado para responder automaticamente. Verifique o modem remoto para ver se ele está definido como resposta automática. Geralmente, uma luz indicadora AA está acesa quando a resposta automática está definida. Defina o modem remoto como atendimento automático se ainda não estiver definido. Para obter informações sobre como verificar e alterar as configurações do modem, consulte a documentação do modem. Use um telnet reverso para inicializar o modem (consulte o capítulo 16).

Atendimento de chamada de modem digital (integrado)

Em um modem externo, é claro se a chamada está sendo atendida, mas os modems internos exigem uma chamada manual para o número de recebimento. Ouça o tom de resposta (ABT). Se você não ouvir um ABT, verifique a configuração das duas seguintes coisas:

1. Verifique se o comando **isdn incoming-voice modem** existe em qualquer interface ISDN que manipule conexões de modem de entrada.
2. Na configuração de linha para o TTY do modem, verifique se o comando **modem inout** existe.

Também é possível que o módulo de switching de chamadas (CSM) não tenha alocado um modem interno para tratar da chamada recebida. Esse problema pode ser causado pelo modem ou pools de recursos configurados para poucas conexões de entrada. Isso também pode significar que o servidor de acesso pode simplesmente estar fora de modems. Verifique a disponibilidade dos modems e ajuste as configurações do pool de modem ou do gerenciador de pool de recursos adequadamente. Se um modem foi alocado e a configuração mostra a **entrada do modem**, reúna as depurações e entre em contato com a Cisco para obter assistência.

Treinamento do modem

Se o modem receptor aumentar o DSR, o treinamento foi bem-sucedido. Falhas de treinamento podem indicar um problema de circuito ou incompatibilidade de modem.

Para chegar à parte inferior de um problema de modem individual, vá para o prompt AT no modem de origem enquanto ele está conectado à linha de interesse do POTS. Se estiver fazendo uma chamada para um modem digital em um servidor de acesso Cisco, esteja preparado para gravar um arquivo .wav da música de treinamento ou da DIL (Digital Disease Learning Sequence, sequência de aprendizagem por defeito digital). O DIL é a partitura musical (sequência PCM) que o modem analógico V.90 de origem instrui o modem digital de recebimento a reproduzir. A sequência permite que o modem analógico detecte qualquer defeito digital no circuito; como múltiplas conversões D/A, uma lei/u-law, bits roubados ou suportes digitais. Se você não ouvir o DIL, os modems não negociaram V.90 em V.8/V.8bis (ou seja, um problema de compatibilidade de modem). Se você ouvir o DIL e um novo treinamento no V.34, o modem analógico decidiu (com base na reprodução DIL) que o V.90 era inviável.

A música tem barulho? Em caso afirmativo, limpe o circuito.

O cliente desiste rapidamente, sem executar o treinamento V.34? Por exemplo, talvez não saiba o que fazer quando ouvir V.8bis. Nesse caso, você deve tentar desativar o V.8bis (portanto, K56Flex) no servidor (se aceitável). Você deve obter um novo firmware de cliente ou trocar o modem do cliente. Como alternativa, a extremidade de discagem pode inserir cinco vírgulas no final da string de discagem. Isso atrasa a escuta do modem chamador e fará com que o tom V.8bis do servidor receptor exceda o tempo limite sem afetar o modem do cliente. Cinco vírgulas na sequência de discagem são uma diretriz geral e podem precisar de ajuste para permitir condições locais.

Estabelecimento de sessão

Neste ponto da sequência, os modems são conectados e treinados. Agora é hora de descobrir se algum tráfego está cruzando corretamente.

Se a linha que recebe a chamada estiver configurada com **autoselect ppp** e a interface assíncrona estiver configurada com o **modo assíncrono interativo**, use o comando **debug modem** para

verificar o processo de autoseleção. À medida que o tráfego entra no link assíncrono, o servidor de acesso examinará o tráfego para determinar se ele é baseado em caracteres ou em pacotes. Dependendo da determinação, o servidor de acesso iniciará uma sessão PPP ou não irá além de ter uma sessão exec na linha.

Uma sequência de seleção automática normal com pacotes LCP PPP de entrada:

```
*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.
```

Se a chamada for uma sessão PPP e **o modo assíncrono dedicado** estiver configurado na interface assíncrona, use o comando **debug ppp negotiation** para ver se algum pacote de solicitação de configuração está vindo da extremidade remota. As depurações mostram como CONFREQ. Se você observar os pacotes PPP de entrada e de saída, vá para "Solução de problemas do PPP". Caso contrário, conecte-se da extremidade de origem da chamada com uma sessão de modo de caractere (ou "exec") (ou seja, uma sessão não PPP).

Observação: se a extremidade de recebimento exibir **modem assíncrono dedicado** na interface assíncrona, um dial-in exec mostrará apenas o que parece ser lixo ASCII aleatório. Para permitir uma sessão de terminal e ainda ter capacidade PPP, use o comando async interface configuration **async mode interative**. Na configuração da linha associada, use o comando **autoselect ppp**.

O modem não pode enviar ou receber dados

Se os modems se conectarem a uma sessão de terminal e nenhum dado aparecer, verifique as seguintes causas possíveis e os cursos de ação sugeridos:

- **A configuração de velocidade do modem não está bloqueada**Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve indicar as velocidades de Tx e Rx configuradas atualmente.Para obter uma explicação da saída do comando **show line**, consulte a seção "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.Se a linha não estiver configurada para a velocidade correta, use o comando de configuração de linha **speed** para definir a velocidade da linha no servidor de acesso ou na linha do roteador. Defina o valor para a velocidade mais alta em comum entre o modem e o servidor de acesso ou a porta do roteador. Para definir a taxa de baud do terminal, use o comando de configuração de linha **speed**. Esse comando define as velocidades de transmissão (para terminal) e de recepção (do terminal).Sintaxe:**velocidade** *bps*Descrição da sintaxe:*bps* - taxa de transmissão em bits por segundo (bps). O padrão é 9600 bps.O

exemplo a seguir define as linhas 1 e 2 em um servidor de acesso Cisco 2509 para 115200 bps:

```
line 1 2
speed 115200
```

Observação: se, por algum motivo, você não puder usar o controle de fluxo, limite a velocidade da linha para 9600 bps. Velocidades mais rápidas podem resultar em perda de dados.Use o comando exec **show line** novamente e confirme se a velocidade da linha está definida com o valor desejado.Quando tiver certeza de que o servidor de acesso ou a linha do roteador está configurada para a velocidade desejada, inicie uma sessão Telnet reversa para o modem através dessa linha. Para obter mais informações, consulte a seção "Estabelecimento de uma sessão Telnet reversa para um modem" no capítulo 16.Use uma linha de comando de modem que inclua o comando "lock DTE speed" para o seu modem. Consulte a documentação do modem para obter a sintaxe exata do comando de configuração.**Observação:** o comando lock DTE speed, que também pode ser conhecido como *port rate adjust* ou *buffered mode*, está frequentemente relacionado à maneira como o modem lida com a correção de erros. Esse comando varia muito de um modem a outro.Bloquear a velocidade do modem garante que o modem sempre se comunique com o roteador ou servidor de acesso Cisco na velocidade configurada na porta auxiliar da Cisco. Se esse comando não for usado, o modem reverte para a velocidade do enlace de dados (a linha telefônica), em vez de se comunicar na velocidade configurada no servidor de acesso.

- **Controle de fluxo de hardware não configurado no modem ou roteador local ou remoto**Use o comando exec **show line** ***aux-line-number*** e procure o seguinte no campo Capabilities (Recursos):

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

Para obter mais informações, consulte Interpretando a Saída de Show Line no Capítulo 16.Se não houver nenhuma menção de controle de fluxo de hardware neste campo, o controle de fluxo de hardware não estará ativado na linha. Recomenda-se o controle de fluxo de hardware para conexões de acesso servidor a modem.Para obter uma explicação da saída do comando **show line**, consulte a seção "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.Configure o controle de fluxo de hardware na linha usando o comando flowcontrol hardware line configuration.Para definir o método de controle de fluxo de dados entre o terminal ou outro dispositivo serial e o roteador, use o comando de configuração de linha **flowcontrol**. Use a forma no desse comando para desativar o controle de fluxo.Sintaxe:**flowcontrol {none | software [lock] [in | saída] | hardware [em | saída]}**Descrição da sintaxe:**none** - Desativa o controle de fluxo.**software** - Define o controle de fluxo do software. Uma palavra-chave opcional especifica a direção: **no** faz com que o software Cisco IOS ouça o controle de fluxo do dispositivo conectado e **sai** faz com que o software envie informações de controle de fluxo ao dispositivo conectado. Se você não especificar uma direção, ambos serão assumidos.**lock** - Torna impossível desligar o controle de fluxo do host remoto quando o dispositivo conectado precisa de controle de fluxo de software. Esta opção se aplica às conexões usando o Telnet ou os protocolos rlogin.**hardware** - Define o controle de fluxo de hardware. Uma palavra-chave opcional especifica a direção: **no** faz com que o software ouça o controle de fluxo do dispositivo conectado e **sai** faz com que o software envie informações de controle de fluxo ao dispositivo conectado. Se você não especificar uma direção, ambos serão assumidos. Para obter mais informações sobre o controle de fluxo de hardware, consulte o manual de hardware fornecido com o roteador.Exemplo:O exemplo a seguir define o controle de fluxo de hardware na linha 7:

```
line 7
flowcontrol hardware
```

Observação: se por algum motivo você não puder usar o controle de fluxo, limite a velocidade da linha para 9600 bps. Velocidades mais rápidas podem resultar em perda de dados.Depois de ativar o controle de fluxo de hardware no servidor de acesso ou na linha do roteador, inicie uma sessão Telnet reversa para o modem através dessa linha. Para obter mais informações, consulte a seção "Estabelecimento de uma sessão Telnet reversa para um modem" no capítulo 16.Use um comando modem que inclua o comando **RTS/CTS Flow** para o seu modem. Esse comando garante que o modem esteja usando o mesmo método de controle de fluxo (ou seja, controle de fluxo de hardware) do servidor de acesso ou roteador Cisco. Consulte a documentação do modem para obter a sintaxe exata do comando de configuração.

- **Comandos de mapa de discador configurados incorretamente**Use o comando exec **privilegiado show running-config** para exibir a configuração do roteador. Verifique as entradas do comando **dialer map** para ver se a palavra-chave **broadcast** está especificada.Se a palavra-chave estiver ausente, adicione-a à configuração.Sintaxe:**dialer map** ***protocol next-hop-address*** **[name** ***hostname*****] [broadcast] [***dial-string***]**Descrição da sintaxe:*protocol* - O protocolo sujeito ao mapeamento. As opções incluem IP, IPX, bridge e snapshot.*next-hop-address* - O endereço de protocolo da interface assíncrona do site oposto.**name** ***hostname*** - Um parâmetro obrigatório usado na autenticação PPP. É o nome do local remoto para o qual o mapa de discador é criado. O nome diferencia maiúsculas de minúsculas e deve corresponder ao nome de host do roteador remoto.**broadcast** - Uma palavra-chave opcional que transmite pacotes (por exemplo, atualizações IP RIP ou IPX RIP/SAP) que é encaminhada ao destino remoto. Em configurações de exemplo de roteamento estático, as atualizações de roteamento não são desejadas e a palavra-chave **broadcast** é omitida.*dial-string* - O número de telefone do site remoto. Todos os códigos de acesso (por exemplo, 9 para sair de um escritório, códigos de discagem internacionais, códigos de área) devem ser incluídos.Certifique-se de que os comandos **dialer map** especifiquem os endereços corretos do próximo salto.Se o endereço do próximo salto estiver incorreto, altere-o usando o comando **dialer map**.Verifique se todas as outras opções dos comandos dialer map estão corretamente especificadas para o protocolo que você está usando.Para obter informações detalhadas sobre como configurar mapas de discadores, consulte o *Guia de Configuração de Rede de Longa Distância do Cisco IOS* e a *Referência de Comandos de Rede de Longa Distância*.
- **Problema com o modem de discagem**Verifique se o modem de discagem está operacional e conectado corretamente à porta correta. Determine se outro modem funciona quando conectado à mesma porta.

A depuração de uma sessão de exec de entrada geralmente se enquadra em algumas categorias principais:

O cliente de discagem não recebe nenhum prompt exec

- **A seleção automática está ativada na linha**Tente acessar o modo exec pressionando Enter.
- **Linha configurada com o comando no exec**Use o comando exec **show line** para exibir o status da linha apropriada.Verifique o campo Capabilities (Recursos) para ver se ele diz "exec

suppressed" (exec suprimido). Se for esse o caso, o comando de configuração de linha **no exec** está ativado.Configure o comando de configuração de linha **exec** na linha para permitir que sessões exec sejam iniciadas. Este comando não tem argumentos ou palavras-chave.O exemplo a seguir ativa o exec na linha 7:

```
line 7
exec
```

- **O controle de fluxo não está habilitado.orO controle de fluxo é ativado somente em um dispositivo (DTE ou DCE).orO controle de fluxo está configurado incorretamente.**Use o comando exec **show line** *aux-line-number* e procure o seguinte no campo Capabilities (Recursos):

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

Para obter mais informações, consulte Interpretando a Saída de Show Line no Capítulo 16.Se não houver nenhuma menção de controle de fluxo de hardware neste campo, o controle de fluxo de hardware não estará ativado na linha. Recomenda-se o controle de fluxo de hardware para conexões de acesso servidor a modem.Para obter uma explicação da saída do comando show line, consulte a seção "Usando comandos de depuração" no capítulo 15.Configure o controle de fluxo de hardware na linha usando o comando de configuração de linha **flowcontrol hardware**. O exemplo a seguir define o controle de fluxo de hardware na linha 7:

```
line 7
flowcontrol hardware
```

Observação: se por algum motivo você não puder usar o controle de fluxo, limite a velocidade da linha para 9600 bps. Velocidades mais rápidas podem resultar em perda de dados.Depois de ativar o controle de fluxo de hardware no servidor de acesso ou na linha do roteador, inicie uma sessão Telnet reversa para o modem através dessa linha. Para obter mais informações, consulte a seção "Estabelecimento de uma sessão Telnet reversa para um modem" no capítulo 16.Use um comando modem que inclua o comando RTS/CTS Flow para seu modem. Esse comando garante que o modem esteja usando o mesmo método de controle de fluxo (ou seja, controle de fluxo de hardware) do servidor de acesso ou roteador Cisco. Consulte a documentação do modem para obter a sintaxe exata do comando de configuração.

- **A configuração de velocidade do modem não está bloqueada**Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve indicar as velocidades de Tx e Rx configuradas atualmente.Para obter uma explicação da saída do comando show line, consulte a seção "Usando comandos de depuração" no capítulo 15.Se a linha não estiver configurada para a velocidade correta, use o comando de configuração da linha de velocidade para definir a velocidade da linha no servidor de acesso ou na linha do roteador. Defina o valor para a velocidade mais alta em comum entre o modem e o servidor de acesso ou a porta do roteador. Para definir a taxa de baud do terminal, use o comando de configuração da linha de velocidade. Esse comando define as velocidades de transmissão (para terminal) e de recepção (do terminal).Sintaxe:**velocidade** *bps*Descrição da sintaxe:*bps* - taxa de transmissão em bits por segundo (bps). O padrão é 9600 bps.Exemplo:O exemplo a seguir define as linhas 1 e 2 em um servidor de acesso Cisco 2509 para 115200 bps:

```
line 1 2
speed 115200
```

Observação: se por algum motivo você não puder usar o controle de fluxo, limite a velocidade da linha para 9600 bps. Velocidades mais rápidas podem resultar em perda de dados.Use o comando exec **show line** novamente e confirme se a velocidade da linha está definida com o valor desejado.Quando tiver certeza de que o servidor de acesso ou a linha do roteador está

configurada para a velocidade desejada, inicie uma sessão Telnet reversa para o modem através dessa linha. Para obter mais informações, consulte a seção "Estabelecimento de uma sessão Telnet reversa para um modem" no capítulo 16.Use um comando modem que inclua o comando **lock** DTE speed para o seu modem. Consulte a documentação do modem para obter a sintaxe exata do comando de configuração.**Observação:** o comando **lock** DTE speed, que também pode ser conhecido como modo de ajuste ou buffer da taxa de porta, geralmente está relacionado à forma como o modem lida com a correção de erros. Esse comando varia muito de um modem a outro.Bloquear a velocidade do modem garante que o modem sempre se comunique com o roteador ou servidor de acesso Cisco na velocidade configurada na porta auxiliar da Cisco. Se esse comando não for usado, o modem reverte para a velocidade do enlace de dados (a linha telefônica) em vez de se comunicar na velocidade configurada no servidor de acesso.

Sessões de discagem veem "lixo"

- **A configuração de velocidade do modem não está bloqueada**Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve indicar as velocidades de Tx e Rx configuradas atualmente.Para obter uma explicação da saída do comando **show line**, consulte a seção "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.Se a linha não estiver configurada para a velocidade correta, use o comando de configuração de linha **speed** para definir a velocidade da linha no servidor de acesso ou na linha do roteador. Defina o valor para a velocidade mais alta em comum entre o modem e o servidor de acesso ou a porta do roteador.Para definir a taxa de baud do terminal, use o comando de configuração de linha **speed**. Esse comando define as velocidades de transmissão (para terminal) e de recepção (do terminal).Sintaxe:**velocidade** ***bps***Descrição da sintaxe:bps de taxa de transmissão em bits por segundo (bps). O padrão é 9600 bps.Exemplo:O exemplo a seguir define as linhas 1 e 2 em um servidor de acesso Cisco 2509 para 115200 bps:linha 1 2velocidade 115200**Observação:** se por algum motivo você não puder usar o controle de fluxo, limite a velocidade da linha para 9600 bps. Velocidades mais rápidas podem resultar em perda de dados.Use o comando exec **show line** novamente e confirme se a velocidade da linha está definida com o valor desejado.Quando tiver certeza de que o servidor de acesso ou a linha do roteador está configurada para a velocidade desejada, inicie uma sessão Telnet reversa para o modem através dessa linha. Para obter mais informações, consulte a seção "Estabelecimento de uma sessão Telnet reversa para um modem" no capítulo 16.Use um comando modem que inclua o comando **lock** DTE speed para o seu modem. Consulte a documentação do modem para obter a sintaxe exata do comando de configuração.**Observação:** o comando **lock** DTE speed, que também pode ser conhecido como *port rate adjust* ou *buffered mode*, é frequentemente relacionado à maneira como o modem lida com a correção de erros. Esse comando varia muito de um modem a outro.Bloquear a velocidade do modem garante que o modem sempre se comunique com o roteador ou servidor de acesso Cisco na velocidade configurada na porta auxiliar da Cisco. Se esse comando não for usado, o modem reverte para a velocidade do enlace de dados (a linha telefônica) em vez de se comunicar na velocidade configurada no servidor de acesso.

Sintoma: A sessão de discagem remota é aberta em uma sessão já existente iniciada por outro usuário. Ou seja, em vez de obter um prompt de login, um usuário de discagem vê uma sessão estabelecida por outro usuário (que pode ser um prompt de comando UNIX, uma sessão de editor de texto e assim por diante).

A sessão de discagem é aberta na sessão existente

- **Modem configurado para DCD sempre alto**O modem deve ser reconfigurado para ter DCD alto apenas no CD. Isso geralmente é feito usando a string de comando do modem **&C1**, mas verifique a documentação do modem para obter a sintaxe exata do seu modem.Talvez seja necessário configurar a linha do servidor de acesso à qual o modem está conectado com o comando de configuração de linha **no exec**. Limpe a linha com o comando **clear line privileged exec**, inicie uma sessão Telnet reversa com o modem e reconfigure o modem para que o DCD esteja alto apenas no CD.Encerre a sessão Telnet inserindo **disconnect** e reconfigure a linha do servidor de acesso com o comando de configuração de linha **exec**
- **O controle do modem não está ativado no servidor de acesso ou roteador**Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve ser show **inout** ou **RIisCD** na coluna Modem. Isso indica que o controle do modem está ativado na linha do servidor de acesso ou roteador.Para obter uma explicação da saída do **comando show line**, consulte a seção "Using Debug Commands" (Usando Comandos de Depuração) no capítulo 15.Configure a linha para controle de modem usando o comando de configuração de linha **modem inout**. O controle do modem agora está ativado no servidor de acesso.**Nota:** Certifique-se de usar o comando **modem inout** em vez do comando **modem dialin** enquanto a conectividade do modem estiver em questão. Este último comando permite que a linha aceite apenas chamadas de entrada. As chamadas efetuadas serão recusadas, tornando impossível estabelecer uma sessão Telnet com o modem para configurá-las. Se quiser habilitar o comando **modem dialin**, faça isso somente depois de ter certeza de que o modem está funcionando corretamente.
- **Cabeamento incorreto**Verifique o cabeamento entre o modem e o servidor de acesso ou roteador. Confirme se o modem está conectado à porta auxiliar no servidor de acesso ou roteador com um cabo RJ-45 enrolado e um adaptador MMOD DB-25. Essa configuração de cabeamento é recomendada e suportada pela Cisco para portas RJ-45. Normalmente, esses conectores são rotulados: Modem.Há dois tipos de cabeamento RJ-45: reto e enrolado. Se você segurar as duas extremidades de um cabo RJ-45 lado a lado, verá oito tiras coloridas, ou pinos, em cada extremidade. Se a ordem dos pinos coloridos for a mesma em cada extremidade, o cabo será reto. Se a ordem das cores estiver invertida em cada extremidade, o cabo estará enrolado.O cabo enrolado (CAB-500RJ) é padrão com o 2500/CS500 da Cisco.Use o comando exec **show line** para verificar se o cabeamento está correto. Veja a explicação da saída do comando **show line** na seção "Using Debug Commands" neste capítulo 15.

O modem receptor de discagem não é desconectado corretamente

- **O modem não está detectando DTR**Digite o comando **Hangup DTR modem**. Esse comando instrui o modem a deixar a portadora cair quando o sinal DTR não estiver mais sendo recebido.Em um modem compatível com Hayes, a string **&D3** é comumente usada para configurar **Hangup DTR** no modem. Para obter a sintaxe exata desse comando, consulte a documentação do modem.
- **O controle do modem não está ativado no roteador ou no servidor de acesso**Use o comando exec **show line** no servidor de acesso ou roteador. A saída da porta auxiliar deve mostrar **inout** ou **RIisCD** na coluna Modem. Isso indica que o controle do modem está ativado na linha do servidor de acesso ou roteador.Para obter uma explicação da saída do comando show

line, consulte a seção "Using Debug Commands" no capítulo 15.Configure a linha para controle de modem usando o comando modem inout line configuration. O controle do modem agora está ativado no servidor de acesso.**Nota:** Certifique-se de usar o comando **modem inout** em vez do comando **modem dialin** enquanto a conectividade do modem estiver em questão. Este último comando permite que a linha aceite apenas chamadas de entrada. As chamadas efetuadas serão recusadas, tornando impossível estabelecer uma sessão Telnet com o modem para configurá-las. Se quiser habilitar o comando **modem dialin**, faça isso somente depois de ter certeza de que o modem está funcionando corretamente.

Troubleshooting de Chamadas de Saída

Enquanto a abordagem de solução de problemas para chamadas recebidas começa na parte inferior, a solução de problemas de uma conexão de saída começa na parte superior. O fluxo geral de raciocínio procura o seguinte:

1. O Roteamento de discagem por demanda (DDR) inicia uma chamada? (Uma resposta sim avança para a próxima pergunta)
2. Se for um modem assíncrono, os scripts de bate-papo emitem os comandos esperados?
3. A chamada chega ao PSTN?
4. A extremidade remota atende a chamada?
5. A chamada é concluída?
6. Os dados estão passando pelo link?
7. A sessão está estabelecida? (PPP ou terminal)

Verificando a operação do discador

Para ver se o discador está tentando fazer uma chamada para seu destino remoto, use o comando **debug dialer events**. Informações mais detalhadas podem ser obtidas do **debug dialer packet**, mas o comando **debug dialer packet** exige muitos recursos e não deve ser usado em um sistema ocupado que tenha várias interfaces de discador operando.

A linha a seguir de saída de eventos do discador de depuração para um pacote IP lista o nome da interface DDR e os endereços de origem e de destino do pacote:

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

Se o tráfego não iniciar uma tentativa de discagem, o motivo mais comum é a configuração incorreta (uma das definições de tráfego interessante, o estado da interface do discador ou o roteamento).

O tráfego não inicia uma tentativa de discagem

- **Faltam ou incorretas definições de "tráfego interessante"**Usando o comando **show running-config**, verifique se a interface está configurada com um **dialer-group** e se há uma **lista de discadores de** nível global configurada com um número correspondente.Certifique-se de que o comando **dialer-list** esteja configurado para permitir um protocolo inteiro ou para permitir o tráfego correspondente a uma lista de acessoVerifique se a lista de acesso declara que os pacotes que passam pelo link são interessantes. Um teste útil é usar o comando exec

privilegiado **debug ip packet [list number]** usando o número da lista de acesso pertinente. Em seguida, tente fazer ping ou enviar tráfego pelo link. Se os filtros de tráfego interessante tiverem sido definidos corretamente, você verá os pacotes na saída de depuração. Se não houver saída de depuração desse teste, a lista de acesso não corresponde aos pacotes.

- **Estado da interface**Use o comando **show interfaces [*interface name*]** para garantir que a interface esteja no estado "up/up (spoofing)".Interface no modo "standby"Outra interface (primária) no roteador foi configurada para usar a interface do discador como uma interface de backup. Além disso, a interface primária não está em um estado de "down/down", que é necessário para retirar a interface do discador do modo de espera. Além disso, um *atraso de backup* deve ser configurado na interface primária, ou o comando **backup interface** nunca será executado.Para verificar se a interface do discador mudará de "standby" para "up/up (spoofing)", geralmente é necessário puxar o cabo da interface primária. Simplesmente desligar a interface primária com o comando de configuração **shutdown** não colocará a interface primária em "down/down", mas a colocará em "administratively down" - não a mesma coisa.Além disso, se a conexão principal for via Frame Relay, a configuração do Frame Relay deverá ser feita em uma subinterface serial ponto-a-ponto, e a companhia telefônica deverá estar passando o bit "Ativo". Essa prática também é conhecida como "LMI de ponta a ponta".A interface está "administrativamente inativa"A interface do discador foi configurada com o comando **shutdown**. Esse também é o estado padrão de qualquer interface quando um roteador Cisco é inicializado pela primeira vez. Use o comando de configuração de interface **no shutdown** para remover esse impedimento.
- **Roteamento incorreto**Emita o comando exec **show ip route [*a.b.c.d*]**, onde *a.b.c.d* é o endereço da interface do discador do roteador remoto. Se **ip unnumbered** for usado no roteador remoto, use o endereço da interface listada no comando **ip unnumbered**.A saída deve mostrar uma rota para o endereço remoto através da interface do discador. Se não houver rota, verifique se as rotas estáticas ou flutuantes foram configuradas examinando a saída de show running-config.Se houver uma rota através de uma interface diferente da interface do discador, a implicação é que o DDR está sendo usado como um backup. Examine a configuração do roteador para verificar se as rotas estáticas ou flutuantes foram configuradas. A maneira mais segura de testar o roteamento, nesse caso, é desabilitar a conexão primária e executar o comando **show ip route [*a.b.c.d*]** para verificar se a rota apropriada foi instalada na tabela de roteamento.**Observação:** se você tentar isso durante as operações da rede ao vivo, um evento de discagem poderá ser acionado. Esse tipo de teste é mais bem realizado durante os ciclos de manutenção programados.

Estabelecendo a chamada

Se o roteamento e os filtros de tráfego interessante estiverem corretos, uma chamada deve ser iniciada. Isso pode ser visto usando **debug dialer events**:

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

Se a causa de discagem for vista, mas não for feita nenhuma tentativa de discagem, o motivo normal é um mapa de discador ou perfil de discador mal configurado.

Chamada não efetuada

Alguns problemas possíveis e ações sugeridas estão listados abaixo:

- **Mapa de discador mal configurado**Use o comando **show running-config** para garantir que a interface de discagem esteja configurada com pelo menos uma instrução *dialer map* que aponta para o endereço do protocolo e o número chamado do local remoto.
- **Perfil de discador configurado incorretamente**Use o comando **show running-config** para garantir que a interface do Discador esteja configurada com um comando **dialer pool X** e que uma interface do discador no roteador esteja configurada com um *dialer pool-member X correspondente*. Se os perfis de discador não estiverem configurados corretamente, você poderá ver uma mensagem de depuração como:
  ```
  Dialer1: Can't place call, no dialer pool set
  ```
  Verifique se uma **string de discador** está configurada.

Chamada de Saída Assíncrona - Verificar Operação do Script de Bate-papo

Se a chamada de saída for uma chamada de modem, um script de bate-papo deverá ser executado para que a chamada continue. Para o DDR baseado em mapa de discador, o script de bate-papo é chamado pelo parâmetro modem-script em um comando dialer map. Se o DDR for baseado no perfil do discador, isso será feito pelo comando **script dialer**, configurado na linha TTY. Ambos os usos dependem de um script de bate-papo existente na configuração global do roteador, por exemplo:

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

Em ambos os eventos, o comando para exibir a atividade do script de bate-papo é **debug chat**. Se a sequência de discagem (ou seja, o número do telefone) usada no **dialer map** ou **dialer string** fosse 5551212, a saída de depuração pareceria com a seguinte:

```
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
```

Os problemas de script de bate-papo podem ser divididos em três categorias:

- Erro de configuração
- Falha do modem
- Falha de conexão

Falha no script de bate-papo

Esta lista mostra as saídas possíveis de debug chat shows e ações sugeridas:

- **nenhum script de bate-papo correspondente encontrado para [número]**Um script de bate-

papo não foi configurado. Adicione um.

- **Discagem do script de bate-papo concluída, status = Tempo limite da conexão esgotado; o host remoto não está respondendo**O modem não está respondendo ao script de bate-papo. Verifique a comunicação com o modem (consulte a Tabela 16-2 no Capítulo 16).
- **Tempo limite esperado: CONNECT***Possibilidade 1*: O modem local não está realmente fazendo a chamada. Verifique se o modem pode fazer uma chamada executando um Telnet reverso para o modem e iniciando manualmente uma discagem.*Possibilidade 2*: O modem remoto não está respondendo. Teste isso discando o modem remoto com um telefone POTS comum.*Possibilidade 3*: O número discado está incorreto. Verifique o número discando-o manualmente. Corrija a configuração, se necessário.*Possibilidade 4*: O treinamento do modem está demorando muito ou o valor TIMEOUT está muito baixo. Se o modem local for externo, ative o volume do alto-falante do modem e ouça os tons de trainup. Se o treinamento for interrompido abruptamente, tente aumentar o valor TIMEOUT no comando **chat-script**. Se o TIMEOUT já tiver 60 segundos ou mais, consulte a seção Treinamento do modem.

Chamada de saída ISDN

Após a primeira suspeita de uma falha de ISDN, em uma BRI ou PRI, sempre verifique a saída de **show isdn status**. Os principais aspectos a serem observados são que a Camada 1 deve estar Ativa e a Camada 2 deve estar em um estado de *MULTIPLE_FRAME_ESTABLISHED*. Consulte a seção "Interpretando a Saída de Status de ISDN" no Capítulo 16 para obter informações sobre como ler essa saída, bem como para obter medidas corretivas.

Para chamadas ISDN de saída, **debug isdn q931** e **debug isdn events** são as melhores ferramentas a serem usadas. Felizmente, a depuração de chamadas de saída é muito semelhante à depuração de chamadas de entrada. Uma chamada bem-sucedida normal pode ser semelhante a esta:

```
*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
```

O valor da causa indica duas coisas.

- O segundo byte do valor de 4 ou 6 bytes indica de onde no caminho de chamada de ponta a ponta foi recebido o DISCONNECT ou o RELEASE_COMP. Isso pode ajudá-lo a localizar o problema.
- O terceiro e o quarto bytes indicam o motivo real da falha. Veja as tabelas a seguir para os significados dos diferentes valores.

Observação: a impressão a seguir geralmente indica uma falha de protocolo mais alto:

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

A falha de autenticação PPP é um motivo típico. Ative **debug ppp negotiation** e **debug ppp authentication** antes de supor que a falha de conexão é necessariamente um problema ISDN

Campos de código de causa

A Tabela 17-9 lista os campos do código de causa ISDN exibidos no seguinte formato dentro dos comandos debug:

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

Campos de código de causa ISDN

Campo	Descrição do valor
0x	Os valores a seguir estão em hexadecimal.
y1	8—Codificação padrão ITU-T.
y2	0—Usuário 1—Rede privada servindo usuário local 2—Rede pública servindo usuário local 3—Rede de trânsito 4—Rede pública servindo usuário remoto 5—Rede privada servindo usuário remoto 7—Rede internacional A—Rede além do ponto de interconexão de rede
z1	Classe (o número hexadecimal mais significativo) do valor de causa. Consulte a próxima tabela para obter informações detalhadas sobre possíveis valores.
z2	Valor (o número hexadecimal menos significativo) do valor de causa. Consulte a próxima tabela para obter informações detalhadas sobre possíveis valores.
a1	(Opcional) Campo de diagnóstico que é sempre 8.
a2	(Opcional) Campo de diagnóstico que é um dos seguintes valores: 0—Desconhecido 1—Permanente 2—Transitório

Valores de causa de ISDN

A tabela a seguir lista descrições de alguns dos valores de causa mais comumente vistos do elemento de informação de causa - o terceiro e o quarto bytes do código de causa. Para obter informações mais completas sobre códigos e valores de ISDN, consulte Entendendo **debug isdn q931** Disconnect Cause Codes.

Valor hexadecimal	Causa	Explicação

81	Número não alocado (não atribuído)	O número ISDN foi enviado ao switch no formato correto; no entanto, o número não é atribuído a nenhum equipamento de destino.
90	Limpeza normal de chamada	A limpeza de chamada normal ocorreu.
91	Usuário ocupado	O sistema chamado confirma a solicitação de conexão, mas não pode aceitar a chamada porque todos os canais B estão em uso.
92	Nenhum usuário está respondendo	Não é possível concluir a conexão porque o destino não responde à chamada.
93	Sem resposta do usuário (alerta do usuário)	O destino responde à solicitação de conexão, mas não completa a conexão dentro do tempo determinado. O problema está na ponta remota da conexão.
95	Chamada rejeitada	O destino é capaz de aceitar a chamada, mas a rejeitou por um motivo desconhecido.
9C	Formato de número inválido	A conexão não pôde ser estabelecida porque o endereço de destino foi apresentado em um formato não reconhecível ou porque o endereço de destino estava incompleto.
9F	Normal, não especificado	Informa a ocorrência de um evento normal quando nenhuma causa padrão se aplica. Nenhuma ação é necessária.
A2	Nenhum circuito/canal disponível	A conexão não pode ser estabelecida porque não há canal apropriado disponível para atender a chamada.
A6	A rede	O destino não pode ser alcançado

	não está funcionando	porque a rede não está funcionando corretamente e a condição pode durar um período prolongado. Uma tentativa imediata de reconexão provavelmente não terá êxito.
AC	Circuito/canal solicitado não disponível	O equipamento remoto não pode oferecer o canal requisitado por uma razão desconhecida. Isso pode ser um problema temporário.
B2	Recurso solicitado não inscrito	O equipamento remoto suporta o serviço suplementar requisitado somente por assinatura. Isso frequentemente é uma referência ao serviço de longa distância.
B9	Capacidade do portador não autorizada	O usuário solicitou um recurso de portador fornecido pela rede, mas não está autorizado a usá-lo. Isso pode ser um problema de assinatura.
D8	Destino incompatível	Indica que foi feita uma tentativa de conexão com equipamentos não ISDN. Por exemplo, para uma linha analógica.
E0	Falta o elemento de informação obrigatório	O equipamento receptor recebeu uma mensagem que não incluía um dos elementos de informação obrigatórios. Isso geralmente ocorre devido a um erro de canal D. Se esse erro ocorrer sistematicamente, informe-o ao seu provedor de serviços ISDN.
E4	Conteúdo do elemento de informação inválido	O equipamento remoto recebeu uma mensagem que inclui informações inválidas no elemento de informação. Isso geralmente ocorre devido a um erro de canal D.

Chamada de saída CAS

Para chamadas de saída via CAS T1 ou E1 e modems digitais integrados, grande parte da solução de problemas é semelhante a outra solução de problemas DDR. O mesmo se aplica a chamadas de modem integradas de saída por uma linha PRI. Os recursos exclusivos envolvidos em fazer uma chamada desta maneira exigem depuração especial no caso de uma falha de chamada.

Quanto a outras situações de DDR, você deve garantir que uma tentativa de chamada seja solicitada. Use **debug dialer events** para este fim. Consulte Verificando a operação do discador.

Para que uma chamada possa ser feita, um modem deve ser alocado para a chamada. Para visualizar esse processo e a chamada subsequente, use os seguintes comandos debug:

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

Observação: o comando **debug cas** apareceu primeiro no IOS versão 12.0(7)T para AS5200 e AS5300. As versões anteriores do IOS usam um **serviço interno de** comando de configuração no nível do sistema junto com o comando exec **modem-mgmt debug rbs**:

Ativando as depurações

```
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
```

Desativando as depurações

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

Observação: a depuração dessas informações em um AS5800 exige a conexão com a placa de tronco. A seguir está um exemplo de uma chamada de saída normal sobre um CAS T1 que é provisionado e configurado 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
```

As depurações para T1s e E1s com outros tipos de sinalização são semelhantes.

Chegar a esse ponto na depuração indica que os modems de chamada e resposta treinaram e conectaram-se e que os protocolos de camada superior podem começar a negociar. Se um modem for alocado corretamente para a chamada de saída, mas a conexão não chegar até aqui, a T1 deverá ser examinada. Consulte o Capítulo 15 para obter informações sobre Troubleshooting de T1.

Solução de problemas do PPP

A solução de problemas da parte PPP de uma conexão começa quando você sabe que a conexão de discagem, ISDN ou assíncrona, foi estabelecida com êxito.

Éimportante entender como é uma sequência PPP de depuração bem-sucedida antes de solucionar problemas de negociação de PPP. Dessa forma, comparar uma sessão de depuração PPP com falha com uma sequência PPP de depuração concluída com êxito economiza tempo e esforço.

A seguir está um exemplo de uma sequência PPP bem-sucedida. Consulte Detalhes de Negociação do LCP do PPP para obter uma descrição detalhada dos campos de saída.

```
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
```

Observação: suas depurações podem aparecer em um formato diferente. Este exemplo mostra o formato de saída de depuração PPP mais recente que foi modificado no IOS versão 11.2(8). Consulte o Capítulo 16 para obter um exemplo de depuração de PPP com as versões mais antigas do IOS.

Detalhes da negociação de PPP LCP

Carimbo de data/hora	Descrição
10:57:15.415	Solicitação de configuração de saída (O CONFREQ). O NAS envia um pacote de solicitação de configuração de PPP de saída ao cliente.
10:57:15.543	Confirmação de configuração de entrada (I CONFACK). O cliente confirma a solicitação de PPP do Montecito.
10:57:16.919	Solicitação de configuração de entrada (I CONFREQ). O cliente deseja negociar o protocolo de retorno de chamada.
10:57:16.919	Rejeição da configuração de saída (O CONFREJ). O NAS rejeita a opção de retorno de chamada.
10:57:17.047	Solicitação de configuração de entrada (I CONFREQ). O cliente solicita um novo conjunto de opções. Observe que o retorno de chamada da Microsoft não foi solicitado desta vez.
10:57:17.047	Confirmação de configuração de saída (O CONFACK). O NAS aceita o novo conjunto de opções.
10:57:17.047	A negociação de PPP LCP foi concluída com êxito. O estado do LCP é "Aberto". Ambos os lados reconheceram (CONFACK) a solicitação de configuração do outro lado (CONFREQ).
10:57:17.047 até 10:57:17.191	A autenticação PPP foi concluída com êxito. Depois que o LCP negocia, a autenticação é iniciada. A autenticação deve ocorrer antes que qualquer protocolo de rede, como o IP, seja entregue. Ambos os lados autenticam com o método negociado durante o LCP. O Montecito está autenticando o cliente usando o CHAP.
10:57:20.55	O estado está aberto para IP Control Protocol (IPCP). Uma rota é negociada e instalada para o

1	peer IPCP, que recebe o endereço IP 1.1.1.1.

Link Control Protocol

Dois tipos de problemas geralmente são encontrados durante a negociação do LCP.

O primeiro ocorre quando um peer faz solicitações de configuração que o outro peer não pode ou não vai confirmar. Embora essa seja uma ocorrência frequente, pode ser um problema se o solicitante insistir no parâmetro. Um exemplo típico é ao negociar AUTHTYPE (também conhecido como "AuthProto"). Por exemplo, muitos servidores de acesso são configurados para aceitar apenas CHAP para autenticação. Se o chamador estiver configurado para fazer apenas a autenticação PAP, CONFREQs e CONFNAKs serão trocados até que um peer ou o outro descarte a conexão.

```
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)
...
...
```

O segundo tipo de problema no LCP é quando apenas CONFREQs de saída são vistos em um ou em ambos os pares, como no exemplo abaixo. Geralmente, esse é o resultado do que é conhecido como *incompatibilidade de velocidade* na camada inferior. Essa condição pode ocorrer no DDR assíncrono ou 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
```

Se a conexão for assíncrona, a causa provável é uma incompatibilidade de velocidade entre o roteador e seu modem. Geralmente, isso é resultado de falha ao bloquear a velocidade DTE do modem para a velocidade configurada da linha TTY. O problema pode ser encontrado em um ou em ambos os pares, portanto, verifique ambos. Consulte Modem Cannot Send or Receive Data anteriormente neste capítulo.

Se os sintomas forem observados quando a conexão for por ISDN, é provável que um peer esteja se conectando a 56K enquanto o outro está a 64K. Embora essa condição seja rara, ela acontece. O problema pode ser um ou ambos os pares, ou possivelmente a companhia telefônica. Use **debug isdn q931** e examine as mensagens SETUP em cada um dos peers. O Recurso do Portador enviado de um peer deve corresponder ao Recurso do Portador visto na mensagem SETUP recebida no outro peer. Como uma possível correção, configure a velocidade de discagem, 56K ou 64K, no **mapa de discador** do comando de nível de interface ou no comando **dialer isdn speed** configurado em map-class.

```
*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
```

Essa situação pode justificar uma chamada para o TAC da Cisco. Colete as seguintes saídas de ambos os colegas antes de ligar para o TAC:

- **show running-config**
- **show version**
- **debug isdn q931**
- **debug isdn events**
- **negociação de debug ppp**

Autenticação

A falha de autenticação é o motivo mais comum para uma falha de PPP. Nomes de usuário e senhas mal configurados ou incompatíveis criam mensagens de erro na saída de depuração.

O exemplo a seguir mostra que o nome de usuário Goleta não tem permissão para discar para o NAS, que não tem um nome de usuário local configurado para esse usuário. Para corrigir o problema, use o comando **username** ***name*** **password** ***password*** para adicionar o nome de usuário "Goleta" ao banco de dados AAA local do 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
```

O exemplo a seguir mostra que o nome de usuário "Goleta" está configurado no NAS. No entanto, a comparação de senha falhou. Para corrigir esse problema, use o comando **username** *name* **password** *password* para especificar a senha de login correta 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 obter mais informações sobre a autenticação PAP, consulte Configuração e Troubleshooting do PPP Password Authentication Protocol (PAP).

Protocolo de controle de rede

Depois que os pares tiverem executado com êxito a autenticação necessária, a negociação será movida para a fase NCP. Se ambos os pares estiverem configurados corretamente, a negociação do NCP pode parecer com o exemplo a seguir, que mostra um PC cliente discando e negociando com um 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
```

[Detalhes da negociação do NCP do PPP]

Carimbo de data/hora	Descrição
21:35:04.190	Solicitação de configuração de saída (O CONFREQ). O NAS envia um pacote de solicitação de configuração de PPP de saída contendo seu endereço IP para o peer.
21:35:04.282	CONFREQ de entrada O peer solicita a compactação de cabeçalho VJ. Ele precisa de um endereço IP para si mesmo, bem como de endereços dos servidores DNS primário e secundário.
21:35:04.306	Config-Reject de Saída (CONFREJ). A compactação do cabeçalho VJ foi rejeitada.
21:35:04.314 até 21:35:04.330	O peer envia uma solicitação para fazer o Protocolo de Controle de Compressão; o protocolo inteiro é rejeitado pelo NAS por meio de uma mensagem PROTREJ. O peer não deve (e não) tentar novamente o CCP.
21:35:04.334	O peer confirma o endereço IP do NAS com um CONFACK.
21:35:07.274	CONFREQ de entrada O peer não solicita mais compactação de cabeçalho VJ, mas ainda precisa de um endereço IP para si mesmo, assim como endereços dos servidores DNS primário e secundário.
21:35:07.294	O NAS envia um CONFNAK contendo o endereço que deseja que o peer use e os endereços dos servidores DNS primário e secundário.
21:35:07.426	O peer envia os endereços de volta para o NAS; uma tentativa de confirmar se os endereços foram recebidos corretamente.
21:35:	O NAS confirma os endereços com um

07.458	CONFACK.
21:35:07.478	Cada lado da conexão que emitiu um CONFACK, a negociação é concluída. O comando **show interfaces Async4** no NAS mostra "IPCP: Abrir".
21:35:07.490	Uma rota de host para o peer remoto é instalada na tabela de roteamento do NAS.

Épossível que os pares negociem simultaneamente mais de um protocolo de Camada 3. Não é raro, por exemplo, ver IP e IPX sendo negociados. Também é possível que um protocolo negocie com êxito enquanto o outro não o faz.

Troubleshooting de NCP

Qualquer problema que ocorra durante a negociação do NCP pode normalmente ser rastreado para as configurações dos pares de negociação. Se a negociação do PPP falhar durante a fase do NCP, consulte as seguintes etapas:

1. Verificar a configuração do protocolo de interfaceExamine a saída do comando exec privilegiado **show running-config**. Verifique se a interface está configurada para suportar o protocolo que você deseja executar na conexão.
2. Verificar o endereço da interfaceConfirme se a interface em questão tem um endereço configurado. Se estiver usando **ip unnumbered [*interface-name*]** ou **ipx ppp-client loopback [*number*]**, verifique se a interface referenciada está configurada com um endereço.
3. Verificar a disponibilidade do endereço do clienteSe o NAS deve emitir um endereço IP para o chamador, certifique-se de que esse endereço esteja disponível. O endereço IP a ser entregue ao chamador pode ser obtido por meio de um dos seguintes métodos:Configure localmente na interface. Verifique a configuração da interface para o comando **peer default ip address a.b.c.d**. Na prática, esse método deve ser usado somente em interfaces que aceitam conexões de um único chamador, como em uma interface assíncrona (*não* em grupo assíncrono).Conjunto de endereços configurado localmente no NAS. A interface deve ter o comando **peer default ip address pool [*pool-name*]**. Além disso, o pool deve ser definido no nível do sistema com o comando **ip local pool [*pool-name*] [*first-address*] [*last-address*]**. O intervalo de endereços definido no pool deve ser grande o suficiente para acomodar tantos chamadores conectados simultaneamente quanto o NAS é capaz.Servidor DHCP. A interface NAS deve ser configurada com o comando **peer default ip address dhcp**. Além disso, o NAS deve ser configurado para apontar para um servidor DHCP com o comando de configuração global **ip dhcp-server [*address*]**.AAA. Se estiver usando TACACS+ ou RADIUS para autorização, o servidor AAA pode ser configurado para entregar um endereço IP específico a um determinado chamador toda vez que o chamador se conectar. Consulte o Capítulo 16 para obter mais informações.
4. Verificar a configuração do endereço do servidorPara retornar os endereços configurados de servidores de nomes de domínio ou servidores Windows NT em resposta a solicitações BOOTP, certifique-se de que os comandos global **async-bootp dns-server [*address*]** e **async-bootp nbns-server [*address*]** estejam configurados.**Observação:** embora o comando **async-bootp subnet-mask [*mask*]** possa ser configurado no NAS, a máscara de sub-rede *não* será negociada entre o NAS e um PC cliente de discagem PPP. Devido à natureza das conexões

ponto-a-ponto, o cliente usa automaticamente o endereço IP do NAS (aprendido durante a negociação de IPCP) como o gateway padrão. A máscara de sub-rede não é necessária nesse ambiente ponto-a-ponto. O PC sabe que se o endereço de destino não corresponder ao endereço local, o pacote deve ser encaminhado para o gateway padrão (NAS) que sempre é alcançado através do link PPP.

Antes de ligar para a equipe do TAC da Cisco Systems

Antes de ligar para o Cisco Systems Technical Assistance Center (TAC), verifique se você leu este capítulo e concluiu as ações sugeridas para o problema do seu sistema.

Além disso, faça o seguinte e documente os resultados para que possamos auxiliá-lo melhor:

Para todos os problemas, colete a saída de **show running-config** e **show version**. Verifique se o comando **service timestamps debug datetime msec** está na configuração.

Para problemas de DDR, colete o seguinte:

- **show dialer map**
- **debug dialer**
- **negociação de debug ppp**
- **debug ppp authentication**

Se a ISDN estiver envolvida, colete:

- **show isdn status**
- **debug isdn q931**
- **debug isdn events**

Se houver modems envolvidos, colete:

- **mostrar linhas**
- **show line [x]**
- **show modem** (se modems integrados estiverem envolvidos)
- **show modem version** (se modems integrados estiverem envolvidos)
- **debug modem**
- **debug modem** csm (se modems integrados estiverem envolvidos)
- **debug chat** (se for um cenário DDR)

Se T1s ou PRIs estiverem envolvidos, colete:

- **show controller t1**

Informações Relacionadas

- Página de Troubleshooting de T1/E1
- Guia de soluções de discagem do Cisco IOS
- Monitorar e manter a interface T1/E1
- Troubleshooting de Negociação PPP
- Troubleshooting de Modems

- Comandos de depuração de modem
- Troubleshooting de ISDN
- Troubleshooting de T1 PRI
- Suporte Técnico e Documentação - Cisco Systems