DFÜ-Technologie: Fehlerbehebungsverfahren

Inhalt

Einführung

Dialup ist einfach die Anwendung des öffentlichen Telefonnetzes (PSTN), das Daten für den Endbenutzer überträgt. Dazu gehört ein Gerät am Kundenstandort (Customer Premises Equipment, CPE), das dem Telefon-Switch eine Telefonnummer sendet, an die eine Verbindung geleitet werden soll. Die Router Cisco 3600, AS5200, AS5300 und AS5800 sind Beispiele für Router, die zusammen mit den Banken für digitale Modems eine PRI ausführen können. Das AS2511 dagegen ist ein Beispiel für einen Router, der mit externen Modems kommuniziert.

Voraussetzungen

Anforderungen

Die Leser dieses Dokuments sollten über folgende Punkte Bescheid wissen:

Der Carrier-Markt ist stark gewachsen, und der Markt verlangt jetzt höhere Modemdichten. Die

Antwort auf diese Notwendigkeit ist eine stärkere Zusammenarbeit mit der Telefonanlage und die Entwicklung des digitalen Modems. Dies ist ein Modem, das direkten digitalen Zugriff auf das PSTN ermöglicht. Infolgedessen wurden schnellere CPE-Modems entwickelt, die das klare Signal nutzen, das digitale Modems genießen. Die Tatsache, dass die digitalen Modems, die über PRI oder BRI mit dem PSTN verbunden sind, Daten über 53.000 unter Verwendung des V.90-Kommunikationsstandards übertragen können, bestätigt den Erfolg der Idee.

Die ersten Zugriffsserver waren Cisco2509 und Cisco2511. Das AS2509 könnte mithilfe externer Modems 8 eingehende Verbindungen unterstützen, das AS2511 könnte 16 unterstützen. Das AS5200 wurde mit zwei PRIs eingeführt und konnte 48 Benutzer mit digitalen Modems unterstützen. Es war ein bedeutender Sprung nach vorn in der Technologie. Die Modemdichten wurden mit Unterstützung von 4 und 8 PRIs beim AS5300 stetig erhöht. Schließlich wurde das AS5800 eingeführt, um die Anforderungen von Installationen der Carrier-Klasse zu erfüllen, die Dutzende von eingehenden T1- und Hunderten von Benutzerverbindungen handhaben müssen.

Einige veraltete Technologien lassen sich in einer historischen Diskussion über Dialer-Technologie erwähnen. 56Kflex ist ein älterer (vor V.90) 56k Modemstandard, der von Rockwell vorgeschlagen wurde. Cisco unterstützt Version 1.1 des 56Kflex-Standards auf seinen internen Modems, empfiehlt jedoch, die CPE-Modems so bald wie möglich auf V.90 zu migrieren. Eine weitere veraltete Technologie ist das AS5100. Das AS5100 war ein Joint Venture zwischen Cisco und einem Modemhersteller. Das AS5100 wurde als Möglichkeit entwickelt, die Modemdichte durch Verwendung von Quad-Modemkarten zu erhöhen. Es umfasste eine Gruppe von AS2511-Karten, die als Karten erstellt wurden und in eine Rückwandplatine integriert wurden, die von Quad-Modemkarten gemeinsam genutzt wurde, sowie eine duale T1-Karte.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Fehlerbehebung bei eingehenden Anrufen

Die Fehlerbehebung für einen eingehenden Anruf beginnt am unteren Ende und funktioniert nach oben. Der allgemeine Argumentationsfluss berücksichtigt Folgendes:

1. Sehen wir den Anruf kommen? (Eine *Ja*-Antwort auf die nächste Frage.)
2. Beendet der Empfänger den Anruf?
3. Wird der Anruf beendet?
4. Werden Daten über die Verbindung übertragen?
5. Ist die Sitzung eingerichtet? (PPP oder Terminal)

Bei Modemverbindungen sieht ein Datenanruf genauso aus wie eine Terminal-Sitzung, die

eingeht, bis das Ende erreicht ist, an dem der Datenanruf zur Aushandlung von PPP weitergeleitet wird.

Stellen Sie bei eingehenden Anrufen mit digitalen Modems zunächst sicher, dass der zugrunde liegende ISDN oder CAS den Anruf erhält. Bei Verwendung eines externen Modems können die ISDN- und CAS-Gruppenabschnitte übersprungen werden.

Fehlerbehebung bei eingehenden ISDN-Anrufen

Verwenden Sie den Befehl **debug isdn q931**. Hier ein Beispiel für eine erfolgreiche Verbindung:

```
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
```

Die Setup-Meldung weist darauf hin, dass eine Verbindung vom Remote-Ende initiiert wird. Die Anrufreferenznummern werden als Paar beibehalten. In diesem Fall ist die Anrufreferenznummer für die eingehende Seite der Verbindung 0x06 und die Anrufreferenznummer für die ausgehende Seite der Verbindung 0x86. Die Träger-Funktion (oft auch als "Bartcap" bezeichnet) teilt dem Router mit, welche Art von Anruf eingeht. In diesem Fall ist die Verbindung vom Typ 0x8890. Dieser Wert gibt "ISDN-Geschwindigkeit 64 Kbit/s" an. Hätte der Bearercap 0x8090A2 gezählt, hätte er "Speech/Voice Call u-law" (Sprachwahl/Telefongespräch-u-law) angegeben.

Wenn keine Setup-Meldung angezeigt wird, sollten Sie die richtige Nummer überprüfen, indem Sie sie manuell anrufen, wenn sie über eine Sprachverbindung bereitgestellt wird. Sie sollten auch den Status der ISDN-Schnittstelle überprüfen (siehe Befehl **show isdn status** für BRI-Fehlerbehebung). Wenn alle Anrufe ausgecheckt werden, stellen Sie sicher, dass der Anrufer den richtigen Anruf durchführt. Wenden Sie sich hierzu an die Telefongesellschaft. Der Anrufer kann den Anruf verfolgen, um zu sehen, wohin er gesendet wird. Wenn es sich bei der Verbindung um eine Fernverbindung handelt, verwenden Sie den Code 1010 für Ferngespräche.

Wenn es sich bei dem eingehenden Anruf um einen asynchronen Modemanruf handelt, stellen Sie sicher, dass die Leitung für Sprachanrufe bereitgestellt ist.

Hinweis: BRI-async-Modemanrufe sind eine Funktion von 3600-Routern mit 12.0(3)T oder höher. Für dieses Modul ist eine kürzlich erfolgte Hardware-Überarbeitung des BRI-Schnittstellennetzwerkmoduls erforderlich. WIC-Module unterstützen keine asynchronen Modemanrufe.

Wenn der Anruf einging, aber nicht abgeschlossen wurde, suchen Sie nach einem Ursachencode (siehe Tabelle 17-10). Ein erfolgreicher Abschluss wird durch connect-ack angezeigt.

Wenn es sich um einen asynchronen Modemanruf handelt, fahren Sie mit dem Abschnitt zur Fehlerbehebung bei eingehenden Modemanrufen fort.

An diesem Punkt ist der ISDN-Anruf verbunden, es wurden jedoch keine Daten über die Verbindung angezeigt. Verwenden Sie den Befehl **debug ppp negotiation**, um festzustellen, ob PPP-Datenverkehr über die Leitung übertragen wird. Wenn kein Datenverkehr angezeigt wird, kann eine Geschwindigkeitsungleichheit vorliegen. Um festzustellen, ob dies der Fall ist,

verwenden Sie den Befehl **show running-config des privilegierten Exec**, um die Router-Konfiguration anzuzeigen. Überprüfen Sie die Befehlseinträge für die **Wählerzuordnung** für die Schnittstellenkonfiguration im lokalen und Remote-Router. Diese Einträge sollten ähnlich wie folgt aussehen:

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

Für Dialer-Profile muss eine Kartenklasse definiert werden, um die Geschwindigkeit festzulegen. Beachten Sie, dass ISDN-Schnittstellen standardmäßig die 64-K-Kommunikationsgeschwindigkeit für jeden Kanal verwenden.

Detaillierte Informationen zum Konfigurieren von Wählplänen und Profilen finden Sie im Konfigurationshandbuch für *Cisco IOS-Wählösungen*, der *Befehlsreferenz für Wählösungen* und dem *Leitfaden zur Schnellkonfiguration von Wählösungen*.

Wenn Sie gültige PPP-Pakete erhalten, funktioniert die Verbindung. Fahren Sie zu diesem Zeitpunkt mit dem Abschnitt zur Fehlerbehebung für PPP fort.

Fehlerbehebung bei eingehenden CAS-Anrufen

Zur Fehlerbehebung für die CAS-Gruppe, die die Verbindung zu den Modems bereitstellt, verwenden Sie die Befehle **Debug-Modem**, **Debug-Modem-CSM** und **Debug-Klasse**.

Hinweis: Der Befehl **debug cas** wurde zuerst in 12.0(7)T für AS5200 und AS5300 angezeigt. Ältere Versionen von IOS verwenden den Konfigurationsbefehlsdienst auf Systemebene intern zusammen mit dem Befehl exec **modem-mgmt debug rbs**. Für das Debuggen dieser Informationen auf einem AS5800 muss eine Verbindung zur Trunk Card selbst hergestellt werden.

Stellen Sie zunächst fest, ob der Telefonfirmenschalter den eingehenden Anruf abgenommen hat. Ist dies nicht der Fall, überprüfen Sie die angerufene Nummer. Schließen Sie dazu ein Telefon an die Telefonleitung der Anruferseite an, und rufen Sie die Nummer an. Wenn der Anruf korrekt eingeht, liegt das Problem beim ursprünglichen CPE. Wenn der Anruf immer noch nicht auf dem CAS angezeigt wird, überprüfen Sie die T1-Schnittstelle (Kapitel 15).Verwenden Sie in dieser Instanz den Befehl **debug Serial interfaces**.

Das folgende Beispiel zeigt eine gute Verbindung mit dem **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
```

In diesem Beispiel wurde der Anruf an ein Modem weitergeleitet. Wenn Ihr Anruf an ein Modem weitergeleitet wurde, fahren Sie unten mit dem Abschnitt zur Fehlerbehebung bei eingehenden Modemanrufen fort.

Fehlerbehebung bei eingehenden Modemanrufen

Verwenden Sie bei der Fehlerbehebung von eingehenden Modemanrufen die folgenden Debugging-Befehle:

- **Debug-Modem**
- **debug modem csm** (für integrierte digitale Modems)

Verwenden Sie die folgenden Debugbefehle zusammen, um anzugeben, dass der neue Anruf eingeht:

- **debug isdn q931**
- **Debug-Cache**

Wenn der Anruf das Modem erreicht, muss das Modem den Anruf annehmen.

Tipps zum Debuggen von externen Modems

Um das Debugging auf einem externen Modem, das an eine TTY-Leitung angeschlossen ist, zu erleichtern, erhöhen Sie die Lautstärke des Lautsprechers. Dies trägt dazu bei, einige Probleme deutlicher zu machen.

Klingelt das Modem, von dem das Modem stammt, bei einem Anruf? Falls nicht, überprüfen Sie die Nummer, und versuchen Sie einen manuellen Anruf von der Außenstelle aus. Versuchen Sie, auch am Empfangsende ein normales Telefon zu verwenden. Ersetzen Sie Kabel und Hardware nach Bedarf.

Anrufübernahme über Async-Modem

Wenn ein externes Modem nicht antwortet, überprüfen Sie die Verkabelung zwischen dem Modem und dem Zugangs-Server oder -Router. Bestätigen Sie, dass das Modem über ein gerolltes RJ-45-Kabel und einen MMOD DB-25-Adapter mit dem TTY- oder AUX-Port am Router verbunden ist. Cisco empfiehlt und unterstützt diese Kabelkonfiguration für RJ-45-Ports. Beachten Sie, dass diese Anschlüsse in der Regel gekennzeichnet sind: *Modem*.

RJ-45-Kabel sind in einigen Ausführungen erhältlich: gerades, gerolltes und Crossover-Kabel. Sie können den Kabeltyp ermitteln, indem Sie die beiden Enden eines RJ-45-Kabels nebeneinander halten. Sie sehen acht farbige Streifen, oder Pins, an jedem Ende.

- Wenn die Reihenfolge der farbigen Pins an beiden Enden identisch ist, ist das Kabel gerade.
- Wenn die Reihenfolge der Farben an beiden Enden umgekehrt ist, wird das Kabel gerollt.
- Das Kabel ist ein Crossover-Kabel, wenn Farben Folgendes anzeigen:

Crossover-Kabel RJ45 zu RJ45:

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

Um sicherzustellen, dass die Signalisierung in Ordnung ist, verwenden Sie den Befehl **show line** (**Befehlszeile anzeigen**) aus Kapitel 16.

Abgesehen von den Kabelproblemen muss ein externes Modem initialisiert werden, um automatisch antworten zu können. Überprüfen Sie das Remote-Modem, ob es auf Auto-Answer

(Automatische Anrufannahme) eingestellt ist. In der Regel leuchtet eine AA-Anzeigeleuchte, wenn die automatische Antwort festgelegt ist. Stellen Sie das Remote-Modem auf Auto-Answer (Automatische Anrufannahme) ein, wenn es noch nicht festgelegt ist. Weitere Informationen zum Überprüfen und Ändern der Modemeinstellungen finden Sie in der Modemdokumentation. Verwenden Sie ein umgekehrtes Telnet, um das Modem zu initialisieren (siehe Kapitel 16).

Digitale (integrierte) Modem-Anrufübernahme

Bei einem externen Modem ist klar, ob der Anruf entgegengenommen wird, bei internen Modems ist jedoch ein manueller Anruf an die Empfangsnummer erforderlich. Achten Sie auf den Freizeichenton (ABT). Wenn Sie keinen ABT hören, überprüfen Sie die Konfiguration für die folgenden beiden Punkte:

1. Stellen Sie sicher, dass der Befehl **isdn incoming-voice modem** unter allen ISDN-Schnittstellen vorhanden ist, die eingehende Modemverbindungen behandeln.
2. Stellen Sie unter der Leitungskonfiguration für den TTY des Modems sicher, dass das **Modem** vorhanden ist.

Es ist auch möglich, dass das Call Switching Module (CSM) kein internes Modem für die Verarbeitung des eingehenden Anrufs zugewiesen hat. Dieses Problem kann durch die Konfiguration von Modem- oder Ressourcenpools für zu wenige eingehende Verbindungen verursacht werden. Dies kann auch bedeuten, dass der Access-Server einfach außerhalb des Modems ist. Überprüfen Sie die Verfügbarkeit von Modems, und passen Sie die Einstellungen für den Modempool oder Ressourcenpool-Manager entsprechend an. Wenn ein Modem zugewiesen wurde und die Konfiguration ein **Modem** anzeigt, sammeln Sie Debug, und wenden Sie sich an Cisco, um Unterstützung zu erhalten.

Modemschulung

Wenn das Modem den DSR anhebt, war die Schulung erfolgreich. Ausübungsfehler können auf ein Schaltungsproblem oder eine Modeminkompatibilität hinweisen.

Um ein einzelnes Modemproblem zu beheben, gehen Sie zur AT-Eingabeaufforderung am ursprünglichen Modem, während es an die POTS-Zeile von Interesse angeschlossen ist. Wenn Sie ein digitales Modem in einem Cisco Access-Server anrufen, sollten Sie darauf vorbereitet sein, eine WAV-Datei der Trainingsmusik oder eine DIL (Digital Impact Learning Sequence) aufzuzeichnen. Die DIL ist die Musikpartie (PCM-Sequenz), die das analoge V.90-Modem, von dem es ausgeht, an das digitale Empfangsmodem sendet, um es wiederzugeben. Mit dieser Sequenz kann das analoge Modem eine digitale Beeinträchtigung im Schaltkreis erkennen. z. B. mehrere D/A-Konvertierungen, ein Gesetz/u-law, raubte Bits oder digitale Pads. Wenn Sie die DIL nicht hören, verhandeln die Modems nicht V.90 in V.8/V.8bis (d. h. ein Modem-Kompatibilitätsproblem). Wenn Sie die DIL und eine Umschulung in V.34 hören, entschied das analoge Modem (auf der Grundlage der DIL-Wiedergabe), dass V.90 nicht möglich ist.

Gibt es in der Musik ein Geräusch? Wenn ja, dann säubern Sie den Stromkreis.

Verzichtet der Kunde schnell, ohne V.34-Schulungen durchzuführen? Zum Beispiel weiß er vielleicht nicht, was zu tun ist, wenn er V.8bis hört. In diesem Fall sollten Sie versuchen, V.8bis (also K56Flex) auf dem Server zu deaktivieren (falls zulässig). Sie sollten eine neue Client-Firmware erhalten oder das Client-Modem austauschen. Alternativ dazu kann am Ende des Wählvorgangs fünf Kommas eingefügt werden. Dadurch wird das Abhören des anrufenden Modems verzögert, und der V.8bis-Ton des empfangenden Servers wird außer Kraft gesetzt, ohne

dass das Client-Modem darunter leidet. Fünf Kommas in der Wählzeichenfolge sind eine allgemeine Richtlinie und müssen möglicherweise angepasst werden, um lokale Bedingungen zu berücksichtigen.

Sitzungsaufbau

An diesem Punkt der Sequenz werden die Modems angeschlossen und geschult. Jetzt ist es an der Zeit herauszufinden, ob ein Datenverkehr richtig überquert wird.

Wenn die Leitung, die den Anruf empfängt, mit **autoselect ppp** konfiguriert ist und die async-Schnittstelle mit dem **asynchronen Modus interaktiv** konfiguriert ist, verwenden Sie den Befehl **debug modem**, um den Autoselect-Prozess zu überprüfen. Wenn der Datenverkehr über die async-Verbindung eingeht, prüft der Zugriffsserver den Datenverkehr, um festzustellen, ob der Datenverkehr zeichenbasiert oder paketbasiert ist. Je nach Bestimmung startet der Zugriffsserver dann entweder eine PPP-Sitzung oder nicht weiter als eine exec-Sitzung in der Leitung.

Eine normale automatische Auswahlsequenz mit eingehenden PPP-LCP-Paketen:

```
*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.
```

Wenn es sich bei dem Anruf um eine PPP-Sitzung handelt und der **async-Modus** auf der asynchronen Schnittstelle konfiguriert ist, verwenden Sie den Befehl **debug ppp negotiation**, um festzustellen, ob Konfigurationserforderungspakete vom Remote-Ende kommen. Die Debug-Meldungen werden als CONFREQ angezeigt. Wenn Sie sowohl eingehende als auch ausgehende PPP-Pakete beobachten, fahren Sie mit "Troubleshooting PPP" (PPP-Fehlerbehebung) fort. Andernfalls stellen Sie eine Verbindung vom ursprünglichen Ende des Anrufs mit einer Sitzung im Zeichenmodus (oder einer Sitzung ohne PPP) her.

Hinweis: Wenn das Empfangsende unter der asynchronen Schnittstelle ein **asynchrones Modem** anzeigt, wird nur ein zufälliger ASCII-Garbage-Modus angezeigt. Um eine Terminalsitzung zuzulassen und weiterhin über eine PPP-Funktion zu verfügen, verwenden Sie den **asynchronen** Schnittstellenkonfigurationsbefehl **async mode interaktiv**. Verwenden Sie unter der Konfiguration der zugeordneten Leitung den Befehl **autoselect ppp**.

Modem kann keine Daten senden oder empfangen

Wenn die Modems eine Verbindung mit einer Terminalsitzung herstellen und keine Daten angezeigt werden, überprüfen Sie die folgenden möglichen Ursachen und vorgeschlagenen Vorgehensweisen:

- **Modemdrehzahleinstellung ist nicht gesperrt**Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte die aktuell konfigurierten Tx- und Rx-Geschwindigkeiten angeben.Eine Erklärung der Ausgabe des Befehls **show line** finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Wenn die Leitung nicht mit der richtigen Geschwindigkeit konfiguriert ist, können Sie mit dem Befehl **Speed** Line Configuration (Leitungsgeschwindigkeit) die Leitungsgeschwindigkeit auf dem Zugriffsserver oder der Router-Leitung festlegen. Stellen Sie den Wert auf die höchste Geschwindigkeit ein, die zwischen dem Modem und dem Port des Zugangs-Servers oder -Routers gemeinsam ist. Um die Terminalbaudrate festzulegen, verwenden Sie den Befehl **Speed** Line Configuration. Dieser Befehl legt sowohl die Übertragungs- (Terminal-) als auch die Empfangsgeschwindigkeit (von Terminal) fest.Syntax:**Geschwindigkeit** *Bit*Syntaxbeschreibung:*bps* - Baudrate in Bit pro Sekunde (bps). Der Standardwert ist 9600 bit/s.Im folgenden Beispiel werden die Zeilen 1 und 2 für einen Cisco 2509-Zugriffsserver auf 115200 bps festgelegt:
  ```
  line 1 2
  speed 115200
  ```
  Hinweis: Wenn Sie aus irgendeinem Grund keine Flusskontrolle verwenden können, begrenzen Sie die Leitungsgeschwindigkeit auf 9600 bps. Schnellere Geschwindigkeiten führen wahrscheinlich zu Datenverlusten.Verwenden Sie den Befehl **show line** exec erneut, und überprüfen Sie, ob die Leitungsgeschwindigkeit auf den gewünschten Wert eingestellt ist.Wenn Sie sicher sind, dass die Zugriffsserver- oder Router-Leitung für die gewünschte Geschwindigkeit konfiguriert ist, starten Sie über diese Leitung eine umgekehrte Telnet-Sitzung mit dem Modem. Weitere Informationen finden Sie im Abschnitt "Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem" in Kapitel 16.Verwenden Sie eine Modem-Befehlszeichenfolge, die den Befehl "lock DTE speed" (DTE-Geschwindigkeit sperren) für Ihr Modem enthält. Genaue Informationen zur Befehlssyntax für die Konfiguration finden Sie in der Modemdokumentation.**Hinweis:** Der Befehl lock DTE speed (DTE-Geschwindigkeit sperren), der auch als *Port-Ratenanpassung* oder *Puffermodus* bezeichnet werden kann, hängt häufig davon ab, wie das Modem die Fehlerkorrektur handhabt. Dieser Befehl ist von Modem zu Modem sehr unterschiedlich.Durch das Sperren der Modemgeschwindigkeit wird sichergestellt, dass das Modem immer mit dem Cisco Access Server oder Router mit der auf dem Cisco AUX-Port konfigurierten Geschwindigkeit kommuniziert. Wenn dieser Befehl nicht verwendet wird, kehrt das Modem zur Geschwindigkeit der Datenverbindung (Telefonleitung) zurück, anstatt mit der auf dem Zugriffsserver konfigurierten Geschwindigkeit zu kommunizieren.
- **Hardware-Flusssteuerung nicht konfiguriert auf lokalem oder Remote-Modem oder Router**Verwenden Sie den Befehl **show line *aux-line-number* exec, und suchen Sie im Feld Capabilities (Funktionen) Folgendes:**
  ```
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
  ```
  Weitere Informationen finden Sie unter Interpretieren der Zeilenausgabe in Kapitel 16.Wenn in diesem Feld die Hardware-Flusssteuerung nicht erwähnt wird, ist die Hardware-Flusssteuerung auf der Leitung nicht aktiviert. Es wird empfohlen, den Hardware-Datenfluss für Verbindungen zwischen Servern zu Modems zu steuern.Eine Erklärung zur Ausgabe des Befehls **show line** finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Konfigurieren Sie die Hardware-Flusssteuerung auf der Leitung mithilfe des Hardware-Leitungskonfigurationsbefehls für die Flusssteuerung.Um die Methode der Datenflusssteuerung zwischen dem Terminal bzw. einem anderen seriellen Gerät und dem Router festzulegen, verwenden Sie den Befehl **Flusssteuerungs-**Leitungskonfiguration.

Verwenden Sie das Formular no dieses Befehls, um die Flusskontrolle zu deaktivieren.Syntax:**Flusskontrolle {keine | software [lock] [in] | out] | Hardware [in | out]}**Syntaxbeschreibung:**none**: Deaktiviert die Flusskontrolle.**software** - Legt die Software-Flusssteuerung fest. Ein optionales Schlüsselwort gibt die Richtung an: **in** bewirkt, dass die Cisco IOS-Software die Flusskontrolle vom angeschlossenen Gerät abhört und **auslöst**, dass die Software Informationen zur Flusskontrolle an das angeschlossene Gerät sendet. Wenn Sie keine Richtung angeben, werden beide angenommen.**lock** - Verhindert, dass die Flusskontrolle vom Remote-Host aus deaktiviert wird, wenn das verbundene Gerät eine Software-Flusskontrolle benötigt. Diese Option gilt für Verbindungen, die Telnet- oder rlogin-Protokolle verwenden.**Hardware** - Legt die Hardware-Flusssteuerung fest. Ein optionales Schlüsselwort gibt die Richtung an: **in** bewirkt, dass die Software die Flusskontrolle vom angeschlossenen Gerät abhört, und **dass** die Software Informationen zur Flusskontrolle an das angeschlossene Gerät sendet. Wenn Sie keine Richtung angeben, werden beide angenommen. Weitere Informationen zur Hardware-Flusskontrolle finden Sie im mit Ihrem Router gelieferten Hardware-Handbuch.Beispiel:Im folgenden Beispiel wird die Hardware-Flusssteuerung auf Zeile 7 festgelegt:

```
line 7
flowcontrol hardware
```

Hinweis: Wenn Sie aus irgendeinem Grund keine Flusskontrolle verwenden können, begrenzen Sie die Leitungsgeschwindigkeit auf 9600 bps. Schnellere Geschwindigkeiten führen wahrscheinlich zu Datenverlusten.Nachdem Sie die Hardware-Flusssteuerung auf dem Zugriffsserver oder der Router-Leitung aktiviert haben, starten Sie über diese Leitung eine umgekehrte Telnet-Sitzung mit dem Modem. Weitere Informationen finden Sie im Abschnitt "Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem" in Kapitel 16.Verwenden Sie eine Modem-Befehlszeichenfolge, die den Befehl **RTS/CTS Flow** für Ihr Modem enthält. Dieser Befehl stellt sicher, dass das Modem dieselbe Methode der Flusskontrolle (d. h. Hardware-Flusskontrolle) verwendet wie der Cisco Access Server oder Router. Genaue Informationen zur Befehlssyntax für die Konfiguration finden Sie in der Modemdokumentation.

- **Falsch konfigurierte Befehle zur Dialerzuordnung**Verwenden Sie den Befehl **show running-config des privilegierten** Exec, um die Router-Konfiguration anzuzeigen. Überprüfen Sie die Befehlseinträge der **Wählerzuordnung**, um festzustellen, ob das **Broadcast-**Schlüsselwort angegeben ist.Wenn das Schlüsselwort fehlt, fügen Sie es zur Konfiguration hinzu.Syntax:**Dialer Map *Protocol next-hop-address* [Name *Hostname*] [Broadcast] [*Wählzeichenfolge*]**Syntaxbeschreibung:*Protocol* - Das Protokoll, das der Zuordnung unterliegt. Zu den Optionen gehören IP, IPX, Bridge und Snapshot.*next-hop-address* - Die Protokolladresse der asynchronen Schnittstelle der anderen Site.**name *hostname* - Ein erforderlicher Parameter, der in der PPP-Authentifizierung verwendet wird.** Dies ist der Name der Remote-Site, für die die Dialer-Zuordnung erstellt wird. Beim Namen wird Groß- und Kleinschreibung unterschieden und muss mit dem Hostnamen des Remote-Routers übereinstimmen.**Broadcast** - Ein optionales Schlüsselwort, das Pakete sendet (z. B. IP-RIP- oder IPX-RIP/SAP-Updates), die an das Remote-Ziel weitergeleitet werden. In statischen Beispielkonfigurationen für das Routing werden keine Routing-Updates gewünscht, und das **Broadcast-**Schlüsselwort wird weggelassen.*Wählzeichenfolge* - Die Telefonnummer des Remote-Standorts. Alle Zugangscodes (z. B. 9 für das Verlassen eines Büros, internationale Wählcodes, Ortsvorwahlen) müssen enthalten sein.Stellen Sie sicher, dass die Befehle **der Wählerzuordnung** die richtigen Next-Hop-Adressen angeben.Wenn die nächste Hop-Adresse falsch ist, ändern Sie sie mit dem Befehl **dialer map (Dialerzuordnung)**.Stellen Sie sicher, dass alle anderen Optionen in den Dialer Map Befehlen korrekt für das Protokoll angegeben sind,

das Sie verwenden.Detaillierte Informationen zum Konfigurieren von Dialerzuordnungen finden Sie im Konfigurationshandbuch für *Cisco IOS Wide-Area Networking* und *der Befehlsreferenz für Wide-Area Networking*.

- **Problem mit dem Wählmodem**Stellen Sie sicher, dass das Modem betriebsbereit und sicher mit dem richtigen Anschluss verbunden ist. Prüfen Sie, ob ein anderes Modem funktioniert, wenn es an denselben Port angeschlossen ist.

Das Debuggen einer eingehenden exec-Sitzung fällt im Allgemeinen in einige Hauptkategorien:

- Wählclient empfängt keine exec-Aufforderung
- Dialup-Sitzung sieht "Müll"
- DFÜ-Sitzung wird in einer vorhandenen Sitzung geöffnet
- Das DFÜ-Empfangsmodem trennt die Verbindung nicht richtig.

Einwahlclient erhält keine exec-Aufforderung

- **Automatische Auswahl ist für Leitung aktiviert.**Versuchen Sie, durch Drücken der Eingabetaste auf den exec-Modus zuzugreifen.
- **Leitung wird mit dem Befehl no exec konfiguriert.**Verwenden Sie den Befehl **show line** exec, um den Status der entsprechenden Zeile anzuzeigen.Überprüfen Sie im Feld "Funktionen", ob "exec unterdrückt" steht. In diesem Fall ist der Befehl **no exec** line configuration aktiviert.Konfigurieren Sie den Befehl **exec**-Leitungskonfiguration in der Zeile, um die Initiierung von Exec-Sitzungen zu ermöglichen. Dieser Befehl hat keine Argumente oder Schlüsselwörter.Im folgenden Beispiel wird die exec-Funktion in Zeile 7 aktiviert:
  ```
  line 7
  exec
  ```
- **Flusssteuerung ist nicht aktiviert.oderDie Flusssteuerung ist nur auf einem Gerät (entweder DTE oder DCE) aktiviert.oderFlusssteuerung ist falsch konfiguriert.**Verwenden Sie den Befehl **show line *aux-line-number* exec, und suchen Sie im Feld Capabilities (Funktionen) Folgendes:**
  ```
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
  ```

  Weitere Informationen finden Sie unter Interpretieren der Zeilenausgabe in Kapitel 16.Wenn in diesem Feld die Hardware-Flusssteuerung nicht erwähnt wird, ist die Hardware-Flusssteuerung auf der Leitung nicht aktiviert. Es wird empfohlen, den Hardware-Datenfluss für Verbindungen zwischen Servern zu Modems zu steuern.Eine Erklärung der Ausgabe des Befehls show line finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Konfigurieren Sie die Hardware-Flusssteuerung auf der Leitung mithilfe des Konfigurationsbefehls **für die Flusssteuerung**. Im folgenden Beispiel wird die Hardware-Flusssteuerung auf Zeile 7 festgelegt:
  ```
  line 7
  flowcontrol hardware
  ```
  Hinweis: Wenn Sie aus irgendeinem Grund keine Flusskontrolle verwenden können, begrenzen Sie die Leitungsgeschwindigkeit auf 9600 bps. Schnellere Geschwindigkeiten führen wahrscheinlich zu Datenverlusten.Nachdem Sie die Hardware-Flusssteuerung auf dem Zugriffsserver oder der Router-Leitung aktiviert haben, starten Sie über diese Leitung eine umgekehrte Telnet-Sitzung mit dem Modem. Weitere Informationen finden Sie im Abschnitt "Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem" in Kapitel 16.Verwenden Sie eine Modem-Befehlszeichenfolge, die den Befehl RTS/CTS Flow für Ihr Modem enthält. Dieser Befehl stellt sicher, dass das Modem dieselbe Methode der Flusskontrolle (d. h. Hardware-Flusskontrolle) verwendet wie der Cisco Access Server oder Router. Genaue

Informationen zur Befehlssyntax für die Konfiguration finden Sie in der Modemdokumentation.

- **Modemdrehzahleinstellung ist nicht gesperrt**Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte die aktuell konfigurierten Tx- und Rx-Geschwindigkeiten angeben.Eine Erklärung der Ausgabe des Befehls show line finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Wenn die Leitung nicht mit der richtigen Geschwindigkeit konfiguriert ist, legen Sie mit dem Befehl Speed Line Configuration (Leitungsgeschwindigkeit konfigurieren) die Leitungsgeschwindigkeit auf dem Zugriffsserver oder der Router-Leitung fest. Stellen Sie den Wert auf die höchste Geschwindigkeit ein, die zwischen dem Modem und dem Port des Zugangs-Servers oder -Routers gemeinsam ist. Verwenden Sie den Konfigurationsbefehl Speed Line (Geschwindigkeit), um die Terminalbaudrate festzulegen. Dieser Befehl legt sowohl die Übertragungs- (Terminal-) als auch die Empfangsgeschwindigkeit (von Terminal) fest.Syntax:**Geschwindigkeit** *Bit*Syntaxbeschreibung:*bps* - Baudrate in Bit pro Sekunde (bps). Der Standardwert ist 9600 bit/s.Beispiel:Im folgenden Beispiel werden die Zeilen 1 und 2 für einen Cisco 2509-Zugriffsserver auf 115200 bps festgelegt:
  ```
  line 1 2
  speed 115200
  ```
  Hinweis: Wenn Sie aus irgendeinem Grund keine Flusskontrolle verwenden können, begrenzen Sie die Leitungsgeschwindigkeit auf 9600 bps. Schnellere Geschwindigkeiten führen wahrscheinlich zu Datenverlusten.Verwenden Sie den Befehl **show line** exec erneut, und überprüfen Sie, ob die Leitungsgeschwindigkeit auf den gewünschten Wert eingestellt ist.Wenn Sie sicher sind, dass die Zugriffsserver- oder Router-Leitung für die gewünschte Geschwindigkeit konfiguriert ist, starten Sie über diese Leitung eine umgekehrte Telnet-Sitzung mit dem Modem. Weitere Informationen finden Sie im Abschnitt "Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem" in Kapitel 16.Verwenden Sie eine Modem-Befehlszeichenfolge, die den Befehl **lock** DTE speed (DTE-Geschwindigkeit sperren) für Ihr Modem enthält. Genaue Informationen zur Befehlssyntax für die Konfiguration finden Sie in der Modemdokumentation.**Hinweis:** Der Befehl **lock** DTE speed (DTE-Geschwindigkeit sperren), der auch als Port-Ratenanpassung oder -gepufferter Modus bezeichnet werden kann, hängt häufig davon ab, wie das Modem mit der Fehlerkorrektur umgeht. Dieser Befehl ist von Modem zu Modem sehr unterschiedlich.Durch das Sperren der Modemgeschwindigkeit wird sichergestellt, dass das Modem immer mit dem Cisco Access Server oder Router mit der auf dem Cisco AUX-Port konfigurierten Geschwindigkeit kommuniziert. Wenn dieser Befehl nicht verwendet wird, kehrt das Modem zur Geschwindigkeit der Datenverbindung (Telefonleitung) zurück, anstatt mit der auf dem Zugriffsserver konfigurierten Geschwindigkeit zu kommunizieren.

Dialupsitzungen sehen "Müll"

- **Modemdrehzahleinstellung ist nicht gesperrt**Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte die aktuell konfigurierten Tx- und Rx-Geschwindigkeiten angeben.Eine Erklärung der Ausgabe des Befehls **show line** finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Wenn die Leitung nicht mit der richtigen Geschwindigkeit konfiguriert ist, können Sie mit dem Befehl **Speed** Line Configuration (Leitungsgeschwindigkeit) die Leitungsgeschwindigkeit auf dem Zugriffsserver oder der Router-Leitung festlegen. Stellen Sie den Wert auf die höchste Geschwindigkeit ein, die zwischen dem Modem und dem Port des Zugangs-Servers oder -Routers gemeinsam ist.Um die Terminalbaudrate festzulegen, verwenden Sie den

Befehl **Speed** Line Configuration. Dieser Befehl legt sowohl die Übertragungs- (Terminal-) als auch die Empfangsgeschwindigkeit (von Terminal) fest.Syntax:**Geschwindigkeit** *bps*Syntaxbeschreibung:bps Baud Rate in Bit pro Sekunde (bps). Der Standardwert ist 9600 bit/s.Beispiel:Im folgenden Beispiel werden die Zeilen 1 und 2 für einen Cisco 2509-Zugriffsserver auf 115200 bps festgelegt:Zeile 1 2Geschwindigkeit 115200**Hinweis:** Wenn Sie aus irgendeinem Grund keine Flusskontrolle verwenden können, begrenzen Sie die Leitungsgeschwindigkeit auf 9600 bps. Schnellere Geschwindigkeiten führen wahrscheinlich zu Datenverlusten.Verwenden Sie den Befehl **show line** exec erneut, und überprüfen Sie, ob die Leitungsgeschwindigkeit auf den gewünschten Wert eingestellt ist.Wenn Sie sicher sind, dass die Zugriffsserver- oder Router-Leitung für die gewünschte Geschwindigkeit konfiguriert ist, starten Sie über diese Leitung eine umgekehrte Telnet-Sitzung mit dem Modem. Weitere Informationen finden Sie im Abschnitt "Einrichten einer umgekehrten Telnet-Sitzung zu einem Modem" in Kapitel 16.Verwenden Sie eine Modem-Befehlszeichenfolge, die den Befehl **lock** DTE speed (DTE-Geschwindigkeit sperren) für Ihr Modem enthält. Genaue Informationen zur Befehlssyntax für die Konfiguration finden Sie in der Modemdokumentation.**Hinweis:** Der Befehl **lock** DTE speed (DTE-Geschwindigkeit sperren), der auch als *Port-Ratenanpassung* oder *Puffer-Modus* bezeichnet werden kann, hängt häufig davon ab, wie das Modem die Fehlerkorrektur handhabt. Dieser Befehl ist von Modem zu Modem sehr unterschiedlich.Durch das Sperren der Modemgeschwindigkeit wird sichergestellt, dass das Modem immer mit dem Cisco Access Server oder Router mit der auf dem Cisco AUX-Port konfigurierten Geschwindigkeit kommuniziert. Wenn dieser Befehl nicht verwendet wird, kehrt das Modem zur Geschwindigkeit der Datenverbindung (Telefonleitung) zurück, anstatt mit der auf dem Zugriffsserver konfigurierten Geschwindigkeit zu kommunizieren.

Symptom: Eine Remote-Einwahlsitzung wird in einer bereits bestehenden Sitzung geöffnet, die von einem anderen Benutzer gestartet wurde. Anstatt eine Anmeldeaufforderung zu erhalten, sieht ein Wählbenutzer eine von einem anderen Benutzer erstellte Sitzung (möglicherweise eine UNIX-Eingabeaufforderung, eine Text-Editor-Sitzung usw.).

DFÜ-Sitzung wird in einer vorhandenen Sitzung geöffnet

- **Modem für DCD immer hoch konfiguriert**Das Modem sollte so umkonfiguriert werden, dass DCD nur auf CD hoch ist. Dies wird in der Regel mithilfe der Befehlszeichenfolge **&C1-**Modem erreicht, die genaue Syntax finden Sie jedoch in der Modemdokumentation.Möglicherweise müssen Sie die Zugriffsserver-Leitung konfigurieren, mit der das Modem mit dem Konfigurationsbefehl **no exec** line verbunden ist. Löschen Sie die Leitung mit dem Befehl **clear line privileged exec**, starten Sie eine umgekehrte Telnet-Sitzung mit dem Modem, und konfigurieren Sie das Modem neu, sodass DCD nur auf CD hoch ist.Beenden Sie die Telnet-Sitzung, indem Sie **disconnect** eingeben und die Zugriffsserver-Leitung mit dem **exec-**Leitungskonfigurationsbefehl neu konfigurieren.
- **Die Modemsteuerung ist auf dem Zugriffsserver oder Router nicht aktiviert.**Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte in der Spalte Modem **Inout** oder **RIisCD** angezeigt werden. Dies zeigt an, dass die Modemsteuerung auf der Leitung des Zugangs-Servers oder -Routers aktiviert ist.Eine Erläuterung der **Ausgabe** der **Befehlszeile** finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Konfigurieren Sie die Leitung für die Modemsteuerung mithilfe des Konfigurationsbefehls **Modem** für die **Inout-**Leitung. Die Modemsteuerung ist jetzt auf dem Zugriffsserver aktiviert.**Hinweis:** Stellen Sie sicher, dass Sie den Befehl **Modem** Inout (**Modemeingang**) anstelle des Befehls **Modem Dialin** verwenden, während die Verbindung des

Modems in Frage steht. Mit diesem Befehl kann die Leitung nur eingehende Anrufe annehmen. Ausgehende Anrufe werden abgelehnt, sodass keine Telnet-Sitzung mit dem Modem aufgebaut werden kann. Wenn Sie den Befehl **Modem Dialin** aktivieren möchten, müssen Sie dies erst tun, wenn Sie sicher sind, dass das Modem richtig funktioniert.

- **Falsche Verkabelung**Überprüfen Sie die Verkabelung zwischen dem Modem und dem Zugriffsserver oder -Router. Bestätigen Sie, dass das Modem über ein gerolltes RJ-45-Kabel und einen MMOD DB-25-Adapter mit dem AUX-Port des Zugangs-Servers oder -Routers verbunden ist. Diese Verkabelungskonfiguration wird von Cisco für RJ-45-Ports empfohlen und unterstützt. Diese Steckverbinder sind in der Regel gekennzeichnet: Modem.Es gibt zwei Arten von RJ-45-Kabeln: gerollt und gerollt. Wenn Sie die beiden Enden eines RJ-45-Kabels nebeneinander halten, sehen Sie an beiden Enden acht farbige Streifen oder Pins. Wenn die Reihenfolge der farbigen Pins an beiden Enden gleich ist, dann ist das Kabel gerade. Wenn die Reihenfolge der Farben an beiden Enden umgekehrt ist, wird das Kabel gerollt.Das Walzkabel (CAB-500RJ) ist standardmäßig mit dem Cisco 2500/CS500 verbunden.Überprüfen Sie mit dem Befehl **show line exec**, ob die Kabel korrekt sind. In diesem Kapitel 15 finden Sie eine Erläuterung der Befehlsausgabe der **show line** im Abschnitt "Verwenden von Debug-Befehlen".

Das DFÜ-Empfangsmodem trennt die Verbindung nicht richtig.

- **Das Modem erkennt DTR nicht.**Geben Sie die Befehlszeichenfolge des **Hangup DTR-Modems ein**. Dieser Befehl weist das Modem an, den Netzbetreiber zu verwerfen, wenn das DTR-Signal nicht mehr empfangen wird.Bei einem Hayes-kompatiblen Modem wird die **&D3-**Zeichenfolge in der Regel zum Konfigurieren von **Hangup DTR** auf dem Modem verwendet. Die genaue Syntax für diesen Befehl finden Sie in der Dokumentation für das Modem.
- **Die Modemsteuerung ist auf dem Router oder Zugriffsserver nicht aktiviert.**Verwenden Sie den Befehl **show line** exec auf dem Zugriffsserver oder Router. Die Ausgabe für den AUX-Port sollte in der Spalte Modem **Inout** oder **RIisCD** angezeigt werden. Dies zeigt an, dass die Modemsteuerung auf der Leitung des Zugangs-Servers oder -Routers aktiviert ist.Eine Erklärung der Ausgabe der Befehlszeile finden Sie im Abschnitt "Verwenden von Debug-Befehlen" in Kapitel 15.Konfigurieren Sie die Leitung für die Modemsteuerung mithilfe des Konfigurationsbefehls für die Inline-Leitung des Modems. Die Modemsteuerung ist jetzt auf dem Zugriffsserver aktiviert.**Hinweis:** Stellen Sie sicher, dass Sie den Befehl **Modem** Inout (**Modemeingang**) anstelle des Befehls **Modem Dialin** verwenden, während die Verbindung des Modems in Frage steht. Mit diesem Befehl kann die Leitung nur eingehende Anrufe annehmen. Ausgehende Anrufe werden abgelehnt, sodass keine Telnet-Sitzung mit dem Modem aufgebaut werden kann. Wenn Sie den Befehl **Modem Dialin** aktivieren möchten, müssen Sie dies erst tun, wenn Sie sicher sind, dass das Modem richtig funktioniert.

Fehlerbehebung bei ausgehenden Anrufen

Während der Fehlerbehebungsansatz für eingehende Anrufe unten beginnt, beginnt die Fehlerbehebung für ausgehende Verbindungen oben. Der allgemeine Argumentationsfluss berücksichtigt Folgendes:

1. Lässt sich ein Anruf über das DFÜ-Routing (Dial on Demand Routing, DDR) initiieren? (Antwort Ja, Fortschritte bei der nächsten Frage)

2. Wenn es sich um ein asynchrones Modem handelt, stellen die Chat-Skripte die erwarteten Befehle aus?
3. Macht der Anruf es zum PSTN?
4. Wird der Anruf vom Remote-Ende angenommen?
5. Wird der Anruf beendet?
6. Werden Daten über den Link übertragen?
7. Ist die Sitzung eingerichtet? (PPP oder Terminal)

Überprüfen der Dialer-Funktion

Um zu sehen, ob der Dialer versucht, einen Anruf an sein Remote-Ziel zu tätigen, verwenden Sie den Befehl **debug dialer events**. Detailliertere Informationen können aus dem **Debug-Dialer-Paket** gewonnen werden, aber der **Debug-Dialer-Paket-**Befehl ist ressourcenintensiv und sollte nicht auf einem ausgelasteten System mit mehreren Dialer-Schnittstellen verwendet werden.

In der folgenden Zeile der Debug Dialer-Ereignisausgabe für ein IP-Paket sind der Name der DDR-Schnittstelle und die Quell- und Zieladresse des Pakets aufgeführt:

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

Wenn der Datenverkehr keinen Wählversuch auslöst, ist der häufigste Grund eine fehlerhafte Konfiguration (entweder eine der interessanten Verkehrsdefinitionen, der Zustand der Dialer-Schnittstelle oder die Routing-Klasse).

Der Datenverkehr initiiert keinen Wählversuch.

- **Fehlende oder falsche Definitionen für "interessanten Datenverkehr"**Stellen Sie mithilfe des Befehls **show running-config** sicher, dass die Schnittstelle mit einer **Dialer-Gruppe** konfiguriert ist und dass eine globale **Dialer-Liste** mit einer übereinstimmenden Nummer konfiguriert ist.Stellen Sie sicher, dass der Befehl **dialer-list** so konfiguriert ist, dass entweder ein ganzes Protokoll zugelassen oder Datenverkehr zugelassen wird, der einer Zugriffsliste entspricht.Vergewissern Sie sich, dass die Zugriffsliste Pakete, die über den Link verlaufen, für interessant erklärt. Ein nützlicher Test ist, den privilegierten exec-Befehl **debug ip packet [Listennummer]** unter Verwendung der Nummer der entsprechenden Zugriffsliste zu verwenden. Versuchen Sie dann, über die Verbindung einen Ping zu senden oder Datenverkehr auf andere Weise zu senden. Wenn die interessanten Datenverkehrsfilter korrekt definiert wurden, werden die Pakete in der Debugausgabe angezeigt. Wenn dieser Test keine Debugausgabe enthält, stimmt die Zugriffsliste nicht mit den Paketen überein.
- **Schnittstellenstatus**Verwenden Sie den Befehl **show interfaces [*interface name*]**, um sicherzustellen, dass sich die Schnittstelle im Zustand "up/up (spoofing)" befindet.Schnittstelle im Standby-ModusEine andere (primäre) Schnittstelle am Router wurde so konfiguriert, dass sie die Dialer-Schnittstelle als Backup-Schnittstelle verwendet. Darüber hinaus befindet sich die primäre Schnittstelle nicht im Zustand "Down/down" (Herunterfahren/Herunterfahren), was erforderlich ist, um die Dialer-Schnittstelle aus dem Standby-Modus zu holen. Außerdem muss eine *Sicherungsverzögerung* auf der primären Schnittstelle konfiguriert werden, oder der Befehl **backup interface** wird niemals erzwungen.Um sicherzustellen, dass die Dialer-Schnittstelle von "Standby" zu "Up/Up (Spoofing)" wechselt, muss das Kabel in der Regel von der primären Schnittstelle abgezogen werden. Wenn Sie die primäre Schnittstelle einfach mithilfe des Konfigurationsbefehls **herunterfahren**, wird die primäre Schnittstelle nicht in

"down/down" gesetzt, sondern stattdessen in "administrativ aus" gesetzt, nicht in das Gleiche.Wenn die primäre Verbindung über Frame Relay erfolgt, muss die Frame-Relay-Konfiguration auf einer Point-to-Point Serial Subschnittstelle erfolgen, und die Telefongesellschaft muss das "aktive" Bit übergeben. Diese Praxis wird auch als "End-to-End LMI" bezeichnet.Die Schnittstelle ist "administrativ deaktiviert".Die Dialer-Schnittstelle wurde mit dem Befehl **shutdown** konfiguriert. Dies ist auch der Standardstatus einer beliebigen Schnittstelle, wenn ein Cisco Router zum ersten Mal gestartet wird. Verwenden Sie den Befehl interface configuration **no shutdown**, um dieses Hindernis zu entfernen.

- **Falsches Routing**Geben Sie den Befehl exec **show ip route [*a.b.c.d*]** ein, wobei *a.b.c.d* die Adresse der Dialer-Schnittstelle des Remote-Routers ist. Wenn **ip unnumbered (nicht nummerierte IP)** auf dem Remote-Router verwendet wird, verwenden Sie die Adresse der Schnittstelle, die im Befehl **ip unnumbered (unnummerierte IP-Adresse)** aufgeführt ist.Die Ausgabe sollte eine Route zur Remote-Adresse über die Dialer-Schnittstelle anzeigen. Wenn keine Route vorhanden ist, stellen Sie sicher, dass statische oder schwimmende statische Routen konfiguriert wurden, indem Sie die Ausgabe von show running-config prüfen.Wenn eine Route über eine andere Schnittstelle als die Dialer-Schnittstelle existiert, impliziert dies, dass DDR als Backup verwendet wird. Überprüfen Sie die Router-Konfiguration, um sicherzustellen, dass statische oder Floating-statische Routen konfiguriert wurden. Der sicherste Weg, das Routing zu testen, besteht in diesem Fall darin, die primäre Verbindung zu deaktivieren und den Befehl **show ip route [*a.b.c.d*]** auszuführen, um zu überprüfen, ob die richtige Route in der Routing-Tabelle installiert wurde.**Hinweis:** Wenn Sie dies während des Live-Netzwerkbetriebs versuchen, kann ein Wählereignis ausgelöst werden. Diese Art von Tests lässt sich am besten in planmäßigen Wartungszyklen durchführen.

Tätigen eines Anrufs

Wenn die Routing- und die interessanten Datenverkehrsfilter korrekt sind, sollte ein Anruf initiiert werden. Dies wird durch die Verwendung von **Debug Dialer-Ereignissen** angezeigt:

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

Wenn die Wählursache angezeigt wird, aber kein Wählversuch unternommen wird, ist der übliche Grund eine falsch konfigurierte Wählzuordnung oder ein falsch konfiguriertes Wählprofil.

Anruf nicht getätigt

Nachfolgend sind einige mögliche Probleme und empfohlene Maßnahmen aufgeführt:

- **Falsch konfigurierte Wählzuordnung**Verwenden Sie den Befehl **show running-config**, um sicherzustellen, dass die Wählschnittstelle mit mindestens einer *Dialer-Map*-Anweisung konfiguriert ist, die auf die Protokolladresse und die angerufene Nummer des Remote-Standorts zeigt.
- **Falsch konfiguriertes Wählprofil**Verwenden Sie den Befehl **show running-config**, um sicherzustellen, dass die Dialer-Schnittstelle mit dem Befehl **Dialer pool X** konfiguriert ist und dass eine Dialer-Schnittstelle auf dem Router mit einem übereinstimmenden *Dialer-Pool-Mitglied X* konfiguriert ist. Wenn Wählprofile nicht ordnungsgemäß konfiguriert sind, wird möglicherweise folgende Fehlerbehebungsmeldung angezeigt:
  ```
  Dialer1: Can't place call, no dialer pool set
  ```

Stellen Sie sicher, dass eine **Wählzeichenfolge** konfiguriert ist.

Async Outbound Calling - Überprüfen der Chat-Script-Operation

Wenn es sich bei dem ausgehenden Anruf um einen Modemanruf handelt, muss ein Chat-Skript ausgeführt werden, damit der Anruf fortgesetzt werden kann. Bei einem DDR, der auf einer Dialerzuordnung basiert, wird das Chat-Skript vom Modem-Script-Parameter in einem Dialer Map-Befehl aufgerufen. Wenn der DDR auf einem Dialer-Profil basiert, wird dies über den in der TTY-Leitung konfigurierten Befehlsskripdialer erreicht. Beide Anwendungen basieren auf einem in der globalen Konfiguration des Routers vorhandenen Chat-Skript. Beispiel:

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

In beiden Fällen lautet der Befehl zum Anzeigen der Chat-Skriptaktivität **Debug-Chat**. Wenn die Wählzeichenfolge (d. h. die Telefonnummer), die im Befehl **Dialer Map** oder **Dialer String** verwendet wird, 5551212 lautete, würde die Debug-Ausgabe wie folgt aussehen:

```
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
```

Chat-Skriptprobleme können in drei Kategorien unterteilt werden:

- Konfigurationsfehler
- Modemfehler
- Verbindungsausfall

Chat-Skriptfehler

Diese Liste zeigt mögliche Ausgaben aus Debug-Chat-Shows und empfohlenen Aktionen:

- **kein passendes Chat-Skript gefunden für [Nummer]**Ein Chat-Skript wurde nicht konfiguriert. Fügen Sie eine hinzu.
- **Chat-Skript-Dialout beendet, Status = Zeitüberschreitung der Verbindung; Remote-Host reagiert nicht**Das Modem reagiert nicht auf das Chat-Skript. Überprüfen Sie die Kommunikation mit dem Modem (siehe Tabelle 16-2 in Kapitel 16).
- **Timeout erwartet: VERBINDEN***Möglichkeit 1*: Das lokale Modem führt den Anruf nicht aus. Stellen Sie sicher, dass das Modem einen Anruf tätigen kann, indem es ein umgekehrtes Telnet zum Modem durchführt und manuell eine Rufnummer initiiert.*Möglichkeit 2*: Das Remote-Modem antwortet nicht. Testen Sie dies, indem Sie das Remote-Modem mit einem normalen POTS-Telefon wählen.*Möglichkeit 3*: Die gewählte Nummer ist falsch. Überprüfen Sie die Nummer, indem Sie sie manuell wählen. Korrigieren Sie ggf. die

Konfiguration.*Möglichkeit 4*: Die Modemschulung dauert zu lange oder der TIMEOUT-Wert ist zu niedrig. Wenn das lokale Modem extern ist, stellen Sie die Lautstärke des Modemlautsprechers ein, und hören Sie sich die Töne zur Fortbildung an. Wenn die Schulung abrupt unterbrochen wird, versuchen Sie, den TIMEOUT-Wert im **Chat-Script-**Befehl zu erhöhen. Wenn der TIMEOUT bereits 60 Sekunden oder länger ist, sehen Sie sich den Abschnitt Modem Trainup an.

Ausgehende ISDN-Anrufe

Wenn der erste Verdacht auf einen ISDN-Ausfall besteht, entweder auf einem BRI oder einem PRI, überprüfen Sie immer den Ausgang vom **show isdn status**. Zu beachten ist vor allem, dass Layer 1 aktiv sein sollte und Layer 2 *MULTIPLE_FRAME_ESTABLISHED* sein sollte. Weitere Informationen zum Lesen dieser Ausgabe sowie Korrekturmaßnahmen finden Sie im Abschnitt "Interpreting Show ISDN Status Output" (ISDN-Statusausgabe anzeigen) in Kapitel 16.

Für ausgehende ISDN-Anrufe sind **debug isdn q931** und **debug isdn event** die besten Tools. Glücklicherweise ähnelt das Debuggen ausgehender Anrufe dem Debuggen eingehender Anrufe. Ein normaler erfolgreicher Anruf könnte wie folgt aussehen:

```
*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
```

Der Ursachenwert weist auf zwei Dinge hin.

- Das zweite Byte des 4- oder 6-Byte-Werts gibt an, von wo aus im End-to-End-Anrufpfad DISCONNECT oder RELEASE_COMP empfangen wurde. Dies kann Ihnen helfen, das Problem zu lokalisieren.
- Das dritte und vierte Byte geben den tatsächlichen Grund für den Ausfall an. Die Bedeutung der verschiedenen Werte finden Sie in den nachfolgenden Tabellen.

Hinweis: Der folgende Ausdruck weist in der Regel auf einen Fehler des höheren Protokolls hin:

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

Der Ausfall der PPP-Authentifizierung ist ein typischer Grund. Aktivieren Sie **Debug-PPP-Aushandlung** und **Debug-PPP-Authentifizierung,** bevor Sie davon ausgehen, dass der Verbindungsausfall zwangsläufig ein ISDN-Problem ist.

Ursachencodefelder

In Tabelle 17-9 sind die ISDN-Ursachencodefelder aufgeführt, die innerhalb der Debugbefehle im folgenden Format angezeigt werden:

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

ISDN-Ursachencodefelder

Feld	Wertbeschreibung
0x	Die folgenden Werte sind hexadezimal.
J1	8 - ITU-T-Standardcodierung.
J2	0 - Benutzer 1 - Privates Netzwerk für lokale Benutzer 2 - Öffentliches Netzwerk für lokale Benutzer 3 - Transit-Netzwerk 4 - Öffentliches Netzwerk für Remote-Benutzer 5 - Privates Netzwerk für Remote-Benutzer 7 - Internationales Netzwerk A - Netzwerk jenseits des Internetarbeitspunkts
z1	Klasse (die bedeutendere Hexadezimalzahl) des Ursachenwerts. Detaillierte Informationen zu möglichen Werten finden Sie in der nächsten Tabelle.
z2	Wert (die weniger signifikante Hexadezimalzahl) des Ursachenwerts. Detaillierte Informationen zu möglichen Werten finden Sie in der nächsten Tabelle.
A1	(Optional) Diagnosefeld, das immer 8 ist.
a2	(Optional) Diagnosefeld mit einem der folgenden Werte: 0 - Unbekannt 1 - Permanent 2 - Transient

ISDN-Ursachenwerte

In der folgenden Tabelle sind Beschreibungen einiger der am häufigsten erkannten Ursachenwerte des Ursacheninformationselements aufgeführt - des dritten und vierten Bytes des Ursachencodes. Ausführlichere Informationen zu ISDN-Codes und -Werten finden Sie unter Understanding **debug isdn q931** Disconnect Cause Codes.

Hex-Wert	Ursache	Erläuterung
81	Nicht zugewiesene (nicht zugewiesene) Nummer	Die ISDN-Nummer wurde im richtigen Format an den Switch gesendet. Die Nummer wird jedoch keinem Zielgerät zugewiesen.
90	Normale Anrufbearbeitung	Die normalen Anrufe wurden gelöscht.

91	Benutzer beschäftigt	Das angerufene System bestätigt die Verbindungsanforderung, kann den Anruf jedoch nicht annehmen, da alle B-Kanäle verwendet werden.
92	Keine Benutzerantwort	Die Verbindung kann nicht hergestellt werden, da das Ziel nicht auf den Anruf reagiert.
93	Keine Antwort vom Benutzer (vom Benutzer benachrichtigt)	Das Ziel antwortet auf die Verbindungsanforderung, kann die Verbindung jedoch nicht innerhalb der vorgegebenen Zeit abschließen. Das Problem liegt am Remote-Ende der Verbindung.
95	Anruf abgelehnt	Das Ziel kann den Anruf annehmen, aber aus einem unbekannten Grund ablehnen.
9 C	Ungültiges Zahlenformat	Die Verbindung konnte nicht hergestellt werden, weil die Zieladresse in einem nicht erkennbaren Format dargestellt wurde oder weil die Zieladresse unvollständig war.
9 F	Normal, nicht angegeben	Meldet das Auftreten eines normalen Ereignisses, wenn keine Standardursache angewendet wird. Keine Aktion erforderlich.
A2	Keine Verbindung/ Kanal verfügbar	Die Verbindung kann nicht hergestellt werden, da kein geeigneter Kanal für den Anruf verfügbar ist.
A6	Netzwerk außer Betrieb	Das Ziel kann nicht erreicht werden, da das Netzwerk nicht ordnungsgemäß funktioniert, und der Zustand kann längere Zeit anhalten. Ein sofortiger Wiederverbindungsversuch ist wahrscheinlich nicht erfolgreich.
Wechselstrom	Angeforderter Schaltkreis/ Kanal nicht verfügbar	Die Remote-Geräte können den angeforderten Kanal aus einem unbekannten Grund nicht bereitstellen. Dies könnte ein vorübergehendes Problem sein.
B2	Angeforderte Einrichtung nicht abonniert	Die Remote-Geräte unterstützen den angeforderten Zusatzdienst nur durch Abonnement. Dies ist häufig ein Verweis auf Ferngespräche.

B9	Trägerleistung nicht autorisiert	Der Benutzer hat eine Trägerfunktion angefordert, die das Netzwerk bereitstellt, aber der Benutzer ist nicht autorisiert, diese zu verwenden. Dies kann ein Abonnementproblem darstellen.
D8	Ungültiges Ziel	Gibt an, dass versucht wurde, eine Verbindung zu Nicht-ISDN-Geräten herzustellen. Beispiel: an eine analoge Leitung.
E0	Obligatorisches Information selement fehlt	Das Empfangsgerät erhielt eine Nachricht, die keine der obligatorischen Informationselemente enthielt. Dies ist in der Regel auf einen D-Channel-Fehler zurückzuführen. Wenn dieser Fehler systematisch auftritt, teilen Sie ihn Ihrem ISDN-Dienstanbieter mit.
E	Ungültiger Inhalt des Information selements	Das Remote-Gerät hat eine Nachricht erhalten, die ungültige Informationen im Informationselement enthält. Dies ist in der Regel auf einen D-Channel-Fehler zurückzuführen.

Ausgehende CAS-Anrufe

Bei ausgehenden Anrufen über CAS T1 oder E1 und integrierte digitale Modems ähnelt ein Großteil der Fehlerbehebung anderen DDR-Fehlerbehebungen. Gleiches gilt auch für ausgehende integrierte Modemanrufe über eine PRI-Leitung. Die einzigartigen Funktionen, die bei einem solchen Anruf auftreten, erfordern ein spezielles Debuggen im Falle eines Anruffehlers.

Wie bei anderen DDR-Situationen müssen Sie sicherstellen, dass ein Anruf angefordert wird. Verwenden Sie zu diesem Zweck **Debug-Dialer-Ereignisse**. Weitere Informationen finden Sie unter Überprüfen der Dialer-Funktion.

Bevor ein Anruf getätigt werden kann, muss dem Anruf ein Modem zugewiesen werden. Um diesen Prozess und den nachfolgenden Aufruf anzuzeigen, verwenden Sie die folgenden Debugbefehle:

- **Debug-Modem**
- **Debug-Modem csm**
- **Debug-Cache**

Hinweis: Der Befehl **debug cas** wurde zuerst in IOS Version 12.0(7)T für AS5200 und AS5300 angezeigt. Ältere Versionen von IOS verwenden einen **internen** Konfigurationsbefehlsdienst auf Systemebene zusammen mit dem Exec-Befehl **modem-mgmt debug rbs**:

Aktivieren von Debuggen

```
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
```

Ausschalten der Debuggen

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

Hinweis: Für das Debuggen dieser Informationen auf einem AS5800 muss eine Verbindung zur Trunk Card hergestellt werden. Im Folgenden sehen Sie ein Beispiel für einen normalen ausgehenden Anruf über einen CAS T1, der für FXS-Ground-Start bereitgestellt und konfiguriert wird:

```
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
```

Debugger für T1s und E1s mit anderen Signalisierungstypen sind ähnlich.

Wenn Sie diesen Punkt beim Debuggen erreichen, wird angezeigt, dass die aufrufenden und antwortenden Modems geschult und verbunden sind und dass die Protokolle höherer Ebenen mit Verhandlungen beginnen können. Wenn ein Modem ordnungsgemäß für den ausgehenden Anruf

reserviert ist, die Verbindung jedoch nicht so weit kommt, muss die T1-Verbindung überprüft werden. Informationen zur T1-Fehlerbehebung finden Sie in Kapitel 15.

Fehlerbehebung PPP

Die Fehlerbehebung für den PPP-Teil einer Verbindung beginnt, wenn Sie wissen, dass die Wählverbindung ISDN oder async erfolgreich eingerichtet wurde.

Es ist wichtig zu wissen, wie eine erfolgreiche PPP-Debug-Sequenz aussieht, bevor Sie die Fehlerbehebung für PPP-Aushandlung durchführen. Auf diese Weise spart Ihnen der Vergleich einer fehlerhaften PPP-Debug-Sitzung mit einer erfolgreich abgeschlossenen Debug-PPP-Sequenz Zeit und Aufwand.

Das nachfolgende Beispiel zeigt eine erfolgreiche PPP-Sequenz. Eine detaillierte Beschreibung der Ausgabefelder finden Sie unter PPP-LCP-Verhandlungsdetails.

```
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
```

Hinweis: Ihre Debuggen können in einem anderen Format angezeigt werden. In diesem Beispiel wird das neuere PPP-Debugausgabeformat veranschaulicht, das in IOS-Version 11.2(8) geändert wurde. In Kapitel 16 finden Sie ein Beispiel für PPP-Debugging mit den älteren Versionen von IOS.

PPP-LCP-Verhandlungsdetails

Zeitst	Beschreibung

empel	
10:57:15:415 Uhr	Ausgehende Konfigurationsanforderung (O CONFREQ). Das NAS-Gerät sendet ein ausgehendes PPP-Konfigurationsanforderungspaket an den Client.
10:57:15,543	Eingehende Konfigurationsbestätigung (I CONFACK). Der Kunde bestätigt Montecitos PPP-Anfrage.
10:57:16,919	Eingehende Konfigurationsanfrage (I CONFREQ). Der Client möchte das Rückrufprotokoll aushandeln.
10:57:16,919	Ablehnen der ausgehenden Konfiguration (O CONFREJ). Das NAS lehnt die Rückrufoption ab.
10:57:17:047	Eingehende Konfigurationsanfrage (I CONFREQ). Der Client fordert einen neuen Satz von Optionen an. Beachten Sie, dass diesmal kein Microsoft-Rückruf angefordert wird.
10:57:17:047	Bestätigung der ausgehenden Konfiguration (O KONFACK). Das NAS akzeptiert die neuen Optionen.
10:57:17:047	Die PPP-LCP-Aushandlung wurde erfolgreich abgeschlossen. Der LCP-Status lautet "Offen". Beide Seiten haben die Konfigurationsanforderung der anderen Seite (CONFREQ) bestätigt (CONFACK).
10:57:17.047 bis 10:57:17.191	Die PPP-Authentifizierung wurde erfolgreich abgeschlossen. Nachdem das LCP ausgehandelt wurde, beginnt die Authentifizierung. Die Authentifizierung muss erfolgen, bevor Netzwerkprotokolle wie IP bereitgestellt werden. Beide Seiten authentifizieren sich mit der während des LCP ausgehandelten Methode. Montecito authentifiziert den Client mithilfe von CHAP.
10:57:20,551	Der Status ist offen für IP Control Protocol (IPCP). Es wird eine Route ausgehandelt und für den IPCP-Peer installiert, dem die IP-Adresse 1.1.1.1 zugewiesen ist.

Link Control Protocol

Bei der LCP-Aushandlung treten in der Regel zwei Arten von Problemen auf.

Der erste Fall tritt ein, wenn ein Peer Konfigurationsanfragen durchführt, die der andere Peer nicht bestätigen kann oder wird. Dies ist zwar häufig der Fall, kann jedoch ein Problem darstellen, wenn der Antragsteller auf dem Parameter besteht. Ein typisches Beispiel ist die Aushandlung von AUTHTYPE (auch bekannt als "AuthProto"). Beispielsweise sind viele Zugriffsserver so konfiguriert, dass sie nur CHAP für die Authentifizierung akzeptieren. Wenn der Anrufer so konfiguriert ist, dass er nur PAP-Authentifizierung durchführt, werden CONFREQs und

CONFNAKs ausgetauscht, bis der eine oder der andere die Verbindung beendet.

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

Das zweite Problem in LCP besteht darin, dass nur ausgehende CONFREQs auf einem oder beiden Peers angezeigt werden, wie im Beispiel unten gezeigt. Dies ist normalerweise das Ergebnis einer *Geschwindigkeitsungleichheit* auf der unteren Ebene. Diese Bedingung kann entweder async oder ISDN DDR auftreten.

```
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
```

Wenn die Verbindung async ist, liegt die wahrscheinliche Ursache in einer Geschwindigkeitsungleichheit zwischen Router und Modem. Dies ist in der Regel darauf zurückzuführen, dass die DTE-Geschwindigkeit des Modems nicht auf die konfigurierte Geschwindigkeit der TTY-Leitung festgelegt wurde. Das Problem kann bei einem oder bei beiden Peers auftreten. Überprüfen Sie daher beide. Siehe Modem Cannot Send or Receive Data

(Modem kann keine Daten senden oder empfangen) weiter oben in diesem Kapitel.

Wenn die Symptome auftreten, wenn die Verbindung über ISDN hergestellt wird, besteht das Problem wahrscheinlich darin, dass ein Peer eine Verbindung mit 56K herstellt, der andere eine Verbindung mit 64K. Obwohl diese Krankheit selten ist, passiert sie. Das Problem kann eine oder beide Peers oder möglicherweise die Telefongesellschaft sein. Verwenden Sie **debug isdn q931**, und überprüfen Sie die SETUP-Meldungen auf jedem der Peers. Die von einem Peer gesendete Träger-Fähigkeit muss mit der Trägerleistung übereinstimmen, die in der SETUP-Nachricht, die auf dem anderen Peer empfangen wurde, angezeigt wird. Konfigurieren Sie als mögliche Lösung entweder in der **Dialer-Zuordnung** auf Schnittstellenebene oder in der **Kommandozeile** des **Dialers die** unter einer Map-Class konfigurierte **Geschwindigkeit** für das Wählen von 56K oder 64K.

```
*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
```

Diese Situation kann einen Anruf beim Cisco TAC rechtfertigen. Erfassen Sie die folgenden Ergebnisse von beiden Peers, bevor Sie das TAC anrufen:

- **show running-config**
- **Anzeigeversion**
- **debug isdn q931**
- **Debug-ISDN-Ereignisse**
- **Debug-ppp-Aushandlung**

Authentifizierung

Eine fehlgeschlagene Authentifizierung ist der häufigste Grund für einen PPP-Ausfall. Falsch konfigurierte oder falsch zugeordnete Benutzernamen und Kennwörter erstellen Fehlermeldungen in der Debug-Ausgabe.

Das folgende Beispiel zeigt, dass der Benutzername Goleta nicht über die Berechtigung zum Einwählen in das NAS-Gerät verfügt, das über keinen für diesen Benutzer konfigurierten lokalen Benutzernamen verfügt. Um das Problem zu beheben, verwenden Sie den Befehl **username *name* password password**, um der lokalen AAA-Datenbank des NAS den Benutzernamen "Goleta" hinzuzufügen:

```
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
```

Das folgende Beispiel zeigt, dass der Benutzername "Goleta" auf dem NAS konfiguriert wird. Der Kennwortvergleich ist jedoch fehlgeschlagen. Um dieses Problem zu beheben, verwenden Sie den **Befehl username *name* password password**, um das richtige Kennwort für Goleta anzugeben:

```
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
```

Weitere Informationen zur PAP-Authentifizierung finden Sie unter Konfiguration und Fehlerbehebung für PPP Password Authentication Protocol (PAP).

Netzwerksteuerungsprotokoll

Nachdem die Peers die erforderliche Authentifizierung erfolgreich durchgeführt haben, wird die Aushandlung in die NCP-Phase verschoben. Wenn beide Peers ordnungsgemäß konfiguriert sind, kann die NCP-Aushandlung wie im folgenden Beispiel aussehen, das zeigt, dass ein Client-PC sich bei einem NAS einwählt und mit einem NAS verhandelt:

```
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
```

Details zur PPP-NCP-Verhandlung

Zeitstempel	Beschreibung
21:35:04.190	Ausgehende Konfigurationsanforderung (O CONFREQ). Das NAS-Gerät sendet ein ausgehendes PPP-Konfigurationsanforderungspaket mit seiner IP-Adresse an den Peer.
21:35:04:282	Eingehende KONFREQ. Der Peer fordert eine VJ-Header-Komprimierung an. Sie benötigt für sich selbst eine IP-Adresse sowie Adressen der primären und sekundären DNS-Server.
21:35:04:306	Outbound Config-Reject (CONFREJ) Die VJ-Header-Komprimierung wird abgelehnt.
21:35:04.314 bis 21:35:04.330	Der Peer sendet eine Anforderung an das Compression Control Protocol. Das gesamte Protokoll wird vom NAS mithilfe einer PROTREJ-Nachricht abgelehnt. Der Peer sollte nicht versuchen (und auch nicht), CCP erneut zu versuchen.
21:35:04:334	Der Peer bestätigt die IP-Adresse des NAS mit einem CONFACK.
21:35:07:274	Eingehende KONFREQ. Der Peer fordert keine VJ-Header-Komprimierung mehr an, benötigt jedoch für sich selbst eine IP-Adresse sowie Adressen der primären und sekundären DNS-Server.
21:35:07.294	Das NAS-Gerät sendet einen CONFNAK mit der Adresse, die der Peer verwenden soll, sowie den Adressen der primären und sekundären DNS-Server.
21:35:07,426	Der Peer sendet die Adressen zurück an das NAS-Gerät. einen Versuch, die ordnungsgemäße Annahme der Adressen zu bestätigen.
21:35:07,458	Das NAS-Gerät erkennt die Adressen mit einem CONFACK.
21:35:07,478	Jede Seite der Verbindung, die einen CONFACK (KONFACK) ausgestellt hat, hat den Verhandlungsabschluss abgeschlossen. Der Befehl **show interfaces Async4** on the NAS shows "IPCP: Öffnen".
21:35:07:49	In der Routing-Tabelle des NAS-Geräts wird eine Host-Route zum Remote-Peer installiert.

0	

Peers können gleichzeitig mehrere Layer-3-Protokolle aushandeln. Es ist beispielsweise nicht ungewöhnlich, dass IP und IPX ausgehandelt werden. Es ist auch möglich, dass ein Protokoll erfolgreich verhandelt, während das andere Protokoll dies nicht tut.

NCP-Fehlerbehebung

Probleme, die während der NCP-Aushandlung auftreten, können in der Regel auf die Konfigurationen der Verhandlungspersonen zurückgeführt werden. Wenn die PPP-Aushandlung während der NCP-Phase fehlschlägt, gehen Sie wie folgt vor:

1. Konfiguration des Schnittstellenprotokolls überprüfenÜberprüfen Sie die Ausgabe des privilegierten exec-Befehls **show running-config**. Überprüfen Sie, ob die Schnittstelle so konfiguriert ist, dass sie das Protokoll unterstützt, das Sie über die Verbindung ausführen möchten.
2. Schnittstellenadresse überprüfenBestätigen Sie, dass für die betreffende Schnittstelle eine Adresse konfiguriert wurde. Wenn Sie **ip unnumbered [*interface-name*]** oder **ipx ppp-client loopback [*number*]** verwenden**,** stellen Sie sicher, dass die referenzierte Schnittstelle mit einer Adresse konfiguriert ist.
3. Überprüfung der Client-AdressenverfügbarkeitWenn das NAS-Gerät dem Anrufer eine IP-Adresse zuweisen soll, stellen Sie sicher, dass eine solche Adresse verfügbar ist. Die IP-Adresse, die dem Anrufer übergeben wird, kann auf eine der folgenden Weisen abgerufen werden:Lokale Konfiguration auf der Schnittstelle Überprüfen Sie die Schnittstellenkonfiguration für den Befehl **peer default ip address a.b.c.d**. In der Praxis sollte diese Methode nur auf Schnittstellen verwendet werden, die Verbindungen von einem einzelnen Aufrufer akzeptieren, z. B. auf einer asynchronen (*nicht* einer Gruppenstasync-Schnittstelle).Der Adresspool wird lokal auf dem NAS konfiguriert. Die Schnittstelle sollte über den Befehl **peer default ip address pool [*pool-name*]** verfügen. Darüber hinaus muss der Pool auf Systemebene mit dem Befehl **ip local pool [*pool-name*] [*first-address*] [*last-address*]** definiert werden. Der im Pool definierte Adressbereich sollte so groß sein, dass so viele gleichzeitig verbundene Anrufer wie das NAS-Gerät unterstützt werden können.DHCP-Server. Die NAS-Schnittstelle muss mit dem Befehl **peer default ip address dhcp** konfiguriert werden. Darüber hinaus muss das NAS-Gerät so konfiguriert werden, dass es mit dem globalen Konfigurationsbefehl **ip dhcp-server [*address*]** auf einen DHCP-Server verweist.AAA Bei Verwendung von TACACS+ oder RADIUS zur Autorisierung kann der AAA-Server so konfiguriert werden, dass er einem bestimmten Anrufer bei jeder Verbindung eine bestimmte IP-Adresse zuweist. Weitere Informationen finden Sie in Kapitel 16.
4. Serveradresskonfiguration überprüfenUm die konfigurierten Adressen der Domänennamenserver oder Windows NT-Server als Antwort auf BOOTP-Anfragen zurückzugeben, stellen Sie sicher, dass die globalen Befehle **async-bootp dns-server [*address*]** und **async-bootp nbns-server [*address*]** konfiguriert sind.**Hinweis:** Während der Befehl **async-bootp subnetzmaske [*mask*]** auf dem NAS konfiguriert werden kann, *wird* die Subnetzmaske nicht zwischen dem NAS und einem PPP-Einwahl-Client-PC ausgehandelt. Aufgrund der Beschaffenheit von Point-to-Point-Verbindungen verwendet der Client automatisch die IP-Adresse des NAS (die bei der IPCP-Aushandlung erlernt wird) als Standard-Gateway. Die Subnetzmaske wird in dieser Point-to-Point-Umgebung nicht benötigt. Der PC weiß, dass, wenn die Zieladresse nicht mit der lokalen Adresse

übereinstimmt, das Paket an das Standard-Gateway (NAS) weitergeleitet werden muss, das immer über die PPP-Verbindung erreicht wird.

Vor dem Anruf beim Cisco Systems TAC Team

Bevor Sie das Cisco Systems Technical Assistance Center (TAC) anrufen, sollten Sie sich vergewissern, dass Sie dieses Kapitel durchgelesen und die für Ihr Systemproblem vorgeschlagenen Maßnahmen abgeschlossen haben.

Führen Sie außerdem die folgenden Schritte aus, und dokumentieren Sie die Ergebnisse, damit wir Ihnen besser helfen können:

Für alle Probleme sollten Sie die Ausgabe von **show running-config** und **show version** erfassen. Stellen Sie sicher, dass der Befehl **service timestamps debug datetime msec** in der Konfiguration vorhanden ist.

Sammeln Sie bei DDR-Problemen Folgendes:

- **Show Dialer Map**
- **Debug Dialer**
- **Debug-ppp-Aushandlung**
- **Debug-ppp-Authentifizierung**

Falls ISDN beteiligt ist, sammeln Sie Folgendes:

- **show isdn status**
- **debug isdn q931**
- **Debug-ISDN-Ereignisse**

Wenn Modems beteiligt sind, sammeln Sie Folgendes:

- **Anzeigen von Zeilen**
- **show line [x]**
- **Modem anzeigen** (wenn integrierte Modems beteiligt sind)
- **Modemversion anzeigen** (wenn integrierte Modems betroffen sind)
- **Debug-Modem**
- **debug modem** csm (wenn integrierte Modems beteiligt sind)
- **Debug-Chat** (bei einem DDR-Szenario)

Wenn T1s oder PRIs beteiligt sind, sammeln Sie Folgendes:

- **Show Controller t1**

Zugehörige Informationen

- T1/E1 Fehlerbehebung Seite
- Cisco IOS-Leitfaden für Wähllösungen
- Überwachung und Wartung der T1/E1-Schnittstelle
- Fehlerbehebung bei Verhandlungen über PPP
- Fehlerbehebung bei Modems
- Modem-Debug-Befehle

- Fehlerbehebung ISDN
- T1 PRI - Fehlerbehebung
- Technischer Support und Dokumentation - Cisco Systems