ダイヤルアップ技術： トラブルシューティング テクニック

目次

はじめに

ダイヤルアップは、端末ユーザのためにデータを搬送する Public Switched Telephone Network（PSTN; 公衆電話交換網）のための機能です。 ダイヤルアップには、接続の宛先となる電話番号を電話交換機に送信する Customer Premises Equipment（CPE; 顧客宅内機器）デバイスが含まれます。 Cisco3600、AS5200、AS5300、AS5800 などは、PRI をデジタル モデムとともに実装する機能があるルータです。 一方、AS2511 は外部モデムと通信するルータです。

前提条件

要件

このドキュメントの読者は次の項目に関する知識が必要です。

現在、通信事業の市場ではその規模の拡大とともに、より高いモデム密度が求められています。 このニーズへの答えは、電話会社の機器とのインターオペラビリティの向上と、デジタル モデムの開発です。 デジタル モデムには PSTN に直接デジタル アクセスする機能があります。 結果として、現在ではデジタル モデムの特長である信号の明瞭さを利用した、より高速な CPE モデムが開発されています。 デジタル モデムは PRI または BRI を通じて PSTN に接続し、V.90 通信規格を使用して 53k 超のデータを伝送できます。

Cisco が初めて市場に投入したアクセス サーバは Cisco2509 および Cisco2511 でした。 AS2509 は外部モデムを使用して 8 つの着信接続を処理でき、AS2511 は 16 の着信接続を処理できました。 2 つの PRI が導入された AS5200 はデジタル モデムを使用して 48 のユーザをサポート可能であり、収容効率が飛躍的に向上しました。 AS5300 では PRI のサポートが 4 から 8 に増え、モデム密度が着実に増加していきました。 最終的に、数十の T1 回線と数百のユーザ接続を処理する通信事業者クラスの設置ニーズに対応するため、AS5800 が導入されました。

ダイヤラ テクノロジーの歩みの中で、現在でも議論の対象にされる旧来のテクノロジーがいくつかあります。 56Kflex は、Rockwell によって提唱された（V.90 以前の）古い 56k モデム規格です。 Cisco では、バージョン 1.1 の 56Kflex 規格を Cisco 製の内部モデムでサポートしていますが、CPE をできるだけ速やかに V.90 に移行することを推奨しています。 もう 1 つの旧来のテクノロジーとして、AS5100 があります。 AS5100 は Cisco とモデム製造元が共同で開発した製品でした。 AS5100 は、クワッド モデム カードを使用してモデム密度を増やす手段として開発されました。 AS5100 ではカードとして組み込まれた AS2511 が必要でした。これらのカードは、クワッド モデム カードとデュアル T1 カードによって共有されるバックプレーンに挿入されていました。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

着信コールのトラブルシューティング

着信コールのトラブルシューティングは、下位層から始め、上位層へと進めていきます。 論理の全般的なフローに従って、次を確認します。

1. コールの着信を確認しましたか（答えがはいの場合は、次の質問に進みます）。
2. 受信端末がコールに応答しましたか。
3. コールが完了しましたか。
4. データがリンクを通過していますか。
5. セッションが確立されましたか。（PPP かターミナル）

モデム接続の場合、PPP のネゴシエーションが始まるまでデータ コールとログインセッションは同じに見えます。

デジタル モデムが動作する着信コールの場合は、基盤となる ISDN または CAS がコールを受信していることを最初に確認します。 外部モデムを使用している場合は、ISDN および CAS のセクションはスキップできます。

ISDN 着信コールのトラブルシューティング

コマンド debug isdn q931 を使用します。 接続が成功した場合の出力例を次に示します。

```
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
```

セットアップ メッセージは、接続がリモート エンドによって開始されようとしていることを示しています。 コールリファレンス番号はペアで維持されています。 この場合、着信側のコールリファレンス番号は 0x06 で、発信側のコールリファレンス番号は 0x86 です。 ベアラケーパビリティは（頻繁に bearercap と言われる）どのようなコールが入っているかルータに告げます。 この場合接続は型 0x8890 です。 この値は「ISDN Speed 64 Kb/s」を示しています。 bearercap が 0x8090A2 の場合は、「Speech/voice call u-law」を示します。

セットアップ メッセージがまったく表示されない場合、その接続が音声に対応していれば番号を手動でコールし、番号が正しいかを確認します。 また、ISDN インターフェイスのステータスもチェックします（詳細については『show isdn status コマンドを使用した BRI のトラブルシューティング』を参照してください）。 これらをチェックしてもまったく問題がない場合は、コールの発信元が正しいコールを行っているかを確認します。 そのためには、電話会社に問い合せます。 コール オリジネーターはどこでそれ見るためにコールをトレースできますか。送信 されるs。 市外接続の場合は、他のキャリアを試してみてください。

着信するコールが非同期モデム コールの場合は、回線が音声コールを許可するように設定されていることを確認してください。

注: BRI 非同期モデム コールは、12.0(3)T 以降が稼働する 3600 ルータの機能です。 この機能には、BRI インターフェイス ネットワーク モジュールの最新のハードウェア リビジョンが必要です。 WIC モジュールは非同期モデム コールをサポートしていません。

コールが着信したにもかかわらず完了しない場合は、原因コードを探します（表 17-10 を参照）。 完了が成功したかどうかは接続応答確認（CONNECT_ACK）によってわかります。

このコールが非同期モデム コールの場合は、「着信モデム コールのトラブルシューティング」のセクションに進んでください。

この時点で ISDN コールは接続していますが、リンク経由で着信したデータはまだ見られません。 debug ppp negotiate コマンドを使用して、PPP トラフィックが回線経由で着信していないかを確認します。 トラフィックが見られない場合は、速度不一致が考えられます。 これが原因かどうかを調べるには、show running-config privileged exec コマンドを使用して、ルータの設定を表示します。 ローカル ルータ内およびリモート ルータ内にある、dialer map インターフェイス設定コマンド エントリをチェックします。 これらのエントリは次のようになっています。

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

ダイヤラ プロファイルの場合、速度を設定するためにマップクラスを定義する必要があります。

デフォルトでは、ISDN インターフェイスは各チャネルで 64K の通信速度の使用を試みることに注意してください。

ダイヤラ マップおよびダイヤラ プロファイルの設定の詳細については、『Cisco IOS ダイヤル ソリューション コンフィギュレーション ガイド』、『ダイヤル ソリューション コマンド リファレンス』、および『ダイヤル ソリューション クイック コンフィギュレーション ガイド』を参照してください。

有効な PPP パケットを受信している場合は、リンクがアップ状態であり、正常に動作しています。 この場合は、「PPP のトラブルシューティング」のセクションに進んでください。

CAS 着信コールのトラブルシューティング

モデムの接続を処理している CAS グループのトラブルシューティングを行うには、debug modem、debug modem csm、debug cas の各コマンドを使用します。

注: debug cas コマンドは、AS5200 および AS5300 用に 12.0(7)T で初めて導入されたものです。 これよりも前のバージョンの IOS では、システム レベルの設定コマンドである service internal と exec コマンド modem-mgmt debug rbs を併用します。 AS5800 でこれらの情報をデバッグするためには、トランク カード自体に接続する必要があります。

最初に、電話会社の交換機が着信コール信号を送るために「オフフック」に移行したかどうかを調べます。 オフフックに移行しなかった場合は、コールしようとしている番号を確認します。 これには、発信側の電話回線に電話機を接続して、その番号をコールします。 コールが正常な場合は、発信元の CPE に問題があります。 コールが依然として CAS 上に現れない場合は、T1（15 章を参照）をチェックします。この場合は debug serial interfaces コマンドを使用します。

次の結果は debug modem CSM を使用した出力例で、良好な接続を示しています。

```
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
```

この例では、コールの宛先がモデムになっていました。 コールの宛先がモデムの場合は、次の「モデム着信コールのトラブルシューティング」のセクションに進んでください。

モデム着信コールのトラブルシューティング

モデム着信コールのトラブルシューティングを行うときは、次のデバッグ コマンドを使用します。

- **debug modem**
- debug modem csm（組み込みデジタル モデムの場合）

次のデバッグ コマンドを組み合せて使用し、新しいコールが着信したかどうかを調べます。

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

コールがモデムに着信している場合、モデムでコールがピックアップされる必要があります。

外部モデムをデバッグする際のヒント

TTY 回線に接続された外部モデムのデバッグを容易にするため、スピーカの音量を上げてください。 これにより、問題がより明確になる場合があります。

発信元モデムがコールしたときに、着信モデムで着信音が鳴るかどうかを確認します。 鳴らない場合は、番号を確認し、リモート サイトから手動コールを試します。 着信端末で通常の電話が使用できることも試します。 必要に応じてケーブルやハードウェアを交換します。

非同期モデム コールのピックアップ

外部モデムが応答していない場合、モデムと、アクセス サーバまたはルータとの間のケーブル接続をチェックします。 モデムがロール型 RJ-45 ケーブルと MMOD DB-25 アダプタを通じて TTY またはルータの補助ポート（AUX ポート）に接続されていることを確認します。 Cisco では RJ-45 ポートを推奨およびサポートしています。 これらのコネクタが一般的に分類されることに注目して下さい: 付いています。)

RJ 45 ケーブル接続は少数入力します入って来ます: まっすぐに、転送される、およびクロスオーバー。 ケーブル配線の種類は、RJ-45 ケーブルの 2 つの端子を並べることで判断できます。 各端子には、8 個の色付きのストリップ（ピン）があります。

- 色の付いたピンの順番が両端で同一である場合には、そのケーブルはストレートです。
- 色の付いたピンの順番が両端で反対であれば、それはロール型ケーブルになります。
- 色が次のようであればケーブルはクロス型です。

RJ45/RJ45 クロスケーブル：

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

シグナリングが正常であることを確認するには、16 章で説明している show line コマンドを使用します。

その他、外部モデムを自動応答のために初期化する必要があります。 リモート モデムが自動応答に設定されているかどうかをチェックします。 通常、自動応答が設定されているときは AA インジケータ ライトがオンになっています。 まだ設定されていない場合は、リモート モデムを自動応答に設定します。 モデム設定の確認および変更の詳細については、モデムのドキュメントを参照してください。 リバース Telnet を使用してモデムを初期化します（16 章を参照）。

デジタル（組み込み）モデム コールのピックアップ

外部モデムではコールが応答中かどうかは明らかですが、内部モデムでは受信番号に手動でコールを行う必要があります。 Answer Back Tone（ABT）が聞こえるかを確かめます。 ABT が聞こえない場合は、次の 2 点について設定をチェックします。

1. 着信モデム接続を処理するすべての ISDN インターフェイスの基に、isdn incoming-voice modem コマンドが存在することを確認します。

2. モデムの TTY の回線設定の基に、modem inout コマンドが存在することを確認します。 また、着信コールを処理する内部モデムが Call Switching Module (CSM; コール スイッチング モジュール) によって割り当てられなかった可能性もあります。 この問題の原因としては、モデムまたはリソース プールで設定されている着信接続の数が少なすぎることが考えられます。 また、アクセス サーバで単にモデム数が足りなくなっている可能性もあります。 モデムのアベイラビリティをチェックし、モデム プールまたはリソース プール マネージャの設定を適切に調整します。 モデムが割り当てられていて、設定に modem inout がある場合は、デバッグ情報を収集し、Cisco に連絡してサポートを受けてください。

モデムの trainup

受信モデムで DSR が上がっていれば、trainup は成功しています。 trainup が失敗している場合、回線の問題か、モデムに互換性がないことが考えられます。

モデムに関する個々の問題の根本的な原因を突き止めるには、発信元モデムを問題のある POTS 回線に接続した状態で AT プロンプトに移ります。 Cisco アクセス サーバ内のデジタル モデムにコールしている場合は、trainup 音源の wav ファイル、つまり Digital Impairment Learning (DIL) シーケンスを記録する準備をします。 DIL は、発信元の V.90 アナログ モデムから着信側のデジタル モデムに対して再生を指示する楽譜 (PCM シーケンス) です。 シーケンスはアナログモデムが回線のデジタル障害を検知するようにします; 複数の D/A 変換、law/u 関連法規、robbedビット、またはデジタル パッドのような。 DIL が聞こえない場合は、モデムが V.8/V.8bis で V.90 をネゴシエートしていません (つまり、モデムの互換性に問題があります)。 DIL が聞こえ、V.34 で再 train している場合、アナログ モデムは (DIL の再生に基づいて) V.90 が実行不可能であると判断しています。

音楽に雑音が混じっているかを確認します。 雑音が混じっている場合は、回線をクリーンアップします。

クライアントが V.34 の training を実行せずにすぐにコールをやめたかどうかを確認します。 たとえば、クライアントは V.8bis を聞いたときに動作できない場合があるとします。 この場合、サーバで V.8bis (したがって K56Flex) を無効にする必要があります (適切な場合)。 新しいクライアント ファームウェアを入手するか、またはクライアント モデムを交換してください。 あるいは、ダイヤル端末でダイヤル文字列の末尾に 5 つのカンマを挿入できます。 これによりコール側モデムの受信が遅れ、クライアント モデムに影響を与えることなく、受信側サーバからの V.8bis のトーンがタイムアウトになります。 ダイヤル文字列内の 5 つのカンマは一般的なガイドラインであり、ローカルでの条件にあわせて調整する必要がある場合もあります。

セッションの確立

ここまでの時点で、モデムは接続され trainup されています。 次に、トラフィックが適切に着信しているかどうかを調べます。

コールを受信している回線で **autoselect ppp** を設定していて、非同期インターフェイスで **async mode interactive** を設定している場合は、**debug modem** コマンドを使用して自動選択処理を確認します。 トラフィックが非同期回線を経由して着信すると、アクセス サーバはトラフィックを調べ、トラフィックがキャラクタ ベースかパケット ベースかを判断します。 次に、アクセス サーバはこの判断に応じて、PPP セッションを開始するか、または回線上で exec セッションを維持します。

PPP の着信 LCP パケットによる正常な自動選択シーケンスは次のようになります。

```
*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.
```

コールが PPP セッションで、非同期インターフェイスに async mode dedicated が設定されている場合は、debug ppp negotiation コマンドを使用して、リモート エンドから到着する設定要求パケットがあるかどうかを確認します。 デバッグではこれらが CONFREQ と表示されます。 着信および発信の両方の PPP パケットが観測される場合は、「PPP のトラブルシューティング」に進んでください。 それ以外の場合は、コールの発信元である端末からキャラクタモード（または「exec」）セッション（つまり、非 PPP セッション）で接続します。

注: 受信側の非同期インターフェイスの下に **async modem dedicated** が表示されている場合、exec ダイヤルインには無意味な ASCII 文字が表示されるだけです。 PPP 機能を有効にしたままでターミナル セッションを許可するには、非同期インターフェイス設定コマンド **async mode interactive** を使用します。 関連する回線の設定の下で、autoselect ppp コマンドを使用します。

モデムがデータを送信または受信できない場合

モデムがターミナル セッションと接続していて、データがまったく到達しない場合は、次の考えられる原因と推奨される対策方針をチェックしてください。

- **モデム速度の設定が固定されていない**アクセス サーバまたはルータで **show line exec** コマンドを使用します。 補助ポートの出力は、現在設定されている Tx および Rx の速度を示します。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。回線が正しい速度に設定されていない場合は、**speed** 回線設定コマンドを使用し、アクセス サーバまたはルータの回線の回線速度を設定します。 モデムと、アクセス サーバまたはルータのポートとの間で共通の最高速度に設定します。 端末のボー レートを設定するには、**speed** 回線設定コマンドを使用します。 このコマンドは、送信（端末へ）と受信（端末から）の両方の速度を設定します。構文：speed bps構文の説明：bps：ビット/秒（bps）でのボーレート。 デフォルトは 9600 bps です。次の例は、Cisco 2509 アクセス サーバの回線 1 および 2 を 115200 bps に設定します。

  ```
  line 1 2
  speed 115200
  ```

  注: 何らかの理由でフロー制御を使用できない場合は、回線速度を 9600 bps に制限します。これ以上速い速度の場合、データが失われる可能性があります。再度 **show line exec** コマンドを使用し、回線速度が望ましい値に設定されたことを確認します。アクセス サーバまたはルータの回線が望ましい速度に設定されていることを確認したら、その回線を経由してモデムへのリバース Telnet セッションを開始します。 詳細については、16 章の「モデムへのリバース Telnet セッションの確立」のセクションを参照してください。使用しているモデムに、「lock DTE speed」コマンドを含むモデム コマンド文字列を使用します。 設定コマンドの

正確な構文については、使用中のモデムのドキュメントを参照してください。**注: lock DTE speed** コマンドは、多くの場合、モデムによるエラー訂正の処理方法に関連して port rate adjust あるいは buffered mode と呼ばれることもあります。 このコマンドはモデムによって大きく異なります。モデム速度をロックすることにより、モデムは Cisco アクセス サーバまたはルータに対して、常に Cisco 補助ポートに設定された速度で通信します。 このコマンドを使用しない場合、モデムはデータ リンク（電話回線）の速度に戻ります。アクセス サーバに設定された速度では通信しません。

- **ハードウェア フロー制御がローカルまたはリモートのモデムまたはルータで設定されていない**show line aux-line-number exec コマンドを使用し、Capabilities フィールドにある次の記述を探します。

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

詳細については、章で第 16 出力される Show line を解読することを参照して下さい。このフィールドにハードウェア フロー制御に関する記述がない場合、ハードウェア フロー制御が回線で有効にされていません。 アクセス サーバからモデムへの接続については、ハードウェア フロー制御を使用することをお勧めします。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。回線のハードウェア フロー制御を設定するには、flowcontrol hardware 回線設定コマンドを使用します。端末またはその他のシリアル デバイスとルータとの間におけるデータ フロー制御の方式を設定するには、**flowcontrol** 回線設定コマンドを使用します。 フロー制御を無効にするには、このコマンドの no 形式を使用します。構文：**flowcontrol** {none **| software [lock] [in | out] | hardware [in |]}**構文の説明：none：フロー制御をオフにします。software：ソフトウェア フロー制御を設定します。 オプションのキーワードは方向を指定します。 **in** を指定すると、Cisco IOS ソフトウェアは接続デバイスからのフロー制御を受信します。**out** を指定すると、Cisco IOS ソフトウェアはフロー制御情報を接続デバイスに送信します。 方向を指定しない場合は両方向と見なされます。lock：接続装置でソフトウェア フロー制御が必要な場合に、リモート ホストからのフロー制御をオフにできないようにします。 このオプションは Telnet または rlogin のプロトコルを使用した接続に適用されます。hardware：ハードウェア フロー制御を設定します。 オプションのキーワードは方向を指定します。 **in** を指定すると、ソフトウェアは接続デバイスからのフロー制御を受信します。**out** を指定すると、Cisco IOS ソフトウェアはフロー制御情報を接続デバイスに送信します。 方向を指定しない場合は両方向と見なされます。 ハードウェア フロー制御の詳細については、ルータに付属しているハードウェアのマニュアルを参照してください。例：次の例は、回線 7 でハードウェア フロー制御を設定します。

```
line 7
flowcontrol hardware
```

注: 何らかの理由でフロー制御を使用できない場合は、回線速度を 9600 bps に制限します。これ以上速い速度の場合、データが失われる可能性があります。アクセス サーバまたはルータの回線でハードウェア フロー制御を有効にした後、その回線を経由してモデムへのリバース Telnet セッションを開始します。 詳細については、16 章の「モデムへのリバース Telnet セッションの確立」のセクションを参照してください。使用しているモデム用の **RTS/CTS Flow** コマンドを含むモデム コマンド文字列を使用します。 このコマンドにより、モデムは Cisco アクセス サーバまたはルータと同じフロー制御方式（つまり、ハードウェア フロー制御）を使用します。 設定コマンドの正確な構文については、使用中のモデムのドキュメントを参照してください。

- **誤った dialer map コマンドの設定**show running-config 特権 EXEC コマンドを使用してルータの設定を表示します。 **dialer map** コマンドのエントリを調べ、**broadcast** キーワードが指定されているかどうかを調べます。キーワードがない場合は設定に追加します。構文：**dialer map protocol next-hop-address [name hostname] [ブロードキャスト] [*ダイヤル ストリング*]**構文の説明：protocol：マッピングの対象となるプロトコルです。 IP、IPX、ブリッジ、およ

びスナップショットから選択できます。next-hop-address：相手サイトの非同期インターフェイスのプロトコル アドレスです。name hostname：PPP 認証で使用される必須パラメータです。 ダイヤラ マップの作成対象となるリモート サイトの名前を指定します。 この名前は大文字小文字が区別され、リモート ルータのホスト名と一致する必要があります。broadcast：リモートの宛先に転送されるパケット（たとえば、IP RIP または IPX RIP/SAP のアップデートなど）をブロードキャストするオプションのキーワードです。 スタティック ルーティングの設定例では、ルーティング アップデートは必要とされておらず、**broadcast** キーワードは省略されています。dial-string：リモート サイトの電話番号です。 アクセス コード（外線につなぐための 9、国際局番、市内局番など）をすべて含める必要があります。dialer map コマンドで正しいネクストホップ アドレスを指定していることを確認します。ネクストホップ アドレスが正しくない場合は、**dialer map** コマンドを使用して変更します。dialer map コマンド内にある他のすべてのオプションが、使用しているプロトコルに対して正しく指定されていることを確認します。ダイヤラ マップの設定の詳細については、『*Cisco IOS Wide-Area Networking 設定ガイド*』および『*Wide-Area Networking コマンド リファレンス*』を参照してください。

- **ダイヤリング モデムに関する問題**ダイヤリング モデムが稼働状態にあり、正しいポートに確実に接続していることを確認します。 同じポートに接続している別のモデムが動作していないかを調べます。

一般に、着信 exec セッションのデバッグは主として次のカテゴリに分けられます。

- ダイヤルアップ クライアントに exec プロンプトが返されない場合
- ダイヤルアップ セッションに「無意味な文字」が表示される場合
- ダイヤルアップ セッションが既存のセッションで開く場合
- ダイヤルアップ受信モデムが正常に接続解除しない場合

ダイヤルアップ クライアントに exec プロンプトが返されない場合

- **自動選択が回線で有効になっている**Enter キーを押して exec モードへのアクセスを試みます。
- **no exec** コマンドが回線に設定されている**show line exec** コマンドを使用し、該当する回線のステータスを表示します。Capabilities フィールドに「exec suppressed」という表示がないかを調べます。 表示されている場合は、**no exec** 回線設定コマンドが有効にされています。回線で **exec** 回線設定コマンドを設定し、exec セッションを開始できるようにします。 このコマンドには引数やキーワードはありません。次の例は、回線 7 で exec をオンにします。

```
line 7
exec
```

- **フロー制御が有効にされていない。またはフロー制御が 1 つのデバイスだけ（DTE か DCE のどちらか）で有効にされているまたはフロー制御の設定に誤りがある**show line aux-line-number exec コマンドを使用し、Capabilities フィールドにある次の記述を探します。

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

詳細については、章で第 16 出力される Show line を解読することを参照して下さい。このフィールドにハードウェア フロー制御に関する記述がない場合、ハードウェア フロー制御が回線で有効にされていません。 アクセス サーバからモデムへの接続については、ハードウェア フロー制御を使用することをお勧めします。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。回線のハードウェア フロー制御を設定するには、**flowcontrol hardware** 回線設定コマンドを使用します。 次の例は、回線 7 でハードウェア フロー制御を設定します。

```
line 7
flowcontrol hardware
```

注: 何らかの理由でフロー制御を使用できない場合は、回線速度を 9600 bps に制限します。これ以上速い速度の場合、データが失われる可能性があります。アクセス サーバまたはルータの回線でハードウェア フロー制御を有効にした後、その回線を経由してモデムへのリバース Telnet セッションを開始します。 詳細については、16 章の「モデムへのリバース Telnet セッションの確立」のセクションを参照してください。使用しているモデム用の RTS/CTS Flow コマンドを含むモデム コマンド文字列を使用します。 このコマンドにより、モデムは Cisco アクセス サーバまたはルータと同じフロー制御方式（つまり、ハードウェア フロー制御）を使用します。 設定コマンドの正確な構文については、使用中のモデムのドキュメントを参照してください。

- **モデム速度の設定が固定されていない**アクセス サーバまたはルータで **show line exec** コマンドを使用します。 補助ポートの出力は、現在設定されている Tx および Rx の速度を示します。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。回線が正しい速度に設定されていない場合は、speed 回線設定コマンドを使用し、アクセス サーバまたはルータの回線の回線速度を設定します。 モデムと、アクセス サーバまたはルータのポートとの間で共通の最高速度に設定します。 端末のボー レートを設定するには、speed 回線設定コマンドを使用します。 このコマンドは、送信（端末へ）と受信（端末から）の両方の速度を設定します。構文：speed bps構文の説明：bps：ビット/秒（bps）でのボーレート。 デフォルトは 9600 bps です。例：次の例は、Cisco 2509 アクセス サーバの回線 1 および 2 を 115200 bps に設定します。

```
line 1 2
speed 115200
```

注: 何らかの理由でフロー制御を使用できない場合は、回線速度を 9600 bps に制限します。これ以上速い速度の場合、データが失われる可能性があります。再度 **show line exec** コマンドを使用し、回線速度が望ましい値に設定されたことを確認します。アクセス サーバまたはルータの回線が望ましい速度に設定されていることを確認したら、その回線を経由してモデムへのリバース Telnet セッションを開始します。 詳細については、16 章の「モデムへのリバース Telnet セッションの確立」のセクションを参照してください。使用しているモデム用の **lock DTE speed** コマンドを含むモデム コマンド文字列を使用します。 設定コマンドの正確な構文については、使用中のモデムのドキュメントを参照してください。**注: lock DTE speed** コマンドは、多くの場合、モデムによるエラー訂正の処理方法に関連して port rate adjust あるいは buffered mode と呼ばれることもあります。 このコマンドはモデムによって大きく異なります。モデム速度をロックすることにより、モデムは Cisco アクセス サーバまたはルータに対して、常に Cisco 補助ポートに設定された速度で通信します。 このコマンドを使用しない場合、モデムはデータ リンク（電話回線）の速度に戻ります。アクセス サーバに設定された速度では通信しません。

ダイヤルアップ セッションに「無意味な文字」が表示される場合

- **モデム速度の設定が固定されていない**アクセス サーバまたはルータで **show line exec** コマンドを使用します。 補助ポートの出力は、現在設定されている Tx および Rx の速度を示します。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。回線が正しい速度に設定されていない場合は、**speed** 回線設定コマンドを使用し、アクセス サーバまたはルータの回線の回線速度を設定します。 モデムと、アクセス サーバまたはルータのポートとの間で共通の最高速度に設定します。端末のボー レートを設定するには、**speed** 回線設定コマンドを使用します。 このコマンドは、送信（端末へ）と受信（端末から）の両方の速度を設定します。構文：**speed bps**構文の説明

：bps：ビット/秒（bps）でのボーレート。 デフォルトは 9600 bps です。例：次の例は、Cisco 2509 アクセス サーバの回線 1 および 2 を 115200 bps に設定します。line 1 2speed 115200**注:** 何らかの理由でフロー制御を使用できない場合は、回線速度を 9600 bps に制限します。 これ以上速い速度の場合、データが失われる可能性があります。再度 **show line exec** コマンドを使用し、回線速度が望ましい値に設定されたことを確認します。アクセス サーバまたはルータの回線が望ましい速度に設定されていることを確認したら、その回線を経由してモデムへのリバース Telnet セッションを開始します。 詳細については、16 章の「モデムへのリバース Telnet セッションの確立」のセクションを参照してください。使用しているモデム用の **lock DTE speed** コマンドを含むモデム コマンド文字列を使用します。 設定コマンドの正確な構文については、使用中のモデムのドキュメントを参照してください。**注: lock DTE speed** コマンドは、多くの場合、モデムによるエラー訂正の処理方法に関連して port rate adjust あるいは buffered mode と呼ばれることもあります。 このコマンドはモデムによって大きく異なります。モデム速度をロックすることにより、モデムは Cisco アクセス サーバまたはルータに対して、常に Cisco 補助ポートに設定された速度で通信します。 このコマンドを使用しない場合、モデムはデータ リンク（電話回線）の速度に戻ります。アクセス サーバに設定された速度では通信しません。

症状： リモート ダイヤルイン セッションが、別のユーザによって開始された既存のセッション内で開きます。 つまり、ログイン プロンプトを取得するのではなく、ダイヤルイン ユーザには別のユーザによって確立されたセッションが表示されます（たとえば UNIX のコマンド プロンプトであったり、テキスト エディタ セッションであったりします）。

ダイヤルアップ セッションが既存のセッションで開く場合

- **モデムが DCD に対して常にハイに設定されている**1 つの CD に対してだけ、DCD がハイになるようにモデムを再設定します。 通常は **&C1** モデム コマンド文字列を使用しますが、ご使用のモデムに対応する正確な構文については、モデムのマニュアルを参照してください。**no exec** 回線設定コマンドを使用して、モデムが接続されているアクセス サーバ回線を設定する必要がある場合があります。 **clear line** 特権 exec コマンドで回線をクリアし、モデムとのリバース Telnet セッションを開始して、DCD が CD に対してだけハイになるようにモデムを再設定します。disconnect と入力して Telnet セッションを終了し、exec 回線設定コマンドを使用してアクセス サーバ回線を再設定します。
- **アクセス サーバまたはルータでモデム制御がイネーブルになっていない**アクセス サーバまたはルータで **show line exec** コマンドを使用します。 補助ポートの出力の [Modem] カラムには **show inout** または **RIisCD** と表示されます。 これは、アクセス サーバまたはルータの回線でモデム制御がイネーブルになっていることを示します。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。**modem inout** 回線設定コマンドを使用して、回線をモデム制御用に設定します。 これで、アクセス サーバでモデム制御が有効になります。**注:** モデムの接続に問題があるときは、必ず **modem inout** コマンドを使用し、**modem dialin** コマンドは使用しないでください。 後者のコマンドでは、回線で着信コールを受け取ることだけしか許可しません。 発信コールは拒否されるため、モデムとの Telnet セッションを確立してモデムを設定できなくなります。**modem dialin** コマンドを有効にする場合は、必ずモデムが正常に機能していることを確認した上で行ってください。
- **ケーブル接続に誤りがある**モデムとアクセス サーバまたはルータ間のケーブル接続をチェックします。 モデムがロール型 RJ-45 ケーブルと MMOD DB-25 アダプタを通じてアクセス サーバまたはルータの補助ポートに接続されていることを確認します。 Cisco では RJ-45 ポートについて、このケーブル構成を推奨およびサポートしています。（これらのコネクタには通常「Modem」というラベルが 付いています。）RJ-45 ケーブルには、次の 2 つのタイプが

あります。 ストレート型とロール型です。 RJ-45 ケーブルの 2 つの端子を並べると、8 個の色付きのピンが双方の端子にあります 色の付いたピンの順番が両端で同一である場合には、そのケーブルはストレートです。 両端の色の順序が逆であれば、そのケーブルはロール型です。Cisco 2500/CS500 では、ロール型ケーブル（CAB-500RJ）が標準です。**show line** EXEC コマンドを使用してケーブル接続が正しいことを確認します。 show line コマンド出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。

ダイヤルアップ受信モデムが正常に接続解除しない場合

- **モデムが DTR を検出していない**Hangup DTR modem コマンド文字列を入力します。 このコマンドは、DTR 信号が受信されなくなったらキャリアをドロップするようにモデムに指示します。Hayes 互換モデムでは、一般に **&D3** 文字列を使用して、モデムで **Hangup DTR** を設定します。 このコマンドの正確な構文については、モデムのドキュメントを参照してください。
- **ルータまたはアクセス サーバでモデム制御が有効ではない**アクセス サーバまたはルータで **show line exec** コマンドを使用します。 補助ポートの出力の [Modem] カラムには **inout** または **RIisCD** と表示されます。 これは、アクセス サーバまたはルータの回線でモデム制御がイネーブルになっていることを示します。show line コマンドの出力の詳細については、15 章の「debug コマンドの使用方法」のセクションを参照してください。modem inout 回線設定コマンドを使用して、回線をモデム制御用に設定します。 これで、アクセス サーバでモデム制御が有効になります。**注:** モデムの接続に問題があるときは、必ず **modem inout** コマンドを使用し、**modem dialin** コマンドは使用しないでください。 後者のコマンドでは、回線で着信コールを受け取ることだけしか許可しません。 発信コールは拒否されるため、モデムとの Telnet セッションを確立してモデムを設定できなくなります。 **modem dialin** コマンドを有効にする場合は、必ずモデムが正常に機能していることを確認した上で行ってください。

発信コールのトラブルシューティング

着信コールのトラブルシューティングが下位層からアプローチを始めるのに対して、発信接続のトラブルシューティングは上位層からアプローチを始めます。 論理の全般的なフローに従って、次を確認します。

1. ダイヤルオンデマンド ルーティング（DDR）がコールを開始しましたか。（答えがはいの場合は、次の質問に進みます）。
2. 非同期モデムの場合、チャット スクリプトから期待されるコマンドが発行されましたか。
3. コールが PSTN の外部に達しましたか。
4. リモート エンドがコールに応答しましたか。
5. コールが完了しましたか。
6. データがリンクを通過していますか。
7. セッションが確立されましたか。（PPP または端末）

ダイヤラの動作の確認

ダイヤラがリモートの宛先にコールを発信しようとしているかどうかを調べるには、debug dialer events コマンドを使用します。 詳細については debug dialer packet を参照してください。ただし、debug dialer packet コマンドはリソースの消費が激しいため、ダイヤラ インターフェイスが

複数動作しているビジー状態のシステムでは使用しないでください。

次の行は IP パケットに対する debug dialer events の出力行で、DDR インターフェイスの名前と、パケットの送信元アドレスおよび宛先アドレスが列挙されています。

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

トラフィックによってダイヤルが開始されない場合、最も可能性のある理由として不適切な設定（対象トラフィックの定義、ダイヤラ インターフェイスの状態、またはルーティングのいずれか）が考えられます。

トラフィックによってダイヤル試行が開始されない場合

- **「対象トラフィック」の定義がない、または正しくない**show running-config コマンドを使用し、インターフェイスに **dialer-group** が設定されていること、および一致する番号で設定されたグローバル レベルの **dialer-list** が存在することを確認します。**dialer-list** コマンドが、プロトコル全体、またはアクセス リストに一致するトラフィックのどちらかを許可するように設定されていることを確認します。アクセス リストで、リンクを通過するパケットが「対象」として宣言されていることを確認します。 これをテストするには、該当するアクセス リストの番号を指定して特権 exec コマンド **debug ip packet [list number]** を使用すると便利です。 次に、リンクに対して ping を試すか、またはトラフィックを送信します。 対象トラフィック フィルタが正しく定義されていれば、パケットがデバッグ出力に表示されます。 このテストでデバッグ出力が表示されない場合は、アクセスリストとパケットが一致していません。
- **インターフェイスの状態**show interfaces [interface name] コマンドを使用し、インターフェイスが「アップ/アップ（スプーフィング）」状態にあることを確認します。インターフェイスが「スタンバイ」モードにあるルータのもう 1 つの（プライマリ）インターフェイスが、ダイヤラ インターフェイスをバックアップ インターフェイスとして使用するように設定されています。 また、プライマリ インターフェイスが「ダウン/ダウン」の状態ではありません。 ダイヤラ インターフェイスがスタンバイ モードから抜け出すためには「ダウン/ダウン」状態にあることが必要です。 さらに、プライマリ インターフェイスで **backup delay** を設定する必要があります。これが設定されていないと **backup interface** コマンドが実行されません。ダイヤラ インターフェイスが「スタンバイ」から「アップ/アップ（スプーフィング）」に変わることを確かめるには、通常、プライマリ インターフェイスからケーブルを抜き取る必要があります。 設定コマンド shutdown を使用してプライマリ インターフェイスをシャットダウンしただけでは、プライマリ インターフェイスは「ダウン/ダウン」にはならず、「管理上のダウン」になります。これらは同じではありません。加えて、プライマリ接続がフレームリレー経由の場合、フレームリレーの設定をポイントツーポイントのシリアル サブインターフェイスで行う必要があり、電話会社で「Active」ビットを渡している必要があります。この方法を「エンドツーエンド LMI」とも呼びます。インターフェイスが「administratively down」にあるダイヤラ インターフェイスに **shutdown** コマンドが設定されています。 Cisco ルータを初めてブートしたときは、どのルータ インターフェイスでもこの状態がデフォルトです。 これを解除するには、インターフェイス設定コマンド **no shutdown** を使用します。
- **ルーティングに誤りがある**exec コマンド show ip route [a.b.c.d]を、リモートルータのダイヤラ インターフェイスの a.b.c.d isthe *アドレス*発行しなさい。 リモート ルータで ip unnumbered を**使用している**場合は、ip unnumbered コマンドでリストされるインターフェイスのアドレスを使用します。出力には、ダイヤラ インターフェイスを経由したリモート アドレスへのルートが示されます。 ルートが存在しない場合は、show running-config の出力を

調べて、スタティック ルートまたはフローティング スタティック ルートがすでに設定されていることを確認します。ダイヤラ インターフェイス以外のインターフェイスを経由するルートが存在する場合は、DDR がバックアップとして使用されています。 ルータの設定を調べ、スタティック ルートまたはフローティング スタティック ルートがすでに設定されているかを確認します。 この場合にルーティングをテストするには、プライマリ接続を無効にし、show ip route [a.b.c.d] コマンドを実行して、適切なルートがルーティング テーブルに設定されていることを確認するのが最も確実な方法です。**注:** この操作をネットワークの稼働中に行うと、ダイヤル イベントがトリガーされることがあります。 この種のテストはあらかじめスケジューリングされたメンテナンス時に行うのが最適です。

コールの送信

ルーティングと対象トラフィック フィルタが正しければ、コールが開始されます。 これは **debug dialer events** を使用して確認できます。

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

ダイヤリング理由が表示されるにもかかわらず、ダイヤル試行がなされない場合、通常はダイヤラ マップまたはダイヤラ プロファイルの設定の誤りが原因です。

コールが発信しない場合

いくつかの考えられる問題と推奨される処理が、次にリストされています。

- **ダイヤラ マップの設定の誤り**show running-config コマンドを使用し、ダイヤリング インターフェイスに少なくとも 1 つの dialer map 文が設定されていて、この文がリモート サイトのプロトコル アドレスと送信先番号を指し示していることを確認します。
- **ダイヤラ プロファイルの設定の誤り**show running-config コマンドを使用し、Dialer インターフェイスに **dialer pool X コマンド**が設定されていて、対応する **dialer pool-member X** がルータのダイヤラ インターフェイスに設定されていることを確認します。 ダイヤラ プロファイルが正常に設定されていない場合、次のようなデバッグ メッセージが表示されることがあります。
  ```
  Dialer1: Can't place call, no dialer pool set
  ```
  dialer string が設定されていることを確認します。

非同期発信コール：チャット スクリプトの動作の確認

発信コールがモデム コールの場合、コールの処理を進めるためにチャット スクリプトを実行する必要があります。 ダイヤラ マップ ベース DDR の場合、チャット スクリプトはダイヤラ マップ コマンド内の modem-script パラメータによって起動されます。 DDR がダイヤラ プロファイル ベースの場合は、TTY 回線で設定されたコマンド script **dialer** によって行われます。 どちらを使用する場合も、ルータのグローバル コンフィギュレーション内に存在する次のようなチャット スクリプトを利用します。

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

いずれの場合でも、チャット スクリプトのアクティビティを表示するコマンドは **debug chat** です。 たとえば **dialer map または dialer string コマンド**内のダイヤル文字列（電話番号）が 5551212 であれば、デバッグ出力は次のようになります。

```
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
```

チャット スクリプトの問題は次の 3 つのカテゴリに分けられます。

- コンフィギュレーション エラー
- モデム障害
- 接続障害

チャット スクリプトの障害

次のリストに、debug chat から可能な出力と推奨される処理を示します。

- **no matching chat script found for [number]**チャット スクリプトがまだ設定されていません。チャット スクリプトを追加します。
- **終わるチャット スクリプト ダイヤルアウト時間を計られるステータス = 接続; remote host not responding**モデムがチャット スクリプトに応答していません。 モデムとの通信を確認します (16 章の表 16-2 を参照) 。
- **タイムアウト期待:** [CONNECT]原因 1： ローカル モデムが実際にコールを発信していません。 モデムへのリバース Telnet を実行してダイヤルを手動で開始し、モデムがコールを発信できることを確認します。原因 2： リモート モデムが応答していません。 通常の POTS 電話を使用してリモート モデムにダイヤリングし、動作をテストします。原因 3： ダイヤルしようとしている番号に誤りがあります。 手動でダイヤリングを行い、番号を確認します。 必要であれば設定を訂正します。原因 4： モデムの trainup に時間がかかりすぎているか、または TIMEOUT の値が小さすぎます。 ローカル モデムが外部の場合は、スピーカの音量を上げて trainup トーンが聞こえるかを確かめます。 trainup が不意に途切れる場合は、chat-script コマンド中の TIMEOUT の値を増やします。 TIMEOUT がすでに 60 秒以上である場合は、この章の「モデムの trainup」のセクションを参照してください。

ISDN 発信コール

BRI または PRI のいずれかで ISDN の障害が最初に疑われる場合は、常に show isdn status からの出力をチェックしてください。 ここで注意する重要な点は、レイヤ 1 が Active であり、レイヤ 2 が *MULTIPLE_FRAME_ESTABLISHED* の状態にあるということです。 この出力の解釈と修正の方法については、16 章の「show isdn status 出力の解釈」を参照してください。

ISDN 発信コールの場合、**debug isdn q931** および **debug isdn events** が最適なツールです。 幸い、発信コールのデバッグは着信コールのデバッグと非常によく似ています。 コールが成功すると通常は次のようになります。

```
*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
```

この理由種別は 2 つのことを示しています。

- 4 バイト値または 6 バイト値の第 2 バイトは、エンドツーエンドのコール パス内のどこから DISCONNECT または RELEASE_COMP を受信したかを示しています。 これを問題の特定に役立てることができます。
- 第 3 バイトおよび第 4 バイトは、障害の実際の理由を示しています。 それぞれの値の意味については、この後の各表を参照してください。

注: 次の出力は、通常は上位層プロトコルの障害を示しています。

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

PPP 認証の失敗が典型的な理由です。 接続障害が必ず ISDN の問題であると見なす前に、debug ppp negotiation および debug ppp authentication をオンにします。

原因コードのフィールド

表 17-9 は、次の形式でデバッグ コマンドに表示される ISDN 原因コードのフィールドを示したものです。

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

ISDN の原因コードのフィールド

フィールド	値説明
0x	これに続く値は 16 進数です。
y1	8--ITU-T 標準符号化
y2	0：ユーザ 1：ローカル ユーザにサービスを提供するプライベート ネットワーク 2：ローカル ユーザにサービスを提供するパブリック ネットワーク 3：中継ネットワーク 4：リモート ユーザにサービスを提供するパブリック ネットワーク 5：リモート ユーザにサービスを提供するプライベート ネットワーク 7：国際ネットワーク A--インターネットワーキング ポイント以降のネットワーク

z1	理由種別のクラス（上位側の 16 進数）。 取り得る値の詳細については、次の表を参照してください。
z2	理由種別の値（下位側の 16 進数）。 取り得る値の詳細については、次の表を参照してください。
a1	（オプション）診断フィールド。常に 8 です。
a2	（オプション）診断フィールド。次のいずれか 1 つの値をとります。 0：不明 1：永続的 2：一時的

ISDN 原因値

次の表は、原因コードの第 3 バイトおよび第 4 バイトである原因情報要素の理由種別について、最もよく見られるものをいくつか説明したものです。 ISDN コードおよび値の詳細については、『debug isdn q931 の接続解除原因コードについて』を参照してください。

16 進値	原因	説明
81	Unallocated (unassigned) number	ISDN 番号は正しい形式でスイッチに送信されました。 しかし、番号がどの宛先装置にも割り当てられていません。
90	正常なコール クリア	正常なコール クリアーが発生しました。
91	ユーザ ビジー	コールされたシステムが接続要求の確認応答をしましたが、B チャネルがすべて使用中のためコールを受け入れることができません。
92	ユーザ応答なし	宛先がコールに応答しないため接続を完了できません。
93	ユーザからの応答なし（ユーザ アラート）	宛先は接続要求に応答しますが、指示された時間内に接続を完了できません。 接続のリモート端末に問題があります。
95	コール拒否	宛先はコールを受け入れる余地がありますが、不明な理由のためコールを拒否しました。
9C	番号形式が不正	宛先アドレスが認識不可能な形式で表現されていたか、または宛先アドレスが不完全だったため、接続を確立できませんでした。
9F	正常、詳細不明	標準の原因が適用されないときの正常なイベントの発生を報告します。 操作は不要です。
A2	利用可能な回路/チャネルなし	コールを受け付けるために使用可能な適切なチャネルがないため、接続を確立できません。
A6	ネットワーク故障	ネットワークが正常に機能していない状態が一定時間以上続いたため、宛先に到

		達できません。 今すぐ再接続しようとしても成功する可能性はほとんどありません。
AC	リクエストされた回路/チャネルの利用不可	不明な理由のため、リモート装置が要求されたチャネルを提供できません。 一時的な問題である場合もあります。
B2	要求されたファシリティが未登録	リモート装置は、登録されている場合のみ、要求された補助サービスをサポートします。 多くの場合、これは長距離サービスへの参照です。
B9	ベアラ機能が無許可	ユーザはネットワークが提供する Bearer Capability を要求しましたが、ユーザにはその使用が許可されていません。 登録の問題である場合もあります。
D8	互換性のない宛先	ISDN 以外の装置への接続が試行されたことを示します。 たとえば、アナログ回線への接続試行などが考えられます。
E0	必須の情報要素が欠如	受信装置でメッセージを受信しましたが、必須情報要素の 1 つが含まれていませんでした。 通常は D チャネルのエラーが原因です。 このエラーがシステム的に発生する場合は、ISDN サービス プロバイダーに報告します。
E4	無効な情報要素コンテンツ	リモート装置でメッセージを受信しましたが、情報要素に無効な情報が含まれています。 通常は D チャネルのエラーが原因です。

CAS 発信コール

CAS の T1 または E1 と組み込みデジタル モデムを経由した発信コールの場合、トラブルシューティングの大半は他の DDR のトラブルシューティングと同様です。 PRI 回線を経由した組み込みモデムの発信コールの場合でも、同じことがいえます。 この方式によるコール発信でコールが失敗した場合には、コール発信に関与している独自の機能について特別なデバッグが必要になります。

他の DDR と同様に、コール試行が要求されたことを確認する必要があります。 これには debug dialer events を使用します。 「ダイヤラの動作の確認」を参照してください。

コールを発信するには、その前にモデムをコール用に割り当てておく必要があります。 このプロセスと以降のコールを確認するには、次のデバッグ コマンドを使用します。

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

注: debug cas コマンドは、AS5200 および AS5300 用に IOS バージョン 12.0(7)T で初めて導入されたものです。 これよりも前のバージョンの IOS では、システムレベルの設定コマンド service internal と exec コマンド modem-mgmt debug rbs を併用します。

デバッグのオン

```
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
```

デバッグのオフ

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

注: AS5800 でこれらの情報をデバッグするためには、トランク カードに接続する必要があります。 次の例は、FXS グラウンド スタート用に設定された、CAS T1 経由の通常の発信コールです。

```
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
```

他のシグナリング タイプの T1 および E1 におけるデバッグも同様です。

デバッグでこの時点にまで達した場合は、コール側および応答側のモデムの train と接続が完了し、より上位層のプロトコルがネゴシエートを開始できることを示しています。 モデムが発信コー

ル用に正しく割り当てられているにもかかわらず、この時点で接続が失敗する場合は、T1 を調べる必要があります。 T1 のトラブルシューティングの詳細については、15 章を参照してください。

PPP のトラブルシューティング

ダイヤル接続、ISDN、または非同期が正常に確立されたことがわかった時点で、PPP 部分のトラブルシューティングを始めます。

PPP ネゴシエーションのトラブルシューティングを行う際は、正常な PPP デバッグ シーケンスの状態をあらかじめ理解しておくことが重要です。 そのうえで、障害を起こした PPP のデバッグ セッションと、正常に完了する PPP デバッグ シーケンスとを比較すれば、時間や手間を省くことができます。

正常な PPP シーケンスの例を次に示します。 出力の各フィールドの詳細説明については、「PPP の LCP ネゴシエーションの詳細」を参照してください。

```
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
```

注: デバッグの表示形式はここに記載されているものと異なる場合があります。 この例は、IOS バージョン 11.2(8) で変更された新しい PPP デバッグ出力形式を示しています。 古いバージョンの IOS における PPP デバッグの例については、16 章を参照してください。

PPP の LCP ネゴシエーションの詳細

タイム	説明

スタンプ	
10:57:15.415	発信設定要求（O CONFREQ）。 NAS は発信 PPP 設定要求パケットをクライアントに送信します。
10:57:15.543	着信設定確認応答（I CONFACK）。 クライアントは Montecito の PPP 要求に対して確認応答します。
10:57:16.919	着信設定要求（I CONFREQ）。 クライアントはコールバック プロトコルのネゴシエートを要求します。
10:57:16.919	発信設定拒否（O CONFREJ）。 NAS はコールバック オプションを拒否します。
10:57:17.047	着信設定要求（I CONFREQ）。 クライアントは新しいオプション セットを要求します。 今度は Microsoft Callback は要求されていません。
10:57:17.047	発信設定確認応答（O CONFACK）。 NAS は新しいオプション セットを受け入れます。
10:57:17.047	PPP の LCP ネゴシエーションが正常に完了しました。 LCP の状態が「Open」になります。 双方が相手の設定要求（CONFREQ）に対して確認応答（CONFACK）を完了しました。
10:57:17.047 〜 10:57:17.191	PPP 認証が正常に完了しました。 LCP ネゴシエートの後、認証が始まります。 認証は、IP など、どのネットワーク プロトコルが送られるよりも先に行う必要があります。 双方は LCP の間、ネゴシエートした方式によって認証を行います。 Montecito は CHAP を使用してクライアントを認証しています。
10:57:20.551	状態は IP Control Protocol（IPCP）に対してオープンです。 IPCP ピア用のルートがネゴシエートされ、設定されます。この経路には IP アドレス 1.1.1.1 が割り当てられます。

リンク コントロール プロトコル

通常、LCP のネゴシエーションでは 2 種類の問題が発生します。

1 つは、一方のピアが設定要求を行ったときに他方のピアが確認応答できない、または確認応答しない、という問題です。 この症状は高い頻度で発生しますが、要求側が同じパラメータを要求し続けると問題になることがあります。 AUTHTYPE（「AuthProto」とも呼ばれます）をネゴシエートするときがその典型的な例です。 たとえば、アクセス サーバの多くは認証に対して CHAP だけを受け入れるように設定されています。 発信者が PAP 認証だけしか実行しないように設定されている場合、どちらか一方のピアが接続を解除するまで CONFREQ と CONFNAK が交換されます。

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

LCP におけるもう 1 つの問題では、次の例のように一方または双方のピアで発信 CONFREQ だけしか見えません。 これは通常、下位層での速度不一致と呼ばれる原因の結果として起こります。 この症状は非同期または ISDN のどちらかの DDR で発生します。

```
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
```

接続が非同期の場合は、ルータとそのモデムとの間での速度不一致が原因と考えられます。 通常、この症状はモデムの DTE 速度を TTY 回線の設定済み速度にロックすることに失敗した結果として起こります。 この問題は一方のピアに見られたり双方のピアに見られたりするため、両方のピアをチェックしてください。 詳細については、この章の「モデムがデータを送信または受信できない場合」を参照してください。

ISDN 経由の接続でこの症状が見られる場合は、一方のピアが 56K で接続していて他方が 64K で接続していることに問題がある可能性があります。 この状態になることはまれですが、発生する可能性はあります。 一方または双方のピア、あるいは電話会社に問題のある可能性があります。 それぞれのピアで debug isdn q931 を使用して SETUP メッセージを調べてください。 一方のピアから送信された Bearer Capability は、他方のピアで受信した SETUP メッセージ内にある Bearer Capability と一致します。 対処方法としては、インターフェイス レベル コマンドの dialer

map、または map-class で設定されているコマンド dialer isdn speed で、ダイヤリング速度を 56K または 64K に設定します。

```
*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
```

この症状が発生した場合は Cisco TAC に連絡してください。 TAC に連絡する前に、双方のピアで次の出力を収集します。

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

認証

PPP が失敗する理由として最もよく見られるのが、認証の失敗です。 ユーザ名およびパスワードの設定ミスや不一致があると、エラー メッセージがデバッグ出力に表示されます。

次の例は、ユーザ名 Goleta が NAS にダイヤルインするための権限を持っておらず、NAS でこのユーザのためのローカル ユーザ名が設定されていないことを示しています。 この問題を修正するには、username name password password コマンドを使用して、ユーザ名「Goleta」を NAS のローカルの AAA データベースに追加します。

```
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
```

次の例は、ユーザ名「Goleta」が NAS で設定されていることを示しています。 しかし、パスワードの比較には失敗しています。 この問題を修正するには、username name password password コマンドを使用して、Goleta 用の正しいログイン パスワードを指定します。

```
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
```

PAP 認証の詳細については、『PPP パスワード認証プロトコル（PAP）の設定とトラブルシューティング』を参照してください。

ネットワーク コントロール プロトコル

ピア同士が要求された認証の実行に成功すると、ネゴシエーションが NCP フェーズに移ります。 両方のピアが正しく設定されていれば、NCP のネゴシエーションは次の例のようになります。この例では、クライアント PC から NAS に対してダイヤルインとネゴシエートを行っています

。

```
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
```

PPP の NCP ネゴシエーションの詳細

タイムスタンプ	説明
21:35:04.190	発信設定要求（O CONFREQ）。 NAS は、自身の IP アドレスを収めた発信 PPP 設定要求パ

	ケットをピアに送信します。
21:35:04.282	着信 CONFREQ。 ピアは VJ ヘッダーの圧縮を実行するよう要求します。 これには、自身の IP アドレスのほか、プライマリおよびセカンダリの DNS サーバのアドレスも必要になります。
21:35:04.306	発信設定拒否（CONFREJ）。 VJ ヘッダーの圧縮は拒否されます。
21:35:04.330 までの 21:35:04.314	ピアは Compression Control Protocol をするために要求を送信 します; 全体のプロトコルは PROTREJ メッセージによって NAS によって拒否されます。 ピアは CCP の再試行を行うべきではなく、実際に再試行していません。
21:35:04.334	ピアは CONFACK によって NAS の IP アドレスの確認応答をします。
21:35:07.274	着信 CONFREQ。 ピアは VJ ヘッダーの圧縮は要求しなくなりましたが、自身の IP アドレスと、プライマリおよびセカンダリの DNS サーバのアドレスは引き続き必要です。
21:35:07.294	NAS は、ピアが必要としているアドレスと、プライマリおよびセカンダリの DNS サーバのアドレスを収めた CONFNAK を送信します。
21:35:07.426	ピアは NAS にアドレスを送り返します; アドレスがきちんと受け取られたことを確認する試み。
21:35:07.458	NAS は CONFACK によってアドレスの確認応答をします。
21:35:07.478	接続の双方の側で CONFACK が発行されたことにより、ネゴシエーションが完了します。 NAS のコマンド **show interfaces Async4 は**「IPCP を示します: 」開いて下さい。
21:35:07.490	リモート ピアへのホスト ルートが NAS のルーティング テーブルに設定されます。

ピア同士が複数のレイヤ 3 プロトコルを同時にネゴシエートする可能性もあります。 これは珍しいことではなく、たとえば IP と IPX が同時にネゴシエートされることがあります。 また、あるプロトコルのネゴシエートに成功しても他のプロトコルのネゴシエートに失敗する可能性もあります。

NCP のトラブルシューティング

通常、NCP のネゴシエーション中に発生する問題はすべて、ネゴシエートしている双方のピアの設定に原因を求めることができます。 NCP フェーズ中に PPP のネゴシエーションが失敗した場合は、次の手順を実行します。

1. インターフェイス プロトコル コンフィギュレーションの確認特権 exec コマンド show running-config の出力を調べます。 インターフェイスが、接続を経由して実行したいプロトコルをサポートするように設定されていることを確認します。
2. インターフェイス アドレスの確認問題のあるインターフェイスにアドレスが設定されてい

ることを確認します。 ip unnumbered [interface-name] または ipx ppp-client loopback [number] を使用する場合は、参照先のインターフェイスにアドレスが設定されていることを確認します。

3. クライアント アドレスのアベイラビリティの確認NAS が IP アドレスを発信者に発行することになっている場合は、そのアドレスが使用可能であることを確認します。 発信者に渡すべき IP アドレスは次のいずれかの方法で取得できます。インターフェイスでローカルに設定する方法。 コマンド **ピア デフォルト IP アドレス a.b.c.d.が**あるようにインターフェイス設定を、この方式 単一 発信者からの接続を許可する使用されるべきではないですしか async （ないグループ非同期）インターフェイスのようなインターフェイスで**実際に**確認して下さい。アドレス プールを NAS でローカルに設定する方法。 インターフェイスに peer default ip address pool [pool-name] コマンドが設定されている必要があります。 また、プールは ip local pool [pool-name] [first-address] [last-address] コマンドを使用してシステムレベルで定義する必要があります。 プールで定義するアドレスの範囲は、NAS が処理できる同時接続発信者の数に対応できるように、十分大きくします。DHCP サーバによる方法。 NAS インターフェイスに peer default ip address dhcp コマンドを設定する必要があります。 さらに、グローバル設定コマンド ip dhcp-server [address] を使用し、DHCP サーバを指し示すように NAS を設定します。AAA による方法。 認証に TACACS+ または RADIUS を使用している場合は、発信者が接続するたびに特定の IP アドレスをその発信者に渡すように、AAA サーバを設定できます。 詳細については 16 章を参照してください。
4. サーバ アドレス コンフィギュレーションの確認BOOTP 要求に対してドメインネーム サーバまたは Windows NT サーバの設定済みアドレスを返すために、グローバルレベル コマンド async-bootp dns-server [address] および async-bootp nbns-server [address] が設定されていることを確認します。**注:** async-bootp subnet-mask [mask] コマンドは NAS で設定できますが、NAS と PPP ダイヤルイン クライアント PC との間でサブネット マスクはネゴシエートされません。 ポイントツーポイント接続の性質上、クライアントは NAS の IP アドレス（IPCP のネゴシエーション中に学習したもの）をデフォルト ゲートウェイとして自動的に使用します。 このポイントツーポイント環境では、サブネット マスクは必要ありません。 PC は、宛先アドレスがローカル アドレスと一致しない場合、パケットをデフォルト ゲートウェイ（NAS）に転送する必要があることを認識しています。NAS には常に PPP リンク経由で到達します。

Cisco TAC チームへのお問い合せの前に

Cisco の Technical Assistance Center（TAC）に問い合せる前に、必ずこの章に目を通し、使用中のシステムでの問題に対して提示されている処置を実行してください。

また、次の情報を収集してその結果を文書化します。TAC チームはこれらの情報を問題解決の参考にすることができます。

すべての問題について、**show running-config** と **show version** の出力を収集します。 コンフィギュレーションに **service timestamps debug datetime msec** コマンドがあることを確認します。

DDR に関する問題の場合は、次の情報を収集します。

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

ISDN に関する問題の場合は、次の情報を収集します。

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

モデムに関する問題の場合は、次の情報を収集します。

- **show lines**
- **show line [x]**
- **show modem**（統合モデムが関与する場合）
- **show modem version**（統合モデムが関与する場合）
- **debug modem**
- debug modem csm（統合モデムが関与する場合）
- **debug chat**（DDR シナリオの場合）

T1 または PRI に関する問題の場合は、次の情報を収集します。

- **show controller t1**

関連情報

- T1/E1 トラブルシューティング ページ
- Cisco IOS ダイヤル ソリューション ガイド
- T1/E1 インターフェイスの監視と管理
- PPP ネゴシエーションのトラブルシューティング
- モデムのトラブルシューティング
- モデム デバッグ コマンド
- ISDN のトラブルシューティング
- T1 PRI に関するトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems