ダイヤルアップ技術：概要と説明

内容

概要
はじめに
表記法
前提条件
使用するコンポーネント
モデムの運用
modem autoconfigure コマンドの使用
モデムへのリバース Telnet セッションの確立
ロータリー グループの使用
show line 出力の解釈
モデムのパフォーマンス情報の収集
ISDN の運用
ISDN のコンポーネント
show isdn status 出力の解釈
ダイヤルオンデマンドルーティング：ダイヤルオンデマンド ルーティング：ダイヤラ インターフェイスの運用
ダイヤルのトリガー
ダイヤラ マップ
ダイヤラ プロファイル
PPP の運用
PPPネゴシエーションのフェーズ
代替の PPP 方式
PPP ネゴシエーションの例（注釈付き）
Cisco TAC チームへのお問い合せの前に
関連情報

概要

この章では、ダイヤルアップ ネットワークに使用するいくつかのテクノロジーを紹介および説明しています。いくつかの **show** コマンドについて設定のヒントや解釈を説明しています。これらのコマンドはネットワークの正常な運用を確認する際に便利です。トラブルシューティングの手順は、このドキュメントの範囲外です。トラブルシューティングの手順については、『*ダイヤルアップのトラブルシューティング*』というタイトルのドキュメントを参照してください。

はじめに

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。

前提条件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの内容は、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。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

モデムの運用

このセクションでは、Cisco ルータを使用したモデムのセットアップ、確認、および使用に関する問題について説明しています。

modem autoconfigure コマンドの使用

Cisco Internetwork Operating System（Cisco IOS）リリース 11.1 以降を使用している場合は、自動的にモデムと通信してモデムを設定するように Cisco ルータを設定できます。

次の手順に従ってルータを設定すると、ルータは自動的に、回線に接続されたモデムの種類の検出を試みてから、モデムを設定します。

1. ルータに接続されたモデムの種類を検出するには、**modem autoconfigure discovery** 回線設定コマンドを使用します。
2. モデムが正常に検出されたら、**modem autoconfigure type** ***modem-name*** **回線設定コマンドを使用してモデムを自動的に設定します。**

ルータにエントリがあるモデムのリストを表示する場合は、**show modemcap** ***modem-name*** **を使用します。show modemcap** コマンドから返されたモデムの値を変更する場合は、**modemcap edit** ***modem-name attribute value*** **回線設定コマンドを使用します。**

これらのコマンドの使用方法については、Cisco IOS のドキュメント『*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*』および『ダイヤル ソリューション コマンド リファレンス』を参照してください。

注：自動設定に*使用*されるmodemcap**エントリ**に&Wを入力しないでください。入力すると、modem autoconfigure が実行されるたびに NVRAM への再書き込みが行われるため、モデムが壊れます。

モデムへのリバース Telnet セッションの確立

Cisco IOS リリース 11.0 以前が稼働している場合は、診断またはモデムの初期設定を行うために、リバース Telnet セッションを確立して、Cisco デバイスと通信するようにモデムを設定する必

要があります。Data Terminal Equipment (DTE; データ端末装置) 側のモデム速度を口ックしている限り、モデムは常に指定した速度でアクセス サーバやルータと通信します。モデム速度の口ックについての情報は、表 16-5 を参照してください。リバース Telnet セッションを介してモデムにコマンドを発行する前に必ず Cisco デバイスの速度を設定していることを確認します。アクセス サーバやルータの速度の設定についても、表 16-5 を参照してください。

モデムをリバース Telnet セッションのために設定するには、回線設定コマンド **transport input telnet** を使用します。ロータリーグループを設定するには (この場合はポート1で)、回線設定コマンド**rotary 1を入力しま**す。これらのコマンドを回線設定の下に置くと、IOSは次の番号で始まるポート範囲で着信接続にIPリスナーを割を割りりり当当り当当てます。

2000	Telnet プロトコル
3,000	Telnet プロトコル、ロータリー付き
4000	ロー TCP プロトコル
5000	ロー TCP プロトコル、ロータリー付き
6000	Telnet プロトコル、バイナリ モード
7000	Telnet プロトコル、バイナリ モード、ロータリー付き
9000	Xremote プロトコル
10,000	XRemote プロトコル、ロータリー付き

モデムへのリバース Telnet セッションを開始するには、次の手順を実行します。

1. 端末からコマンド**telnet ip-address 20yy**を使用します。ここで、*ip-address*はシスコデバイス上のアクティブな接続インターフェイスのIPアドレスで、yyはモデムが接続されている回線番号です。たとえば、次のコマンドは、IPアドレスが192.169.53.52のCisco 2501ルータの補助ポートに接続します。**telnet 192.169.53.52 2001**。一般に、この種の Telnet コマンドは、対象となる IP アドレスに **ping** できる、ネットワーク上のすべての場所から発行できます。**注：ほとんどの**シスコルータでは、ポート01が補助ポートです。Ciscoアクセスサーバでは、補助ポートは最後のTTY +1です。たとえば、2511の補助ポートはポート17 (16 TTYポート+ 1) です。 補助ポート番号を探すには、常に **show line** exec コマンドを使用します。特に、2600 シリーズおよび 3600 シリーズでは、各種の非同期モジュール サイズに対応するため、連続しないポート番号が使用されています。
2. 接続が拒否される場合、指定したアドレスおよびポートにリスナーが存在しないか、またはだれかがすでにそのポートに接続している可能性があります。接続先のアドレスとポート番号を確認します。さらに、**modem inout** コマンドまたは **modem DTR-active** コマンドと、**transport input all** コマンドが、接続しようとしている回線の回線設定にあることも確認します。ロータリー機能を使用する場合は、回線設定に **rotary n コマンドがあることも確認します。ここで n はロータリー グループの番号です。**だれかがすでに接続しているかどうかを調べるには、ルータに Telnet して **show line *n* コマンドを使用します。**回線が使用中であることを示すアスタリスクを探します。CTS がハイで、DSR がハイでないことを確認します。ポート番号 n の現在のセッションを接続解除するには、**clear line *n* コマンドを使用します**。それでも接続が拒否される場合は、モデムによって Carrier Detect (CD; キャリア検知) が常時アサートされている可能性があります。モデムを回線から接続解除し、リバース Telnet セッションを確立してから、モデムを接続します。
3. Telnet 接続に成功したら、AT と入力して、モデムから OK の応答が返されることを確認します。
4. モデムが応答しない場合は、次の表を参照してください。

次の表 16-1 では、モデムとルータ間の接続性に関する問題の症状についての考えられる原因が概説されており、それらの問題のソリューションが説明されています。

表 16-1：モデムとルータ間が接続不能

考えられる原因	推奨される対策

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	1. 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** 出力の説明は、15 章の『debug コマンドの使用』を参照してください。
	2. **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。
	例：次の例は、着信および発信の両方のコールについて回線を設定する方法を示しています。
	`line 5`
	`modem inout`
	注：モデムの接続に問題がある場合は、**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、モデムとの Telnet セッションを確立してモデムを設定することができません。**modem dialin** コマンドを使用する場合は、必ずモデムが正常に機能していることを確認してから使用してください。

モデムの設定が誤っているか、またはセッションがハングしている可能性がある	**AT&FE1Q0** と入力して出荷時のデフォルトに戻し、モデムが文字をエコー バックして出力を返すように設定されていることを確認します。モデムのセッションはハングすることがあります。「**^U**」を使用して回線をクリアし、「**^Q**」を使用してフロー制御（XON）を開きます。 パリティ設定を確認します。
ケーブル接続に誤りがある	1. 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。） 2. **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** コマンド出力の説明は、15 章の『debug コマンドの使用』セクションを参照してください。
ハードウェアに問題がある	1. 正しいケーブル接続を行っていること、および、すべての接続が良好であることを確認します。 2. すべてのハードウェアについて損傷がないことをチェックします。ケーブル接続（配線の損傷）、アダプタ（ピンのゆるみ）、アクセス サーバ ポート、およびモデムについてチェックします。 3. ハードウェアに関するトラブルシューティングについての詳細は、3 章の『ハードウェアとブートの問題のトラブルシューティング』を参照してください。

ロータリー グループの使用

アプリケーションによっては、ユーザのグループが特定のルータ上のモデムを共有する必要がある場合があります。この種のアプリケーションとしては、Cisco Dialout Utility などがあります。基本的に、ユーザは使用可能なモデムに接続された 1 つのポートに接続します。非同期回線をロータリー グループに追加するには、単に **rotary *n* と入力します。ここで n は、非同期回線用設定のロータリー グループの番号です。**次の例を参照してください。

```
line 1 16
```

```
 modem InOut
 transport input all
 rotary 1
 speed 115200
 flowcontrol hardware
```

この回線設定によって、ユーザは **telnet 192.169.53.52 3001**（通常の Telnet の場合）と入力することで、ロータリー グループに接続できます。その他には、ロー TCP に対してポート 5001、バイナリ Telnet（Cisco Dialout Utility が使用）に対してポート 7001、Xremote 接続に対してポート 10001 などを使用できます。

注：Cisco Dialout Utilityの設定を確認するには、画面の右下にあるDialout Utilityアイコンをダブルクリックし、More>ボタンを押します。次に、Configure Ports> ボタンを押します。ロータリー グループを使用する場合は、ポートが 7000 の範囲内であることを確認します。Dialout Utility の対象が個別のモデムである場合は、ポートが 6000 の範囲内であることを確認します。また、PC でのモデムのロギングもイネーブルにしてください。これを行うには、次のシーケンスを選択します。[Start]-> [Control Panel]-> [Modems] **-> (Ciscoダイヤルアウトモデムを選択) – > [Properties] -> [Connection] -> [Advanced] ..->ログファイルを記録します。**

show line 出力の解釈

モデムからアクセス サーバやルータへの接続に関してトラブルシューティングを行う際に、**show line** *line-number* **exec コマンドからの出力が役立ちます。show line** コマンドからの出力を次に示します。

```
as5200-1#show line 1
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
   1 TTY 115200/115200-    -      -    -    -      0       0     0/0       -

Line 1, Location: "", Type: ""
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: No Exit Banner
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
Modem state: Hanging up
  modem(slot/port)=1/0, state=IDLE
  dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
Group codes:    0
Modem hardware state: CTS noDSR  noDTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: never
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed transports are lat pad telnet rlogin udptn v120 lapb-ta.
Preferred is l
```

```
at pad telnet rlogin udptn v120 lapb-ta.
No output characters are padded
No special data dispatching characters
as5200-1#
```

接続性の問題が発生すると、重要な出力が Modem State フィールドと Modem Hardware State フィールドに表示されます。

注：モデムハードウェア状態フィールドは、各プラットフォームの**show line出力に**表示されません。場合によっては、代わりに Modem State フィールドに信号状態が表示されます。

表 16-2 には、**show line** コマンドの出力から抜粋した Modem State および Modem Hardware State の典型的な文字列が示されています。さらに、それぞれの状態の意味についても説明されています。

表 16-2：show line 出力の Modem State および Modem Hardware State

Modem State（モデム状態）	**Modem Hardware State（モデムハードウェア状態）**	**意味**
Idle	CTS noDSR DTR	これらの出力は、アクセス サーバまたはルータとモデム間の接続に対してモデム状態が正常であることを示しています（着信コールがないとき）。 これ以外の出力は一般に問題があることを示しています。

	RTS	
Ready	-	モデム状態が Idle ではなく Ready の場合は次の点を調べてください。 1. アクセス サーバまたはルータでモデム制御が設定されていません。**modem inout** 回線設定コマンドで、アクセス サーバまたはルータを設定します。 2. 回線上にセッションが存在します。**show users** exec コマンドを使用し、必要であれば **clear line** 特権 exec コマンドを使用してセッションを停止します。 3. DSR がハイです。これには次の 2 つの理由が考えられます。 ケーブル接続に問題があります。コネクタで DB-25 ピン 6 を使用していてピン 8 がない場合は、ピンを 6 から 8 に移動するか、または適切なコネクタを入手する必要があります。モデムが、DCD に対して常にハイとなるように設定されています。1 つの CD (1) に対してだけ、DCD がハイになるようにモデムを再設定する必要があります。 通常は **&C1** モデム コマンドを使用しますが、使用しているモデムのための正確な構文についてはモデムのドキュメンテーションを参照してください。使用しているソフトウェアでモデム制御がサポートされていない場合は、**no exec** 回線設定コマンドで、モデムの接続先であるアクセス サーバ回線を設定する必要があります。**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 回線設定コマンドでアクセス サーバ回線を再設定します。
Ready	noCTS noDSR DTR RR	noCTS 文字列が Modem Hardware State フィールドに表示される場合、次の 4 つの理由のうちいずれか 1 つが考えられます。 1. モデムの電源がオフです。 2. モデムがアクセス サーバに正しく接続されていません。モデムからアクセス サーバへのケーブル接続をチェックします。 3. ケーブル接続が正しくありません (ロール型 MDCE かストレート型 MDTE、ただしピンの移動はなし)。 推奨されるケーブル接続設定については、この表の前述の説明

	TS(2)	を参照してください。 4. モデムがハードウェア フロー制御のために設定されていません。**no flowcontrol hardware** 回線設定コマンドを使用し、アクセス サーバでのハードウェア フロー制御をディセーブルにします。次に、リバースTelnetセッションを介してモデムのハードウェアフロー制御を有効にします。（モデムのマニュアルを参照し、この章の前半にある「モデムへのリバースTelnetセッションの確立」の項を参照してください）。**flowcontrol hardware** 回線設定コマンドで、アクセス サーバでのハードウェア フロー制御を再びイネーブルにします。
Ready	CTSDSRDTRRTS(2)	noDSR 文字列ではなく DSR 文字列が Modem Hardware State フィールドに表示される場合、次のどちらかの理由が考えられます。 1. ケーブル接続が正しくありません（ロール型 MDCE かストレート型 MDTE、ただしピンの移動はなし）。 推奨されるケーブル接続設定については、この表の前述の説明を参照してください。 2. モデムが、DCD に対して常にハイとして設定されています。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。通常は **&C1** モデム コマンドを使用しますが、使用しているモデムのための正確な構文についてはモデムのドキュメンテーションを参照してください。**no exec** 回線設定コマンドで、モデムの接続先であるアクセス サーバ回線を設定します。**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ます。exec 回線設定コマンドでアクセス サーバ回線を再設定します。
Ready	CTS*DSR*DTRR	この文字列が Modem Hardware State フィールドに表示される場合、おそらくアクセス サーバでモデム制御がイネーブルではありません。**modem inout** 回線設定コマンドを使用して、回線でのモデム制御をイネーブルにします。アクセス サーバまたはルータ回線でのモデム制御の設定については、この表の前述の説明を参照してください。

	TS(2)	

（1）CD = Carrier Detect（キャリア検知）

(2)信号の横の*は、次の2つのいずれかを示します。信号が過去数秒以内に変更されたか、選択したモデム制御方式によって使用されていません。

モデムのパフォーマンス情報の収集

このセクションでは、Cisco AS5x00 アクセス サーバ ファミリに見られる MICA デジタル モデムについて、そのパフォーマンス データを収集するための方法を説明しています。パフォーマンス データは傾向分析に使用できるほか、パフォーマンスに関する問題が発生した場合のトラブルシューティングに役立ちます。以降に示す数値を読むときには、現実の回線環境では、通常 100% の成功を実現するのは不可能であることを念頭においてください。モデムで達成される Call Success Rate（CSR; 接続成功率）は、回線の品質、クライアント モデム ユーザベース、および使用されている変調セットによって決まる相関的要素です。V.34 コールにおける典型的な CSR の割合は 95 % です。V.90 コールでは 92 % の接続成功率を期待できます。早期廃棄はほぼ 10 % の割合で発生します。

アクセス サーバでのモデム動作の概容を調べるには、次の各コマンドを使用します。

- **show modem**
- **show modem summary**
- **show modem connect-speeds**
- **show modem call-stats**

個々のモデム接続のトラブルシューティングを行うときや、傾向分析用のデータを収集するときは、次の情報が役立ちます。

- debug modem csm
- modem call-record terse
- show modem op（MICA）/AT@E1（Microcom）（接続中）
- show modem log（接続解除後の対象セッションのログ）
- ANI（発信者の番号）
- 時刻
- クライアント モデムのハードウェアまたはファームウェアのバージョン
- クライアントから得られる有益な情報（接続後）：ATI6、ATI11、AT&V、AT&V1 など
- クライアント モデムからのトレインアップ試行時のオーディオ記録（.wav ファイル）

以降の各セクションでは、コマンドの詳細といくつかの共通の傾向について説明しています。

show modem / show modem summary

show modem コマンドでは、個々のモデムに関する情報が表示されます。次の数値から、個々のモデムの状態を確認できます。

```
router# show modem
  Codes:
  * - Modem has an active call
  C - Call in setup
```

```
  T - Back-to-Back test in progress
  R - Modem is being Reset
  p - Download request is pending and modem cannot be used for taking calls
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down
  d - DSP software download is required for achieving K56flex connections
  ! - Upgrade request is pending
                Inc calls     Out calls     Busied   Failed  No       Succ
  Mdm  Usage    Succ   Fail   Succ   Fail   Out      Dial    Answer   Pct.
* 1/0    17%      74      3      0      0       0        0       0     96%
* 1/1    15%      80      4      0      0       0        1       1     95%
* 1/2    15%      82      0      0      0       0        0       0    100%
  1/3    21%      62      1      0      0       0        0       0     98%
  1/4    21%      49      5      0      0       0        0       0     90%
* 1/5    18%      65      3      0      0       0        0       0     95%
```

ルータにあるすべてのモデムの集計値を表示するには **show modem summary** コマンドを使用します。

```
router#show modem summary
         Incoming calls       Outgoing calls      Busied   Failed   No    Succ
Usage  Succ    Fail  Avail    Succ    Fail  Avail    Out      Dial     Ans   Pct.
   0%  6297     185     64       0       0      0        0        0     0     97%
```

表 16-3：show modem のフィールド

フィールド	説明
Incoming calls および Outgoing calls	モデムにダイヤルインしたコール数、およびモデムからダイヤルしたコール数 • Usage：すべてのモデムが使用中であるシステム稼働時間の合計の割合 • Succ：接続に成功したコール数の合計 • Fail：接続に成功しなかったコール数の合計 • Avail：システム内で使用可能なモデムの総数
Busied Out	モデムが **modem busy** コマンドまたは **modem shutdown** コマンドによってアウト オブ サービスにされた回数の合計
Failed Dial	モデムが接続解除しなかった試行、またはダイヤル トーンがまったくなかった試行の合計
No Ans	コール呼び出しが検出されたもののモデムによるコールへの応答がなかった回数の合計
Succ Pct.	使用可能なモデムの総数のうち接続に成功したものの割合

show modem call-stats の出力

```
compress  retrain lostCarr  rmtLink  trainup hostDrop wdogTimr inacTout
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
 Total    9       41      271     3277        7     2114        0        0
```

表 16-4：show modem call-stats のフィールド

rmtLink	エラー訂正が有効であり、リモート モデムに接続しているクライアント システムによってコールが接続解除されたことを示します。
hostDrop	IOS ホスト システムによってコールが接続解除されたことを示します。一般的な理由には次のものがあります。アイドルタイムアウト、電話会社からの回線クリア、またはクライアントからのPPP LCPtermreq。接続解除の原因を特定するには、modem call-record terse か AAA アカウンティングを使用するのが最適な方法です。

その他の接続解除理由が占める割合は、通常は全体の 10% 未満です。

show modem connect-speeds の出力

```
router>show modem connect 33600 0
 Mdm   26400  28000  28800  29333  30667  31200  32000  33333  33600 TotCnt
Tot      614      0   1053      0      0   1682      0      0    822   6304

router>show modem connect 56000 0
 Mdm   48000  49333  50000  50666  52000  53333  54000  54666  56000 TotCnt
Tot      178    308     68     97     86     16      0      0      0   6304
```

V.34 の速度の分布を確認します。T1 で Channel Associated Signaling (CAS; チャネル連携信号) を使用している場合は、26.4 にピークがあります。 ISDN(PRI)T1の場合、ピークは31.2である必要があります。また、いくつかのK56Flex、V.90速度を探します。V.90 接続がない場合、ネットワーク トポロジに問題がある可能性があります。

modem call-record terse (11.3AA/12.0T) コマンドについて

このコマンドは、exec コマンドというよりも、対象となるアクセス サーバのシステム レベルで発行する設定コマンドです。ユーザが接続を解除すると、次のようなメッセージが表示されます。

```
*May 31 18:11:09.558: %CALLRECORD-3-MICA_TERSE_CALL_REC: DS0 slot/contr/chan=2/0/18,
slot/port=1/29, call_id=378, userid=cisco, ip=0.0.0.0, calling=5205554099,
called=4085553932, std=V.90, prot=LAP-M, comp=V.42bis both,
init-rx/tx b-rate=26400/41333, finl-rx/tx brate=28800/41333, rbs=0, d-pad=6.0 dB,
retr=1, sq=4, snr=29, rx/tx chars=93501/94046, bad=5, rx/tx ec=1612/732, bad=0,
time=337, finl-state=Steady, disc(radius)=Lost Carrier/Lost Carrier,
disc(modem)=A220 Rx (line to host) data flushing - not OK/EC condition - locally
detected/received
DISC frame -- normal LAPM termination
```

show modem operational-status コマンド

exec コマンド **show modem operational-status** は、モデムの接続に関係のある現在のパラメータ（最新のパラメータ）を表示します。

このコマンドの項目が記載されているドキュメントは、『*Cisco IOS リリース 12.0 ダイヤル ソリューション コマンド リファレンス*』です。**show modem operational-status** は MICA モデム専用です。Microcomモデムの同等のコマンドは**modem at-mode / AT@E1**です。**modem at-mode <slot>/<port>コマンドを使用してモデムに接続し**て、**AT@E1**コマンドを発行します。**modem at-mode** コマンドについての詳細は『*Cisco AS5300 ソフトウェア コンフィギュレーション ガイド*』を、**AT@E1** コマンドについての詳細は『*Microcom のモデム モジュール用 AT コマンド セットとレジスタの要約のコマンド リファレンス*』を、それぞれ参照してください。

次の手順に従って、ユーザが着信しようとしているモデムを判別します。

1. **show user** コマンドを発行し、ユーザが接続している TTY を探します。
2. **show line** コマンドを使用し、モデムのスロット番号やポート番号を探します。

クライアント側のパフォーマンス データの収集

傾向分析のため、クライアント側のパフォーマンス データを収集することはたいへん重要です。次の情報を常に収集するように努めてください。

- クライアントのハードウェア モデルやファームウェアのバージョン（クライアントのモデムでコマンド **ATI3I7** を使用することにより取得可能）
- クライアントから報告される接続解除理由（**ATI6** または **AT&V1** を使用）

クライアント端末で使用できるその他の情報としては、PC の modemlog.txt および ppplog.txt もあります。これらのファイルを生成するには、PC で具体的に設定する必要があります。

パフォーマンス データの分析

モデム システムのパフォーマンス データの収集と分析が完了したら、改善の必要性のある残りのパターンやコンポーネントについて調べる必要があります。

特定のサーバ モデムに関する問題

show modem または **show modem call-stats** を使用し、トレインアップ障害率や不正接続解除率が異常に高いモデムを探します（MICA）。 モデムの隣接ペアに問題がある場合は、おそらく DSP がハングしているか、DSP からの応答がありません。復旧するには、該当する HMM に対して **copy flash modem** を使用します。モデムが最新バージョンのポートウェアで動作していることを確認してください。すべてのモデムが正常に設定されていることを確認するには、回線設定で設定コマンド **modem autoconfigure type mica/microcom_server** を使用します。コールが接続解除されるたびに必ずモデムが自動設定されるようにするには、exec コマンド **debug confmodem** を使用します。設定の誤ったモデムを修正するには、リバース Telnet セッションを確立する必要があります。

特定の DS0 に関する問題

DS0 に関する問題はまれにしか起こりませんが、起こる可能性はあります。正常に機能しない DS0 を見つけるには、**show controller t1 call-counters** コマンドを使用し、TotalCalls が異常に高く TotalDuration が異常に低い DS0 を探します。疑わしいDS0をターゲットにするには、T1のシリアルインターフェイスで設定コマンド**isdn service dsl, ds0 busyout**を使用して、他のDS0をビジーアウトする必要がある場合があります。**show controller t1 call-countersの出力は次のようになります。**

```
TimeSlot   Type   TotalCalls   TotalDuration
    1       pri         873       1w6d
    2       pri         753       2w2d
    3       pri         4444      00:05:22
```

この場合は、タイムスロット 3 が明らかに疑わしいチャネルです。

その他の共通の傾向

Cisco TAC で確認されている共通の傾向について、そのいくつかを次に示します。

1. 不正な回線パス次の問題が起きている場合、Public Switched Telephone Network（PSTN; 公衆電話交換網）を経由して不正な回線パスを取得している可能性があります。長距離電話に問題があるが、市内電話には問題がない（またはその逆）。ある特定の時間帯のコールに問題がある。特定のリモート交換機からのコールに問題がある。
2. 長距離電話に関する問題長距離電話が正しく機能しない、またはまったく機能しない（ただし市内サービスは正常である）場合は、次のように対処します。必ずデジタル回線からデジタル交換機に接続し、チャネルバンクには接続しない。長距離用に使用している回線パスについて電話会社に調査を依頼する。
3. 特定の通話エリアからのコールに関する問題特定の地域または交換機からのコールに問題が発生する傾向がある場合は、電話会社からネットワーク トポロジを入手する必要があります。アナログからデジタルへの変換が複数必要な場合、V.90/K56flex モデムは接続できません。また、V.34 は多少劣化する場合があります。非統合のデジタル交換機またはアナログ交換機によって稼働しているエリアでは、アナログからデジタルへの変換が必要です。

ISDN の運用

ISDN とは、端末ユーザが利用できる一連のデジタル サービスの集まりを指す言葉です。音声、データ、テキスト、グラフィックス、音楽、ビデオその他の素材データを、既存の電話回線を経由した単一のエンドユーザ端末から、端末ユーザに提供できるように、ISDN では電話ネットワークがデジタル化されます。ISDN の提案者は、現行の電話ネットワークとほとんど同様でありながら、デジタル送信と各種の新サービスを兼ね備えた世界的なネットワークを想定しています。

ISDN は、サブスクライバ サービス、ユーザ/ネットワーク インターフェイス、およびネットワーク機能とインターネットワーク機能の標準化を目指しています。サブスクライバ サービスの標準化では、一定レベルの国際的な互換性を確立しようとしています。ユーザ/ネットワーク インターフェイスの標準化では、サードパーティ製造業者によるこれらのインターフェイスの開発やマーケティングが促進されます。ネットワーク機能およびインターネットワーク機能の標準化では、ISDN ネットワーク同士の相互通信を容易にすることで、世界規模での接続性という目標の達成を目指します。

ISDN の応用例としては、高速なイメージ アプリケーション（Group IV FAX など）、在宅勤務産業のための家庭用電話回線の増設、高速なファイル転送、ビデオ会議などがあります。もちろん、音声も ISDN の一般的な応用例です。

ホーム アクセスの市場はさまざまなテクノロジーの間で分化する傾向にあります。DSL やケーブルなど比較的安価な新技術が利用できるようになった地域では、ISDN が家庭向け市場から姿を消そうとしています。しかしビジネスの分野では、大量のデータを転送したり、v.90 によるダイヤルイン アクセスを提供したりするために、PRI T1/E1 という形態で引き続き ISDN が利用されています。

ISDN のコンポーネント

ISDN のコンポーネントには、端末、ターミナル アダプタ（TA）、ネットワーク終端デバイス、回線終端装置、交換機終端装置があります。ISDN の端末は 2 種類に分けられます。ISDN 専用の端末のことを、Terminal Equipment type 1（TE1; 端末装置タイプ 1）と呼びます。 DTE など、ISDN 規格が登場する前にすでに存在していた非 ISDN 端末のことを、Terminal Equipment type 2（TE2; 端末装置タイプ 2）と呼びます。TE1 は 4 線のツイストペア デジタル リンクを通じて ISDN ネットワークに接続します。TE2 はターミナル アダプタを通じて ISDN ネットワークに接続します。ISDN TAは、スタンドアロンデバイスまたはTE2内部のボードのいずれかです。TE2がスタンドアロンデバイスとして実装されている場合、標準の物理層インターフェイスを介してTAに接続します。例として、EIA/TIA-232-C（旧 RS-232-C）、V.24、V.35 があります。

TE1 および TE2 のデバイスを越えて、ISDN ネットワークの次の接続点となるのが、Network Termination type 1（NT1; ネットワーク終端タイプ 1）デバイスまたは Network Termination type 2（NT2; ネットワーク終端タイプ 2）デバイスです。これらは、4 線のサブスクライバ配線から従来の 2 線ローカル ループに接続するネットワーク終端デバイスです。北アメリカでは、NT1 は Customer Premises Equipment（CPE; 顧客宅内機器）です。その他の地域では、NT1 は通信事業者が提供するネットワークの一部です。NT2 は NT1 よりも複雑なデバイスで、通常はデジタルの Private Branch Exchange（PBX; 構内交換機）に見られます。これらはレイヤ 2 および 3 のプロトコル機能および集中サービスを実行します。NT1/2デバイスも存在します。これは、NT1とNT2の機能を組み合わせた単一のデバイスです。

ISDN では多数のリファレンス ポイントが規定されています。これらのリファレンス ポイントは TA や NT1 といった機能グループ間の論理インターフェイスを定義します。ISDN のリファレンス ポイントには次のものがあります。

- R：非 ISDN 装置と TA 間のリファレンス ポイント。
- S：ユーザ端末と NT2 間のリファレンス ポイント。
- T：NT1 デバイスと NT2 デバイス間のリファレンス ポイント。
- U：NT1 デバイスと通信事業者ネットワーク内の回線終端装置との間のリファレンス ポイント。U リファレンス ポイントは北アメリカだけに関連するものです。北アメリカでは NT1 の機能が通信事業者ネットワークによって提供されていません。

ISDN の設定例を次に示します。この例では 3 台のデバイスがセントラル オフィスの ISDN 交換機に接続しています。うち 2 台のデバイスは ISDN 互換であり、S リファレンス ポイントを通じて NT2 デバイスに接続できます。3 台目のデバイス（標準の非 ISDN 電話）は R リファレンス ポイントを通じて TA に接続します。これらのデバイスは、NT1とNT2の両方を置き換えるNT1/2デバイスにも接続できます。表示されていませんが、同様のユーザステーションは右端のISDNスイッチに接続されています。

ISDN の設定例

```
2503B#show running-config
Building configuration...

Current configuration:
!
version 11.1
service timestamps debug datetime msec
service udp-small-servers
service tcp-small-servers
!
hostname 2503B
!
!
username 2503A password
ip subnet-zero
isdn switch-type basic-5ess
!
interface Ethernet0
 ip address 172.16.141.11 255.255.255.192
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 description phone#5553754
 ip address 172.16.20.2 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 300
 dialer map ip 172.16.20.1 name 2503A broadcast 5553759
 dialer-group 1
 ppp authentication chap
!
no ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
line vty 0 4
!
end

2503B#
```

ISDN のサービス

ISDN の Basic Rate Interface（BRI; 基本速度インターフェイス）サービスは、2 つの B チャネルと 1 つの D チャネル（2B+D）を提供します。BRI Bチャネルサービスは64 kbpsで動作し、ユーザデータの伝送を意図しています。BRI Dチャネルサービスは16 kbpsで動作し、制御およびシグナリング情報を伝送することを目的としていますが、特定の状況下ではユーザデータ伝送をサポートできます。D チャネルのシグナリング プロトコルはレイヤ 1 からレイヤ 3 までの OSI 参照モデルで構成されます。また、BRI はフレーム同期制御その他のオーバーヘッドも提供し、これによって総ビット レートが 192 kbps にまで増加します。BRI物理層仕様は、International Telecommunication Union Telecommunication Standardization Sector（ITU-T；国際電気通信連合電気通信標準化部門）です。(旧国際電信電話諮問委員会(CCITT))I.430

ISDN の Primary Rate Interface (PRI; 一次群速度インターフェイス) サービスは、北アメリカおよび日本において 23 の B チャネルと 1 つの D チャネルを提供し、1.544 Mbps の総ビット レートを実現しています (PRI の D チャネルは 64 kbps で運用されます)。ヨーロッパやオーストラリアその他の地域の ISDN PRI は、30 の B チャネルと 1 つの 64 kbps D チャネルを提供し、2.048 Mbps の総インターフェイス レートを実現しています。PRI の物理層の仕様は ITU-T の I.431 です。

レイヤ 1

ISDN 物理層 (レイヤ 1) のフレーム形式は、フレームが発信 (端末からネットワークへ) か着信 (ネットワークから端末へ) かによって異なります。 両方の物理層インターフェイスを図 16-1 に示します。

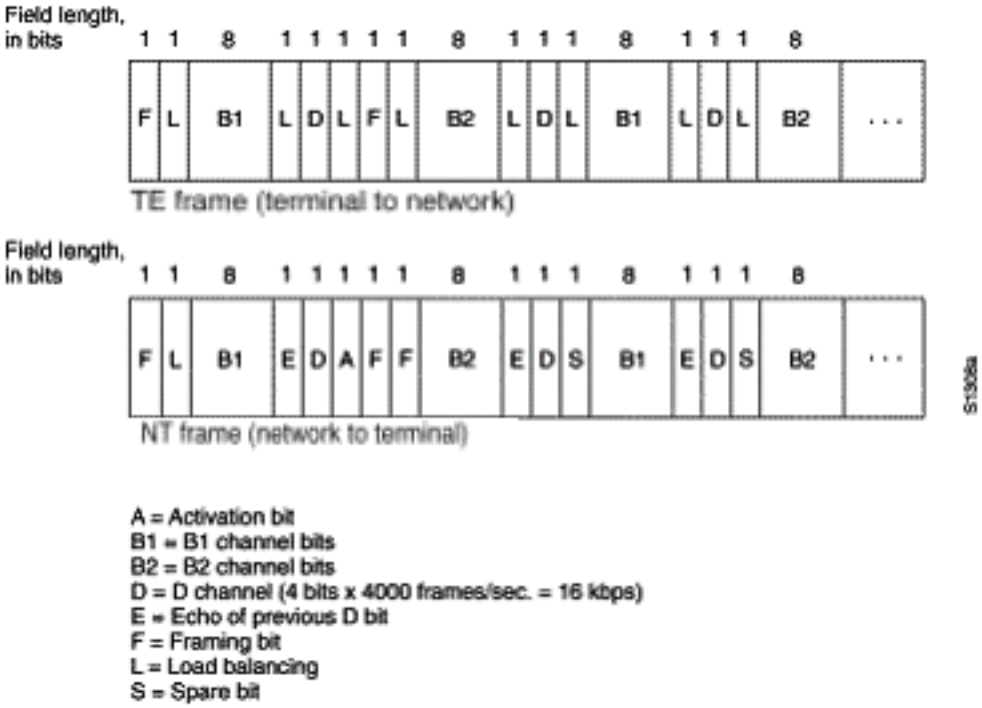

図 16-1：ISDN 物理層のフレーム形式

フレームは 48 ビット長で、そのうち 36 ビットがデータを表します。ISDN 物理層フレームの各ビットは次のように使用されます。

- F：同期の提供。
- L：平均ビット値の調整。
- E：受動バス上にある複数の端末でチャネルのコンテンションが起こったときにそれを解決するために使用。
- A：デバイスをアクティブにする。
- S：未割り当て。
- B1、B2、および D：ユーザ データ用。

複数の ISDN ユーザ デバイスを 1 つの回線に物理的に接続できます。この設定では、2 台の端末が同時に送信を行った場合にコリジョンが発生する可能性があります。そのため、ISDN ではリンクのコンテンションを判断するための機能が提供されています。NT が TE から D ビットを受信すると、NT はそのビットを次の E ビット位置にエコー バックします。TE では、次の E ビットが最後に送信された D ビットと同じであることを想定します。

複数の端末では、事前確立された優先順位に対応する特定数の端末（「信号なし」を示しているもの）を先に検出しない限り、D チャネルへの送信を行うことはできません。TE が エコー（E）チャネル内でビットを検出し、そのビットが D ビットと異なる場合、TE はただちに送信を停止する必要があります。この簡単な手続きによって、一度に 1 台の端末だけしか自身の D メッセージを送信できなくなります。D メッセージの送信に成功すると、端末は送信の前に、より連続性のある D メッセージの検出を求められ、それによって自身の優先順位が下がります。端末は、同じ回線上にある他のすべてのデバイスが D メッセージを送信する機会を得られるまで、自分の優先順位を上げることはできません。電話接続は他のすべてのサービスよりも優先され、シグナリング情報は非シグナリング情報よりも優先されます。

レイヤ 2

ISDN シグナリング プロトコルのレイヤ 2 は、Link Access Procedure on the D channel（LAPD; D チャネル用リンク アクセス手順）と呼ばれます。LAPD は High-Level Data Link Control（HDLC; ハイレベル データリンク制御）および Link Access Procedure, Balanced（LAPB; 平衡型リンク アクセス手順）によく似ています。 LAPD はその正式名称が示すように、D チャネルにおいて制御情報およびシグナリング情報のフローと受信を正しく行うために使用されます。LAPD のフレーム形式（図 16-2 を参照）は HDLC のものと非常によく似ており、また HDLC と同じように、監視用の情報と番号未指定制フレームを使用しています。LAPD プロトコルは ITU-T Q.920 および ITU-T Q.921 で正式に規定されています。

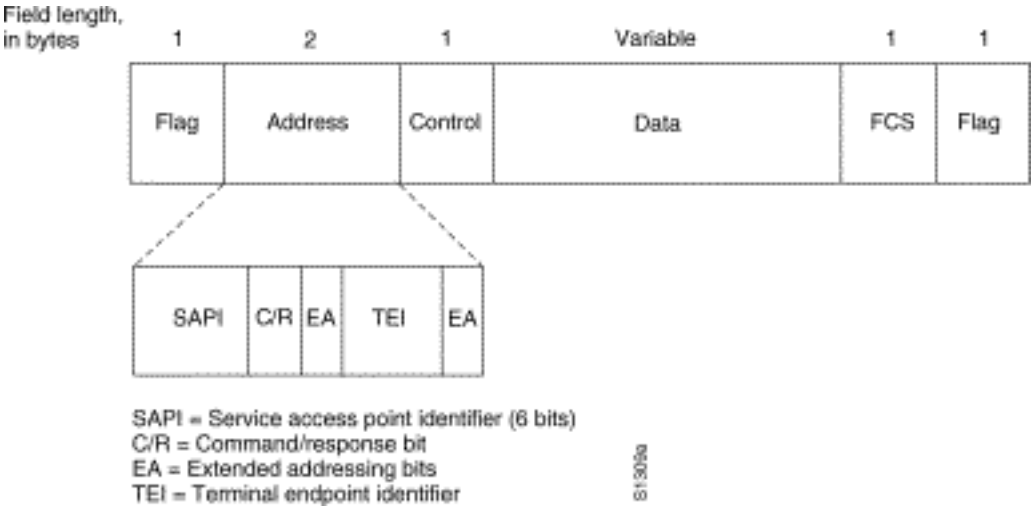

図 16-2：LAPD のフレーム形式

LAPD の Flag フィールドおよび Control フィールドは HDLC のものとまったく同じです。LAPD の Address フィールドは 1 バイト長か 2 バイト長のどちらかになります。最初のバイトの拡張アドレスビットが設定されている場合、アドレスは1バイトです。設定されていない場合、アドレスは2バイトです。最初のアドレスフィールドバイトには、LAPDサービスがレイヤ3に提供されるポータルを示すサービスアクセスポイント識別子(SAPI)が含まれます。C/Rビットは、フレームにコマンドが含まれているか応答が含まれているかを示します。Terminal Endpoint Identifier（TEI; ターミナル エンドポイント識別子）フィールドは、1 台の端末か複数台の端末かのどちらかを識別します。すべてが 1 の TEI はブロードキャストを示します。

レイヤ 3

ISDNシグナリングには、次の2つのレイヤ3仕様が使用されます。ITU-T（旧称 CCITT）I.450（ITU-T Q.930とも呼ばれる）およびITU-T I.451（別名ITU-T Q.931）。 これらのプロトコルは一体となって、ユーザツーユーザ、回線交換、およびパケット交換の各接続をサポートします。コールの確立、コールの終了、情報、その他といった各種のメッセージが規定され

ており、SETUP、CONNECT、RELEASE、USER INFORMATION、CANCEL、STATUS、DISCONNECT などがあります。

これらのメッセージは機能的には X.25 プロトコルで提供されているものと同じです（詳細は、19 章の『X.25 接続のトラブルシューティング』を参照してください）。 図 16-3 は ITU-T I.451 から抜粋したもので、ISDN 回線交換コールの典型的な各ステージを示しています。

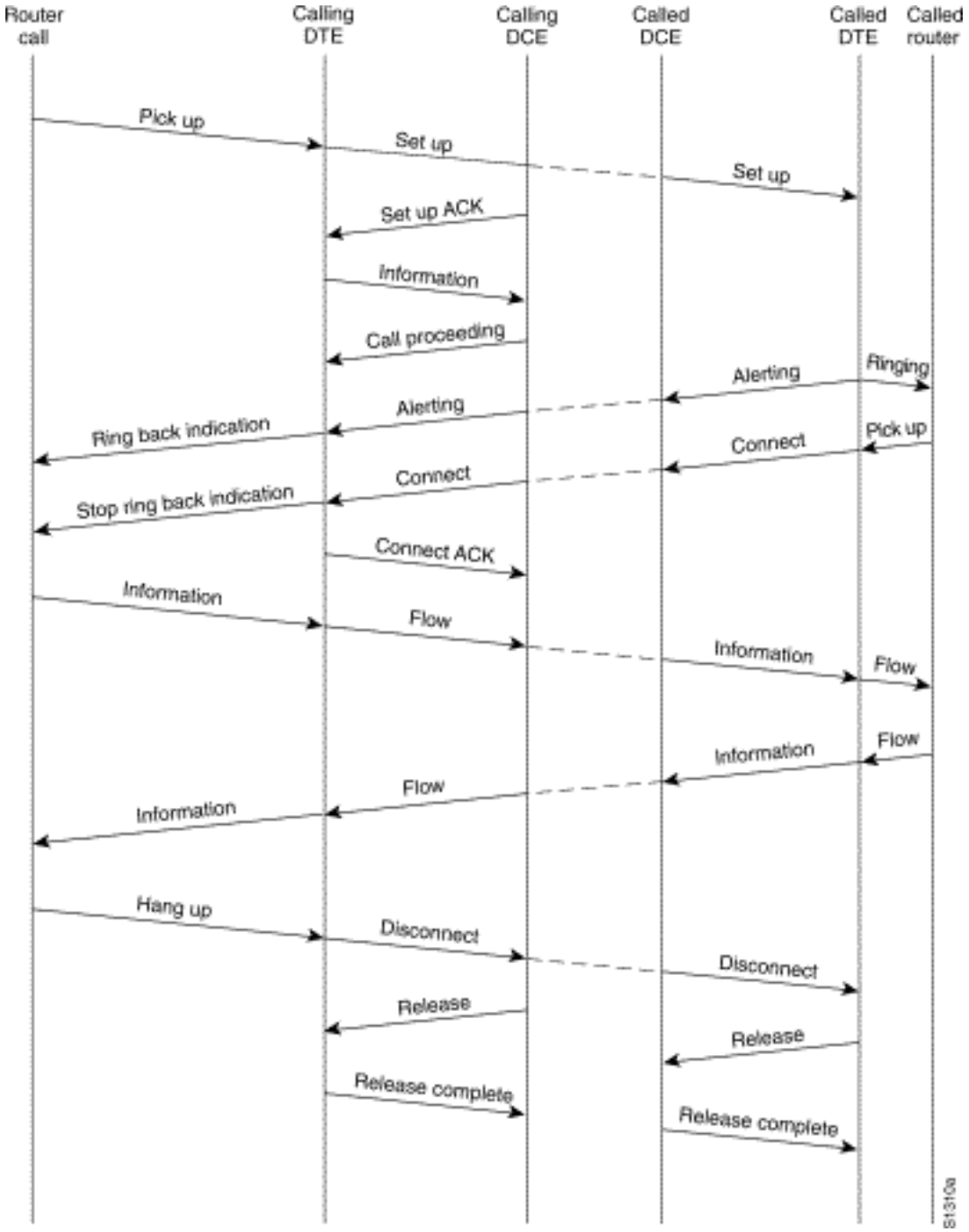

図 16-3 ISDN 回線交換コールの各ステージ

show isdn status 出力の解釈

ルータと電話会社の交換機との間における ISDN 接続について、その現在の状態を調べるには、**show isdn status** コマンドを使用します。このコマンドでサポートされている 2 種類のインターフェイスは BRI と PRI です。

```
3620-2#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
        dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 88, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI = 97, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
        TEI 88, ces = 1, state = 5(init)
            spid1 configured, no LDN, spid1 sent, spid1 valid
            Endpoint ID Info: epsf = 0, usid = 0, tid = 1
        TEI 97, ces = 2, state = 5(init)
            spid2 configured, no LDN, spid2 sent, spid2 valid
            Endpoint ID Info: epsf = 0, usid = 1, tid = 1
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000003
```

表 16-5：BRI の場合の show isdn status

フィールド	意味
レイヤ 1 ステータス：DEACTIVATED	BRI インターフェイスが回線上の信号を検知していないことを示します。この状態の理由としては次の 5 つが考えられます。 • BRI インターフェイスが停止している。設定を調べ、BRI インターフェイスに **shutdown** コマンドが指定されていないかをチェックします。または、**show interface** コマンドの出力から、「administratively down」の状態を示しているものがないか調べます。コンフィギュレーション ユーティリティを使用し、BRI インターフェイスに **no shutdown** を入力します。exec プロンプトで **clear interface bri** コマンドを入力し、BRI インターフェイスが再起動することを確認します。 • ケーブル接続に問題がある。ケーブルを交換する必要があります。必ずストレート型 RJ-45 ケーブルを使用します。ケーブルを調べるには、RJ-45 ケーブルの両端を並べて比べます。ピンが同じ順序で並んでいればケーブルはストレート型です。ピンの順序が逆であればケーブルはロール型です。ケーブルを交換します。 • ルータの ISDN BRI ポートで NT1 デバイスが必要な場合がある。ISDN では、NT1 は顧客宅内機器とセントラル オフィスの交換機器との間のインターフェイスを提供するデバイスです。ルータに内部 NT1 がない場合は

	、NT1 を入手して BRI ポートに接続します。BRIまたはターミナルアダプタがNT1のS/Tポートに接続されていることを確認します。外部NT1の正しい動作を確認するには、製造元のマニュアルを参照してください。 • 回線が正しく機能していない可能性がある。通信事業者に連絡し、接続の運用方法と switchtype の設定を確認します。 • ルータが正しく機能しているか確認する。ハードウェアが障害や誤作動を起こしている場合は、必要に応じて交換します。

Layer 2 Status：State = TEI_ASSIGNED	必要に応じて switchtype の設定と SPIDS をチェックします (SPIDS は日本国内では使用されません)。インターフェイス固有の ISDN 交換機設定により、グローバルの交換機設定は無効にされます。SPID ステータスは、交換機が SPIDS を受け入れたかどうかを示します (有効または無効)。 サービス プロバイダーに連絡してルータの設定を確認します。SPIDの設定を変更するには、**isdn *spidn***インターフ**エイスコンフィギュレーションコ**マンドを使用します。ここで、**n *は対象となるチャネルに応じて 1 または 2 のどちらかになります。*** 指定の SPID を削除するには、このコマンドの **no** 形式を使用します。
	`isdn spidn spid-number [ldn]`
	`no isdn spidn spid-number [ldn]`
	構文の説明：
	`spid-number`
	登録先のサービスを識別する番号。この値は ISDN サービス プロバイダーから割り当てられるもので、通常は 10 桁の電話番号に追加の桁が付いています。
	`ldn`
	(オプション) Local Directory Number (LDN; 市内電話番号)。サービス プロバイダーから割り当てられる 7 桁の番号です。着信セットアップ メッセージ内の交換機がこの情報を提供します。市内電話を含めない場合、交換機へのアクセスは許可されますが、他の B チャネルで着信コールを受信できない場合があります。スイッチとルータの間のレイヤ2ネゴシエーションを表示するには、特権execコマンド**debug isdn q921**を使用します。q921デバッグについては、『*Debugコマンドリファレンス*』を参照してください。デバッグでは CPU リソースが大量に占有されるため、使用の際は注意してください。

```
5200-1# show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
```

```
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
    Total Allocated ISDN CCBs = 0
5200-1#
```

show isdn status コマンドが動作しない場合、または PRI が表示されない場合は、**show isdn service** コマンドを使用します。設定で、T1/E1 コントローラに **pri-group** コマンドが指定されていることを確認します。このコマンドが表示されない場合は、**pri-group** コマンドでコントローラを設定します。

チャネライズド T1/PRI コントローラを持つ Cisco ルータの設定例を次に示します。

```
controller t1 0
framing esf
line code b8zs
pri-group timeslots 1-24
```

表 16-6：PRI での show isdn status

フィールド	意味
レイヤ 1 ステータス ：DEACTIVATED	PRI インターフェイスが回線上の T1/E1 フレーム同期を検知していないことを示します。この状態の理由としては次のことが考えられます。 • PRI インターフェイスが停止している。設定を調べ、serial0:23 インターフェイスに **shutdown** コマンドが指定されていないかをチェックします。または、**show interface** コマンドの出力から、「administratively down」の状態を示しているものがないか調べます。コンフィギュレーション ユーティリティを使用し、対象のインターフェイスにコマンド **no shutdown** を入力します。execプロンプトで**コマンド clear controller T1/E1 nを入力**し、PRIインターフェイスが再起動していることを確認します。 • ケーブル接続に問題がある。ケーブルを交換する必要があります。必ずストレート型 RJ-45 ケーブルを使用します。ケーブルを調べるには、RJ-45 ケーブル

	の両端を並べて比べます。ピンが同じ順序で並んでいればケーブルはストレート型です。ピンの順序が逆であればケーブルはロール型です。ケーブルを交換します。 • 回線が正しく機能していない可能性がある。通信事業者に連絡し、接続の運用方法と switchtype の設定を確認します。 • ルータが正しく機能しているか確認する。ハードウェアが障害や誤作動を起こしている場合は、必要に応じて交換します。
Layer 2 Status：State = TEI_ASSIGNED	switchtype の設定をチェックします。インターフェイス固有の ISDN 交換機設定により、グローバルの交換機設定は無効にされます。T1/E1 がプロバイダーの交換機と一致するように設定されていることを確認します（T1/E1 に関する問題については 15 章を参照してください）。 スイッチとルータの間のレイヤ2ネゴシエーションを表示するには、特権execコマンド**debug isdn q921**を使用します。q921デバッグについては、『*Debugコマンドリファレンス*』を参照してください。デバッグでは CPU リソースが大量に占有されるため、使用の際は注意してください。
使用中のコール数/コール制御ブロック数/割り当てられたISDNコール制御ブロックの総数	これらの数値は、処理中のコールの数と、これらのコールをサポートするために割り当てられたリソースの数を示します。割り当てられた CCB の数が使用中の CCB の数よりも大きい場合は、CCB の解放に問題があると考えられます。着信コール用に使用可能な CCB があることを確認します。

ダイヤルオンデマンドルーティング：ダイヤルオンデマンド ルーティング：ダイヤラ インターフェイスの運用

Dial on Demand Routing（DDR; ダイヤルオンデマンド ルーティング）は、WAN の接続性を必要なときだけ、プライマリ リンクとして、あるいは非ダイヤルのシリアルリンクのバックアップとして提供する経済的な手段です。

ダイヤラ インターフェイスは、コールの発着信機能がある任意のルータ インターフェイスとして

定義されます。この一般的な用語と、（D が大文字表記になっている実際の）**Dialer インターフェイス**という用語とは区別が必要です。後者は、ルータの 1 つまたは複数の物理インターフェイスを制御するように設定された論理インターフェイスを指し、ルータ コンフィギュレーションでは interface Dialer X と表記されます。これ以降、特に断りがない限り、「ダイヤラ」という用語を一般的な意味で使用します。

ダイヤラインターフェイスの設定には、次の2種類があります。ダイヤラマップベース（レガシー DDRとも呼ばれる）、ダイヤラプロファイル。どちらの方式を使用するかは、ダイヤル接続を必要とする状況によって異なります。ダイヤラ マップ ベースの DDR は IOS バージョン 9.0 で、ダイヤラ プロファイルは IOS バージョン 11.2 で、それぞれ初めて導入されたものです。

ダイヤルのトリガー

DDR は、実際にはルーティングの単なる拡張であり、*対象パケット*がダイヤラ インターフェイスにルーティングされて、ダイヤル発信がトリガーされます。以降の各セクションでは、対象トラフィックの定義に伴う概念と、DDR 接続に使用されるルーティングについて説明しています。

対象パケット

*対象*とは、ダイヤル発信をトリガーするか、またはダイヤル リンクがすでにアクティブな場合にはダイヤラ インターフェイス上のアイドル タイマーをリセットする、パケットやトラフィックを表すための言葉です。パケットが対象と見なされるためには、次の条件を満たす必要があります。

- パケットが、アクセス リストで定義されている「許可」基準を満たしている。
- アクセス リストがダイヤラ リストから参照されているか、またはパケットがダイヤラ リストによって一様に許可されているプロトコルのものである。
- ダイヤラ グループを使用することによって、ダイヤラ リストがダイヤラ インターフェイスと関連付けられている。

パケットが自動的に（デフォルトで）対象と見なされることは決してありません。 対象パケットの定義は、ルータまたはアクセス サーバの設定の中で明示的に宣言する必要があります。

ダイヤラ グループ

ルータやアクセス サーバの各ダイヤラ インターフェイスの設定には、必ず **dialer-group** コマンドがあります。**dialer-group** コマンドがない場合、対象パケットの定義とインターフェイスとが論理的にリンクされていません。コマンドの構文を次に示します。

```
dialer-group [group number]
```

group number は、特定のインターフェイスが属するダイヤラ アクセス グループの番号です。このアクセス グループは **dialer-list** コマンドで定義します。許容される値は、1 ~ 10 の正の整数です。0 は許容されません。

インターフェイスは、単一のダイヤラアクセスグループにのみ関連付けることができます。複数のダイヤラグループ割り当ては許可されません。2 つ目のダイヤラ アクセス グループの関連付けを行うと、1 つ目は無効になります。ダイヤラ アクセス グループは **dialer-group** コマンドで定義されます。**dialer-list** コマンドは、アクセス リストをダイヤラ アクセス グループに関連付けます。

指定したダイヤラ グループに一致するパケットによって、接続要求がトリガーされます。

パケットの宛先アドレスは、関連する **dialer-list** コマンドの中で指定されたアクセス リストで評価されます。一致するものがあれば、コールが開始されるか（接続がまだ確立されていない場合）、またはアイドル タイマーがリセットされます（コールが現在接続中の場合）。

ダイヤラ リスト

dialer-list グローバル設定コマンドは、DDR ダイヤラ リストを定義して、ダイヤリングをプロトコル別に、またはプロトコルとアクセス リストとの組み合せ別に制御するために使用されます。対象パケットは、プロトコルレベルの許可に一致するパケット、または次の **dialer-list** コマンド内のリストで許可されたパケットです。**dialer-list dialer-group protocol protocol-name {permit | deny | list** *access-list-number* **| access-group}**

dialer-group ***は、任意の dialer-group インターフェイス設定コマンドの中で識別されるダイヤラ アクセス グループの番号です。***

*protocol-nameは、次*のプロトコルキーワードの1つです。appletalk、bridge、clns、clns_es、clns_is、decnet、decnet_router-L1、decnet_router-L2、decnet_node、ip、ipx、vines、または xns。

permit は、プロトコル全体へのアクセスを許可します。

deny は、プロトコル全体へのアクセスを拒否します。

list は、プロトコル全体よりも細かく定義するためにアクセス リストを使用することを指定します。

access-list-number ***は DECnet、Banyan VINES、IP、Novell IPX、または XNS の標準アクセス リストまたは拡張アクセス リストで指定されるアクセス リスト番号です。これには、Novell IPX 拡張 Service Access Point（SAP; サービス アクセス ポイント）のアクセス リストとブリッジング タイプも含まれます。***サポートされているアクセス リストの種類と番号については表 16-7 を参照してください。

access-group ***は、clns filter-set コマンドおよび clns access-group コマンドで使用するフィルタ リスト名です。***

表 16-7：プロトコル別のアクセス リスト番号範囲

アクセス リストの種類	**アクセス リスト番号範囲（10 進数）**
AppleTalk	600-699
Banyan VINES（標準）	1-100
Banyan VINES（拡張）	101-200
DECnet	300-399
IP（標準）	1-99
IP（拡張）	100-199
Novell IPX（標準）	800-899
Novell IPX（拡張）	900-999
トランスペアレント ブリッ	200-299

ジング	
XNS	500-599

Access List

ダイヤル接続を介して送信されるネットワーキング プロトコルごとに、アクセス リストを設定できます。一般には、コストを管理するために、アクセス リストを設定することで、ルーティング更新などの特定のトラフィックによって接続が開始または維持されるのを防ぐことが望まれます。対象および非対象のトラフィックを定義する目的でアクセス リストを作成するときに、「非対象パケットはダイヤル リンクを通過できない」とは宣言していないことに注意します。アクセス リストでは単に、アイドル タイマーをリセットしないこと、および接続を独自に開始しないことを指定するだけです。ダイヤル接続がアップ状態である限り、リンクを経由した非対象パケットのフローは従来どおり許可されます。

たとえば、EIGRP がルーティング プロトコルとして実行されているルータで、EIGRP パケットを非対象と宣言し、他のすべての IP トラフィックを対象として宣言するアクセス リストを設定できます。

```
access-list 101 deny eigrp any any
access-list 101 permit ip any any
```

アクセス リストは、ダイヤル リンクを通過する可能性のあるすべてのプロトコルについて設定できます。どのプロトコルにおいても、**access-list permit** 文がない場合でのデフォルト動作では、すべてのトラフィックが拒否されることに注意してください。アクセス リストが存在せず、プロトコルを許可する **dialer-list** コマンドがなければ、そのプロトコルは非対象になります。実際には、プロトコルに対応するダイヤラ リストがなければ、これらのパケットはリンクを通過しません。

すべてをまとめて設定する場合の設定例

すべての要素を適切に設定することで、パケットの「対象」ステータスを決める詳細なプロセスを調べることができます。この例では、IP および IPX が、ダイヤル リンクの通過を許可されるプロトコルです。ユーザは、ブロードキャストやルーティング更新によってコールが開始されたりリンクが維持されたりするのを防ごうとしています。

```
!
interface async 1
 dialer-group 7
!
access-list 121 deny eigrp any any
access-list 121 deny ip any host 255.255.255.255
access-list 121 permit ip any any
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 903 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 903 permit -1
!
dialer-list 7 protocol ip list 121
dialer-list 7 protocol ipx list 903
!
```

パケットが**対象**と見なされるには、**interface async 1** を通過する前に、*access-list 121* 文によっ

てパケットが許可されている必要があります。この例では、EIGRP パケットは拒否され、同様に他のすべてのブロードキャスト パケットも拒否されます。一方、その他の IP トラフィックはすべて許可されます。これは EIGRP パケットのリンクの通過を妨げないことに注意します。「これらのパケットによってアイドル タイマーがリセットされたり、ダイヤル試行が開始されたりしない」という意味にすぎません。

同様に、**access-list 903** では、IPX RIP、SAP、および GNS の各要求を非対象と宣言し、同時に他のすべての IPX トラフィックを対象として宣言しています。これらの拒否文がなければ、ダイヤル接続がほとんどダウンしません。IPX ネットワークではこれらの種類のパケットが絶えず流れているため、非常に高額な電話料金が請求されます。

非同期インターフェイスで **dialer-group 7** を設定しているため、対象トラフィック フィルタ (つまりアクセス リスト) をインターフェイスに結合するために **dialer-list 7** を必要とすることがわかります。**dialer-list** 文はプロトコルごとに 1 つ必要であり、かつ *1 つだけしか設定できません。これにより、ダイヤラ リスト番号がインターフェイスのダイヤラ グループ番号と同じになります*。

繰り返しますが、対象トラフィックの定義のために設定したアクセス リストの中で **deny 文を使用しても、拒否されたパケットのリンクの通過は妨げられません。**

debug dialer コマンドを使用すると、ダイヤル試行をトリガーするアクティビティを確認できます。

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

この例では、送信元アドレスが 172.16.1.111 で宛先アドレスが 172.16.2.22 の IP トラフィックによって、インターフェイス Async1 でダイヤル試行がトリガーされたことがわかります。

ルーティング

定義された対象パケットは、コールを開始するために正しくルーティングする必要があります。ルーティングプロセスは、次の2つの点に依存します。ルーティングテーブルエントリと、パケットをルーティングする「up」インターフェイス。

インターフェイス : アップ/アップ (スプーフィング)

パケットをインターフェイスにルーティングするか、またはインターフェイス経由でルーティングするためには、次の **show interfaces** の出力に見られるように、そのインターフェイスがアップ/アップの状態である必要があります。

```
Montecito# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is . . .
```

接続されていないダイヤラ インターフェイスではどんな動作になるのでしょうか。プロトコルがインターフェイスで動作していない場合は、自動的に「インターフェイス自身がアップ状態ではない」と見なされます。このインターフェイスに依存しているルートはルーティング テーブルからフラッシュされ、トラフィックはそのインターフェイスにルーティングされなくなります。この結果、インターフェイスによってコールが開始されません。

この可能性を回避するソリューションは、ダイヤラ インターフェイスに対して**アップ/アップ (スプーフィング)** という状態を許可します。インターフェイスはどれもダイヤラ インターフェイスとして設定できます。たとえば、Serial または Async のインターフェイスでも、**dialer in-band** コマンドまたは **dialer dtr** コマンドをインターフェイスの設定に追加することで、ダイヤラにすることが可能です。もともとダイヤラ インターフェイスであるインターフェイス (BRI および PRI) に対しては、これらのコマンド行は不要です。 show interface の出力は次のようになります。

```
Montecito# show interfaces bri 0
BRI0 is up, line protocol is up (spoofing)
  Hardware is BRI
  Internet address is . . .
```

つまり、インターフェイスが**アップ/アップ**を「装い」、それによって関連するルートが有効のままになることにより、パケットをインターフェイスにルーティングできます。

場合によっては、ダイヤラ インターフェイスが**アップ/アップ (スプーフィング)** にならない状況もあります。 **show interface** の出力で、インターフェイスが administratively down として表示されることがあります。

```
Montecito# show interfaces bri 0
BRI0 is administratively down, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

administratively down とは、単にインターフェイスが **shutdown** コマンドで設定されている、という意味にすぎません。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。これを修正するには、インターフェイス設定コマンドである **no shutdown** を使用します。

また、インターフェイスがスタンバイ モードとして表示されることもあります。

```
Montecito# show interfaces bri 0
BRI0 is standby mode, line protocol is down
  Hardware is BRI
  Internet address is . . .
```

この状態は、インターフェイスが別のインターフェイスのバックアップとして設定されていることを示しています。接続に対して、障害に備えた冗長性が必要なときは、ダイヤラ インターフェイスをバックアップとしてセットアップできます。そのためには、次のコマンドをプライマリ接続のインターフェイスに追加します。

```
backup interface [interface]
backup delay [enable-delay] [disable-delay]
```

backup interface コマンドが設定されていると、バックアップとして使用されているインターフェイスは、プライマリ インターフェイスが**ダウン/ダウン**状態に移行するまでスタンバイ モードになります。その時点で、バックアップとして設定されているダイヤラ インターフェイスは、**アップ/アップ (スプーフィング)** 状態に移行し、ダイヤル イベントを待ちます。

スタティック ルートとフローティング スタティック ルート

パケットをダイヤラ インターフェイスにルーティングするための最も安全な方法として、スタティック ルーティングを使用する方法があります。これらのルートは、次のコマンドを使用して手動でルータまたはアクセス サーバの設定に入力します。

ip route prefix *mask* {address | *interface*} [*distance*]

*プレフィックスなしでもアクセスできます。*宛先のIPルートプレフィクス。

*mask:*宛先のプレフィックスマスク。

*address　:*宛先ネットワークに到達するために使用できるネクストホップのIPアドレス。

Interface : 発信トラフィックに使用するネットワークインターフェイス。

距離:（オプション）アドミニストレーティブディスタンス。この引数はフローティング スタティック ルートで使用されます。

スタティック ルートは、ダイヤル リンクがリモート サイトへのただ 1 つの接続である場合に使用します。スタティック ルートは値が 1 のアドミニストレーティブ ディスタンスを持っています。このため、同じ宛先へのダイナミック ルートよりも優先されます。

一方、フローティング スタティック ルート（事前定義のアドミニストレーティブ ディスタンスを持つスタティック ルート）は、バックアップ DDR のシナリオで使用されるのが普通です。これらのシナリオでは、RIP や EIGRP などのダイナミック ルーティング プロトコルによって、パケットがプライマリ リンクを経由してルーティングされます。

標準スタティック ルート（アドミニストレーティブ ディスタンス = 1）は EIGRP（アドミニストレーティブ ディスタンス = 90）または RIP（アドミニストレーティブ ディスタンス = 120）のどちらよりも優先されます。 スタティック ルートを使用すると、プライマリがアップ状態で、トラフィックが通過できる場合であっても、パケットがダイヤル回線経由でルーティングされます。ただし、スタティック ルートのアドミニストレーティブ ディスタンスが、ルータで使用中のどのダイナミック ルーティング プロトコルのアドミニストレーティブ ディスタンスよりも大きくなるように設定されていると、「より適した」ルート（よりアドミニストレーティブ ディスタンスが小さいルート）がないときだけ、フローティング スタティック ルートが使用されます。

backup interface コマンドの使用によってバックアップ DDR が起動している場合は、いくぶん状況が異なります。プライマリが**アップ状態**の間、ダイヤラ インターフェイスはスタンバイ モードのままであるため、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 ルートを設定できます。ダイヤラ インターフェイスは、プライマリ インターフェイスが**ダウン/ダウン**に移行するまで、接続を試みることはありません。

接続において、必要なスタティック（またはフローティング スタティック）ルートの数は、ダイヤラ インターフェイスでのアドレッシングによって決まります。2 つのダイヤラ インターフェイス（2 台のルータにそれぞれ 1 つずつ）が共通のネットワークまたはサブネットを共有している場合では、必要なスタティック ルートは通常は 1 つだけです。このスタティック ルートは、ネクストホップ アドレスとしてリモート ルータのダイヤラ インターフェイスのアドレスを使用する、リモートの LAN を指し示します。

例

例 1：ダイヤルは、番号付きインターフェイスを使用しているただ 1 つの接続です。1 つのルートで十分です。

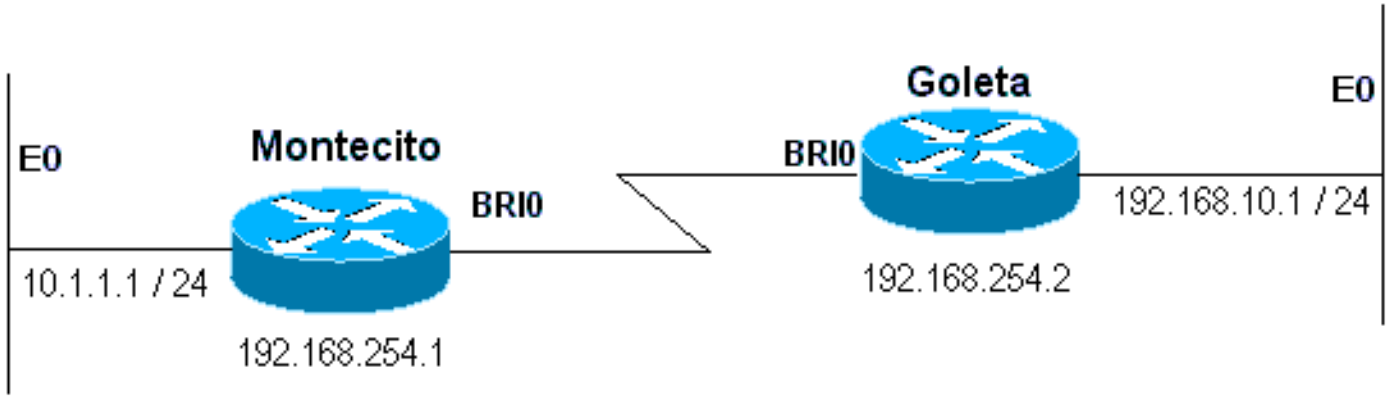

図 16-4：番号付きインターフェイスを使用するダイヤル

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1
```

例 2：ダイヤルは、番号未指定インターフェイスを使用しているただ 1 つの接続です。これは1つのルートだけで設定できますが、2つのルートを設定するのが一般的です。リモートルータのLANインターフェイスへのホストルートと、リモートLANインターフェイス経由のリモートLANへのルート。これは、レイヤ 3 からレイヤ 2 へのマッピングに関する問題を防ぐためのものです。この問題は結果としてカプセル化の障害を起こす可能性があります。

2 台のデバイスのダイヤラ インターフェイスが番号付きであるものの、同じネットワークまたはサブネットにない場合にも、この方法が使用されます。

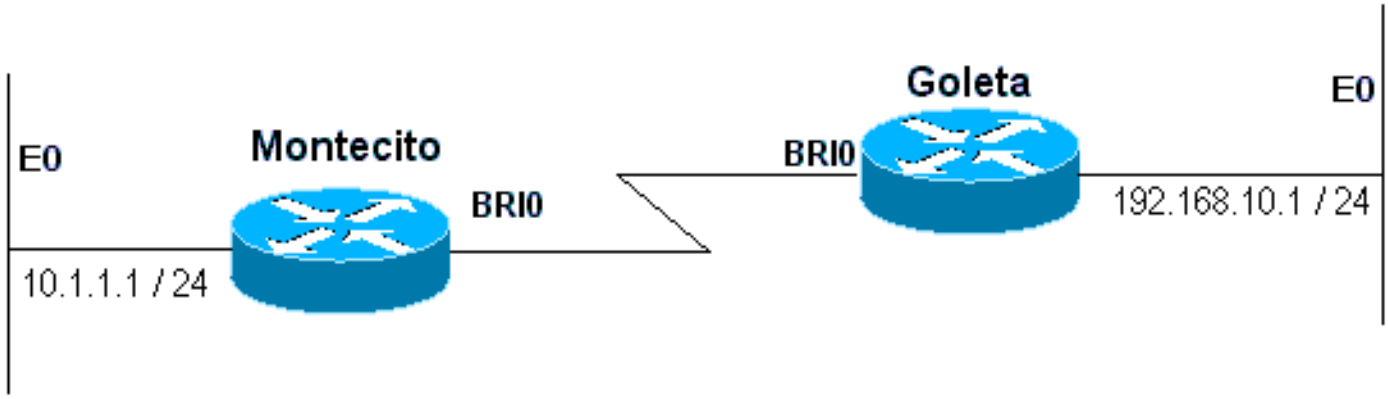

図 16-5：番号なしインターフェイスを使用するダイヤル

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1
ip route 192.168.10.1 255.255.255.255 BRI0
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 10.1.1.1 255.255.255.255 BRI0
```

例 3：ダイヤルは、番号付きインターフェイスを使用しているバックアップ接続です。フローテ

ィング スタティック ルートが 1 つ必要です。

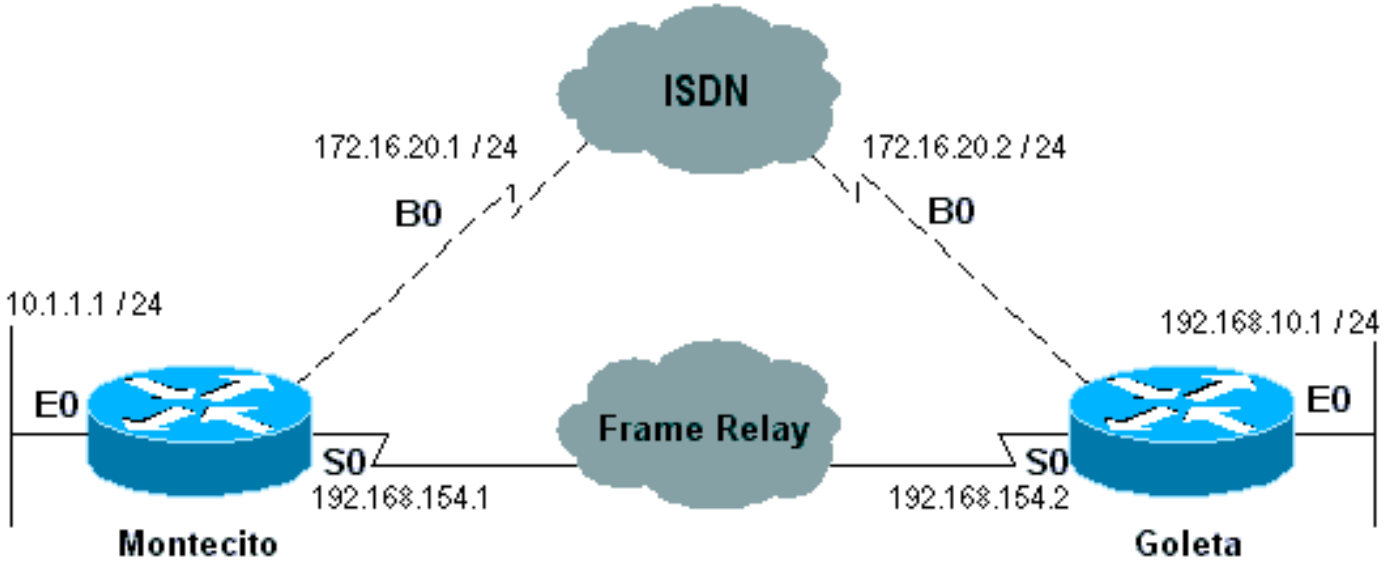

図 16-6：番号付きインターフェイスを使用するバックアップ

```
Montecito:
ip route 192.168.10.0 255.255.255.0 172.16.20.2 200
Goleta:
ip route 10.1.1.0 255.255.255.0 172.16.20.1 200
```

例 4：ダイヤルは、番号未指定インターフェイスを使用しているバックアップ接続です。上の例 2 と同様に、2 台のデバイスのダイヤラ インターフェイスが番号付きであるものの、同じネットワークまたはサブネットにない場合にも、この方法が使用されます。

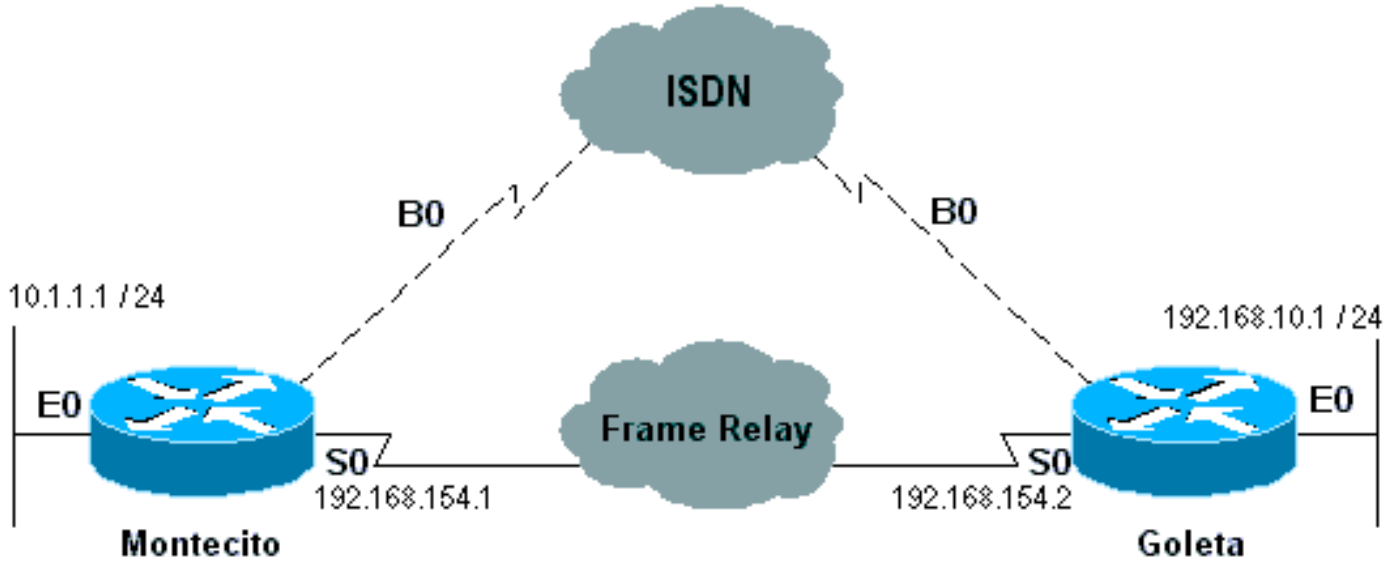

図 16-7：番号なしインターフェイスを使用するバックアップ

```
Montecito:
ip route 192.168.10.0 255.255.255.0 192.168.10.1 200
ip route 192.168.10.1 255.255.255.255 BRI0 200
Goleta:
ip route 10.1.1.0 255.255.255.0 10.1.1.1 200
ip route 10.1.1.1 255.255.255.255 BRI0 200
```

ダイヤラ マップ

ダイヤラ マップ ベース (レガシー) DDR は強力で包括的ですが、その制限のためにスケーリングや拡張性が影響を受けます。ダイヤラ マップ ベース DDR の基本的な考え方は、宛先別のコール指定と物理インターフェイスの設定との間で静的なバインディングを行うことです。

しかし、ダイヤラ マップ ベース DDR には数多くの利点もあります。フレームリレー、ISO CLNS、LAPB、スナップショット ルーティングをはじめ、Cisco ルータがサポートしているすべてのルーティング プロトコルをサポートしています。デフォルトでは、ダイヤラ マップ ベース DDR はファースト スイッチングをサポートしています。

インターフェイスを発信呼び出し用に設定するときは、リモートの宛先ごとと、リモート宛先での異なる送信先番号ごとに、ダイヤラ マップを 1 つずつ設定する必要があります。たとえば、ある ISDN BRI から、B チャネルごとに異なる市内電話番号を持つ別の ISDN BRI インターフェイスにダイヤルするときに、マルチリンク PPP 接続を必要とする場合は、リモート番号ごとにダイヤラ マップが 1 つずつ必要になります。

```
!
interface bri 0
 dialer map ip 172.16.20.1 name Montecito broadcast 5551234
 dialer map ip 172.16.20.1 name Montecito broadcast 5554321
!
```

ダイヤラ マップの設定順序が意味を持つ場合もあります。2 つ以上のダイヤラ マップ コマンドが同じリモート アドレスを参照している場合、ルータやアクセス サーバは接続の確立に成功するまで、それらのコマンドを 1 つずつ順番に試行します。

注：IOSは、コールを受信するルータ上にダイヤラマップを動的に構築できます。ダイヤラ マップは、認証されたユーザ名とネゴシエートされた発信者 IP アドレスに基づいて作成されます。動的なダイヤラ マップは **show dialer map** コマンドの出力だけに表示されます。ルータまたはアクセス サーバの実行コンフィギュレーションには表示されません。

コマンド構文

次の場合には、下記の形式の **dialer map** インターフェイス設定コマンドを使用します。

- 1 つまたは複数のサイトをコールするようにシリアル インターフェイスまたは ISDN インターフェイスを設定する場合、または
- 複数のサイトからコールを受信する場合

このコマンドの 1 つ目の形式におけるすべてのオプションを次に示します。特定のダイヤラ マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

```
dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
[broadcast] [modem-script modem-regexp] [system-script system-regexp]
[dial-string[:isdn-subaddress]]
```

次の場合には、下記の形式の **dialer map** コマンドを使用します。

- 1 つまたは複数のサイトにコールを行うようにシリアル インターフェイスまたは ISDN インターフェイスを設定する場合、および

- 複数のサイトからのコールを認証する場合
  ```
  dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64]
  [broadcast] [dial-string[:isdn-subaddress]]
  ```

ブリッジングをサポートするようにシリアル インターフェイスまたは ISDN インターフェイスを設定するには、次の形式の **dialer map** コマンドを使用します。

```
dialer map bridge [name hostname] [spc] [broadcast] [dial-string[:isdn-subaddress]]
```

次の宛先にコールを行うように非同期インターフェイスを設定するには、下記の形式の **dialer map コマンドを使用します。**

- システム スクリプトを必要とする単一のサイト、またはモデム スクリプトが割り当てられていない単一のサイト、あるいは
- 単一回線上、複数回線上、またはダイヤラ ロータリー グループ上の複数のサイト
  ```
  dialer map protocol next-hop-address [name hostname] [broadcast]
  [modem-script modem-regexp] [system-script system-regexp] [dial-string]
  ```

シンタックスの説明

- *protocol*：プロトコル キーワード。次のいずれかを使用します。**appletalk、bridge、clns、decnet、ip、ipx、novell、snapshot、vines、またはxns。**
- *next-hop-address：**パケットの宛先となるアドレスとの照合に使用されるプロトコル アドレス。*bridge プロトコル キーワードでは、この引数は使用されません。
- **name**：（オプション）ローカル ルータまたはアクセス サーバの通信相手となるリモート システムを示します。着信コールでリモート システムを認証するために使用します。
- *hostname：**（オプション）大文字小文字を区別する、リモート デバイスの名前または ID（通常はホスト名）。*** ISDN インターフェイスを持つルータでは、**hostname フィールドに、発信元の回線 ID から提供される番号（Calling Line Identification（CLI*; 発呼回線 ID*）、発信者番号、および Automatic Number Identification（ANI; 自動番号識別）が使用可能な場合）を含めることができます。**
- **spc**：（オプション）顧客機器と交換機との間の半永久接続を指定します。このオプションは、ドイツにおける ISDN BRI と 1TR6 ISDN 交換機との間の回線、およびオーストラリアにおける ISDN PRI と TS-014 交換機との間の回線だけで使用します。
- **速度56 | 64** -（オプション）使用する回線速度をキロビット/秒で示すキーワードと値。ISDN だけで使用します。デフォルトの速度は 64 kbps です。
- **broadcast**：（オプション）ブロードキャストをこのプロトコル アドレスに転送する必要があることを示します。
- **modem-script**：（オプション）接続に使用するモデム スクリプトを示します（非同期インターフェイス用）。
- *modem-regexp：**（オプション）モデム スクリプトが照合される正規表現（非同期インターフェイス用）。***
- **system-script**：（オプション）接続に使用するシステム スクリプトを示します（非同期インターフェイス用）。
- *system-regexp：**（オプション）システム スクリプトが照合される正規表現（非同期インターフェイス用）。***
- *dial-string[:isdn-subaddress]：**（オプション）定義済みのアクセス リスト（および、ISDN マ*

ルチポイント接続に使用されるオプションのサブアドレス番号）に照合される指定ネクストホップ アドレスが指定されたパケットの認識後、ただちにダイヤル元のデバイスに送られる電話番号。 ダイヤル文字列と ISDN サブアドレスを使用する場合は、必ずコマンドラインの最後の項目として指定します。

ダイヤラ プロファイル

注：この項では、「ダイヤラインターフェイス」という用語は設定されたインターフェイスを指します。ルータまたはアクセスサーバの物理インターフェイスには接続されません。

IOS バージョン 11.2 で導入され、DDR に実装されたダイヤラ プロファイルは、論理インターフェイスの設定と物理インターフェイスの設定を分離することを、その基本的な目的としています。また、ダイヤラ プロファイルにより、論理コンフィギュレーションと物理コンフィギュレーションをコール単位で動的にバインドできます。

ダイヤラ プロファイルは次の操作を行う場合に役立ちます。

- コールを発信または着信するためのインターフェイス（ISDN、非同期、または同期シリアル）を共有する場合
- 任意の設定をユーザ単位で変更する場合（ダイヤラ プロファイルの第 1 フェーズにおけるカプセル化を除く）
- 多数の宛先にブリッジングする場合
- スプリット ホライズンの問題を回避する場合

ダイヤラ プロファイルを使用すると、物理インターフェイスの設定を、コールに必要な論理コンフィギュレーションから分離できます。また、論理および物理コンフィギュレーション同士を、コール単位でまとめて動的にバインドできます。

ダイヤラ プロファイルは、次の要素で構成されています。

- 1つ*以上のダイヤル*文字列（それぞれが1つの宛先サブネットワークに到達するために使用される）を含むダイヤラインターフェイス（論理エンティティ）の設定
- **ダイヤラ マップ クラス。指定されたダイヤル文字列へのすべてのコールに関するすべての特性を定義します。**
- ダイヤラ インターフェイスで使用される、順序付けされた、物理インターフェイスの**ダイヤラ プール。**

ある宛先サブネットワークへの発信コールと同じ宛先サブネットワークからの着信コールはすべて、同じダイヤラ プロファイルを使用します。

Dialer インターフェイスの設定には、特定の宛先サブネットワーク（およびその宛先サブネットワークを経由して到達する任意のネットワーク）への到達に必要な、すべての文字列が含まれます。 同じダイヤラインターフェイスに対して複数のダイヤル文字列を指定できます。各ダイヤル文字列は、異なるダイヤラマップクラスに関連付けることができます。ダイヤラ マップ クラスは、指定されたダイヤル文字列への任意のコールに関するすべての特性を定義します。たとえば、ある宛先に対するマップ クラスでは 56 kbps の ISDN 速度を指定するとします。別の宛先に対するマップ クラスでは 64 kbps の ISDN 速度を指定する場合があります。

Dialer インターフェイスはそれぞれダイヤラ プールを使用します。ダイヤラ プールは物理インターフェイスのプールで、各物理インターフェイスはそれぞれに割り当てられた優先順位を基準として順序付けされます。1 つの物理インターフェイスを複数のダイヤラ プールに割り当てて、コンテンションを優先順位に従って解決できます。ISDN の BRI インターフェイスおよび PRI イン

ターフェイスでは、任意のダイヤラ プールによって予約された B チャネルの最小番号と最大番号について、制限を設定できます。ダイヤラ プールによって予約されたチャネルは、トラフィックがプール宛てに送信されるまでアイドルのままになります。

ダイヤラ プロファイルを使用して DDR を設定すると、物理インターフェイスには、カプセル化と、インターフェイスが属するダイヤラ プール以外には、コンフィギュレーションの設定は存在しなくなります。

注：前段落には例外が1つあります。認証が完了する前に適用されるコマンドについては、ダイヤラ プロファイルにおいてではなく、物理（つまり BRI または PRI）インターフェイスにおいて設定する必要があります。ダイヤラ プロファイルは PPP 認証コマンド（または LCP コマンド）を物理インターフェイスにコピーしません。

図 16-8 はダイヤラ プロファイルの典型的な応用例です。ルータAには、サブネットワーク1.1.1.0とのダイヤルオンデマンドルーティング用のダイヤラインターフェイス1と、サブネットワーク2.2.2.0とのダイヤルオンデマンドルーティング用のダイヤラインターフェイス2があります。ダイヤラインターフェイス1のIPアドレスはネットワーク1.1.1.0のノードですネットワーク2.2.2.0のノードとして使用します。

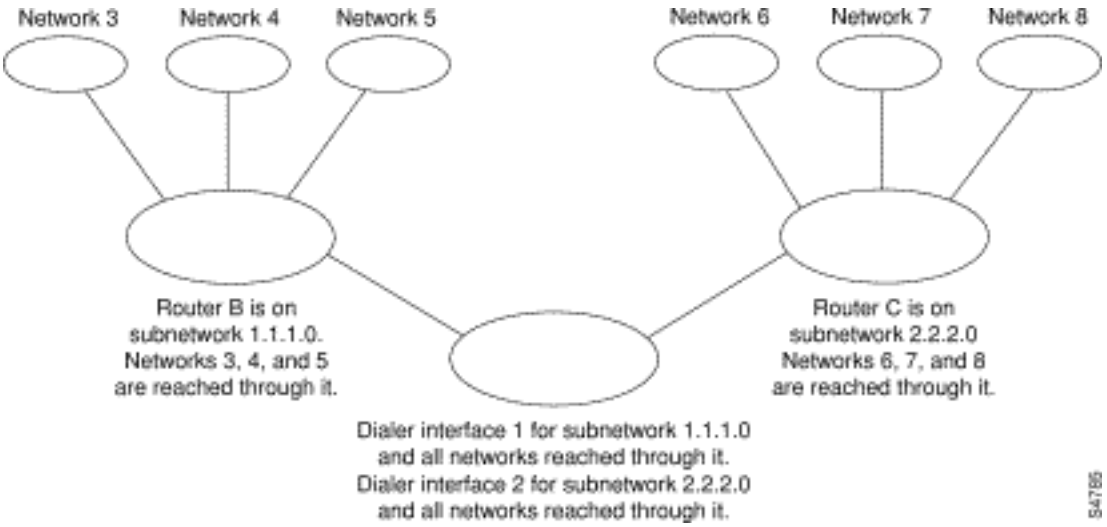

図 16-8：ダイヤラ プロファイル アプリケーションの典型的な応用例

1 つのダイヤラ インターフェイスは 1 つのダイヤラ プールしか使用しません。しかし、物理インターフェイスは 1 つまたは複数のダイヤラ プールのメンバにすることができ、ダイヤラ プールには複数の物理インターフェイスをメンバとして指定できます。

図 16-9 に、ダイヤラ インターフェイス、ダイヤラ プール、および物理インターフェイスの概念の関係を示します。ダイヤラインターフェイス0はダイヤラプール2を使用します。物理インターフェイスBRI 1はダイヤラプール2に属し、プール内で特定のプライオリティを持ちます。物理インターフェイスBRI 2もダイヤラプール2に属しています。競合はプール内の物理インターフェイスのプライオリティレベルに基づいて解決されるため、BRI 1とBRI 2にはプール内で異なるプライオリティを割り当てる必要があります。たとえば、ダイヤラ プール 2 で、BRI 2 に優先順位 100 を、BRI 1 に優先順位 50 を、それぞれ割り当てます（優先順位 50 は優先順位 100 よりも高い順位です）。プール内では BRI 2 の優先順位が高いため、そのコールが先に発信されます。

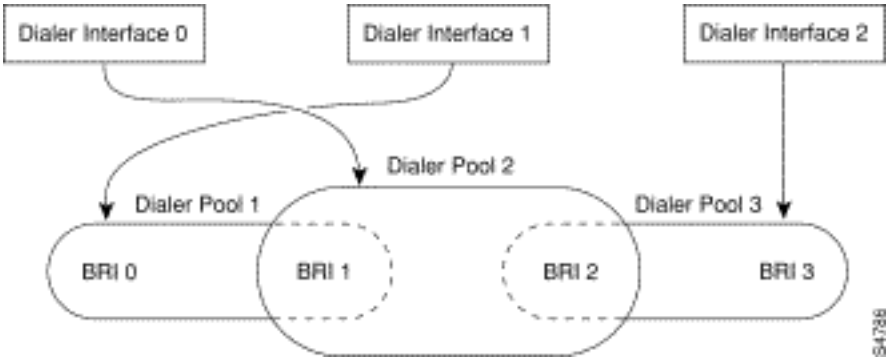

図 16-9：ダイヤラ インターフェイス、ダイヤラ プール、および物理インターフェイス間の関係

ダイヤラ プロファイルの設定手順

コマンド	目的
interface dialer *number*	ダイヤラ インターフェイスを作成します。
ip address *address mask*	ダイヤラ インターフェイスの IP アドレスとマスクを、コールされる宛先ネットワーク内のノードとして指定します。
encapsulation ppp	PPP のカプセル化を指定します。
dialer remote-name *username*	リモート ルータの CHAP 認証名を指定します。
dialer string *dial-string* class *class-name*	コールするリモートの宛先と、この宛先へのコールの特性を定義するマップ クラスを指定します。
dialer pool*number*	この宛先へのコールに使用するダイヤリング プールを指定します。
dialer-group *group-number*	ダイヤラ インターフェイスをダイヤラ グループに割り当てます。
dialer-list dialer-group protocol protocol-name {permit |	コールをトリガーできる「対象」パケットを定義するための、リスト番号別アクセス リスト、またはプロトコルおよびリスト番号別アクセス リストを指定します。

deny | list *access-list-number*}	

PPP の運用

Point-to-Point Protocol (PPP) は、最も広く普及しているリンク層トランスポート プロトコルで、ダイヤルおよび非ダイヤル (多くの場合は非ダイヤル) の同期または非同期のシリアル接続に対する最適なプロトコルとして、SLIP が完全に流用されたものです。PPPは1989年にRFC 1134で定義されました。これはRFC1661の一連のRFCによって廃止され、RFC1990 (PPPマルチリンク) など、プロトコルの要素を定義する多数のRFCがありますプロトコル)、RFC2125 (PPP帯域幅割り当てプロトコル)、およびその他の多数。RFC のオンライン リポジトリについては次を参照してください。

http://www.ietf.org/rfc.html

おそらく、最善とされる PPP 定義は RFC1661 です。この RFC では次のように定義されています。

Point-to-Point Protocol (PPP) は、ポイントツーポイント リンク上でマルチプロトコルのデータグラムを伝送するための標準の方式を規定します。PPP は次の 3 つの主要なコンポーネントで構成されています。

1. マルチプロトコルのデータグラムをカプセル化する方式。
2. データリンク接続を確立、設定、およびテストする Link Control Protocol (LCP) 。
3. 各種ネットワーク層プロトコルを確立および設定する Network Control Protocol (NCP) ファミリ。

PPPネゴシエーションのフェーズ

PPPネゴシエーションは、次の3つのフェーズで構成されます。Link Control Protocol (LCP; リンク コントロール プロトコル) 、認証、および Network Control Protocol (NCP; ネットワーク コントロール プロトコル) の 3 つのフェーズで構成されます。 それぞれが順序どおりに実行され、その後非同期または ISDN の接続が確立されます。

LCP

PPP はクライアント/サーバ モデルに従っていません。すべての接続がピアツーピアです。したがって、発信者と受信者が存在するときは、ポイントツーポイント接続の両方の端末で、ネゴシエートされたプロトコルとパラメータが一致している必要があります。

ネゴシエーションが始まると、PPP 接続を確立しようとしているそれぞれのピアは Configure Request (**debug ppp negotiation** で表示されるもので、以後 CONFREQ と表記) を送信する必要があります。 CONFREQ にはリンク デフォルトではないオプションがすべて含まれています。これらのオプションにはしばしば、Maximum Receive Unit (MRU) 、Async Control Character Map (ACCM) 、Authentication Protocol (AuthProto) 、Magic Number などが含まれます。また、マルチリンク PPP で使用される Maximum Receive Reconstructed Unit (MRRU) および Endpoint Discriminator (EndpointDisc) も見られます。

どの CONFREQ への応答にも次の 3 つの可能性があります。

- Configure-Acknowledge（CONFACK）。ピアがオプションを認識して CONFREQ 内の値に一致した場合は、必ずこの応答が発行されます。
- Configure-Reject（CONFREJ）。CONFREQ 内のいずれかのオプションが認識されない場合（ベンダー固有のオプションなど）、またはいずれかのオプションがピアの設定の中で明示的に禁止されている場合は、必ずこの応答が送られます。
- Configure-Negative-Acknowledge（CONFNAK）。ピアが CONFREQ 内のオプションをすべて認識したものの、それらの値を受け入れることができない場合は、必ずこの応答が送られます。

2 つのピアは、双方が CONFACK を送信するか、ダイヤル接続が切断するか、あるいはネゴシエーションが完了できないことを一方または双方のピアが示すまで、CONFREQ、CONFREJ、および CONFNAK の交換を続けます。

[Authentication]

LCP のネゴシエーションが正常に完了して AuthProto の同意に達すると、次に認証が行われます。認証は RFC1661 では必須ではありませんが、すべてのダイヤル接続において強く推奨されます。場合によっては、適切な操作が必要です。ダイヤラプロファイルが重要なケースです。

PPP の認証には、主に Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP）の 2 つの種類があります。これらは RFC1334 によって定義され、RFC1994 によって更新されています。

PAP は比較的シンプルですが、平文のパスワードがダイヤル接続を経由して送られるため、安全性では劣ります。CHAP では平文パスワードがダイヤル接続を経由して送られることが決してないため、より安全です。

次のどちらかの環境では PAP が必要になる場合があります。

- クライアント アプリケーションの大規模なインストール ベースで、CHAP がサポートされていない場合
- CHAP の実装がベンダー間で異なり、互換性がない場合

認証について説明するときは、接続の両端にあるデバイスが担う役割を区別するために、「要求者」および「認証者」という用語を使用すると便利です（ただしどちらのピアも両方の役割を果たすことができます）。「要求者」とは、ネットワークアクセスを要求し、認証情報を提供するデバイスを指します。「オーセンティケータ」は、認証情報の有効性を確認し、接続を許可または拒否します。ルータ間で DDR 接続がなされるときは、双方のピアが両方の役割を担うのが普通です。

PAP

PAP は非常にシンプルです。LCP のネゴシエーションが正常に完了すると、要求者はリンクを経由してユーザ名/パスワードの組み合せを繰り返し送信し、認証者が ACK で応答するか、またはリンクが切断するまで、送信を続けます。認証者は、ユーザ名/パスワードの組み合せが有効ではないと判断した場合、リンクを接続解除できます。

CHAP

CHAP は PAP よりも多少複雑です。認証者は身元証明要求を要求者に送信し、要求者は値でこ

れに応答します。値は、「単方向ハッシュ」関数を使用して身元証明要求と CHAP パスワードをハッシュすることにより計算されます。計算された値は、要求者の CHAP ホスト名（実際のホスト名と異なる場合もあります）とともに**応答メッセージとして認証者に送られます。**

認証者は応答メッセージ内のホスト名を読み取り、そのホスト名から予測されるパスワードを検索します。そして、要求者が実行したものと同じハッシュ関数を実行し、要求者が応答メッセージで送信してきたものと予測される値を計算します。計算の結果、値が一致すれば、認証は成功します。認証に失敗した場合は接続解除されることになります。

[AAA]

PAP または CHAP を実現するために、TACACS+ や RADIUS といった Authentication, Authorization and Accounting（AAA; 認証、認可、およびアカウンティング）サービスが使用されることがあります。

NCP

認証が成功すると、NCP フェーズが開始します。LCP と同様に、双方のピアは CONFREQ、CONFREJ、CONFNAK、および CONFACK を交換し合います。ただし、このネゴシエーションフェーズでは、ネゴシエート中の要素は、IP、IPX、ブリッジング、CDP などの上位レイヤのプロトコルに関して行われる必要があります。これらのプロトコルの 1 つまたは複数がネゴシエートされる可能性があります。ここでは、最も一般的に使用されていて、他のプロトコルもまったく同様な方式で動作するということから、RFC1332 で定義されている Internet Protocol Control Protocol（IPCP）を中心に説明しています。関連する他の RFC もありますが、次のものに限定されるわけではありません。

- RFC1552（IPX 制御プロトコル）
- RFC1378（AppleTalk 制御プロトコル）
- RFC1638（ブリッジング制御プロトコル）
- RFC1762（DECnet 制御プロトコル）
- RFC1763（Vines 制御プロトコル）

このほか、Cisco Discovery Protocol Control Protocol（CDPCP）が NCP の中でネゴシエートされる場合もありますが、一般的ではありません。通常、Cisco TAC エンジニアは、CDP パケットが無限に呼び出されるのを防ぐために、任意のすべてのダイヤラ インターフェイスで no cdp enable コマンドを設定することを推奨しています。

IPCP でネゴシエートされる主な要素は、それぞれのピアのアドレスです。各ピアは2つの状態のいずれかになります。「IPアドレスが付けられている」または「IP アドレスが付けられていない」のいずれかになります。ピアにすでにアドレスがある場合は、そのアドレスを CONFREQ の中で他方のピアに送ります。他方のピアがそのアドレスを受け入れることができる場合は、CONFACK が返されます。アドレスを受け入れることができない場合は、ピアが使用すべきアドレスを持つ CONFNAK が応答として返されます。

ピアにアドレスがない場合は、アドレス0.0.0.0を持つCONFREQを送信します。これにより、他のピアにアドレスを割り当てるように指示されます。これは、適切なアドレスを持つCONFNAKの送信によって実現されます。

これ以外の選択肢が IPCP でネゴシエートされる場合もあります。一般に、ドメインネームサーバ(DNS)とNetBIOSネームサーバ(DNS)のプライマリアドレスとセカンダリアドレスが表示されます。これは、情報RFC1877で説明されています。IP圧縮プロトコル(RFC1332)も一般的です。

代替の PPP 方式

代替の PPP 方式には、マルチリンク PPP、マルチシャーシ PPP、そしてバーチャル プロファイルがあります。

マルチリンク PPP

Multilink Point-to-Point Protocol（MLP; マルチリンク PPP）機能は、複数の WAN リンクに渡る負荷バランシングの機能を提供します。また同時に、マルチベンダー間のインターオペラビリティ、パケットのフラグメント化と適切なシーケンシング、および、送受信双方のトラフィックに関する負荷計算も実現します。Cisco の実装によるマルチリンク PPP では、RFC1717 で規定されている、パケットのフラグメント化とシーケンシングの仕様がサポートされています。

マルチリンク PPP ではパケットのフラグメント化が可能です。これらのフラグメントは、複数のポイントツーポイント リンクを経由して同じリモート アドレスに同時に送信できます。これらの複数のリンクは、定義したダイヤラ負荷しきい値に応じてアップします。負荷の計算は、特定のサイト間のトラフィックの必要性に応じて、受信トラフィック、送信トラフィック、あるいは両方に関して実行できます。MLP ではオンデマンド帯域幅が提供されており、WAN リンク全体の伝送待ち時間が減少します。

マルチリンク PPP は、ダイヤルオンデマンド ロータリー グループと PPP カプセル化の両方をサポートするように設定された、次のインターフェイス タイプ（単一または複数）において動作します。

- 非同期シリアル インターフェイス
- BRI
- PRI

コンフィギュレーション

非同期インターフェイスでマルチリンク PPP を設定するには、DDR と PPP カプセル化をサポートするように、非同期インターフェイスを設定します。次に、PPP カプセル化、オンデマンド帯域幅、およびマルチリンク PPP をサポートするように、Dialer インターフェイスを設定します。ただし、場合によっては非同期インターフェイスをさらに追加してもパフォーマンスが改善されないことがあります。デフォルトの MTU サイズでは、V.34 モデムを使用する 3 つの非同期インターフェイスがマルチリンク PPP でサポートされます。しかし、MTU が小さい場合や、短いフレームの大量バーストが発生する場合は、しばしばパケットが廃棄されることがあります。

単一の ISDN BRI または PRI インターフェイスでマルチリンク PPP をイネーブルにする場合は、別途ダイヤラ ロータリー グループを定義する必要はありません。これは、ISDN インターフェイスはデフォルトでダイヤラ ロータリー グループであるためです。PPP 認証手順を使用しない場合は、電話サービスから発信者 ID 情報を渡す必要があります。

負荷しきい値番号は必須です。単一の ISDN BRI インターフェイスでのマルチリンク PPP の設定例については、次の「*1 つの ISDN インターフェイスでのマルチリンク PPP の例*」を参照してください。

マルチリンク PPP を設定してマルチリンク バンドルを無制限に接続する場合は、**dialer idle-timeout** コマンドを使用して非常に大きな値のアイドル タイマーを設定します。**dialer-load threshold 1**コマンドは、*n個のリンクのマルチリンクバンドルを無期限に接続し続けません*。また、**dialer-load threshold 2コマンドは、2個のリンクのマルチリンクバンドルを無期限に接続し続け**

ません。

複数の ISDN BRI または PRI インターフェイスでマルチリンク PPP をイネーブルにするには、Dialer ロータリー インターフェイスをセットアップしてマルチリンク PPP 用に設定します。そして、個々の BRI を別々に設定し、それらをそれぞれ同じロータリー グループに追加します。下記の「*複数の ISDN インターフェイスでのマルチリンク PPP の例*」を参照してください。

1 つの ISDN インターフェイスでのマルチリンク PPP の例

次の例は、BRIインターフェイス0でマルチリンクPPPを有効にします。1つのBRIを設定すると、ダイヤラロータリーグループの設定は必要ありません（ISDNインターフェイスはデフォルトではロータリーグループです）。

```
interface bri 0
ip address 171.1.1.7 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 30
 dialer load-threshold 40 either
 dialer map ip 172.16.20.2 name Goleta 5551212
 dialer-group 1
 ppp authentication pap
 ppp multilink
```

複数の ISDN インターフェイスでのマルチリンク PPP の例

次の例では、複数の ISDN BRI について、マルチリンク PPP 用の同じダイヤラ ロータリー グループに属するように設定しています。**dialer rotary-group** コマンドを使用し、各 ISDN BRI をそのダイヤラ ロータリー グループに割り当てます。ダイヤラ ロータリー グループの番号は Dialer インターフェイスの番号（この場合は番号 0）と一致する必要があります。

```
interface BRI0
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface BRI1
 no ip address
 encapsulation ppp
 dialer rotary-group 0
!
interface Dialer0
 ip address 172.16.20.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 172.16.20.2 name Goleta broadcast 5551212
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

マルチシャーシ マルチリンク PPP

マルチリンク PPP は、単一のエンドシステムに対して、複数のリンクで構成される論理パイプ

（*バンドル*とも呼ばれます）を通じてパケットの分割と再結合を行う機能を提供します。マルチリンク PPP ではオンデマンド帯域幅が提供されており、WAN リンク全体の伝送待ち時間が減少します。

これに対して、Multichassis Multilink PPP（MMP; マルチシャーシ マルチリンク PPP）は、複数のルータで異なるリモート アドレスを使用してリンクを終端するための追加機能を提供します。また、MMP ではアナログとデジタルの両方のトラフィックを扱うこともできます。

この機能は、ダイヤルイン ユーザのプールが大量にあり、単一のアクセス サーバが十分なダイヤルイン ポートを提供できないような場合に対応するためのものです。MMP では、会社から自社ユーザに対して単一のダイヤルアップ番号を提供し、アナログとデジタル両方の通話で同じソリューションを適用することが可能です。この機能により、たとえばインターネット サービス プロバイダーは、単一の ISDN ロータリー番号を複数のルータを通じて複数の ISDN PRI に割り当てることができます。

ここで説明している MMP コマンドについての詳細は、『*Cisco ダイヤル ソリューション コマンド リファレンス*』を参照してください。この章に記載されている他のコマンドのドキュメントについては、コマンド リファレンスのマスター インデックスやオンライン検索を利用して参照してください。

MMP は、Cisco 7500、4500、2500 の各シリーズ プラットフォーム、そして、同期シリアル、非同期シリアル、ISDN BRI、ISDN PRI、および Dialer の各インターフェイスでサポートされています。

MMP では電話会社の交換機の再設定は不要です。

コンフィギュレーション

ルータまたはアクセス サーバが、*スタック グループ*と呼ばれるピアのグループに属するように設定されます。スタックグループのすべてのメンバーはピアです。スタックグループには、永続的なリードルータは必要ありません。どのスタック グループも単一のアクセス番号から送られてくるコールに応答できます。アクセス番号は通常は ISDN PRI ハント グループです。コールは、ルータやモデム、ISDN ターミナル アダプタ、PC カードといった、リモート ユーザのデバイスから送られてくる可能性があります。

*スタック グループ*のあるメンバとの接続が確立されると、そのメンバがコールを所有します。2 つ目のコールが同じクライアントから送られ、別のルータがそのコールに応答した場合は、そのルータがトンネルを確立し、そのコールに属するすべてのパケットを、コールを所有しているルータに転送します。トンネルを確立し、コールを所有しているルータにトンネル経由でコールを転送するプロセスは、*コール マスターへの PPP リンクの投影*と呼ばれることがあります。

より強力なルータが使用できる場合には、そのルータをスタック グループのメンバとして設定し、他のスタック グループ メンバがトンネルを確立してすべてのコールをそのルータに転送できます。この場合、他のスタック グループ メンバは、単にコールに応答して、トラフィックをより強力な*オフロード*ルータに転送するだけです。

注：スタックグループメンバ間のWAN回線の遅延が大きくなると、スタックグループの動作が非効率になる可能性があります。

スタック グループ内での MMP のコール処理、送信権要求、およびレイヤ 2 転送の各動作は、次のようになります。図 16-10 もあわせて参照してください。

1. 1 つ目のコールがスタック グループに到着すると、ルータ A が応答します。
2. 送信権要求で、ルータ A はすでにコールを所有しているので、送信権を獲得します。ルータ A は、リモート デバイスとのそのセッションにおける*コール マスター*になります。また、ルータ A は *マスター バンドル インターフェイス*へのホストと呼ばれることもあります。
3. コールを開始したリモート デバイスでより多くの帯域幅が必要になると、グループに対して 2 つ目のマルチリンク PPP コールを行います。
4. 2 つ目のコールが到着すると、ルータ D がそれに応答し、スタック グループに知らせます。ルータ A はそのリモート デバイスとのセッションをすでに処理しているので、送信権を獲得します。
5. ルータ D はルータ A へのトンネルを確立し、ロー PPP データをルータ A に転送します。
6. ルータ A はパケットの再アセンブルと再シーケンシングを行います。
7. さらに多くのコールがルータ D に到着し、それらもまたルータ A に属するものであれば、追加されたトラフィックを処理できるようにルータ A とルータ D 間のトンネルが拡張されます。ルータ D はルータ A への追加のトンネルを確立しません。
8. さらに多くのコールが到着し、他のいずれかのルータがそれらに応答した場合には、そのルータもまたルータ A へのトンネルを確立し、ロー PPP データをルータ A に転送します。
9. 再アセンブルされたデータは、あたかもそれらが 1 つの物理リンクを経由して到着したかのように、企業ネットワークに渡されます。

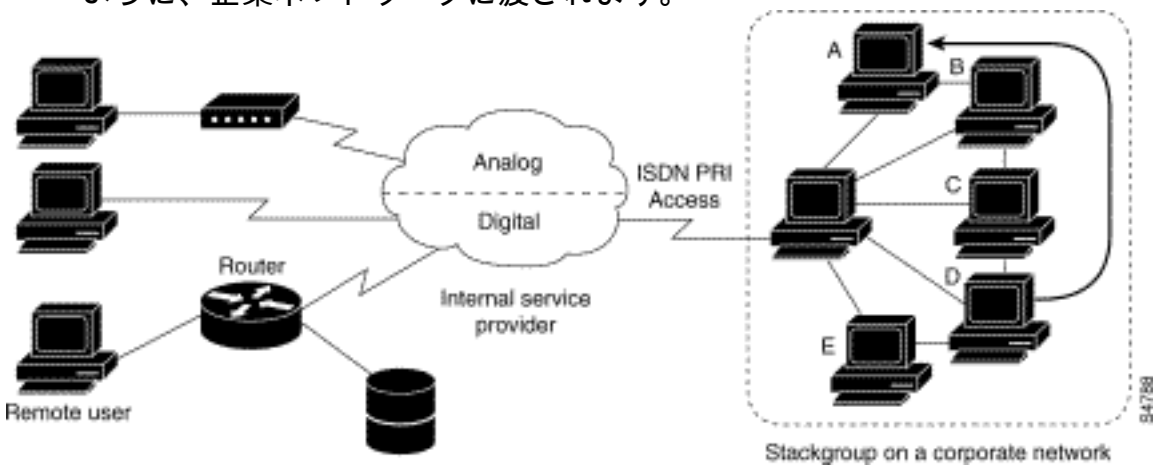

図 16-10 : マルチシャーシ マルチリンク PPP の典型的なシナリオ

図 16-11 では、前の図とは対照的にオフロード ルータを実現しています。スタック グループに属するアクセス サーバは、コールに応答し、トンネルを確立して、Cisco 4700 ルータにコールを転送します。このルータは送信権を獲得してすべてのコールのコール マスターになっています。Cisco 4700 は、スタック グループを通じて送られてくるすべてのパケットの再アセンブルと再シーケンシングを行います。

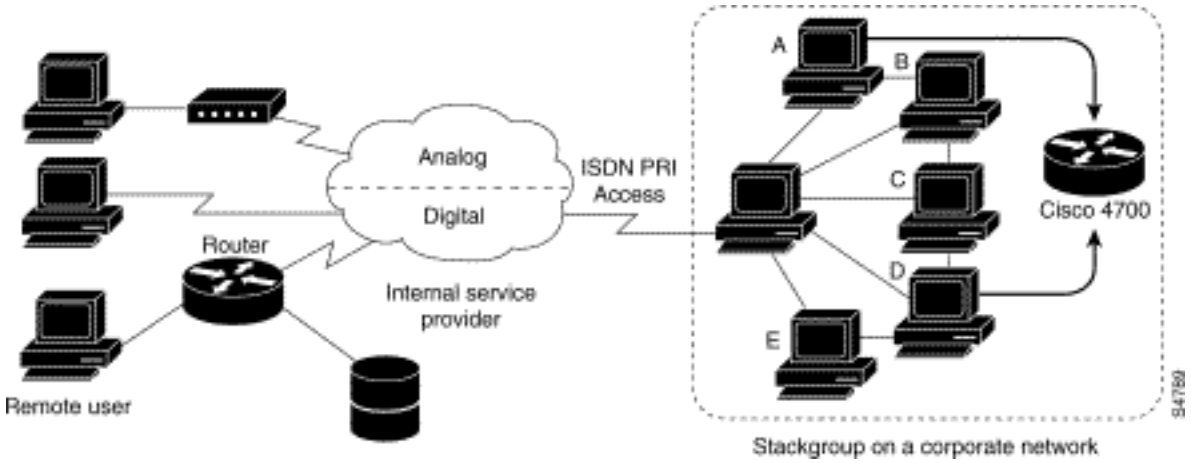

図 16-11：オフロード ルータをスタック グループ メンバとして持つマルチシャーシ マルチリンク PPP

注：異なるアクセスサーバ、スイッチング、およびルータプラットフォームを使用して、スタックグループを構築できます。ただし、Cisco AS5200 などのユニバーサル アクセス サーバを ISDN と組み合わせないでください。これは 4x00 プラットフォームなどのアクセス サーバだけと組み合わせる必要があります。セントラル オフィスからのコールは無秩序に割り当てられるため、この組み合せの結果、アナログ コールがデジタル専用のアクセス サーバに配送されて処理ができなくなる恐れがあります。

ルータのグループで MMP をサポートするためには、次のものをサポートするように各ルータを設定する必要があります。

- マルチリンク PPP
- Stack Group Bidding Protocol（SGBP）
- MMP をサポートするためにインターフェイス コンフィギュレーションをクローニングする際に使用されるバーチャル テンプレート

仮想プロファイル

バーチャル プロファイルは、ダイヤルイン コールの受信時にバーチャル アクセス インターフェイスを動的に作成、設定でき、コール終了時にインターフェイスを動的にティア ダウンできる、一意な Point-to-Point Protocol（PPP）アプリケーションです。バーチャル プロファイルは単純な PPP および Multilink PPP（MLP; マルチリンク PPP）で動作します。

バーチャル プロファイルのバーチャル アクセス インターフェイスの設定情報は、バーチャル テンプレート インターフェイスから、または Authentication, Authorization and Accounting（AAA; 認証、認可、およびアカウンティング）サーバに格納されているユーザ固有の設定から、あるいはその両方から、生成できます。

バーチャル プロファイルで使用されるユーザ固有の AAA コンフィギュレーションは*インターフェイス コンフィギュレーションであり、LCP のネゴシエーション時にダウンロードされます。*ユーザ単位コンフィギュレーションと呼ばれるもう 1 つの機能もまた、AAA サーバから取得されるコンフィギュレーション情報を使用します。ただし、ユーザ単位のコンフィギュレーションでは、NCP のネゴシエーション時にダウンロードされるネットワーク コンフィギュレーション（アクセス リストやルート フィルタなど）が使用されています。

バーチャル プロファイルのバーチャル テンプレート インターフェイス、および AAA コンフィギュレーションによる、バーチャル アクセス インターフェイスの設定は、次の 2 つの規則に従います。

- バーチャル アクセス アプリケーションはそれぞれ、クローニングするためのテンプレートを最大でも 1 つしか持つことができない。ただし、クローニングするための AAA コンフィギュレーションは複数持つことができます（バーチャル プロファイルの AAA 情報と AAA ユーザ単位コンフィギュレーション。これらにはさらに複数のプロトコルに対応した設定が含まれる場合もあります）。
- バーチャル プロファイルがバーチャル テンプレートによって設定されると、そのテンプレートは他のすべてのバーチャル テンプレートよりも高い優先順位を持つ。

考えられるコンフィギュレーション シーケンスについての詳細は、後述の「他の Cisco ダイヤル機能とのインターオペラビリティ」のセクションを参照してください。コンフィギュレーション シーケンスは、バーチャル テンプレート インターフェイスをクローニングする MLP や別のバー

チャル アクセス機能の有無によって異なります。

この機能は MLP をサポートしているすべての Cisco IOS プラットフォームで動作します。

このセクションで説明されているコマンドについての詳細は、Cisco IOS ドキュメント セットの『*ダイヤル ソリューション コマンド リファレンス*』の「バーチャル プロファイル コマンド」の章を参照してください。この章に記載されている他のコマンドのドキュメントについては、コマンド リファレンスのマスター インデックスやオンライン検索を利用して参照してください。

背景説明

このセクションでは、バーチャル プロファイル アプリケーションの設定を始める前にその理解に役立つ、バーチャル プロファイルに関する背景について説明しています。

制約事項

重複するネットワーク アドレスがバーチャル アクセス インターフェイスに作成されることのないように、バーチャル テンプレート インターフェイスでは番号未指定アドレスを使用することをお勧めします。

前提条件

バーチャル プロファイルで AAA インターフェイス コンフィギュレーション情報を使用するには、ルータを AAA 用に設定し、AAA サーバを、ユーザ固有のインターフェイス コンフィギュレーション AV ペアを持つように設定する必要があります。関連する AV ペア（RADIUS サーバ上）の始まりは次のようになります。

```
cisco-avpair = "lcp:interface-config=...",
```

等号（=）の後の情報には任意の Cisco IOS インターフェイス設定コマンドを指定できます。たとえば次の行のようになります。

```
cisco-avpair = "lcp:interface-config=ip address 200.200.200.200
255.255.255.0",
```

バーチャル プロファイルでバーチャル テンプレート インターフェイスを使用するには、バーチャル テンプレートをバーチャル プロファイル用に特別に定義する必要があります。

他の Cisco ダイヤル機能とのインターオペラビリティ

バーチャル プロファイルは、Cisco の DDR、Multilink PPP（MLP; マルチリンク PPP）、および ISDN などのダイヤラと協調動作します。

物理インターフェイスの DDR コンフィギュレーション

バーチャル プロファイルは、バーチャル アクセス インターフェイス アプリケーションが他に設定されていないときに、次の DDR コンフィギュレーション状態において物理インターフェイスと完全に協調動作します。

- ダイヤラ プロファイルがインターフェイス用に設定されているとき。ダイヤラ プロファイルがバーチャル プロファイルの設定の代わりに使用されます。
- DDR がインターフェイスで設定されていないとき。バーチャル プロファイルによって現在の設定は無効になります。
- レガシー DDR がインターフェイスで設定されているとき。バーチャル プロファイルによって現在の設定は無効になります。

注：ダイヤラーインターフェイス (任意のISDNダイヤラを含む) が使用されている場合、その設定は仮想プロファイル設定ではなく物理インターフェイスで使用されます。

バーチャル アクセス インターフェイスのコンフィギュレーションに対するマルチリンク PPP の効果

表 16-8 に示すように、バーチャル アクセス インターフェイスの正確な設定は次の 3 つの要因によって決まります。

- バーチャル プロファイルが、バーチャル テンプレートによって、または AAA によって、またはその両方によって、あるいはそのどちらにもよらずに、設定されているかどうか。表ではこれらの状態をそれぞれ「VP VT のみ」、「VP AAA のみ」、「VP VT および VP AAA」、「VP なし」と表記しています。
- ダイヤラ インターフェイスの有無。
- MLP の有無。列の見出し「MLP」は、MLP をサポートし、バーチャル テンプレート インターフェイスからクローニングされる、任意のバーチャル アクセス機能を表しています。

表 16-8 で、「マルチリンク VT」は、バーチャル テンプレート インターフェイスが MLP または MLP を使用するバーチャル アクセス機能に対して定義された場合、これがクローニングされることを意味します。

表 16-8 : バーチャル プロファイル コンフィギュレーションのクローニング シーケンス

バーチャル プロファイルの設定	MLP ダイヤラなし	MLP ダイヤラ	MLP なしダイヤラなし	MLP なしダイヤラ
VP VT のみ	VP VT	VP VT	VP VT	VP VT
VP AAA のみ	（マルチリンク VT）VP AAA	（マルチリンク VT）VP AAA	VP AAA	VP AAA
VP VT および VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA	VP VT VP AAA
VP なし	（マルチリン	ダイヤラ	バーチャル アクセス インターフェイスは作	バーチャル アクセス インターフェイスは作

	ク VT)		成されません。	成されません。

表内のどの枠についても、各項目の順序が重要です。VP VT が VP AAA よりも上にある枠は、最初にバーチャル プロファイルのバーチャル テンプレートがインターフェイスでクローニングされ、それからユーザ用の AAA インターフェイスの設定が適用されることを意味します。ユーザ固有の AAA インターフェイス コンフィギュレーションが設定に追加され、競合する物理インターフェイスやバーチャル テンプレート設定コマンドはすべて無効になります。

バーチャル テンプレートを使用する他の機能とのインターオペラビリティ

バーチャル プロファイルはバーチャル テンプレート インターフェイスをクローニングするバーチャル アクセス アプリケーションとも協調動作します。バーチャル アクセス アプリケーションはそれぞれ、クローニングするためのテンプレートをたかだか 1 つしか持つことができませんが、複数の AAA コンフィギュレーションからクローニングすることは可能です。

バーチャル プロファイルとその他のバーチャル テンプレート アプリケーションとのやり取りは次のようになります。

- バーチャル プロファイルがイネーブルになっていて、そのためのバーチャル テンプレートが定義されている場合、そのバーチャル プロファイルのバーチャル テンプレートが使用される。
- バーチャル プロファイルが AAA だけによって設定されている場合 (バーチャル プロファイルのためのバーチャル テンプレートが定義されていない場合)、別のバーチャル テンプレート アプリケーション (VPDN など) のバーチャル テンプレートをバーチャル アクセス インターフェイスでクローニングできる。
- バーチャル テンプレートが存在する場合、バーチャル プロファイルの AAA コンフィギュレーションまたは AAA ユーザ単位コンフィギュレーションよりも前に、バーチャル テンプレートがバーチャル アクセス インターフェイスでクローニングされる。AAA ユーザ単位コンフィギュレーションが使用される場合は、一番最後に適用される。

用語

この章で使用している新しい用語または一般的でない用語を次に示します。

AV ペア：AAAサーバの設定パラメータ。ユーザ固有の許可要求に応答して、AAAサーバがルータに送信するユーザ設定の一部。ルータは個々の AV ペアを Cisco IOS ルータ設定コマンドと解釈し、AV ペアを順に適用します。この章では、AV ペアという用語を、RADIUS サーバでのインターフェイス コンフィギュレーション パラメータの意味で使用しています。

バーチャル プロファイルのインターフェイス コンフィギュレーションの AV ペアは次のような形式をとることができます。

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
```

クローニング：特定のバーチャル テンプレートからの設定コマンドを適用してバーチャル アクセス インターフェイスを作成、設定すること。バーチャル テンプレートは、汎用的なユーザ情報とルータ固有の情報のソースとなります。クローニングの結果、バーチャル アクセス インターフェイスが作成され、テンプレート内のコマンドがすべて設定されます。

バーチャル アクセス インターフェイス：動的に作成されて一時的に存在する、一意なバーチャル インターフェイスのインスタンス。バーチャル アクセス インターフェイスは、バーチャル プロファイルやバーチャル プライベート ダイヤルアップ ネットワークなど、各種のアプリケーションによってさまざまに作成、設定されます。

バーチャル テンプレート インターフェイス：特定のユーザまたは特定の用途向けに作成される汎用のインターフェイス コンフィギュレーションに、ルータ固有の情報が加えられたもの。バーチャル テンプレート インターフェイスは、必要に応じてバーチャル インターフェイスに適用される Cisco IOS インターフェイス コマンドのリストの形式をとります。

バーチャル プロファイル：特定のユーザのコールイン時に動的に作成され、コールの接続解除時に動的にティア ダウンされる、一意なバーチャル アクセス インターフェイスのインスタンス。特定のユーザのバーチャル プロファイルは、バーチャル テンプレート インターフェイスによって、または AAA サーバに格納されているユーザ固有のインターフェイス コンフィギュレーションによって、あるいは、バーチャル テンプレート インターフェイスと AAA からのユーザ固有のインターフェイス コンフィギュレーションの両方によって、設定できます。

バーチャル アクセス インターフェイスの設定は、バーチャル テンプレート インターフェイスで始まり（存在する場合）、その後に、特定のユーザのダイヤルイン セッションに対応したユーザ固有コンフィギュレーションのアプリケーション（存在する場合）が続きます。

PPP ネゴシエーションの例（注釈付き）

この例では、ping によってルータ *Montecito* と *Goleta* との間に ISDN リンクが始動します。この例ではタイムスタンプが記載されていませんが、通常はグローバル設定コマンド **service timestamps debug datetime msec** を使用することを推奨いたします。

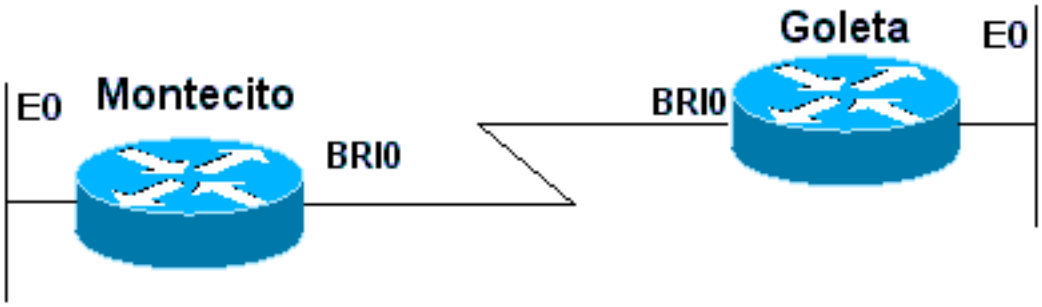

図 16-12：ルータ-ISDN-ルータ

これらのデバッグはMontecitoから行われます。しかし、Goletaのデバッグは同様に見えるだろう。

注：デバッグは別の形式で表示されることがあります。この出力は古い PPP デバッグ形式であり、IOS バージョン 11.2(8) で導入された修正版よりも前のものです。 新しいバージョンの IOS における PPP デバッグの例については、17 章を参照してください。

```
Montecito#show debugging

  PPP:

    PPP authentication debugging is on

    PPP protocol negotiation debugging is on
```

A
Montecito#**ping 172.16.20.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 172.16.20.2, timeout is 2 seconds:

B
%LINK-3-UPDOWN: Interface BRI0: B-Channel 1, changed state to up

C
ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5

C
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

D
PPP BRI0: B-Channel 1: received config for type = 0x3 (AUTHTYPE)
value = 0xC223 digest = 0x5 acked

D
PPP BRI0: B-Channel 1: received config for type = 0x5 (MAGICNUMBER)
value = 0x28FC9083 acked

E
PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0xC021): rcvd id 0x65

F
ppp: config ACK received, type = 3 (CI_AUTHTYPE), value = C223

F
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 29EBD1A7

G
PPP BRI0: B-Channel 1: Send CHAP challenge id=1 to remote

H
PPP BRI0: B-Channel 1: CHAP challenge from Goleta

J
PPP BRI0: B-Channel 1: CHAP response id=1 received from Goleta

K
PPP BRI0: B-Channel 1: Send CHAP success id=1 to remote

L
PPP BRI0: B-Channel 1: remote passed CHAP authentication.

M
PPP BRI0: B-Channel 1: Passed CHAP authentication with remote.

N
ipcp: sending CONFREQ, type = 3 (CI_ADDRESS), Address = 172.16.20.1

P
ppp BRI0: B-Channel 1: Negotiate IP address: her address 172.16.20.2 (ACK)

Q
ppp: ipcp_reqci: returning CONFACK.

R
PPP BRI0: B-Channel 1: state = ACKsent fsm_rconfack(0x8021): rcvd id 0x25

```
S
 ipcp: config ACK received, type = 3 (CI_ADDRESS), Address = 172.16.20.1

T
 BRI0: install route to 172.16.20.2

U
 %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0: B-Channel 1,
changed state to up
```

A：ダイヤル試行を開始するためにトラフィックが生成されます。

B：接続が確立されます（この例では ISDN デバッグは使用していません）。

LCP の開始：

C：*Montecito* から、AUTHTYPE および MAGICNUMBER のための LCP 設定要求が送信されます。

D：*Goleta* からその CONFREQ が送信されます。MAGICNUMBER の値が *Montecito* から送信された値と同じ場合は、回線がループしている可能性が高いといえます。

E：*Montecito* から、*Goleta* の CONFREQ への確認応答が送信されたことを示しています。

F：*Montecito* で *Goleta* からの CONFACK を受信します。

認証フェーズの開始：

G、H：*Montecito* と *Goleta* で、認証のために相互の身元証明要求を行います。

J：*Goleta* が身元証明要求に応答します。

K、L：Goleta が正常に認証を通過します。

M - GoletaからMontecitoへのメッセージ:authentication successful.

NCP ネゴシエーションの開始：

N、P：各ルータが CONFREQ の中で、自身に設定された IP アドレスを送信します。

Q、R：*Montecito* から、*Goleta* の CONFREQ への CONFACK が送信されます。

S - ?その逆も同様です

T、U：*Montecito* から *Goleta* へのルートが設置され、インターフェイス上のプロトコルが「アップ」状態に変わり、NCP ネゴシエーションが正常に完了したことを示します。

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

- Cisco IOS ダイヤル ソリューション ガイド
- ダイヤル アクセスに使用されるインターフェイス、コントローラ、および回線の概要
- モデム回線でのルーティング
- シリアル ポートと T1/E1 トランクの設定
- DDR インターネットワークの設計
- DDR 設定のための判断と準備
- DDR タイトルの設定
- PPP テクノロジー概要
- ISDN インターネットワークの設計
- ISDN スイッチ タイプ、コード、および値
- ISDN 回線のプロビジョニング
- テクニカル サポートとドキュメント – Cisco Systems