

シリアル回線の問題に関するトラブルシューティング

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[show interfaces serial コマンドを使用するトラブルシューティング](#)

[show interfaces serial](#)

—

—

[総インターフェイストラフィックの 1% を超える入力エラーの増加](#)

—

—

[show controllers コマンドの使用](#)

[debug コマンドの使用](#)

[拡張 ping テストの使用](#)

[ping テストの実行](#)

[クロッキング問題のトラブルシューティング](#)

[クロッキング概要](#)

[クロッキング問題の原因](#)

[クロッキング問題の検出](#)

[クロッキング問題の切り分け](#)

[クロッキング問題のソリューション](#)

[バッファの調整](#)

[システム バッファの調整](#)

[保留キュー制限の実装](#)

[プライオリティ キューイングを使用したボトルネックの緩和](#)

[特殊なシリアル回線のテスト](#)

[CSU と DSU のループバック テスト](#)

[HDLC リンクや PPP リンク用の CSU と DSU のローカル ループバック テスト](#)

[HDLC リンクや PPP リンク用の CSU と DSU のリモート ループバック テスト](#)

[show interfaces serial コマンドに関する詳細情報](#)

[show interfaces serial のパラメータ](#)

[T1 のトラブルシューティング](#)

[show controller t1 コマンドを使用するトラブルシューティング](#)

[show controller t1 の状態](#)

[T1 エラー イベントのトラブルシューティング](#)

[ISDN スイッチ タイプと PRI グループが正しく設定されていることの検証](#)

[シグナリング チャネルの検証](#)

[PRI のトラブルシューティング](#)

[ハードウェア ループバック プラグ テストの実行](#)

[E1 のトラブルシューティング](#)

[show controller e1 コマンドを使用するトラブルシューティング](#)

[E1 エラー イベントのトラブルシューティング](#)

[ISDN スイッチ タイプと PRI グループが正しく設定されていることの検証](#)

[シグナリング チャネルの検証](#)

[PRI のトラブルシューティング](#)

[関連情報](#)

概要

この章では、一般的なトラブルシューティング情報、およびシリアル接続のトラブルシューティングのためのツールとテクニックについての説明が紹介されています。この章は次のセクションで構成されています。

- **show interfaces serial** コマンドを使用するトラブルシューティング
- **show controllers** コマンドの使用
- **debug** コマンドの使用
- 拡張 **ping** テストの使用
- クロッキング問題のトラブルシューティング
- バッファの調整
- 特殊なシリアル回線のテスト
- **show interfaces serial** コマンドに関する詳細情報
- T1 問題のトラブルシューティング
- E1 問題のトラブルシューティング

前提条件

要件

このドキュメントの読者は次の定義に関する知識が必要です。

- DTE = data terminal equipment (データ端末装置)
- CD = Carrier Detect (キャリア検知)
- CSU = channel service unit (チャネル サービス ユニット)
- DSU = digital service unit (デジタル サービス ユニット)
- SCTE = serial clock transmit external (シリアル クロック送信外部)
- DCE = data circuit-terminating equipment (データ回線終端装置)
- CTS = clear-to-send (クリア ツー センド)
- DSR = data-set ready (データセット レディ)
- SAP = Service Advertising Protocol (サービス アドバタイジング プロトコル)
- IPX = Internetwork Packet Exchange

- FDDI = Fiber Distributed Data Interface (ファイバ分散データ インターフェイス)
- ESF = Extended Superframe Format (拡張スーパーフレーム フォーマット)
- B8ZS = binary eight-zero substitution
- LBO = Line Build Out (回線整合)

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、クリアな (デフォルト) 設定で作業を開始しています。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。

show interfaces serial コマンドを使用するトラブルシューティング

show interfaces serial EXEC コマンドの出力には、シリアル インターフェイスに特化した情報が表示されます。図 15-1 には、ハイレベル データリンク コントロール (HDLC) のシリアル インターフェイスでの **show interfaces serial EXEC** コマンドの出力が示されています。

このセクションでは、**show interfaces serial** コマンドを使用してワイドエリア ネットワーク (WAN) 環境でのシリアル回線の接続問題を診断する方法を説明しています。後続のセクションでは、コマンド出力の重要なフィールドをいくつか取り上げて説明しています。

この表示に示されている他のフィールドは、この章の後のセクション「**show interfaces serial** コマンドに関する詳細情報」で詳細に説明されています。

シリアル回線 : show interfaces serial のステータス行の状態

show interfaces serial で表示されるインターフェイス ステータス行 (図 15-1 参照) では、下記の 5 つの問題ステートが識別される可能性があります。

- Serial x is down, line protocol is down
- Serial x is up, line protocol is down
- Serial x is up, line protocol is up (looped)
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

図 15-1 : HDLC show interface serial コマンドの出力

```

monet>show interfaces serial 0
Serial 0 is up, line protocol is up --Interface status line
Hardware is MCI Serial
Internet address is 131.108.156.98, subnet mask is 255.255.255.240
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 5762 drops, input queue 0/75, 301 drops
Five minute input rate 9000 bits/sec, 16 packets/sec
Five minute output rate 9000 bits/sec, 17 packets/sec
5780806 packets input, 785841604 bytes, 0 no buffer
Received 757 broadcasts, 0 runts, 0 giants
146124 input errors, 87243 CRC, 58857 frame, 0 overrun, 0 ignored, 3 abort
5298821 packets output, 765669598 bytes, 0 underruns
0 output errors, 0 collisions, 2941 interface resets, 0 restarts
2 carrier transitions
Carrier transitions
Framing errors
Interface resets
Input errors
Output drops
Input Drops
Abort errors

```

15-1 シリアル回線： show interfaces serial のステータス行の状態：この表には、インターフェイスのステータス状態、その状態に関連する可能性のある問題、それらの問題に対するソリューションが示されています。

ステータス行の状態	考えられる問題	解決策
Serial x is up, line protocol is up		これは正常なステータス行の状態です。操作は不要です。
Serial x is down, line protocol is down	<ul style="list-style-type: none"> 通常、ルータで CD シグナルが検出されていない（つまり、CD がアクティブではない）ことを示す。 電話会社の問 	<ol style="list-style-type: none"> CSU/DSU で LED をチェックして、CD がアクティブかどうかを確認する。あるいは、回線にブレークアウトボックスを挿入して CD シグナルをチェックする。 適切なケーブルとインターフェイスが使用されていることを確認する（ハードウ

<p style="writing-mode: vertical-rl; text-orientation: upright;">ot oc ol is do wn (D TE m od e)</p>	<p>題：回線がダウンになっているか、回線が CSU/DSU に接続されていない。</p> <ul style="list-style-type: none"> • ケーブル接続に障害があるか、ケーブル接続が正しくない。 • ハードウェア障害 (CSU/DSU)。 	<p>エア インストールのドキュメントを参照)。</p> <ol style="list-style-type: none"> 3. ブレークアウト ボックスを挿入して、制御線をすべてチェックする。 4. 使用している専用回線その他のキャリア サービスに問い合せて、問題がないかどうかを確認する。 5. 障害のある部品を交換する。 6. ルータのハードウェアの障害が疑われる場合は、シリアル回線を他のポートに切り替える。これで接続が回復した場合は、前に接続されていたインターフェイスに問題があります。
<p style="writing-mode: vertical-rl; text-orientation: upright;">Se ria l is up , lin e pr ot oc ol is do wn (D TE m od e)</p>	<ul style="list-style-type: none"> • ローカルカリモートのルータの設定が誤っている。 • リモートのルータからキープライブが送信されていない。 • 専用回線その他のキャリア サービスの問題：ノイズの多い回線、あるいは、誤設定されているか障害が発生しているスイッチ。 • ケーブル上のタイミングの問題 (CSU/DSU で SCTE が設定されていない)。ローカルカリモートの CSU/DSU の障害 	<ol style="list-style-type: none"> 1. モデム、CSU、あるいは DSU をローカル ループバック モードに設定し、show interfaces serial コマンドを使用して、回線プロトコルがアップするかどうかを確認する。これで回線プロトコルがアップになったら、問題はおそらく電話会社の問題カリモート ルータの障害です。 2. リモート エンドに問題がありそうな場合は、リモートのモデム、CSU、あるいは DSU でステップ 1 を繰り返す。 3. ケーブル接続をすべて確認する。正しいインターフェイス、正しい CSU/DSU、正しい電話会社のネットワーク終端ポイントにケーブルが接続されていることを確認します。どのケーブルがどのインターフェイスに接続されているかを確認するには、show controllers EXEC コマンドを使用します。 4. debug serial interface

- ローカルカリモートの CSU/DSU の障害。
- ルータのハードウェア障害（ローカルあるいはリモート）。

EXEC コマンドをイネーブルにする。注意：デバッグの出力には、CPU プロセスでの高い優先度が割り当てられているので、システムが使用できなくなる可能性があります。そのため、debug コマンドは、絞り込まれた問題のトラブルシューティングか、Cisco のテクニカルサポート スタッフとのトラブルシューティング セッション中に限定的に使用してください。さらに、ネットワークのトラフィック量が低い時間帯やユーザが少ない時間帯に debug コマンドを使用するのがベストです。デバッグをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

5. 回線プロトコルがローカルループバック モードでアップにならず、debug serial interface EXEC コマンドの出力でキープアライブ カウンタが増加していない場合、ルータのハードウェアの問題が疑われます。ルータのインターフェイス ハードウェアを交換してください。
6. これで回線プロトコルがアップになって、キープアライブ カウントが増加したら、ローカル ルータには問題はありません。この章で後述されている「クロッキング問題のトラブルシューティング」セクションと「CSU と DSU のループバック テスト」セクションでの説明に従って、シリアル回

		<p>線のトラブルシューティングを行ってください。</p> <p>7. ルータのハードウェアの障害が疑われる場合は、シリアル回線を他のポートに切り替える。これで接続が回復した場合は、前に接続されていたインターフェイスに問題があります。</p>
<p>Serial is up, line protocol is down (DCE mode)</p>	<ul style="list-style-type: none"> • clockrate インターフェイス設定コマンドがない。 • DTE デバイスで SCTE モードがサポートされていないか、SCTE モード用には設定されていない。 • リモートの CSU や DSU の障害。 • ケーブル接続に障害があるか、ケーブル接続が正しくない。 • ルータのハードウェア障害。 	<ol style="list-style-type: none"> 1. シリアル インターフェイスに clockrate インターフェイス設定コマンドを追加する。構文: clock rate bps シンタクスの記述: <i>bps</i>: ビット/秒での要求クロックレート。1200、2400、4800、9600、19200、38400、56000、64000、72000、125000、148000、250000、500000、800000、1000000、1300000、2000000、4000000、あるいは 8000000。 2. 可能な場合は、DTE デバイスを SCTE モードに設定する。使用している CSU/DSU で SCTE がサポートされていない場合は、Cisco ルータのインターフェイスで SCTE をディセーブルにする必要がある可能性があります。この章で後述されているセクション「送信クロックの反転」を参照してください。 3. 正しいケーブルが使用されていることを確認する。 4. それでも回線プロトコルがダウンしている場合、ハードウェア障害かケーブル接続の問題である可能性があります。ブレークアウトボックスを挿入して、配線を確認します。 5. 必要に応じて障害のある部品を交換する。

<p>Serialisup, line protocol is up (looped)</p>	<p>回線にループが発生している。ループが最初に検出されると、キーパライブ パケット内のシーケンス番号がランダムな数字に変わります。リンク経由で同じランダム番号が返されてくる場合は、ループが存在します。</p>	<ol style="list-style-type: none"> 1. show running-config 特権 EXEC コマンドを使用して、何らかのループバック インターフェイス設定コマンド エントリを検索する。 2. loopback インターフェイス設定コマンド エントリが見つかった場合は、no loopback インターフェイス設定コマンドを発行してループを排除する。 3. loopback インターフェイス設定コマンドが見つからない場合は、CSU/DSU を調べて、マニュアル ループバック モードに設定されているかどうかを確認する。そのように設定されている場合は、マニュアル ループバックをディセーブルにする。 4. CSU か DSU をリセットして、回線ステータスを確認する。回線プロトコルがアップする場合は、他の操作は不要です。 5. CSU か DSU がマニュアル ループバック モードに設定されていない場合、専用回線その他のキャリア サービスに問い合せて、回線のトラブルシューティングのサポートを求めてください。
<p>Serialisup, line protocol is down (di</p>	<ul style="list-style-type: none"> • 電話会社のサービスの問題によりエラー率が高い。 • CSU か DSU のハードウェアの問題。 • 不良ルータ ハードウェア (インターフェイス)。 	<ol style="list-style-type: none"> 1. シリアル アナライザとブレイクアウト ボックスで回線をトラブルシューティングする。トグルしている CTS シグナルと DSR シグナルを検索する。 2. CSU/DSU をループさせる (DTE ループ)。問題が続く場合は、ハードウェアに問題がある可能性があります。問題がなくなった場合は、電話会社に問題がある可能性があります。 3. 必要に応じて不良ハードウェアを交換する (CSU、

sa bl ed)		DSU、スイッチ、ローカル またはリモートのルータ)。
Se ria l x is ad mi nis tra tiv ely do wn , lin e pr ot oc ol is do wn	<ul style="list-style-type: none"> • ルータのコン フィギュレー ションに shutdown イン ターフェイ ス設定コマン ドがある。 • IP アドレスの 重複。 	<ol style="list-style-type: none"> 1. ルータのコンフィギュレー ションで shutdown コマン ドをチェックする。 2. no shutdown インターフェ イス設定コマンドを使用して、shutdown コマンドを 無効にする。 3. show running-config 特権 EXEC コマンドか show interfaces EXEC コマンド を使用して、同一の IP ア ドレスがないことを確認す る。 4. 重複アドレスがある場合は 、その IP アドレスの一方 を変更して競合を解消する 。

シリアル回線：シリアル リンクでの出力廃棄の増加

show interfaces serial コマンドの出力 (図 15-1 参照) には、システムから転送バッファにパケッ
トが渡されようとした際に使用できるバッファがない場合の出力廃棄が示されています。

症状：シリアル リンクでの出力廃棄が増加している。

表 15-2 シリアルライン: シリアル リンクでの出力廃棄の増加：この表では、この症状を引き起こ
す可能性のある問題の概要と推奨のソリューションが概説されています。

考えられる 問題	解決策
シリアル インターフ ェイスへの 入力レート が、シリア ルリンク で利用可能 な帯域幅を 超過してい る。	<ol style="list-style-type: none"> 1. アクセス リストの使用やその他の手段 で、ルーティング アップデートや SAP アップデートなどの定期的なブ ロードキャストトラフィックを最小化す る。たとえば、ipx sap-interval インタ ーフェイス設定コマンドを使用して、 SAP アップデート間の遅延を大きくし ます。 2. hold-queue out インターフェイス設定 コマンドを使用して、出力保留キュー のサイズを小刻み (たとえば、25

	<p>%) に増加させる。</p> <p>3. 該当のインターフェイスで、頻繁に使用されるプロトコルとしてファーストスイッチングをオフにする。たとえば、<code>no ip route-cache</code> インターフェイス設定コマンドを入力して、IP ファーストスイッチングをオフにします。他のプロトコルのコマンド構文については、Cisco IOS のコンフィギュレーションガイドとコマンドリファレンスを参照してください。</p> <p>4. プライオリティ リストを作成して、低速のシリアル リンクにプライオリティキューイングを実装する。プライオリティ リストの設定についての情報は、Cisco IOS のコンフィギュレーションガイドとコマンドリファレンスを参照してください。</p> <p>注: 特定の状況では、出力廃棄を受容することができません。たとえば、リンクが過剰に使用されていることがわかっていて、その状況を緩和する方法がない場合、パケットを保留するよりも廃棄した方が望ましい場合があります。TCP/IP や Novell IPX などの、フロー制御がサポートされていてデータの再送が可能なプロトコルがこれに該当します。一方、DECnet やローカルエリアトランスポートなどの一部のプロトコルはパケットの廃棄の影響を受け易く、再送機能は、たとえ有ったとしても、不十分なものです。</p>
--	---

シリアル回線：シリアル リンクでの入力廃棄の増加

`show interfaces serial EXEC` コマンドの出力 (図 15-1 参照) には、インターフェイスからの過剰なパケットが引き続きシステムで処理中であることが示されています。

症状：シリアル リンクでの入力廃棄が増加している。

表 15-3：シリアル回線：シリアル リンクでの入力廃棄の増加：この表では、この症状を引き起こす可能性のある問題の概要と推奨のソリューションが概説されています。

考えられる問題	解決策
<p>入力レートがルータのキャパシティを超過しているか、入力キューが出力キューのサイズを超過している。</p>	<p>注: 通常、入力廃棄の問題が発生するのは、イーサネット、トークンリング、FDDI などのより高速なインターフェイスとシリアル インターフェイス間でトラフィック</p>

	<p>クがルーティングされる場合です。トラフィックが軽い場合は、問題はありません。トラフィックレートが増加するに従って、パケットドロップの発生が始まります。このような輻輳の時間帯に、ルータではパケットが廃棄されます。</p> <ol style="list-style-type: none"> 1. パケットを廃棄しているインターフェイスに対して、共通の宛先インターフェイスでの出力キューを増加させる。 hold-queue out インターフェイス設定コマンドを使用します。 show interfaces の出力に廃棄が表示されなくなるまで、これらのキューを小刻み（たとえば、25%）に増加させます。デフォルトの出力保留キューの制限は100 パケットです。 2. hold-queue in インターフェイス設定コマンドを使用して入力キューのサイズを縮小し、入力廃棄を強制的に出力廃棄にさせる。出力廃棄の方が入力廃棄よりもルータのパフォーマンスへの影響が小さくなります。デフォルトの入力保留キューは75 パケットです。
--	---

シリアル回線：総インターフェイストラフィックの1%を超える入力エラーの増加

show interfaces serial の出力（図 15-1 参照）に入力エラーが示されている場合、これらのエラーには発生源が何通りか考えられます。可能性の高い発生源を「表 15-4」にまとめてあります。

注: 巡回冗長検査（CRC）エラー、フレーミングエラー、あるいは総インターフェイストラフィックの1%を超える打ち切り（abort）などの何らかの入力エラーの値は、切り分けや修復が必要なある種のリンクの問題を示しています。

症状：総インターフェイストラフィックの1%を超える入力エラーの増加。

表 15-4：シリアル回線：総インターフェイストラフィックの1%を超える入力エラーの増加

考えられる問題	解決策
<p>この症状には、次の原因が考えられます。</p> <ul style="list-style-type: none"> • 電話会社の機器の障害 • ノイズの多いシリアル回線 • 不適切なクロッキング設定 (SCTE 未設定) • 不適切なケーブルあるいは長すぎるケーブル • 不良ケーブルあるいは不良接続 • 不良 CSU あるいは不良 DSU • 不良ルータ ハードウェア • ルータと DSU の間で使用されているデータコンバータやその他のデバイス 	<p>注: WAN やシリアル ネットワークにルータを接続している場合には、データコンバータを使用しないことを強く推奨いたします。</p> <ol style="list-style-type: none"> 1. シリアル アナライザを使用して、入力エラーの発生源を割り出す。エラーを検出した場合、ルータの外部のデバイスにハードウェアの問題やクロックのミスマッチがあることが考えられます。 2. ループバックと ping テストを使用して、具体的な問題の発生源を割り出す。詳細は、この章で後述されているセクション「trace コマンドの使用」とセクション「CSU と DSU のループバックテスト」を参照してください。 3. パターンを見つける。たとえば、エラーが一定の間隔で発生する場合、ルーティングアップデートの送信のような定期的な機能に関連するものである可能性があります。

シリアル回線：シリアル回線での入力エラーのトラブルシューティング

表 15-5：この表では、show interfaces serial コマンドで表示される (図 15-1 参照) ささまざまなタイプの入力エラー、それらのエラーを引き起こしている可能性のある問題、それらの問題に対するソリューションが説明されています。

入力エラーのタイプ (カッコ内はフィールド名)	考えられる問題	解決策

CRC エラー (CRC)	<p>CRC エラーが発生するのは、CRC の計算が検査に通らず、データが破損していることが示されている場合で、これには下記の理由があります。</p> <ul style="list-style-type: none"> • ノイズの多いシリアル回線 • シリアルケーブルが長すぎるか、CSU/DSU からルータへのケーブルがシールドされていない。 • DSU で SCTE モードがイネーブルになっていない。 • CSU 回線クロックが不適切に設定されている。 • T1 リンクでの ones density の問題 (不適切なフレーミングやコーディングの仕様)。 	<ol style="list-style-type: none"> 1. 回線が転送要件に対して十分にクリーンであることを確認する。必要な場合は、ケーブルにシールドを施します。 2. ケーブルが推奨の長さである 15.24 m (50 フィート) あるいは T1 リンクでは 7.62 m (25 フィート) に収まっていることを確認する。 3. すべてのデバイスが共通の回線クロックに対して適切に設定されていることを確認する。ローカルとリモートの DSU で SCTE を設定します。使用している CSU/DSU で SCTE がサポートされていない場合は、この章で後述されているセクション「送信クロックの反転」を参照してください。 4. ローカルとリモートの CSU/DSU が、専用回線その他のキャリアサービス (たとえば、ESF/B8ZS) で使用されているのと同じフレーミングとコーディングのスキームに設定されていることを確認する。 5. 使用している専用回線その他のキャリアサービスに問い合わせ、回線での整合性テストを実施させる。
フレー	フレーミング エラ	1. 回線が転送要件に対

ミング
エラー
(frame
)

ーが発生するのは、
パケットが 8 ビッ
ト境界で終わってい
ない場合で、これに
は下記の理由があり
ます。

- ノイズの多いシ
リアル回線
- 不適当に指定さ
れたケーブル;
シリアルケーブ
ルは余りに長い
です; CSU また
は DSU からの
ルータへのケー
ブルは保護され
ません
- SCTE モードは
DSU で有効に
なりません;
CSU ライン ク
ロックは間違っ
て設定されてい
ます; クロック
の 1 つはローカ
ル コンピユー
タの時刻のため
に設定されます
- T1 リンクでの
ones density の
問題 (不適切な
フレーミングや
コーディングの
仕様) 。

して十分にクリーン
であることを確認す
る。 必要な場合は
、ケーブルにシールド
を施します。 適
切なケーブルを使用
していることを確認
します。

2. ケーブルが推奨の長
さである 15.24
m (50 フィート
) あるいは T1 リン
クでは 7.62 m (25
フィート) に収まっ
ていることを確認す
る。
3. すべてのデバイスが
共通の回線クロック
を使用するように適
切に設定されている
ことを確認する。
ローカルとリモート
の DSU で SCTE を
設定します。 使用
している CSU/DSU
で SCTE がサポー
トされていない場合
は、この章で後述さ
れているセクション
「送信クロックの反
転」を参照してくだ
さい。
4. ローカルとリモート
の CSU/DSU が、専
用回線その他のキャ
リア サービス (た
とえば、
ESF/B8ZS) で使用
されているのと同じ
フレーミングとコー
ディングのスキーム
に設定されているこ
とを確認する。
5. 使用している専用回
線その他のキャリア
サービスに問い合せ
て、回線での整合性
テストを実施させる

		。
<p>打ち切られた転送 (abort)</p>	<p>Aborts は、ビット列の不正なシーケンスを示します (データの中に連続する 7 個以上の "1" のビット)。これには次の理由が考えられます。</p> <ul style="list-style-type: none"> • DSU で SCTE モードがイネーブルになっていない。 • CSU 回線クロックが不適切に設定されている。 • シリアル ケーブルが長すぎるか、CSU や DSU からルータへのケーブルがシールドされていない。 • T1 リンクでの ones density の問題 (不適切なフレーミングやコーディングの仕様)。 • 転送途中で終了されたパケット : 通常、原因はインターフェイスのリセットやフフレーミングエラー。 • ハードウェアの問題 : 不良回線、不良 CSU/DSU、あるいはリモートルータでの不良送信インターフェイス。 	<ol style="list-style-type: none"> 1. すべてのデバイスが共通の回線クロックを使用するように適切に設定されていることを確認する。ローカルとリモートの DSU で SCTE を設定します。使用している CSU/DSU で SCTE がサポートされていない場合は、この章で後述されているセクション「送信クロックの反転」を参照してください。 2. 必要な場合は、ケーブルにシールドを施します。ケーブルが推奨の長さである 15.24 m (50 フィート) あるいは T1 リンクでは 7.62 m (25 フィート) に収まっていることを確認する。すべての接続が良好であることを確認します。 3. リンクの両端でハードウェアをチェックする。必要に応じて、障害のある機器を交換します。 4. データ レートを低下させて、打ち切り (abort) の頻度が下がるかどうか確認する。 5. ローカルとリモートのループバックテストを使用して、打ち切り (abort) が発生している箇所を判別する。この章で後述されているセ

		<p>クション「特殊なシリアル回線のテスト」を参照してください。</p> <p>6. 使用している専用回線その他のキャリアサービスに問い合せて、回線での整合性テストを実施させる。</p>
--	--	---

シリアル回線：シリアルリンクでのインターフェイスリセットの増加

show interfaces serial EXEC コマンドの出力 (図 15-1 参照) に示されているインターフェイスリセットは、キープアライブパケットの欠落によるものです。

症状：シリアルリンクでのインターフェイスリセットが増加している。

表 15-6: この表では、この症状を引き起こす可能性のある問題の概要と推奨のソリューションが概説されています。

考えられる問題	解決策
<p>この症状には、次の原因が考えられます。</p> <ul style="list-style-type: none"> • リンクでの輻輳 (通常は出力廃棄に関連)。 • CD 遷移を引き起こす不良回線。 • CSU、DSU、あるいはスイッチで考えられるハードウェアの問題。 	<p>インターフェイスのリセットが発生した場合、show interfaces serial コマンドの出力の他のフィールドを調べて、問題の発生源を判別します。インターフェイスのリセットでの増加が記録されているとの前提で、下記のフィールドを検査します。</p> <ol style="list-style-type: none"> 1. 高頻度の show interfaces serial 出力の output drops がある場合、セクション「シリアルライン参照して下さい: この章のシリアルリンクの Output drops を」、先に高めること。 2. show interfaces serial で示されている carrier transitions フィールドをチェックする。インターフェイスのリセットが登録されていてキャリア遷移が高頻度な場合、不良リンクや不良な CSU や DSU が問題である可能性が高くなります。専用回線やキャリアサービスに問い合せて、必要に

	<p>応じて障害機器を交換してください。</p> <p>3. show interfaces serial で示されている input errors フィールドを検査する。インターフェイスのリセットが増加していて入力エラーが高頻度な場合、不良リンクや不良 CSU/DSU が問題である可能性が高くなります。専用回線その他のキャリアサービスに問い合せて、必要に応じて障害機器を交換してください。</p>
--	---

シリアル回線：シリアルリンクでのキャリア遷移カウントの増加

キャリアシグナルに中断がある（リンクのリモートエンドでのインターフェイスのリセットなど）と常に、**show interfaces serial EXEC** コマンドの出力にはキャリア遷移が表示されます。

症状：シリアルリンクでのキャリア遷移カウントが増加している。

表 15-7 では、この症状を引き起こす可能性のある問題の概要と推奨のソリューションが概説されています。

表 15-7：シリアル回線：[シリアルリンクでのキャリア遷移カウントの増加](#)

考えられる問題	解決策
<p>この症状には、次の原因が考えられます。</p> <ul style="list-style-type: none"> ケーブルの物理的分離、赤や黄色の T1 アラーム、ネットワークのどこかへの落雷などの外部発生源による回線の中断。 障害のあるスイッチ、DSU、あるいはルータのハードウェア。 	<ol style="list-style-type: none"> リンクの両端でハードウェアをチェックする。ブレークアウトボックスやシリアルアナライザを接続してテストし、問題の発生源を判別します。 アナライザやブレークアウトボックスで外部の問題が何も判別できない場合は、ルータのハードウェアをチェックする。 必要に応じて、障害のある機器を交換します。

[show controllers コマンドの使用](#)

シリアル回線をトラブルシューティングする際の重要な診断ツールには **show controllers EXEC** コマンドもあります。このコマンド構文はプラットフォームにより異なります。

- Cisco 7000 シリーズ ルータのシリアル インターフェイスの場合は、**show controllers cbus EXEC** コマンドを使用する。
- Cisco アクセス製品の場合は、**show controllers EXEC** コマンドを使用する。
- AGS、CGS、および MGS の場合は、**show controllers mci EXEC** コマンドを使用する。

図 15-2 には、**show controllers EXEC** コマンドによる出力が示されています。このコマンドは、ファストシリアル インターフェイス プロセッサ (FSIP) カードを装備した Cisco 7000 シリーズ ルータで使用されています。このコマンド出力をチェックして、チャンネル サービス ユニット / デジタル サービス ユニット (CSU/DSU) が適切なインターフェイスに接続されていることを確認します。マイクロコードのバージョンをチェックして、それが最新であるかどうかを確認することもできます。

図 15-2: **show controllers cbus**

```
Harold>show controllers cbus
Switch Processor 5, hardware version 11.1, microcode version 10.7
Microcode loaded from system
512 Kbytes of main memory, 128 Kbytes cache memory
4 256 byte buffers, 4 1024 byte buffers, 312 1520 byte buffers
1024 byte system buffer
Restarts: 0 line down, 0 hung output, 0 controller error
FSIP 0, hardware version 1.0, microcode version 175.0
Microcode loaded from system
Interface 0 - Serial 0/0, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 1 - Serial 0/1, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 2 - Serial 0/2, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
Interface 3 - Serial 0/3, electrical interface is Universal (cable unattached)
22 buffer RX queue threshold, 23 buffer TX queue limit, buffer size 1520
TX queue length is 0
ift 0001, rql 12, tq 0000 0000, tq 23
Transmitter delay is 0 microseconds
```

Microcode version

Interface and attached cable information

Cisco 2000、Cisco 2500、Cisco 3000、および Cisco 4000 シリーズのアクセス サーバとルータでは、**show controllers EXEC** コマンドを使用します。図 15-3 は Basic Rate Interface (BRI) からの **show controllers** コマンド出力および Cisco 2503 アクセス サーバのシリアルインターフェイスを示します。(ことに注目して下さい出力は示されていません。)

show controllers の出力には、インターフェイス チャンネルの状態、および、そのインターフェイスにケーブルが接続されているかが示されます。図 15-3 では、serial interface 0 に RS-232 DTE ケーブルが接続されています。serial interface 1 にはケーブルが接続されていません。

図 15-4 には、**show controllers mci** コマンドによる出力が示されています。このコマンドが使用されるのは、AGS、CGS、および MGS の各ルータでだけです。電気インターフェイスが、V.35、EIA/TIA-449、あるいはそれ以外の電気インターフェイスタイプではなく、UNKNOWN と表示されている場合、不適切に接続されたケーブルが問題であると考えられます。不良アプリケーションやカードの内部配線の可能性もあります。電気インターフェイスが UNKNOWN になっている

場合、`show interfaces serial EXEC` コマンドでの対応表示には、そのインターフェイスと回線プロトコルがダウンであると表示されます。

図 15-3: show controllers

```
Maude>show controllers
BRI unit 0
D Chan Info:
Layer 1 is DEACTIVATED
D channel is
deactivated

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B1 Chan Info:
Layer 1 is DEACTIVATED
B channel 1 is
deactivated

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

B2 Chan Info:

[. . .]
LANCE unit 0, idb 0x9515C, ds 0x96F00, regaddr = 0x2130000, reset_mask 0x2
IB at 0x40163F4: mode=0x0000, mcfilter 0000/0000/0000/0000
station address 0000.0c0a.28a7 default station address 0000.0c0a.28a7
buffer size 1524

[. . .]
0 missed datagrams, 0 overruns, 0 late collisions, 0 lost carrier events
0 transmitter underruns, 0 excessive collisions, 0 tdr, 0 babbles
0 memory errors, 0 spurious initialization done interrupts
0 no enp status, 0 buffer errors, 0 overflow errors
0 one_col, 0 more_col, 3 deferred, 0 tx_buff
0 throttled, 0 enabled
Lance csr0 = 0x73

HD unit 0, idb = 0x98D28, driver structure at 0x9AADD0
buffer size 1524 HD unit 0, RS-232 DTE cable
Attached cable on
serial interface 0

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns

HD unit 1, idb = 0x9C1B8, driver structure at 0x9DF60
buffer size 1524 HD unit 1, No DCE cable
No attached cable on
serial interface 1

[. . .]
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
```

図 15-4: show controllers mci

Electrical interface identified as type UNKNOWN, suggesting a hardware failure or improperly connected cable.

```
MCI 1, controller type 1.1, microcode version 1.0
 128 Kbytes of main memory, 4 Kbytes cache memory
16 system TX buffers, largest buffer size 1520
Restarts: 0 line down, 0 hung output, 0 controller error
Interface 0 is Ethernet1, station address 0000.0c00.3b09
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
Interface 1 is Serial2, electrical interface is UNKNOWN
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
High speed synchronous serial interface
Interface 3 is Serial3, electrical interface is V.35 DTE
 22 total RX buffers, 9 buffer TX queue limit, buffer size 1520
Transmitter delay is 0 microseconds
High speed synchronous serial interface
```

debug コマンドの使用

さまざまな **debug** 特権 EXEC コマンドにより、多くのインターネットワーキング イベントについてのプロトコル ステータスとネットワーク アクティビティに関連する診断情報がもたらされます。

注意： デバッグの出力には、CPU プロセスでの高い優先度が割り当てられているので、システムが使用できなくなる可能性があります。このため、**debug** コマンドは、絞り込まれた問題のトラブルシューティングか、Cisco のテクニカルサポート スタッフとのトラブルシューティング セッション中に限定して使用してください。さらに、ネットワークのトラフィック量が低い時間帯やユーザが少ない時間帯に **debug** コマンドを使用するのがベストです。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。**debug** コマンドの使用が終わったら、**no debug** コマンドを個別に使用するか、または **no debug all** コマンドを使用して、必ず **debug** コマンドを無効にしてください。

シリアルの問題と WAN の問題をトラブルシューティングする際には、下記の **debug** コマンドが便利です。これらのコマンドそれぞれの情報と出力についての詳細は、**debug** コマンド リファレンスの公開情報を参照してください。

- **debug serial interface** : HDLC キープアライブ パケットが増加しているかどうかを確認します。HDLC キープアライブ パケットが増加していない場合は、インターフェイス カードまたはネットワークに、タイミングに関する問題があります。
- **debug x25 events** : 相手先選択接続 (SVC) のオープンとクローズのような X.25 のイベントを検出します。この結果の「cause and diagnostic」情報はイベント レポートにあります。
- **debug lapb** : 平衡型リンク アクセス手順 (LAPB) あるいはレベル 2 の X.25 情報を出力します。
- **debug arp** : ルータが ARP パケットで、WAN クラウドの相手側にあるルータに関する情報を送信しているか、あるいは相手側にあるルータについて学習しているかどうかが表示されます。TCP/IP ネットワークの一部のノードが応答していて、それ以外のノードが応答していない場合に、このコマンドを使用します。
- **debug frame-relay lmi** : フレーム リレー スイッチとルータで LMI パケットの送受信が行われているかどうかを判別するのに有効なローカル管理インターフェイス (LMI) 情報を取得します。
- **debug frame-relay events** : ルータとフレーム リレー スイッチ間で通信が行われているかど

うかを判別します。

- **debug ppp negotiation** : ポイントツーポイント プロトコル (PPP) オプションがネゴシエートされている PPP スタートアップ時に転送されている PPP パケットが表示されます。
- **debug ppp packet** : 送受信されている PPP パケットを表示します。このコマンドは低レベルのパケット ダンプを表示します。
- **debug ppp errors** : PPP 接続のネゴシエーションと操作に関連する PPP エラー (不正フレームや誤形式フレームなど) が表示されます。
- **debug ppp chap** : PPP チャレンジ ハンドシェイク認証プロトコル (CHAP) とパスワード認証プロトコル (PAP) のパケット交換が表示されます。
- **debug serial packet** : 送受信されているスイッチド マルチメガビット データ サービス (SMDS) パケットが表示されます。この表示には、パケットが送信されなかった理由や受信でエラーが発生した理由を示すエラー メッセージも含まれています。SMDS に関して、このコマンドでは、SMDS パケットが送受信される際の SMDS ヘッダー全体とペイロードデータの一部がダンプされます。

拡張 ping テストの使用

ping コマンドは便利なテストで、Cisco のインターネットワーキング デバイスをはじめ多くのホスト システムで利用可能です。TCP/IP においては、この診断ツールは Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) のエコー要求としても知られています。

注: `show interfaces serial` の表示に入力エラーが高レベルで登録されている場合には、ping コマンドは特に有効です。図 15-1 を参照してください。

シスコのインターネットワーキング デバイスでは、多数の ping パケットを次々と送出することを自動化するメカニズムを備えています。図 15-5 には、拡張 ping オプションを指定するのに使用されるメニューが示されています。この例では、20 件の連続 ping が指定されています。一方、使用しているシリアル回線でコンポーネントをテストする際には、1000 件の ping のように、はるかに大きい値を指定する必要があります。

図 15-5: ping

```
Betelgeuse# ping
Protocol [ip]:
Target IP address: 129.44.12.7
Repeat count [5]: 20 ping count specification
Datagram size [100]: 64
Timeout in seconds [2]:
Extended commands [n]: yes Extended commands selected option
Source address:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]: 0xFFFF Data pattern specification
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 64-byte ICMP Echos to 129.44.12.7, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

ping テストの実行

通常、シリアル回線の ping テストは次のように行います。

1. CSU や DSU をローカル ループバック モードにする。
2. さまざまなデータ パターンとパケット サイズを送信するように拡張 ping コマンドを設定する。図 15-6 と図 15-7 には、それぞれ、すべて 0 (1500 バイト) の ping とすべて 1 (1500 バイト) の ping の 2 つの有効な ping テストが示されています。
3. `show interfaces serial` コマンドの出力 (図 15-1 を参照) を検査して、入力エラーが増加したかどうかを判別する。入力エラーが増加していない場合、ローカル ハードウェア (DSU、ケーブル、ルータのインターフェイス カード) はおそらく良好な状態です。テスト シーケンスで CRC エラーとフレーミング エラーが大量に報告されているものと仮定すると、クロッキングの問題である確率が高くなります。CSU と DSU でタイミングの問題をチェックします。この章で後述されているセクション「クロッキング問題のトラブルシューティング」を参照してください。
4. クロッキングの設定が正しく、適切に動作していると判断される場合は、CSU あるいは DSU をリモート ループバック モードにする。
5. ping テストを繰り返し、入力エラーの統計情報の変化を探す。
6. 入力エラーが増加している場合は、シリアル回線か CSU/DSU のどちらかに問題があります。WAN のサービス プロバイダーに問い合せて、CSU か DSU を交換します。問題が解決しない場合は、テクニカルサポートの担当者にお問い合わせください。

図 15-6: ALI-Zeros 1500-Byte ping Test

```

yowzers#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte packet size — Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
All zeros ping — Validate reply data? [no]:
Data pattern [0xABCD]: 0x0000
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0x0000
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
yowzers#

```

図 15-7 : All-Ones 1500-Byte ping Test

```

zounds#ping
Protocol [ip]:
Target IP address: 192.169.51.22
Repeat count [5]: 100
1500 byte packet size --- Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address: 192.169.51.14
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
All ones ping --- Data pattern [0xABCD]: 0xffff
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 192.169.51.22, timeout is 2 seconds:
Packet has data pattern 0xFFFF
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/6/8 ms
zounds#

```

クロッキング問題のトラブルシューティング

シリアル接続でクロッキングの競合が発生すると、長期に渡り接続サービスが途絶えたり、パフォーマンスが低下したりする場合があります。このセクションはクロック上の問題の重要な側面を論議します: クロック上の問題原因、クロック上の問題を検出する、クロック上の問題およびクロック問題のソリューションを隔離します。

クロッキング概要

CSU/DSU では、通過するデータからデータ クロックを導出しています。クロックを復元するために、CSU/DSU ハードウェアはパススルーされたデータの 8 ビット毎にの少なくとも 1 つの 1 ビット値を受け取る必要があります; これは *ones density* として知られています。ones density が維持されると、ハードウェアではデータ クロックの信頼性を回復できます。

最近の T1 実装では、一般的に、B8ZS (binary eight-zero substitution) コーディングによる拡張スーパーフレーム フォーマット (ESF) フレーミングが使用されます。B8ZS では、シリアルリンクで 0 が連続して 8 つ送信されると、特殊なコードに置き換えられるスキームが提供されます。このコードは後で接続のリモート エンドで解釈されます。この手法により、ones density のデータ ストリームからの独立性が保証されます。

古い T1 実装では、スーパーフレーム フォーマット (SF) フレーミングとも呼ばれる D4 と交互マーク反転 (AMI) コーディングが使用されます。AMI では、B8ZS のようなコーディングスキームは使用されません。この場合、データ ストリームから独立して ones density が維持されないため、転送できるデータのタイプは制限を受けます。

シリアル通信での他の重要な要素に、シリアル クロック送信外部 (SCTE) ターミナル タイミングがあります。SCTE は、ルータなどのデータ端末装置 (DTE) デバイスから、CSU/DSU などのデータ通信装置 (DCE) デバイスにエコーバックされるクロックです。

DCE デバイスで内部クロックの代わりに SCTE を使用して DTE からのデータをサンプリングする場合、CSU/DSU とルータ間のケーブルに位相偏移があったとしても、エラーなしでデータをサンプリングできる方がよいでしょう。64 Kbps よりも高速なシリアル転送には、SCTE の使用が推奨されます。使用している CSU/DSU で SCTE がサポートされていない場合は、この章で後述されているセクション「送信クロックの反転」を参照してください。

クロッキング問題の原因

一般的には、次のいずれかが、シリアル WAN の相互接続でのクロッキング問題の原因として考えられます。

- 不適切な DSU の設定
- 不適切な CSU の設定
- 15.24 m (50 フィート) よりも長い、あるいはシールドされていない仕様外のケーブル
- ノイズが多いか、あるいは脆弱なパッチ パネルの接続
- 1 列にまとめて接続された複数のケーブル

クロッキング問題の検出

シリアル インターフェイスでのクロッキングの競合を検出するには、次のように入力エラーを探します。

1. リンクの両端のルータで **show interfaces serial EXEC** コマンドを使用する。
2. コマンド出力を検査して、CRC、フレーミング エラー、打ち切り (abort) を探す。
3. これらの手順のいずれかで、インターフェイスでのトラフィックのエラーが約 0.5 ~ 2.0 % の範囲を超えていることが示されている場合、WAN のどこかにクロッキング問題があるものと考えられます。
4. 次のセクション「クロッキング問題の切り分け」での概説に従って、クロッキングの競合の発生源を割り出す。
5. 障害のあるパッチ パネルを迂回するか、修理する。

クロッキング問題の切り分け

クロッキングの競合が入力エラーの原因であると考えられる場合、エラーの発生源を割り出すには、次の手順が有効です。

1. この章で前述されているセクション「CSU と DSU のループバック テスト」での説明に従って、一連の ping テストとループバック テスト (ローカルとリモートの両方) を実行する。
2. 問題の発生源である接続の端末、あるいは、回線に問題があるかどうかを判別する。ローカル ループバック モードで、ping テストでのさまざまなパターンとサイズ (たとえば、1500 バイトのデータグラム) を実行する。特にルータへのシリアル ケーブルや CSU/DSU が問題である場合、単一のパターンとパケット サイズでのテストでは、エラーから役立つ情報は引き出せません。
3. **show interfaces serial EXEC** コマンドを使用して、入力エラー カウントが増加しているかどうか、および、どこで頻繁に発生しているかを判別する。

入力エラーが接続の両端で頻繁に発生している場合は、ほとんどが CSU のクロッキングに問題があります。

入力エラーが一端で発生している場合は、おそらく DSU のクロッキングかケーブル接続の問題です。

一端での打ち切り (abort) は、他端が不良情報を送信しているか、回線の問題があることを示しています。

注: 常に **show interfaces serial** コマンドの出力 (図 15-1 を参照) を参照して、エラー カウントの変化をすべてログするか、あるいは特定のエラー カウントが変化していないかどうかに注意してください。

クロッキング問題のソリューション

表 15-8 シリアルライン: クロック上の問題およびソリューション: この表は問題のもとに基づいてクロック上の問題のための推奨される解決策の、輪郭を描いたものです。

考えられる問題	解決策
不適切な CSU の設定	<ol style="list-style-type: none"> 1. 両端の CSU でのクロック ソース (ローカルあるいは回線) の設定が一致しているかどうかを判別する。 2. CSU が一致しない場合、ようにそれらを設定して下さい。通常行は出典です。 3. インピーダンスが物理的 な行のそれと一致するようにするために CSU の LBO 設定をチェックして下さい。CSU を設定する上での情報は、使用している CSU のハードウェアのドキュメントを参照してください。
不適切な DSU の設定	<ol style="list-style-type: none"> 1. 両端の DSU で SCTE モードがイネーブルになっているかどうかを判別する。 2. 接続の両端で SCTE がイネーブルになっていない場合は、これをイネーブルにする。 3. ones density が維持されていることを確認する。これには、専用回線その他のキャリア サービスで使用されているものと同じフレーミングとコーディングのスキーム (たとえば、ESF と B8ZS) が DSU で使用されている必要があります。フレーミングとコーディングのスキームについての情報は、専用回線のプロバイダーに確認してください。 4. 使用しているキャリア サービスで AMI コーディングが使用されている場合は、リンクの両端で送信クロックを反転させるか、DSU をビットスタッフ モードで稼働させる。DSU を設定する上での情報は、使用している DSU のハードウェアのドキュメントを参照してください。

ルータに接続されたケーブルが仕様外	ケーブルが 15.24 m (50 フィート) よりも長い場合は、もっと短いケーブルを使用する。ケーブルがシールドされていない場合は、シールドケーブルに交換する。
-------------------	---

送信クロックの反転

SCTE がサポートされていない CSU/DSU で 64 Kbps よりも高速でシリアル接続しようとしている場合、ルータで送信クロックを反転させる必要がある可能性があります。送信クロックを反転させると、データシグナルとクロックシグナル間のフェーズのずれが補正されます。

送信クロックを反転させるのに使用される具体的なコマンドはプラットフォームにより異なります。Cisco 7000 シリーズのルータでは、`invert-transmit-clock` インターフェイス設定コマンドを入力します。Cisco 4000 シリーズのルータでは、`dte-invert-txc` インターフェイス設定コマンドを使用します。

使用しているルータに対して確実に適切なコマンド構文を使用するために、使用しているルータやアクセスサーバのユーザガイド、および Cisco IOS のコンフィギュレーションガイドとコマンドリファレンスを参照してください。

注: 比較的古いプラットフォームでは、クロックを反転させるためには、物理的なジャンパを設定し直す必要がある場合があります。

バッファの調整

帯域幅の使用率が過剰 (70 % 超) になると、全体的なパフォーマンスが低下し、散発的に障害が発生する可能性があります。たとえば、DECnet のファイル転送では、ネットワークのいずれかの箇所で廃棄されているパケットにより、障害が発生する可能性があります。

状況が非常に悪い場合は、リンクの帯域幅を増加させる必要があります。ところが、帯域幅を増加させることが必要ではない場合もあれば、即座には現実的ではない場合もあります。シリアル回線の境界域付近での過剰使用の問題を解決する 1 つの方法は、ルータでのデータバッファの使用具合を制御することです。

注意: 一般的には、Cisco のテクニカルサポート担当者の密接なサポートで作業していない限り、システムバッファの調整は行わないでください。ルータでシステムバッファを不適切に調整すると、使用しているハードウェアとネットワークのパフォーマンスに大きな悪影響が及ぶ可能性があります。

バッファの使用具合を制御するには、次の 3 つの選択肢のいずれかを使用します。

- ・システムバッファに関連するパラメータを調整する。
- ・入力と出力のキュー (保留キュー) で保留されるパケットの数を指定する。
- ・トラフィックが転送用にどのようにキューイングされるかを優先付けをする (出力キューイングの優先度) 。

これらの選択肢に関連する設定コマンドは、Cisco IOS のコンフィギュレーションガイドとコマンドリファレンスを参照してください。

次のセクションでは、シリアル/WAN の相互接続で接続性とパフォーマンスの問題の解決に有効な、これらの選択肢の適用がふさわしい状況を識別する方法、および、これらの選択肢を使用す

る方法に焦点を当てています。

システムバッファの調整

2人の一般のバッファの種類 on Cisco ルータがあります: ハードウェア バッファおよびシステムバッファ。システム管理者が直接に設定できるのは、システム バッファだけです。ハードウェア バッファは各インターフェイスに関連付けられた受信バッファと転送バッファとして個別に使用され、(特に設定されていない場合は、)システム ソフトウェア自体によりダイナミックに管理されます。

システム バッファはメイン システム メモリに関連付けられており、さまざまなサイズのメモリ ブロックに割り当てられています。使用しているシステム バッファのステータスを判別するのに便利なコマンドは、**show buffers EXEC** コマンドです。図 15-8 には、**show buffers** コマンドによる出力が示されています。

図 15-8 : show buffers コマンドの出力

```
Cookie-Monster>show buffers
Buffer elements:
  401 in free list (500 max allowed)
  87777499 hits, 0 misses, 0 created
Small buffers, 104 bytes (total 120, permanent 120):
  114 in free list (20 min, 250 max allowed)
  70005538 hits, 6 misses, 2 trims, 2 created
Middle buffers, 600 bytes (total 90, permanent 90):
  88 in free list (10 min, 200 max allowed)
  25696696 hits, 27 misses, 27 trims, 27 created
Big buffers, 1524 bytes (total 90, permanent 90):
  90 in free list (5 min, 300 max allowed)
  8214530 hits, 15 misses, 366 trims, 366 created
Large buffers, 5024 bytes (total 5, permanent 5):
  5 in free list (0 min, 30 max allowed)
  15017 hits, 12 misses, 16354 trims, 16354 created
Huge buffers, 18024 bytes (total 3, permanent 0):
  2 in free list (0 min, 4 max allowed)
  297582 hits, 17 misses, 30 trims, 33 created
0 failures (0 no memory)
```

Trims

Created

Failures

show buffers の出力には、次の項目があります。

- **total** : プール内のバッファの総数。これには使用済みバッファと未使用バッファが含まれています。
- **permanent** : プール内の割り当て済みバッファの固定数。これらのバッファは常にプール内にあり、削除することはできません。
- **in free list** : 現在プール内にあって利用可能なバッファの数。
- **min** : ルート プロセッサ (RP; Route Processor) でフリー リスト内に確保を試みる必要のあるバッファの最小数。min パラメータは、任意の指定された時間でのプールからのバッファのデマンドを予測するのに使用されます。フリー リスト内のバッファの数が min の値よりも低い場合、RP ではプールのためのバッファをさらに多く作成しようとします。
- **max allowed** : フリー リスト内に許可されるバッファの最大数。max allowed パラメータでは、不要になったバッファがプール内で占有されるのが防止され、そのメモリは後の使用に備えてシステムに明け渡されます。フリー リスト内のバッファの数が最大の allowed の値よりも大きい場合、RP ではプールからバッファを切り離す必要があります。
- **hits** : 要求されているプールからのバッファの数。hits カウンタにより、どのプールがバッファの上限のデマンドに適合する必要があるのかを判別する機構が提供されます。
- **失敗**は追加バッファが必要となったことバッファが要求された RP が検出する 回数を確認し

- 。(すなわち、フリーリストのバッファ番号は min. を下回りました) ミス カウンターは追加バッファを作成するために RP が強制された回数を表示します。
- **trims** : フリー リスト内のバッファの数が上限のバッファ数を上回った際に、RP によりプールから切り離されたバッファの数。
- **created** : プール内で作成されたバッファの数。フリー リスト内のバッファの数がバッファの下限を下回るか、フリー リスト内のバッファがゼロであることにより廃棄が発生するまで、バッファのデマンドが増加していると、RP ではバッファを作成します。
- **failures** : 追加のバッファの作成が試行された後にもかかわらず、リクエストに対してバッファを許可するのに失敗した数。failures の数は、バッファの不足により廃棄されたパケットの数を示しています。
- **no memory** : 追加のバッファを作成するのにメモリが不足したために発生した障害の数。

図 15-8 にある **show buffers** コマンドの出力では、大きいバッファに対する **trims** フィールドと **created** フィールドの値が高くなっています。これらのフィールドの高頻度を受け取る場合、設定されるシステムバッファのために**最大フリーな値**を増加することによってシリアルリンクのパフォーマンスを向上できます。トリムはフリーリストのバッファ番号が**最大値**によって許可されたバッファの数を超過したときに RP がプールから整えたバッファ番号を確認します。

buffers max free 数値グローバル設定コマンドを使用して、フリー システム バッファの数を増加させます。設定する値は、**show buffers** コマンドの出力の **total** フィールドに示された合計値の約 150 % である必要があります。**show buffers** の出力に切り離されたバッファと作成されたバッファが表示されなくなるまで、この手順を繰り返します。

show buffers コマンドの出力で、**no memory** フィールド (図 15-8 の出力の最終行を参照) に大量の障害が示されている場合、ルータでシステムバッファの使用を削減するか、共有またはメインメモリ (物理 RAM) の総量を増加させる必要があります。お客様のテクニカルサポート担当者に連絡して、サポートを求めてください。

保留キュー制限の実装

保留キューは、ルータの各インターフェイスで発信パケットと着信パケットの保存に使用されるバッファです。ルータでパケットが廃棄されるよりも先にキューイングされたデータパケットの数を増加させるには、**hold-queue** インターフェイス設定コマンドを使用します。**show interfaces** の出力に廃棄が表示されなくなるまで、これらのキューを小刻み (たとえば、25 %) に増加させます。デフォルトの出力保留キューの制限は 100 パケットです。

注: プロセス スイッチングされたパケットとルータにより作成される定期的なアップデートには、**hold-queue** コマンドが使用されます。

hold-queue コマンドを使用して、次のような条件でパケットが廃棄されないようにし、シリアルリンクのパフォーマンスを向上させます。

- 使用しているアプリケーションでは廃棄が許容されず、プロトコルでは比較的長い遅延を許容できる。DECnet はこの両方の基準に適合するプロトコルの例です。ローカルエリアトランスポート (LAT) では遅延が許容されないため、これにはあてはまりません。
- インターフェイスが非常に低速である。帯域幅が低いか、使用率が利用可能な帯域幅を散発的に超過することが予想されます。

注: 出力保留キューに指定する数値を増加させると、システム バッファの数を増加させる必要がある場合があります。使用する値は、ネットワークで予想されるトラフィックに関係付けられたパケットのサイズに依存します。

プライオリティ キューイングを使用したボトルネックの緩和

プライオリティ キューイングはリストベースの制御機構で、トラフィックをインターフェイスごとにプライオリティ付けできます。プライオリティ キューイングには、次の 2 つのステップがあります。

1. プロトコル タイプとプライオリティ レベルごとにプライオリティ リストを作成する。
2. 特定のインターフェイスにプライオリティ リストを割り当てる。

これらのステップの両方とも、**priority-list** グローバル設定コマンドのバージョンを使用します。さらに、**priority-list** の指定項目から **access-list** グローバル設定コマンドを参照することにより、さらに高度なトラフィック制御を適用できます。プライオリティ リストを定義する例とプライオリティ キューイングに関連するコマンド構文についての詳細は、Cisco IOS のコンフィギュレーション ガイドとコマンド リファレンスを参照してください。

注: プライオリティ キューイングではサイズの異なる 4 つのキューが自動的に作成されます。これにより、使用しているコンフィギュレーションにある保留キューの設定がすべて上書きされます。

プライオリティ キューイングを使用して、次のような条件でパケットが廃棄されないようにし、シリアル リンクのパフォーマンスを向上させます。

- インターフェイスが低速な場合、転送されるトラフィック タイプは多様で、ターミナルトラフィックのパフォーマンスを向上させる必要があります。
- 散発的に非常に負荷が重くなる (特定の回数で発生するファイル転送など) ようなシリアルリンクがある場合、トラフィックが重い期間中にどのタイプのトラフィックを廃棄するかを選択するのに、プライオリティ キューイングが有効です。

一般的には、プライオリティ キューを実装する際には、デフォルトのキューの数で開始します。プライオリティキューイングをイネーブルにしたら、**show interfaces serial EXEC** コマンドで出力の廃棄を監視します。高プライオリティに設定したトラフィック キューで出力の廃棄が発生していることが報告された場合は、(**priority-list** グローバル設定コマンドの **queue-limit** キーワード オプションを使用して) キューイングできるパケットの数を増加させます。高プライオリティ キューでのデフォルトの **queue-limit** 因数は 20 パケットで、中プライオリティ キューでは 40、通常プライオリティ キューでは 60、低プライオリティ キューでは 80 です。

注: Digital Equipment CorporationDEC LAT トラフィックのブリッジングを行う際には、ルータでのパケットの廃棄はほとんど許容されておらず、廃棄が発生すると LAT セッションが突然終了する可能性があります。ルータで出力パケットが廃棄されていて、シリアル回線の帯域幅使用率を 50 % 程度にする場合、**queue-limit** キーワードで指定される高優先度キュー深度は約 100 が通常の運用値です。ルータでパケットが廃棄されていて、使用率が 100 % の場合は、他の回線が必要で

DEC LAT をブリッジングしている場合、LAT 圧縮で輻輳を緩和するという方法もあります。**interface configuration** コマンドの **bridge-group** グループ名 **lat-compression** で LAT 圧縮を実装できます。

特殊なシリアル回線のテスト

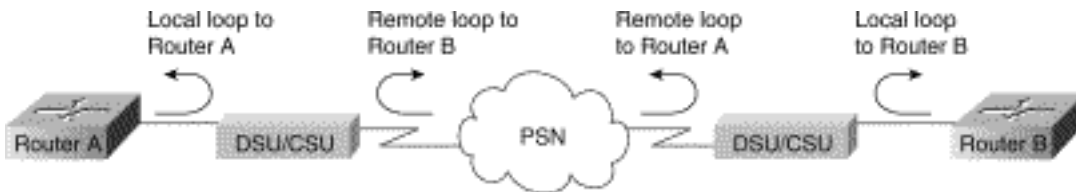
ルータで使用できる基本診断機能以外にも、さまざまな補助ツールやテクニックを使用して、ケーブル、スイッチング機器、モデム、ホスト、およびリモート インターネットワークワーキング ハードウェアの状態を判別できます。詳細は、使用している CSU、DSU、シリアル アナライザ、ある

いはその他の機器のドキュメントを参照してください。

CSU と DSU のループバック テスト

`show interfaces serial EXEC` コマンドの出力に、シリアル回線がアップしているながら、回線プロトコルがダウンしていることが示されている場合は、CSU/DSU ループバック テストを使用して、問題の発生源を判別します。ローカル ループバック テストを最初に行い、次にリモート テストを行います。図 15-9 には CSU/DSU のローカルとリモートのループバック テストの基本的なトポロジが示されています。

図 15-9: CSU/DSU



注: これらのテストはもともと汎用的なもので、インターネットワーキング システムの CSU や DSU への接続を前提とするものです。一方、このテストは組み込み CSU/DSU 機能によるマルチプレクサへの接続でも本質的に同じです。X.25 やフレームリレー パケット スイッチド ネットワーク (PSN) 環境ではループバックという概念はないため、X.25 やフレームリレー ネットワークにはループバック テストは適用されません。

HDLC リンクや PPP リンク用の CSU と DSU のローカル ループバック テスト

次のリストには、組み込みシステム診断機能とともにループバック テストを実行する一般的な手順が示されています。

1. CSU/DSU をローカル ループ モードに設定する (使用しているベンダーのドキュメントを参照)。ローカル ループ モードで、T1 回線クロックの使用を止めて、DSU でローカル クロックを使用するように設定します。
2. `show interfaces serial EXEC` コマンドを使用して、「line protocol is down」から「line protocol is up (looped)」にステータスが変化するかどうか、あるいは、ダウンしたままの状態かどうかを判別する。
3. CSU や DSU がローカル ループバック モードにある場合に回線プロトコルがアップする場合、問題はシリアル回線のリモート エンドで発生していることが示唆されます。ステータス回線が変化しない場合、問題はルータ、接続ケーブル、あるいは CSU/DSU にある可能性があります。
4. 問題がローカルであると示される場合は、`debug serial interface` 特権 EXEC コマンドを使用する。
5. CSU/DSU をローカル ループ モード以外にする。回線プロトコルがダウンしている場合、`debug serial interface` コマンドの出力には、キープアライブ カウンタが増加していないことが示されます。
6. CSU/DSU をローカル ループ モードに戻す。これにより、キープアライブ パケットの増加が始まります。具体的には、`mineseen` と `yourseen` のキープアライブが 10 秒ごとに増加します。この情報は、`debug serial interface` の出力に示されます。キープアライブが増加しない場合、インターフェイスカードがネットワークにタイミング上の問題があると考えられます。タイミング問題の修正に関する情報は、この章で前述されているセクション「クロッキング問題のトラブルシューティング」を参照してください。キープアライブが増加しな

い場合、インターフェイスカードがネットワークにタイミング上の問題があると考えられます。タイミング問題の修正に関する情報は、この章で前述されているセクション「クロッキング問題のトラブルシューティング」を参照してください。

7. ローカルのルータ、CSU/DSU のハードウェア、および接続されているケーブルをチェックする。ケーブルが推奨の長さである 15.24 m (50 フィート) あるいは T1 リンクでは 7.62 m (25 フィート) に収まっていることを確認します。ケーブルが適切なポートに接続されていることを確認します。必要に応じて、障害のある機器を交換します。

図 15-10 には HDLC シリアル接続での `debug serial interface` コマンドによる出力が示されており、キープアライブの消失により回線がダウンしてインターフェイスがリセットされています。

図 15-10: debug serial interface

```
router# debug serial interface

Serial1: HDLC nyseq 636119, mineseen 636119, yourseen 515032, line up
Serial1: HDLC nyseq 636120, mineseen 636120, yourseen 515033, line up
Serial1: HDLC nyseq 636121, mineseen 636121, yourseen 515034, line up
Serial1: HDLC nyseq 636122, mineseen 636122, yourseen 515035, line up
Serial1: HDLC nyseq 636123, mineseen 636123, yourseen 515036, line up
Serial1: HDLC nyseq 636124, mineseen 636124, yourseen 515037, line up
Serial1: HDLC nyseq 636125, mineseen 636125, yourseen 515038, line up
Serial1: HDLC nyseq 636126, mineseen 636126, yourseen 515039, line up
Serial1: HDLC nyseq 636127, mineseen 636127, yourseen 515040, line up
Serial1: HDLC nyseq 636128, mineseen 636127, yourseen 515041, line up
Serial1: HDLC nyseq 636129, mineseen 636129, yourseen 515042, line up
Serial1: HDLC nyseq 636130, mineseen 636130, yourseen 515043, line up
Serial1: HDLC nyseq 636131, mineseen 636130, yourseen 515044, line up
Serial1: HDLC nyseq 636132, mineseen 636130, yourseen 515045, line up
Serial1: HDLC nyseq 636133, mineseen 636130, yourseen 515046, line down
```

1 missed
keepalive

3 missed
keepalives

Line goes
down,
interface
resets

HDLC リンクや PPP リンク用の CSU と DSU のリモート ループバック テスト

ローカルのハードウェアは正常に動作しているものの、シリアルリンクを経由する接続を確立しようとするとき依然として問題が発生する場合は、リモート ループバック テストを実行して問題の原因を切り分けます。

注: このリモート ループバック テストでは、HDLC カプセル化が使用されていて、先行するローカル ループ テストはこのテストの直前に実行されたものと想定しています。

ループバック テストを実行するには、次の手順に従ってください。ループバック テストを実行するには、次の手順に従ってください。

1. リモートの CSU/DSU をリモート ループ モードに設定する (使用しているベンダーのドキュメントを参照) 。
2. `show interfaces serial EXEC` コマンドを使用して、ステータス行が「Serial x is up, line protocol is up (looped).」と表示されていて回線プロトコルがアップ状態のままか、ステータス行が「line protocol is down.」と表示されていてダウン状態になったか判断する。
3. 回線プロトコルがアップ状態のまま (looped) の場合、問題は (リモート CSU/DSU とリモート ルータ間の) シリアル接続のリモート エンド側にある可能性が高くなります。 リモート側でローカルとリモートのテストを実行し、問題の原因を切り分けます。
4. リモート ループバック モードがアクティブな際に回線ステータスが「line protocol is down」に変わる場合は、ones density が適切に維持されていることを確認する。専用回線その他のキャリア サービスで使用されているものと同じフレーミングとコーディングのスキーム (たえば、ESF と B8ZS) を使用するように、CSU/DSU が設定されている必要が

あります。

5. 問題が解決されない場合は、WAN のネットワーク管理者かサービス組織にお問い合わせください。

[show interfaces serial コマンドに関する詳細情報](#)

これに続くサブセクションでは、**show interfaces serial** コマンドのパラメータ、構文説明、サンプル出力表示、およびフィールドの説明が紹介されています。

[show interfaces serial のパラメータ](#)

シリアル インターフェイスに関する情報を表示するには、**show interfaces serial** 特権 EXEC コマンドを使用します。

```
show interfaces serial [number] [accounting] show interfaces serial [number [:channel-group]]
[accounting] (Cisco 4000 series) show interfaces serial [slot | port [:channel-group]]
[accounting] (Cisco 7500 series) show interfaces serial [type slot | port-adapter | port]
[serial] (ports on VIP cards in the Cisco 7500 series) show interfaces serial [type slot | port-
adapter | port] [:t1-channel] [accounting | crb] (CT3IP in Cisco 7500 series)
```

[構文の説明](#)

- 番号オプション。 リッスンするようにします。
- 会計オプションの。 各プロトコル タイプのパケットの数を表示する インターフェイスを通して送信された。
- チャンネルグループ-オプションの。 MIP の NPM か a との Cisco 4000 シリーズ Cisco 7500 シリーズ、0 から 23 の範囲で T1 チャンネルグループ番号を、channel-group controller configuration コマンドで定義されて規定します。
- *slot* : スロット情報は該当するハードウェア マニュアルに記載されています。
- *port* : ポート情報は該当するハードウェア マニュアルに記載されています。
- *port-adapter* : ポート アダプタの互換性に関する情報は該当するハードウェア マニュアルに記載されています。
- *t1-channel* -オプションの。 CT3IP に関しては、T1 チャンネルは 1 と 28 間の数です。
- CT3IP 上の T1 チャンネルには 1 から 28 までの番号が付けられています。これは他の Cisco 製品で使用されている、従来のゼロから始める方式 (0 ~ 27) とは異なります。これは、チャネルライズド T3 機器内部の T1 チャンネルに対する電話会社での番号付け方式と一貫性を持たせるようにしたためです。
- *crb* オプションの。 インターフェイス ルーティングおよびブリッジ 情報を示します。

[コマンドモード](#)

特権 EXEC

[使用上のガイドライン](#)

Cisco 4000 シリーズでこのコマンドが最初に使用されたのは、Cisco IOS リリース 10.0 です。Cisco 7000 シリーズでこのコマンドが最初に使用されたのは、Cisco IOS リリース 11.0 で、Cisco IOS リリース 11.3 で CT3IP を含むように修正されています。

表示例

次に、同期シリアル インターフェイスでの **show interfaces** コマンドの出力例を示します。

```
Router# show interfaces serial Serial 0 is up, line protocol is up Hardware is MCI Serial
Internet address is 150.136.190.203, subnet mask is 255.255.255.0 MTU 1500 bytes, BW 1544 Kbit,
DLY 20000 usec, rely 255/255, load 1/255 Encapsulation HDLC, loopback not set, keepalive set (10
sec) Last input 0:00:07, output 0:00:00, output hang never Output queue 0/40, 0 drops; input
queue 0/75, 0 drops Five minute input rate 0 bits/sec, 0 packets/sec Five minute output rate 0
bits/sec, 0 packets/sec 16263 packets input, 1347238 bytes, 0 no buffer Received 13983
broadcasts, 0 runts, 0 giants 2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort 1
carrier transitions 22146 packets output, 2383680 bytes, 0 underruns 0 output errors, 0
collisions, 2 interface resets, 0 restarts
```

フィールドの説明

表 15-9 : **show interfaces serial** のフィールドの説明 : この表では、出力中の重要なフィールドが説明されています。

フィールド	説明
シリアルは ...あ りま す{の 上で }...管 理上 ダウ ンし てい ます	インターフェイスのハードウェアが現在アクティブになっている (キャリアが検出されている) かどうか、あるいは、管理者によってダウンにされているかが示される。
行プ ロト コル はあ りま す{の 上で }	プロトコルを処理するソフトウェア プロセスで回線が使用可能 (キープアライブが成功している) と認識されているかどうか、あるいは、管理者によってダウンにされているかが示される。
行プ ロト コル はあ りま す{の 上で }	プロトコルを処理するソフトウェア プロセスで回線が使用可能 (キープアライブが成功している) と認識されているかどうか、あるいは、管理者によってダウンにされているかが示される。
Hard ware	ハードウェアのタイプが指定される。

is	
Internet address is	インターネット アドレスとサブネット マスクが指定される。
MTU	インターフェイスの Maximum Transmission Unit (MTU; 最大伝送ユニット)。
BW	インターフェイスに設定されている帯域幅パラメータの値 (Kbps) が表示される。この帯域幅パラメータが使用されるのは、IGRP メトリックを算出するためだけです。デフォルト (T1 では 1536 か 1544、標準同期シリアル回線では 56) に一致しない回線速度でシリアル回線にインターフェイスが接続されている場合、bandwidth コマンドを使用して、そのシリアル回線に適切な回線速度を指定します。
DLY	マイクロ秒単位でのインターフェイスの遅延。
rely	255 に対する比率で表されたインターフェイスの信頼性 (255/255 が 100 % の信頼性) で、5 分間の幾何平均で算出される。
負荷	255 に対する比率で表されたインターフェイスの信頼性 (255/255 が 100 % の信頼性) で、5 分間の幾何平均で算出される。
カプセル化 (Encapsulation)	インターフェイスに割り当てられているカプセル化メソッド。
ループバック	ループバックが設定されているかどうかを示される。
keep alive	キープアライブが設定されているかどうかを示される。
Last input	インターフェイスで最後にパケットが正常に受信されてから現在までの時間数、分数、秒数。インターフェイスの障害がいつ発生したかを知る場合に役立ちます。
Last output	最後のパケットがインターフェイスによって送信されたので時間数、分および秒。最後のパケットがインターフェイスによって送信されたので時間数、分および秒。
output hang	転送にかかった時間が長すぎたためにインターフェイスが最後にリセットされてから現在までの時間数、分数、秒数 (あるいは、なし)。最後のフィールドのいずれかの時間数が 24 を超過すると、日数と時間数が表示されます。フィールドがオーバーフローすると、アスタリスク (*) が表示されます。

Output queue, drops input queue, drops	出力キューと入力キュー内のパケット数。各数値の後にスラッシュ (/) とキューの最大サイズ、およびキューがフルになったために廃棄されたパケット数が続きます。
5 minute input rate 5 minute output rate	過去 5 分間に転送された 1 秒間あたりの平均ビット数とパケット数。この 5 分間の入出力レートを使用できるのは、任意の 5 分間での 1 秒あたりのトラフィックの概算値としてのみです。これらのレートは 5 分間の時間定数による指数加重平均です。この平均がその期間中のトラフィックの均一なストリームの瞬間的なレートの 2% に収まる前には、時間定数 4 つ分の期間が経過する必要があります。
packets input	システムでエラーなしで受信されたパケットの総数。
バイト	システムで受信されたエラーのないパケット内のデータと MAC のカプセル化が含まれる総バイト数。
no buffer	メインシステム内のバッファスペースがないために廃棄された受信パケット数。無視された数と比較します。イーサネットネットワークでのブロードキャストストームとシリアル回線でのノイズのバーストが、no input buffer イベントの原因となることがよくあります。
Received... broadcast	インターフェイスで受信されたブロードキャストパケットとマルチキャストパケットの総数。
runts	メディアの最小パケットサイズよりも小さいために廃棄されたパケット数。
giants	メディアの最大パケットサイズよりも大きいために廃棄されたパケット数。
入力エラー	no buffer、runts、giants、CRCs、frame、overrun、ignored、および abort の総数。これ以外に入力関連エラーでもこのカウントは増加する可能性があるため、この総数は他のカウントの合計と等しくならない可能性があります。
CRC	発信元のステーションまたは遠端のデバイスによって生成された CRC が、受信データから計算したチェックサムと一致しない。シリアルリンクの場合、通常、CRC フィールドで示されるものは、ノイズ、ゲインヒット、あるいはデータリンクでのその他の転送上の問題です。
frame	CRC エラーおよび非整数のオクテットを持った

	め、正しく受信されなかったパケットの数。シリアル回線の場合、通常、これはノイズやその他の転送上の問題による結果です。
overrun	入力レートがレシーバのデータ処理能力を超えたために、シリアルレシーバハードウェアが受信データをハードウェアバッファに渡すことができなかった回数。
ignored	インターフェイスのハードウェアの内部バッファでの動作が低速なため、インターフェイスで無視された受信パケットの数。ブロードキャストストームおよびノイズのバーストによって、ignored のカウントが増加する場合があります。
中断	シリアルインターフェイスでのビット列の不正なシーケンス。通常、これはシリアルインターフェイスとデータリンク機器間のクロッキングの問題を示しています。
carrier transitions	シリアルインターフェイスのキャリア検出シグナルでステートが変わった回数。たとえば、データキャリア検出 (DCD) がダウンになってからアップに戻る場合、carrier transitions カウンタは 2 回増加します。キャリア検出回線でステートが頻繁に変わっている場合、モデムが回線の問題が示されています。
packets output	システムで転送されたメッセージの総数。
bytes output	データと MAC のカプセル化を含む、システムで転送された総バイト数。
Underruns	ルータの処理能力を超えた速度でトランスミッタが動作した回数。一部のインターフェイスでは、これは報告されない可能性があります。
出力エラー	検査中のインターフェイスからのデータグラムの最終的な送信を妨害したすべてのエラーの総数。この数は列挙された出力エラー数の合計値と等しくなることがありません。これは、データグラムによっては、複数のエラーや、個別に集計されるどのカテゴリにも属さないエラーがあるためです。
コリジョン	イーサネットのコリジョンのために再送されたメッセージ数。通常、過剰に拡張された LAN (イーサネットやトランシーバのケーブルが長すぎるか、ステーション間に設置されたリピータが 2 基よりも多いか、カスケード接続されたマルチポートトランシーバが多すぎる) がこの原因です。一部のコリジョンは通常のもので、ところが、コリジョン率が 4 ~ 5 % 前後に上昇する場合は、セグメント上に問題のある機器がないことを確認することや、既存のステーションの一部を新しいセグメントに移動すること、あるいはその両

	方を検討する必要があります。出力パケットでは、コリジョンを起こしたパケットは一度だけカウントされます。
interface resets	インターフェイスが完全にリセットされた回数。インターフェイスリセットは、送信のためにキューイングされたパケットが数秒以内に送られなかった場合に発生する可能性があります。シリアル回線では、転送クロックシグナルを供給していない誤動作モデム、あるいは、ケーブル接続の問題でこれが発生する場合があります。シリアルインターフェイスのキャリア検出ラインがアップになっていながら、回線プロトコルがダウンしていることがシステムで検出された場合、システムではインターフェイスを再起動するための対応として間歇的にリセットをかけます。また、インターフェイスがループバックまたはシャットダウンされたときにも、インターフェイスのリセットが発生することがあります。
再起動	コントローラがエラーにより再起動された回数。
alarm indications, remote alarms, rx LOF, rx LOS	CSU/DSU アラーム数、フレームの受信消失とシグナルの受信消失の発生数。
BER inactive, NELR inactive, FELR inactive	ビットエラーレート (BER) アラーム、近端ループリモート (NELR)、および遠端ループリモート (FELR) に関する G.703-E1 カウンタのステータス。NELR や FELR は設定できないことに注意してください。

T1 のトラブルシューティング

このセクションでは、ダイヤルイン カスタマーのための T1 回線のトラブルシューティングの方法と手順について説明しています。

show controller t1 コマンドを使用するトラブルシューティング

このコマンドでは、そのコントローラのハードウェアに特有のコントローラのステータスが表示されます。ここで表示される情報は、通常、テクニカル サポートのスタッフが診断タスクを行う際にのみ役立ちます。

NMP (ネットワーク管理プロセッサ) や MIP (マルチチャネル インターフェイス プロセッサ) では、ポート アダプタに照会して現在のステータスを確認できます。T1 リンクに関する統計情報を表示するには、**show controller t1** コマンドを発行します。

スロットおよびポート番号を指定すると、15 分ごとの統計が表示されます。 **show controller t1 EXEC** コマンドでは、物理層とデータリンク層の問題を論理的にトラブルシューティングするための情報が提供されます。このセクションでは、**show controller t1** コマンドを使用して論理的にトラブルシューティングを行う方法を説明しています。

T1 エラーのほとんどは、誤設定された回線が原因で発生します。回線コーディング、フレーミング、およびクロック ソースは、お客様のサービス プロバイダーの提案に従って設定されていることを確認してください。

[show controller t1 の状態](#)

T1 コントローラは、次の 3 つ状態のいずれかになっている可能性があります。

- 管理上ダウン
- 下
- 上

[T1 コントローラが管理上ダウンになっているか。](#)

コントローラは手動でシャットダウンされた場合、管理上ダウンしています。このエラーを修復するには、コントローラを再起動する必要があります。

1. イネーブル モードに入ります。 `maui-nas-03>en`
Password:
`maui-nas-03#`
2. グローバル コンフィギュレーション モードに入ります。 `maui-nas-03#configure terminal`
Enter configuration commands, one per line. End with CNTL/Z. `maui-nas-03(config)#`
3. コントローラ設定モードに入ります。 `maui-nas-03(config)#controller t1 0 maui-nas-03(config-controlle)#`
4. コントローラを再起動する。 `maui-nas-03(config-controlle)#shutdown maui-nas-03(config-controlle)#no shutdown`

[回線がアップしているか。](#)

T1 コントローラと回線がアップしていない場合、**show controller t1 EXEC** コマンド出力に次のメッセージのいずれかが表示されているか確認してください。

- Receiver has loss of frame
- Receiver has loss of signal

[T1 レシーバでフレーム消失があるか。](#)

T1 レシーバでフレーム消失がある場合、次の手順に従ってください。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。コントローラのフレーミング フォーマットは、実行コンフィ

ギューレーションまたは `show controller t1` コマンドの出力で確認できます。フレーミングフォーマットを変更するためにフレーム作成{SF を使用して下さい | 下記に示されているようにコントローラコンフィギュレーションモードの ESF}コマンド:`maui-nas-03#configure terminal` Enter configuration commands, one per line. Ctrlキーを押しながら Z キーを押して終了します。`maui-nas-03(config)#controller t1 0 maui-nas-03(config-controller)#framing esf`

2. もう一方のフレーミング フォーマットを試用して、アラームが消えるか確認します。

3. `cablelength` を使用してライン構築設定を変更して下さい{長く / 不足分}コマンド。

ラインビルドアウト (LBO) では、デバイスから回線内の最初のリピータまでの距離に基づいて、デシベルの損失が補正されます。デバイスからリピータまでの距離が長いと、その距離に要した損失を補正するために、回線上の信号強度を高める必要があります。

ビルドアウト設定についての詳細は、お客様のサービス プロバイダーに問い合せて、さらに Cisco IOS(R) コマンド リファレンスを参照してください。

それでも問題が解決しない場合は、次の「T1 レシーバでシグナル消失があるか。」セクションを参照してください。

T1 レシーバでシグナル消失があるか。

T1 レシーバでシグナル消失がある場合、次の手順に従ってください。

1. インターフェイス ポートと、T1 サービス プロバイダーの機器 (または T1 端末機器) をつなぐケーブルが正しく接続されていることを確認する。ケーブルが正しいポートに接続されているか確認します。必要な場合は、ケーブルを接続し直してください。
2. ケーブルの整合性を確認する。ケーブルに破損またはその他の物理的異常がないか調べます。ピン配置の設定が正しいことを確認します。必要な場合は、ケーブルを交換します。
3. ケーブル コネクタを確認します。送信および受信ペア、またはオープン受信ペアが反転していると、エラーの原因となります。Line 1 に及び 2.レシーブ ペアをセット ラインに 4 及び 5.送信 ペアを設定して下さい。RJ 45 ジャッキのピンはピンによって 1 が直面するメタルピンが付いているジャッキを検知するとき一番左側のピンである 8. ~ 1 の番号がついています。次の図を参照してください。図 15-10: RJ-45



4. ロールオーバー ケーブルを使用してみる。

各ステップが終了した後で `show controller t1 EXEC` コマンドを発行して、コントローラにエラーが発生していないか確認します。

回線がループバック モードになっているかを、`show controller t1` コマンドの出力で確認します。回線をループバック モードにするのはテスト目的の場合に限ります。

ループバックをオフにするには、次のように、コントローラ コンフィギュレーション モードで `no loopback` コマンドを使用します。

```
maui-nas-03(config-controller)#no loopback
```

コントローラで何らかのエラーが表示されているか。

show controller コマンドの出力をチェックして、コントローラにアラームが表示されているか確認します。

以降、さまざまなアラームとその修復に必要な手順を説明します。

受信 (RX) アラーム表示信号 (AIS) (青) :

アラーム表示信号 (AIS) を受信した場合、そのポートに接続された機器のアップストリームの回線にアラームが発生していることが示されています。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。一致していない場合は、コントローラのフレーミング フォーマットを回線に一致させるように変更します。
2. お客様のサービス プロバイダーに問い合わせて、電話会社部分での誤設定をチェックする。

受信 (RX) リモート アラーム表示 (RAI) (黄) :

RAI を受信した場合、遠端の機器でアップストリームの機器から受信しているシグナルに関して問題があることが示されています。

1. 外部ループバック ケーブルをポートに挿入します。ループバック プラグを製作するには、この章のセクション「ループバック プラグの製作」を参照してください。
2. 何らかのアラームがあるかどうかをチェックする。アラームが何も表示されていない場合、ローカルのハードウェアはおそらく良好な状態です。その場合、次の手順を実行します。配線を確認します。詳細は、セクション「T1 レシーバでシグナル消失があるか。」を参照してください。リモート エンドで設定を確認し、ポート設定と一致するか確認します。問題が続くようであれば、サービス プロバイダーに問い合わせてください。
3. ループバック プラグを取りはずして、T1 回線に再接続します。
4. 配線を確認します。詳細は、セクション「T1 レシーバでシグナル消失があるか。」を参照してください。
5. ルータの電源をオフ/オンします。
6. T1 回線を別のポートに接続します。そのポートを回線の設定に合せて設定します。これで問題が解消した場合は、一方のポートに問題があります。T1 回線を元のポートに再接続します。「T1 エラー イベントのトラブルシューティング」セクションに進む。問題が解決しない場合は、次の手順を実行します。
7. セクション「ハードウェア ループバック プラグ テストの実行」での説明に従って、ハードウェア ループ テストを実行する。
8. T1 コントローラ カードを交換します。
9. 「T1 エラー イベントのトラブルシューティング」セクションに進む。

トランスミッタがリモート アラームを送信 (赤) :

赤アラームが表示されるのは、CSU で T1 回線でのフレーミング パターンの同期ができない場合です。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。一致していない場合は、コントローラのフレーミング フォーマットを回線に一致させるように変更します。

2. リモート エンドで設定を確認し、ポート設定と一致するか確認します。
3. お客様のサービス プロバイダーにお問い合わせください。

送信 (TX) リモート アラーム表示 (RAI) (黄) :

インターフェイスで送信された RAI は、インターフェイスで遠端の機器から受信しているシグナルに関して問題があることを示しています。

1. リモート エンドで設定を確認し、ポート設定と一致するか確認します。
2. 送信 RAI には、遠端の機器からのシグナルに関して T1 ポート/カードに発生している問題の性質を示すその他のアラームが付随しているはずです。

その状態をトラブルシューティングして、送信 RAI を解決します。

送信 (TX) AIS (青) :

次の手順に従って、送信 (TX) AIS (青) を解決します。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。一致していない場合は、不一致を修正します。
2. ルータの電源をオフ/オンします。
3. T1 回線を別のポートに接続します。そのポートを回線の設定に合わせて設定します。
4. セクション「ハードウェア ループバック プラグ テストの実行」での説明に従って、ハードウェア ループ テストを実行する。
5. T1 コントローラ カードを交換します。
6. 「T1 エラー イベントのトラブルシューティング」セクションに進む。

T1 エラー イベントのトラブルシューティング

`show controller t1 EXEC` コマンドでは、問題のトラブルシューティングに利用できるエラー メッセージが表示されます。以降、いくつかのエラー メッセージとそのエラーの修復方法を説明します。

エラー カウンタが増加しているかどうかを確認するには、繰り返し `show controller t1` コマンドを実行します。現在の間隔でのカウンタの値を記録します。

フレーミングと回線コーディングの設定については、お客様のサービス プロバイダーにお問い合わせください。経験的には、B8ZS 回線コーディングと ESF フレーミングの組み合わせ、および、AMI 回線コーディングと SF フレーミングの組み合わせが適切な方法です。

Slip Secs カウンタが増加中 :

T1 回線でスリップがある場合、クロッキングの問題が示されています。T1 プロバイダー (電話会社) から、宅内装置 (CPE) を同期させるクロッキングが供給されます。

1. クロック ソースがネットワークから導出されていることを確認する。これは、「Clock Source is Line Primary」を探すことにより確認できます。注: T1 1 T1 これに該当する場合は、プライマリ クロックに指定された T1 回線が適切に設定されていることを確認してください。
2. コントローラ コンフィギュレーション モードで T1 クロック ソースを適切に設定する。

```
maui-nas-03(config-controlle)#clock source line primary
```

Framing Loss Seconds カウンタが増加中：

Framing Loss Seconds カウンタが増加している場合は、次の手順に従ってください。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。 フレーム作成を探すことによってありますこれをチェックできます{ESF/show controller t1 出力の SF}。
2. フレーミングフォーマットを変更するためにフレーム作成{SF を使用して下さい | 下記に示されているようにコントローラコンフィギュレーションモードの ESF}コマンド:maui-nas-03(config-controlle)#framing esf
3. cablelength を使用して行構築を変更して下さい{長く | 不足分}コマンド。

ビルドアウト設定についての詳細は、お客様のサービス プロバイダーに問い合わせて、さらに Cisco IOS(R) コマンド リファレンスを参照してください。

回線コード違反は増加しています:

Line Code Violations が増加している場合は、次の手順に従ってください。

1. ポートに設定された回線コーディングが、回線のフレーミング フォーマットと一致していることを確認する。 これは、show controller t1 の出力で Line Code is {B8ZS/AMI} を探すことによりチェックできます。
2. linecoding を変更するために、ラインコード{友を使用して下さい | 下記に示されているようにコントローラコンフィギュレーションモードの b8zs} コマンド:maui-nas-03(config-controlle)#linecode b8zs
3. cablelength を使用して行構築を変更して下さい{長く | 不足分}コマンド。

ビルドアウト設定についての詳細は、お客様のサービス プロバイダーに問い合わせて、さらに Cisco IOS(R) コマンド リファレンスを参照してください。

ISDN スイッチ タイプと PRI グループが正しく設定されていることの検証

show running-config コマンドを使用して、ISDN スイッチ タイプと PRI グループのタイムスロットが適切に設定されていることを確認します。 適切な値については、お客様のサービス プロバイダーにお問い合わせください。

ISDN スイッチ タイプと PRI グループの変更方法

```
maui-nas-03#configure terminal maui-nas-03(config)#isdn switch-type primary-5ess maui-nas-03(config)#controller t1 0 maui-nas-03(config-controlle)#pri-group timeslots 1-24
```

シグナリング チャネルの検証

エラー カウンタ類が増加していないのに問題が残っている場合は、シグナリング チャネルがアップになっていて、適切に設定されていることを確認します。

1. show interface serial x:23 コマンドを実行する。この x にはインターフェイス番号を指定します。
2. インターフェイスがアップになっているかどうかを確認する。 インターフェイスがアップしていない場合は、no shutdown コマンドを使用してインターフェイスをアップします。

```
maui-nas-03#config terminal Enter configuration commands, one per line. End with CNTL/Z.
```

```
maui-nas-03(config)#interface serial 0:23 maui-nas-03(config-if)#no shutdown
```

3. カプセル化が PPP であることを確認する。 インターフェイスで PPP が使用されていない場合は、 インターフェイス コンフィギュレーション モードで `encapsulation ppp` コマンドを使用して、これを修正します。 `maui-nas-03(config-if)#encapsulation ppp`
4. ループバックが設定されているかどうかを確認する。 ループバックはテストの目的にだけ設定します。 `no loopback` コマンドを使用して、ループバックを削除します。 `maui-nas-03(config-if)#no loopback`
5. ルータの電源をオフ/オンします。
6. 問題が解消されない場合は、お客様のサービス プロバイダーあるいは Cisco の TAC にお問い合わせください。

PRI のトラブルシューティング

PRI のトラブルシューティングを行う際には常に、両端で T1 が問題なく稼働しているかどうかをチェックする必要があります。 上記のように、レイヤ 1 の問題が解決されたら、レイヤ 2 とレイヤ 3 の問題を検討します。

show isdn status コマンドを使用するトラブルシューティング

すべての ISDN インターフェイスのスナップショットを表示するには、`show isdn status` コマンドを使用します。 これにより、レイヤ 1、2、3 のステータスが表示されます。

1. レイヤ 1 がアクティブであることを確認する。 レイヤ 1 のステータスは、T1 がダウンしていない限り、常に ACTIVE と表示されているはずですが、`show isdn status` でレイヤ 1 が DEACTIVATED と表示される場合、T1 回線の物理的な接続に問題があります。 セクション「[T1 コントローラが管理上ダウンになっているか。](#)」を参照してください。 T1 が管理上ダウンにはなっていないことも確認してください。 T1 コントローラをアップにするには、`no shutdown` コマンドを使用します。

2. レイヤ 2 の状態が MULTIPLE_FRAME_ESTABLISHED であることをチェックする。

望ましいレイヤ 2 の状態は Multiple_Frame_Established で、これはレイヤ 2 フレームの交換が行われており、レイヤ 2 の初期化が完了していることを示しています。

レイヤ 2 が Multiple_Frame_Established ではない場合、`show controller t1 EXEC` コマンドを使用して、問題を診断します。 この章の「[show controller t1 コマンドを使用するトラブルシューティング](#)」セクションを参照してください。

`show isdn status` は現在のステータスのスナップショットなので、Multiple_Frame_Established が表示されているにもかかわらず、レイヤ 2 の状態がアップとダウンに頻繁に切り替わる場合があります。 レイヤ 2 が安定した状態であることを確認するには、`debug isdn q921` コマンドを使用します。

`debug isdn q921` コマンドでは、D チャンネル上のルータで行われているデータ リンク レイヤ (レイヤ 2) のアクセス手順が表示されます。

必要に応じて、`logging console` コマンドか `terminal monitor` コマンドを使用して、デバッグメッセージが表示されるように設定されていることを確認します。

注: 実稼働環境では、コンソール ロギングがディセーブルになっていることを確認してください。 `show logging` コマンドを入力します。 ロギングがイネーブルになっている場合、コンソールポートがログ メッセージで過負荷状態になるとアクセス サーバが断続的にフリーズする可能性があります。

あります。 `no logging console` コマンドを入力します。

注: `debug isdn q921` がオンになっていて、`debug` 出力を何も受け取っていない場合、コールを発信するか、コントローラをリセットして `debug` 出力を取得します。

1. レイヤ 2 が安定していることを確認する。 `debug` 出力で、サービスの状態がアップとダウンに頻繁に切り替わっていないことを示すメッセージを探す必要があります。 次のタイプの `debug` 出力が表示されている場合、回線は安定していません。 Mar 20 10:06:07.882: %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:23, TEI 0 changed to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:23, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected as clock source
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:23, TEI 0 changed to up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller T1 0, changed state to up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:23, changed state to up

レイヤ 2 が安定しているようには見えない場合、この章で前述されている「T1 エラー イベントのトラブルシューティング」を参照してください。

2. 送信 (TX) 側と受信 (RX) 側の両方で SAPI メッセージだけが表示されていることを確認する。 Mar 20 10:06:52.505: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:23: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:23: RX <- RRf sapi = 0 tei = 0 nr = 0
3. レイヤ 2 で初期化が再試行されていることを示す SABME メッセージが表示されていないことを確認する。 通常、これが表示されるのは、ポール要求 (RRp) を転送していて、スイッチからの応答 (RRf) を受信していないか、あるいはその逆である場合です。 次に SABME メッセージの例を示します。 Mar 20 10:06:21.702: ISDN Se0:23: RX <- SABMEp sapi = 0 tei = 0
Mar 20 10:06:22.494: ISDN Se0:23: TX -> SABMEp sapi = 0 tei = 0 SABME メッセージが表示されている場合は、`show running-config` コマンドを使用して、ISDN スイッチ タイプと PRI グループのタイムスロットが適切に設定されていることを確認します。 適切な値については、お客様のサービス プロバイダーにお問い合わせください。 ISDN スイッチ タイプと PRI グループの変更方法
maui-nas-03#configure terminal maui-nas-03(config)#isdn switch-type primary-5ess maui-nas-03(config)#controller t1 0 maui-nas-03(config-controller)#pri-group timeslots 1-24
4. `show interfaces serial x:23` コマンドを使用して、D チャンネルがアップになっていることを確認する。 D チャンネルがアップになっていない場合は、`no shutdown` コマンドを使用してアップにします。 maui-nas-03(config)#interface serial 0:23 maui-nas-03(config-if)#no shutdown
5. カプセル化が PPP であるかどうかを確認する。 そうでない場合は、`encapsulation ppp` コマンドを使用してカプセル化を設定します。 maui-nas-03(config-if)#encapsulation ppp
6. インターフェイスがループバック モードになっているかどうかを確認する。 通常の運用では、インターフェイスはループバック モードではない必要があります。 maui-nas-03(config-if)#no loopback
7. ルータの電源をオフ/オンします。
8. 問題が解消されない場合は、お客様のサービス プロバイダーあるいは Cisco の TAC にお問い合わせください。

[ハードウェア ループバック プラグ テストの実行](#)

ハードウェア ループバック プラグ テストを使用して、ルータに何らかの問題があるかどうかをテストできます。ハードウェア ループバック プラグ テストでルータの問題が検出されなかった場合、問題は回線の他の部分にあります。

ループバック プラグの製作

次の手順でループバック プラグを製作します。

1. 機能している RJ-45 か RJ-48 のケーブルをカッターで切断して、一端にコネクタが付いた 5 インチのケーブルを製作する。
2. ワイヤの被覆をはがします。
3. ピン 1 につながるワイヤとピン 4 につながるワイヤを撚り合わせる。
4. ピン 2 につながるワイヤとピン 5 につながるワイヤを撚り合わせる。

RJ-45/48 ジャッキのピンはピンによって 1 が直面するメタルピンが付いているジャッキを検知するとき一番左側のピンである 8. ~ 1 の番号がついています。

ループバック プラグ テストの実行

次の手順でループバック プラグテストを実行します。

1. 対象の T1 ポートにプラグを挿入する。
2. **write memory** コマンドを使用して、ルータの設定を保存する。

```
maui-nas-03#write memory
Building configuration... [OK]
```
3. カプセル化を HDLC に設定する。

```
maui-nas-03#config terminal Enter configuration commands,
one per line. End with CNTL/Z. maui-nas-03(config)#interface serial 0 maui-nas-03(config-
if)#enc maui-nas-03(config-if)#encapsulation HDLC maui-nas-03(config-if)#^Z
```
4. **show running-config** コマンドを使用して、インターフェイスに IP アドレスが設定されているかどうかを確認する。インターフェイスに IP アドレスが設定されていない場合は、一意なアドレスを取得して、そのアドレスをサブネット マスク 255.255.255.0 でインターフェイスに割り当てます。

```
maui-nas-03(config)#ip address 172.22.53.1 255.255.255.0
```
5. **clear counters** コマンドを使用して、インターフェイスのカウンタをクリアします。

```
maui-
nas-03#clear counters Clear "show interfaces" counters on all interfaces [confirm] maui-
nas-03#
```
6. この章で前述されている「拡張 ping テストの使用」セクションで説明されているように、拡張 ping テストを実行する。

E1 のトラブルシューティング

このセクションでは、ダイヤルイン カスタマーのための E1 回線のトラブルシューティングの方法と手順について説明しています。

show controller e1 コマンドを使用するトラブルシューティング

このコマンドでは、そのコントローラのハードウェアに特有のコントローラのステータスが表示されます。ここで表示される情報は、通常、テクニカル サポートのスタッフが診断タスクを行う際にのみ役立ちます。

NMP (ネットワーク管理プロセッサ) や MIP (マルチチャネル インターフェイス プロセッサ) では、ポート アダプタに照会して現在のステータスを確認できます。E1 リンクに関する統計

情報を表示するには、**show controller e1** コマンドを発行します。スロットおよびポート番号を指定すると、15分ごとの統計が表示されます。

show controller e1 EXEC コマンドでは、物理層とデータリンク層の問題を論理的にトラブルシューティングするための情報が提供されます。このセクションでは、**show controller e1** コマンドを使用して論理的にトラブルシューティングを行う方法を説明しています。

E1 エラーのほとんどは、誤設定された回線が原因で発生します。回線コーディング、フレーミング、クロックソース、および回線終端（平衡型あるいは不平衡型）は、お客様のサービスプロバイダーの提案に従って設定されていることを確認ください。

show controller e1 の状態

E1 コントローラは、次の3つ状態のいずれかになっている可能性があります。

- 管理上ダウン
- 下
- 上

E1 コントローラが管理上ダウンになっているか。

コントローラは手動でシャットダウンされた場合、管理上ダウンしています。このエラーを修復するには、コントローラを再起動する必要があります。

1. イネーブル モードに入ります。maui-nas-03>**enable** Password: maui-nas-03#
2. グローバル コンフィギュレーション モードに入ります。maui-nas-03#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z. maui-nas-03(config)#
3. コントローラ設定モードに入ります。maui-nas-03(config)#**controller e1 0** maui-nas-03(config-controlle)#
4. コントローラを再起動する。maui-nas-03(config-controlle)#**shutdown** maui-nas-03(config-controlle)#**no shutdown**

回線がアップしているか。

E1 回線がアップしていない場合、回線コンフィギュレーションが適切でリモート エンドの設定に一致していることを確認します。

1. 回線とリモート エンドのフレーミングをチェックする。E1 回線では、フレーミングは CRC4 か noCRC4 のいずれかです。
2. 回線とリモート エンドの回線コーディングをチェックする。回線コーディングは AMI か HDB3 のいずれかです。
3. 回線の終端が平衡型か不平衡型 (75 Ωか 120 Ω) に設定されているかどうかをチェックする。

適切な設定についての詳細は、お客様のサービスプロバイダーにお問い合わせください。ローカルとリモート エンドのデバイスの両方に対して、必要に応じた変更を加えます。

E1 コントローラと回線がアップしていない場合、**show controller e1 EXEC** コマンド出力に次のメッセージのいずれかが表示されているか確認してください。

- Receiver has loss of frame

- Receiver has loss of signal

E1 レシーバでフレーム消失があるか。

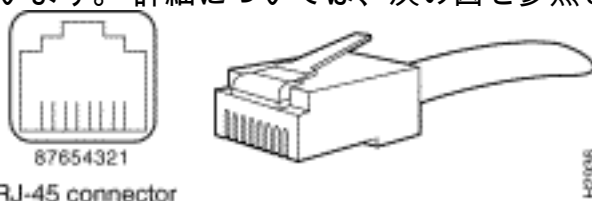
E1 レシーバでフレーム消失がある場合は、次の手順を実行してください。

1. ポートに設定されたフレーミング フォーマットが、回線のフレーミング フォーマットと一致していることを確認する。コントローラのフレーミング フォーマットは、実行コンフィギュレーションまたは **show controller e1** コマンドの出力で確認できます。フレーミング フォーマットを変更するために、フレーム化 {CRC4 を使用して下さい | 下記に示されているようにコントローラコンフィギュレーションモードの **CRC4**} コマンド無し:
maui-nas-03#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. maui-nas-03(config)#**controller E1 0 maui-nas-03(config-controller)#framing CRC4**
2. もう一方のフレーミング フォーマットを試用して、アラームが消えるか確認します。それでも問題が解決しない場合は、次の「E1 レシーバでシグナル消失があるか。」セクションを参照してください。
3. リモート エンドのフレーミング フォーマットをチェックする。
4. リモート エンドの回線コーディングをチェックする。

E1 レシーバでシグナル消失があるか。

E1 レシーバでシグナル消失がある場合は、次の手順を実行してください。

1. インターフェイス ポートと、E1 サービス プロバイダーの機器 (または E1 端末機器) をつなぐケーブルが正しく接続されていることを確認する。ケーブルが正しいポートに接続されているか確認します。必要な場合は、ケーブルを接続し直してください。
2. ケーブルの整合性を確認する。ケーブルに破損またはその他の物理的異常がないか調べます。ピン配置の設定が正しいことを確認します。必要な場合は、ケーブルを交換します。
3. ケーブル コネクタを確認します。送信および受信ペア、またはオープン受信ペアが反転していると、エラーの原因となります。Line 1 に及び 2.レシーブ ペアをセット ラインに 4 及び 5.送信 ペアを設定して下さい。RJ-48 ジャッキのピンはピンによって 1 が直面するメタルピンが付いているジャッキを検知するとき一番左側のピンである 8. ~ 1 の番号がついています。詳細については、次の図を参照してください。図 15-11: RJ-45



4. ローカルオーバー ケーブルを使用してみる。
5. 遠端ブロック エラーがあるかどうかをチェックする。このエラーがある場合は、ローカルエンドでのレシーバのリード線に問題があります。TAC に問い合せて、サポートを依頼してください。

各ステップが終了した後で **show controller e1 EXEC** コマンドを発行して、コントローラにエラーが発生していないか確認します。

回線グループバック モードか。

回線グループバック モードになっているかを、**show controller e1** コマンドの出力で確認します

。回線をループバックモードにするのはテスト目的の場合に限ります。

ループバックをオフにするには、次のように、コントローラ コンフィギュレーション モードで `no loopback` コマンドを使用します。

```
maui-nas-03(config-controlle)#no loopback
```

コントローラで何らかのエラーが表示されているか。

`show controller` コマンドの出力をチェックして、コントローラにアラームが表示されているか確認します。

以降、さまざまなアラームとその修復に必要な手順を説明します。

レシーバ (RX) でのリモートアラーム：

リモートアラームを受信した場合、そのポートに接続された機器のアップストリームの回線にアラームが発生していることが示されています。

1. ポートに設定されたフレーミングフォーマットが、回線のフレーミングフォーマットと一致していることを確認する。一致していない場合は、コントローラのフレーミングフォーマットを回線に一致させるように変更します。
2. リモートエンド機器の回線コーディングをチェックする。正しい設定に関してはサービスプロバイダーに連絡して下さい。必要に応じて、誤設定をすべて修正します。
3. 外部ループバックケーブルをポートに挿入します。ループバックプラグを製作するには、この章で前述されているセクション「ループバックプラグの製作」を参照してください。
4. 何らかのアラームがあるかどうかをチェックする。アラームが何も表示されていない場合、ローカルのハードウェアはおそらく良好な状態です。その場合、次の手順を実行します。配線を確認します。詳細は、セクション「E1 レシーバでシグナル消失があるか。」を参照してください。リモートエンドで設定を確認し、ポート設定と一致するか確認します。問題が続くようであれば、サービスプロバイダーに問い合わせてください。
5. ループバックプラグを取り外して、E1 回線を再接続する。
6. 配線を確認します。詳細は、セクション「E1 レシーバでシグナル消失があるか。」を参照してください。
7. ルータの電源をオフ/オンします。
8. E1 回線を別のポートに接続する。そのポートを回線の設定に合わせて設定します。これで問題が解消した場合は、一方のポートに問題があります。E1 回線を元のポートに接続する。「E1 エラー イベントのトラブルシューティング」セクションに進む。問題が解決しない場合は、次の手順を実行します。
9. セクション「ハードウェア ループバックプラグ テストの実行」での説明に従って、ハードウェア ループ テストを実行する。
10. E1 コントローラ カードを交換する。
11. 「E1 エラー イベントのトラブルシューティング」セクションに進む。

トランスミッタがリモートアラームを送信 (赤)：

赤アラームが表示されるのは、CSU で E1 回線でのフレーミングパターンの同期ができない場合です。

1. ポートに設定されたフレーミングフォーマットが、回線のフレーミングフォーマットと一

致していることを確認する。一致していない場合は、コントローラのフレーミングフォーマットを回線に一致させるように変更します。

2. リモート エンドで設定を確認し、ポート設定と一致するか確認します。
3. 外部ループバック ケーブルをポートに挿入します。ループバック プラグを製作するには、この章で前述されているセクション「ループバック プラグの製作」を参照してください。
4. 何らかのアラームがあるかどうかをチェックする。アラームが何も表示されていない場合、ローカルのハードウェアはおそらく良好な状態です。その場合、次の手順を実行します。配線を確認します。詳細は、セクション「E1 レシーバでシグナル消失があるか。」を参照してください。問題が続くようであれば、サービス プロバイダーに問い合わせてください。
5. E1 回線を別のポートに接続する。そのポートを回線の設定に合わせて設定します。これで問題が解消した場合は、一方のポートに問題があります。E1 回線を元のポートに接続する。「E1 エラー イベントのトラブルシューティング」セクションに進む。問題が解決しない場合は、次の手順を実行します。
6. セクション「ハードウェア ループバック プラグ テストの実行」での説明に従って、ハードウェア ループ テストを実行する。
7. E1 コントローラ カードを交換する。
8. 「E1 エラー イベントのトラブルシューティング」セクションに進む。
9. お客様のサービス プロバイダーにお問い合わせください。

E1 エラー イベントのトラブルシューティング

`show controller e1 EXEC` コマンドでは、問題のトラブルシューティングに利用できるエラー メッセージが表示されます。以降、いくつかのエラー メッセージとそのエラーの修復方法を説明します。

エラー カウンタが増加しているかどうかを確認するには、繰り返し `show controller e1` コマンドを実行します。現在の間隔でのカウンタの値を記録します。フレーミングと回線コーディングの設定については、お客様のサービス プロバイダーにお問い合わせください。

Slip Secs カウンタが増加中 :

E1 回線でスリップがある場合、クロッキングの問題が示されています。E1 プロバイダー (電話会社) から、宅内装置 (CPE) を同期させるクロッキングが供給されます。

1. クロック ソースがネットワークから導出されていることを確認する。これは、「Clock Source is Line Primary」を探すことにより確認できます。注: E1 1 E1 これに該当する場合は、プライマリ クロックに指定された E1 回線が適切に設定されていることを確認してください。
2. コントローラ コンフィギュレーション モードで E1 クロック ソースを適切に設定する。
`maui-nas-03(config-controller)#clock source line primary`

Framing Loss Seconds カウンタが増加中 :

Framing Loss Seconds カウンタが増加している場合は、次の手順に従ってください。

1. ポートに設定されたフレーミングフォーマットが、回線のフレーミングフォーマットと一致していることを確認する。これは、`show controller e1` の出力で `Framing is {CRC4|no CRC4}` を探すことによりチェックできます。

2. フレーミングフォーマットを変更するためにフレーム作成{CRC4 を使用して下さい / 下記に示されているようにコントローラコンフィギュレーションモードの CRC4} コマンド無し

```
maui-nas-03(config-controlle)#framing crc4
```

Line Code Violations が増加中 :

Line Code Violations が増加している場合は、次の手順に従ってください。

1. ポートに設定された回線コーディングが、回線のフレーミング フォーマットと一致していることを確認する。これは、**show controller e1** の出力で *Line Code is {AMI/HDB3}* を探すことによりチェックできます。
2. linecoding を変更するために、ラインコード{友を使用して下さい / 下記に示されているようにコントローラコンフィギュレーションモードの hdb3} コマンド:maui-nas-03(config-controlle)#linecode ami

ISDN スイッチ タイプと PRI グループが正しく設定されていることの検証

show running-config コマンドを使用して、ISDN スイッチ タイプと PRI グループのタイムスロットが適切に設定されていることを確認します。適切な値については、お客様のサービス プロバイダーにお問い合わせください。

ISDN スイッチ タイプと PRI グループの変更方法

```
maui-nas-03#configure terminal maui-nas-03(config)#isdn switch-type primary-net5 maui-nas-03(config)#controller e1 0 maui-nas-03(config-controlle)#pri-group timeslots 1-31
```

シグナリング チャネルの検証

エラー カウンタ類が増加していないのに問題が残っている場合は、シグナリング チャネルがアップになっていて、適切に設定されていることを確認します。

1. **show interface serial x:15** コマンドを実行する。この x にはインターフェイス番号を指定します。
2. インターフェイスがアップになっているかどうかを確認する。インターフェイスがアップしていない場合は、**no shutdown** コマンドを使用してインターフェイスをアップします。
maui-nas-03#config terminal Enter configuration commands, one per line. End with CNTL/Z.
maui-nas-03(config)#interface serial 0:15 maui-nas-03(config-if)#no shutdown
3. カプセル化が PPP であることを確認する。インターフェイスで PPP が使用されていない場合は、インターフェイス コンフィギュレーション モードで **encapsulation ppp** コマンドを使用して、これを修正します。maui-nas-03(config-if)#encapsulation ppp
4. ループバックが設定されているかどうかを確認する。ループバックはテストの目的にだけ設定します。 **no loopback** コマンドを使用して、ループバックを削除します。maui-nas-03(config-if)#no loopback
5. ルータの電源をオフ/オンします。
6. 問題が解消されない場合は、お客様のサービス プロバイダーあるいは Cisco の TAC にお問い合わせください。

PRI のトラブルシューティング

PRI のトラブルシューティングを行う際には、両端で E1 が問題なく稼働しているかどうかをチェックする必要があります。上記のように、レイヤ 1 の問題が解決されたら、レイヤ 2 とレイヤ

3 の問題を検討します。

[show isdn status コマンドを使用するトラブルシューティング](#)

すべての ISDN インターフェイスのスナップショットを表示するには、**show isdn status** コマンドを使用します。これにより、レイヤ 1、2、3 のステータスが表示されます。

1. レイヤ 1 がアクティブであることを確認する。レイヤ 1 のステータスは、E1 がダウンしていない限り、常に ACTIVE と表示されているはずですが、**show isdn status** でレイヤ 1 が DEACTIVATED と表示される場合、E1 回線の物理的な接続に問題があります。セクション「E1 コントローラが管理上ダウンになっているか。」を参照してください。E1 が管理上ダウンにはなっていないことも確認してください。E1 コントローラをアップにするには、**no shutdown** コマンドを使用します。
2. レイヤ 2 の状態が MULTIPLE_FRAME_ESTABLISHED であることをチェックする。

望ましいレイヤ 2 の状態は Multiple_Frame_Established で、これは ISDN スイッチとエンドデバイス間のスタートアップ プロトコルが確率されており、レイヤ 2 フレームの交換が行われていることを示しています。

レイヤ 2 が Multiple_Frame_Established ではない場合、**show controller e1 EXEC** コマンドを使用して、問題を診断します。この章の「**show controller e1** コマンドを使用するトラブルシューティング」セクションと「E1 エラー イベントのトラブルシューティング」セクションを参照してください。

show isdn status は現在のステータスのスナップショットなので、Multiple_Frame_Established が表示されているにもかかわらず、レイヤ 2 の状態がアップとダウンに頻繁に切り替わる場合があります。**debug isdn q921** コマンドを使用して、レイヤ 2 の安定性を確認します。

[debug q921 コマンドの使用](#)

debug isdn q921 コマンドでは、D チャネル上のルータで行われているデータ リンク レイヤ (レイヤ 2) のアクセス手順が表示されます。

必要に応じて、**logging console** コマンドか **terminal monitor** コマンドを使用して、**debug** メッセージが表示されるように設定されていることを確認します。

注: 実稼働環境では、コンソール ロギングがディセーブルになっていることを確認してください。**show logging** コマンドを入力します。ロギングがイネーブルになっている場合、コンソールポートがログ メッセージで過負荷状態になるとアクセス サーバが断続的にフリーズする可能性があります。**no logging console** コマンドを入力します。

注: **debug isdn q921** がオンになっていて、**debug** 出力を何も受け取っていない場合、コールを発信するか、コントローラをリセットして **debug** 出力を取得します。

1. レイヤ 2 が安定していることを確認する。**debug** 出力で、サービスの状態がアップとダウンに頻繁に切り替わっていないことを示すメッセージを探す必要があります。次のタイプの **debug** 出力が表示されている場合、回線は安定していません。Mar 20 10:06:07.882:
%ISDN-6-LAYER2DOWN: Layer 2 for Interface Se0:15, TEI 0
changed to down
Mar 20 10:06:09.882: %LINK-3-UPDOWN: Interface Serial0:15, changed state to down
Mar 20 10:06:21.274: %DSX1-6-CLOCK_CHANGE: Controller 0 clock is now selected
as clock source

```
Mar 20 10:06:21.702: %ISDN-6-LAYER2UP: Layer 2 for Interface Se0:15, TEI 0
changed to up
Mar 20 10:06:22.494: %CONTROLLER-5-UPDOWN: Controller E1 0, changed state to up
Mar 20 10:06:24.494: %LINK-3-UPDOWN: Interface Serial0:15, changed state to up
```

レイヤ 2 が安定しているようには見えない場合、この章で前述されている「E1 エラー イベントのトラブルシューティング」を参照してください。

2. 送信 (TX) 側と受信 (RX) 側の両方で SAPI メッセージだけが表示されていることを確認

する。 Mar 20 10:06:52.505: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:06:52.505: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.505: ISDN Se0:15: TX -> RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRp sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: TX -> RRf sapi = 0 tei = 0 nr = 0
Mar 20 10:07:22.509: ISDN Se0:15: RX <- RRf sapi = 0 tei = 0 nr = 0

3. レイヤ 2 で初期化が再試行されていることを示す SABME メッセージが表示されていないことを確認する。通常、これが表示されるのは、ポール要求 (RRp) を転送していて、スイッチからの応答 (RRf) を受信していないか、あるいはその逆である場合です。次に SABME メッセージの例を示します。 SABME メッセージに対して ISDN スイッチからの応答があるはず (UA フレームの受信) 。 Mar 20 10:06:21.702: ISDN Se0:15: RX <- SABMEp sapi = 0 tei = 0

Mar 20 10:06:22.494: ISDN Se0:15: TX -> SABMEp sapi = 0 tei = 0 SABME メッセージが表示されている場合は、 **show running-config** コマンドを使用して、ISDN スイッチタイプと PRI グループのタイムスロットが適切に設定されていることを確認します。適切な値については、お客様のサービスプロバイダーにお問い合わせください。 ISDN スイッチタイプと PRI グループの変更方法

```
maui-nas-03#configure terminal maui-nas-03(config)#isdn switch-type
primary-net5 maui-nas-03(config)#controller e1 0 maui-nas-03(config-controller)#pri-group
timeslots 1-31
```

4. **show interfaces serial x:15** コマンドを使用して、D チャンネルがアップになっていることを確認する。D チャンネルがアップになっていない場合は、 **no shutdown** コマンドを使用してアップにします。 maui-nas-03(config)#interface serial 0:15 maui-nas-03(config-if)#no shutdown

5. カプセル化が PPP であるかどうかを確認する。 そうでない場合は、 **encapsulation ppp** コマンドを使用してカプセル化を設定します。 maui-nas-03(config-if)#encapsulation ppp

6. インターフェイスがループバック モードになっているかどうかを確認する。 通常の運用では、インターフェイスはループバック モードではない必要があります。 maui-nas-03(config-if)#no loopback

7. ルータの電源をオフ/オンします。

8. 問題が解消されない場合は、お客様のサービスプロバイダーあるいは Cisco の TAC にお問い合わせください。

関連情報

- [テクニカルサポート - Cisco Systems](#)