Cisco IOS XR ソフトウェアでの PPP の設定

ここでは、Cisco IOS XR ソフトウェアの POS インターフェイスとシリアル インターフェイスでのポイントツーポイント プロトコル（PPP）に関連した作業について説明します。

- PPP 認証プロトコルのイネーブル化と設定
- PPP 認証のディセーブル化
- オプションの PPP timeout パラメータと retry パラメータの変更
- マルチリンク PPP の設定

PPP インターフェイス設定の機能履歴

リリース	変更点
リリース 2.0	Cisco CRS-1 ルータに PPP 認証が追加されました。
リリース 3.0	変更ありません。
リリース 3.3.0	Cisco XR 12000 シリーズ ルータでは、PPP カプセル化で設定したシリアル インターフェイスがサポートされるようになりました。
リリース 3.4.0	変更ありません。
リリース 3.4.1	Cisco XR 12000 シリーズ ルータでは、マルチリンク PPP がサポートされるようになりました。
リリース 3.5.0	変更ありません。
リリース 3.6.0	変更ありません。
リリース 3.7.0	変更ありません。
リリース 3.8.0	変更ありません。

この章の構成

- 「その他の参考資料」（P.350）

PPP 認証設定の前提条件

POS インターフェイスまたはシリアル インターフェイスで PPP 認証を設定する前に、次のタスクと条件を満たしていることを確認します。

- この設定作業を行うには、Cisco IOS XR ソフトウェアのシステム管理者が、対応するコマンド タスク ID を含むタスク グループに関連付けられたユーザ グループにユーザを割り当てる必要があります。すべてのコマンド タスク ID は、各コマンド リファレンスおよび『*Cisco IOS XR Task ID Reference Guide*』に記載されています。

  タスク グループの割り当てについてサポートが必要な場合は、システム管理者に連絡してください。ユーザ グループおよびタスク ID の詳細については、『*Cisco IOS XR Software System Security Configuration Guide*』の「*Configuring AAA Services on Cisco IOS XR Software* 」モジュールを参照してください。
- 使用しているハードウェアが POS インターフェイスまたはシリアル インターフェイスをサポートしている必要があります。
- 対応するモジュールの説明に従って、**encap ppp** コマンドを使用し、インターフェイスで PPP のカプセル化をイネーブルにしました。
  - POS インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでの POS インターフェイスの設定*」モジュールを参照してください。
  - シリアル インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでのシリアル インターフェイスの設定*」モジュールを参照してください。

PPP 認証について

インターフェイスに PPP 認証が設定されている場合、ホストは、PPP 接続を確立する前に他のホストがセキュア パスワードを使用して自身を一意に識別することを求めます。このパスワードは一意で、両方のホストで認識されています。

PPP は、次の認証プロトコルをサポートします。

- チャレンジ ハンドシェイク認証プロトコル（CHAP）
- Microsoft による CHAP プロトコルの拡張版（MS-CHAP）
- パスワード認証プロトコル（PAP）

POS インターフェイスまたはシリアル インターフェイス上で初めて PPP をイネーブルにしたときは、対象のインターフェイスで CHAP、MS-CHAP、PAP のいずれかのシークレット パスワードを設定するまで、そのインターフェイスでの認証はイネーブルになりません。インターフェイスで PPP を設定する場合、次の点に気を付けてください。

- CHAP、MS-CHAP、PAP は単一のインターフェイスに設定できますが、一度に使用される認証方式は 1 つだけです。使用される認証プロトコルの順序は、LCP ネゴシエーション中のピアによって決定されます。使用される最初の認証方式は、ピアによってもサポートされます。

- PAP は、POS インターフェイスおよびシリアル インターフェイスで使用可能な最小のセキュア認証プロトコルです。POS インターフェイスおよびシリアル インターフェイス経由で送信される情報について、より高レベルのセキュリティを確保するため、PAP 認証に加えて CHAP または MS-CHAP 認証を設定することをお勧めします。
- PPP 認証をイネーブル化またはディセーブル化しても、リモート装置に対して自身の認証を行うローカル ルータの動作には影響しません。
- **ppp authentication** コマンドは、インターフェイス上で CHAP、MS-CHAP、PAP 認証が選択される順序を指定するときにも使用されます。CHAP、MS-CHAP、PAP は、任意の順序でイネーブル化できます。3 つのすべての方式をイネーブル化すると、リンク ネゴシエーションでは、最初に指定された方式が要求されます。ピアが 2 番目の方式の使用を提案した場合、または最初の方式を拒否した場合は、2 番目の方式が試行されます。リモート装置の中には、1 つの方式しかサポートしないものがあります。方式の順序は、適切な方式で正しくネゴシエーションするためにリモート装置の機能で指定された方式と、求められるデータ ライン セキュリティのレベルに基づいて決定されます。PAP ユーザ名とパスワードはクリア テキスト文字列として送信されます。この文字列は、代行受信や再利用が可能です。

注意 **aaa authentication ppp** コマンドを使わずに設定した *list-name* 値を使用すると、インターフェイスはピアを認証できません。**ppp** キーワードを指定した **aaa authentication** コマンドの実装についての詳細は、『*Cisco IOS XR System Security Command* Reference』の「*Authentication,* Authorization, and Accounting Commands on Cisco IOS XR Software」モジュールおよび『*Cisco IOS XR System Security Configuration Guide*』の「*Configuring AAA Services on Cisco IOS XR Software*」モジュールを参照してください。

PAP 認証

PAP は、リモート ノードに対し、2 ウェイ ハンドシェイクを使用してそのアイデンティティを確立するためのシンプルな方式を提供します。2 台のホスト間で PPP リンクが確立した後、ユーザ名とパスワードのペアは認証が確認されるまで、または接続が終了するまで、リモート ノードによってリンクを経由して（クリア テキストで）繰り返し送信されます。

PAP はセキュアな認証プロトコルではありません。パスワードはリンクを経由してクリア テキストで送信され、プレイバック攻撃やトライアルアンドエラー攻撃からの保護機能はありません。リモート ノードは、ログイン試行の頻度とタイミングを管理しています。

CHAP 認証

CHAP は RFC 1994 で定義され、3 ウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。次の手順に、CHAP プロセスの概要を示します。

ステップ 1 CHAP オーセンティケータがピアにチャレンジ メッセージを送信します。

ステップ 2 ピアは 1 ウェイ ハッシュ関数で算出された値で応答します。

ステップ 3 オーセンティケータは、応答を、独自の計算で予測したハッシュ値と照合します。値が一致すると、認証は成功します。値が一致しないと、接続は終了します。

この認証方式は、オーセンティケータとピアでのみ認識されている CHAP パスワードによって決まります。CHAP パスワードは、リンク経由では送信されません。認証は 1 ウェイですが、相互認証に同じ CHAP パスワード セットを使用することで、CHAP のネゴシエーションを双方向に行うことができます。

（注） 有効な CHAP 認証には、両方のホストの CHAP パスワードが同一であることが必要です。

MS-CHAP 認証

Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）は、Microsoft バージョンの CHAP で、RFC 1994 の拡張です。MS-CHAP では、CHAP と同じ認証プロセスが使用されます。ただし、認証は、Microsoft Windows NT または Microsoft Windows 95 を実行する PC と、ネットワーク アクセス サーバ（NAS）として動作する Cisco ルータまたはアクセス サーバとの間で行われます。

（注） 有効な MS-CHAP 認証には、両方のホストの MS-CHAP パスワードが同一であることが必要です。

PPP 認証の設定方法

ここでは、次の手順について説明します。

- 「PAP、CHAP、MS-CHAP 認証のイネーブル化」（P.320）
- 「PAP 認証パスワードの設定」（P.323）
- 「CHAP 認証パスワードの設定」（P.325）
- 「MS-CHAP 認証パスワードの設定」（P.327）

PAP、CHAP、MS-CHAP 認証のイネーブル化

ここでは、シリアル インターフェイスまたは POS インターフェイスで PAP、CHAP、MS-CHAP 認証をイネーブルにする手順について説明します。

前提条件

次のモジュールの説明に従って、**encapsulation ppp** コマンドを使用し、インターフェイスで PPP のカプセル化をイネーブルにする必要があります。

- POS インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでの POS インターフェイスの設定*」モジュールを参照してください。
- インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでのシリアル インターフェイスの設定*」モジュールを参照してください。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*

3. **ppp authentication** *protocol* [*protocol* [*protocol*]] [*list-name* | **default**]
4. **end**
   または
   commit
5. **show ppp interfaces** {*type interface-path-id* | **all** | **brief** {*type interface-path-id* | **all** | **location** *node-id*} | **detail** {*type interface-path-id* | **all** | **location** *node-id*} | **location** *node-id*}

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp authentication** *protocol* [*protocol* [*protocol*]] [*list-name*	**default**] **例：** `RP/0/RP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access`	インターフェイスで CHAP、MS-CHAP、または PAP をイネーブルにし、インターフェイスで CHAP、MS-CHAP、PAP 認証が選択される順序を指定します。 • *protocol* 引数を、**pap**、**chap**、または **ms-chap** に置き換えます。 • *list name* 引数を、使用する認証方式のリストの名前に置き換えます。リストを作成するには、『*Cisco IOS XR System Security Command* Reference』の「*Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software*」モジュールに記載されている説明に従って **aaa authentication ppp** コマンドを使用します。 • リストの名前を指定しないと、デフォルトが使用されます。デフォルトのリストは、『*Cisco IOS XR System Security Command* Reference』の「*Authentication, Authorization, and Accounting Commands on Cisco IOS XR Software*」モジュールに記載されている説明に従って **aaa authentication ppp** コマンドで指定します。

	コマンドまたはアクション	目的

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show ppp interfaces** {*type interface-path-id* | **all** | **brief** {*type interface-path-id* | **all** | **location** *node-id*} | **detail** {*type interface-path-id* | **all** | **location** *node-id*} | **location** *node-id*} **例：** `RP/0/RP0/CPU0:router# show ppp interfaces serial 0/2/0/0`	インターフェイスの PPP ステート情報を表示します。 • *type interface-path-id* 引数を入力すると、特定のインターフェイスの PPP 情報が表示されます。 • **brief** キーワードを入力すると、ルータのすべてのインターフェイス、特定のインターフェイス インスタンス、または特定のノードのすべてのインターフェイスの簡易出力が表示されます。 • **all** キーワードを入力すると、ルータにインストールされているすべてのノードの詳細な PPP 情報が表示されます。 • **location** *node-id* キーワード引数を入力すると、指定したノードの詳細な PPP 情報が表示されます。 リンク制御プロトコル（LCP）またはネットワーク制御プロトコル（NCP）に適用される PPP ステートには、7 つのステートがあります。

関連情報

対応する項の説明に従って、PAP、CHAP、または MS-CHAP 認証のパスワードを設定します。

- インターフェイスで PAP をイネーブルにする場合は、「PAP 認証パスワードの設定」（P.323）の説明に従って PAP 認証のユーザ名とパスワードを設定します。
- インターフェイスで CHAP をイネーブルにする場合は、「CHAP 認証パスワードの設定」（P.325）の説明に従って CHAP 認証のユーザ名とパスワードを設定します。
- インターフェイスで MS-CHAP をイネーブルにする場合は、「MS-CHAP 認証パスワードの設定」（P.327）の説明に従って MS-CHAP 認証のユーザ名とパスワードを設定します。

PAP 認証パスワードの設定

ここでは、シリアル インターフェイスまたは POS インターフェイスで PAP 認証をイネーブルにして設定する手順について説明します。

（注） PAP は、POS およびインターフェイスで使用可能な最小のセキュア認証プロトコルです。POS およびインターフェイス経由で送信される情報について、より高レベルのセキュリティを確保するため、PAP 認証に加えて CHAP または MS-CHAP 認証を設定することをお勧めします。

前提条件

「PAP、CHAP、MS-CHAP 認証のイネーブル化」（P.320）の説明に従って、**ppp authentication** コマンドを使用し、インターフェイスで PAP 認証をイネーブルにする必要があります。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp pap sent-username** *username* **password** [**clear** | **encrypted**] *password*
4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp pap sent-username** *username* **password** [**clear** | **encrypted**] *password* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified`	インターフェイスでリモートのパスワード認証プロトコル（PAP）サポートをイネーブルにし、ピアに対する PAP 認証要求に **sent-username** コマンドと **password** コマンドを含めます。 • *username* 引数を、PAP 認証要求で送信するユーザ名に置き換えます。 • **password clear** を入力してパスワードのクリア テキスト暗号化を選択するか、パスワードがすでに暗号化されている場合は **password encrypted** を入力します。 • **ppp pap sent--username** コマンドを使用すると、複数の username および password コンフィギュレーション コマンドを、インターフェイス上にあるこのコマンドの単一コピーに置き換えることができます。 • **ppp pap sent-username** コマンドは、インターフェイスごとに設定する必要があります。 • リモートの PAP サポートでは、デフォルトでディセーブルになっています。

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

CHAP 認証パスワードの設定

ここでは、CHAP 認証をイネーブルにし、シリアル インターフェイスまたは POS インターフェイスで CHAP パスワードを設定する手順について説明します。

前提条件

「PAP、CHAP、MS-CHAP 認証のイネーブル化」（P.320）の説明に従って、**ppp authentication** コマンドを使用し、インターフェイスで CHAP 認証をイネーブルにする必要があります。

制約事項

両ホストのエンドポイントに同じ CHAP パスワードを設定する必要があります。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp chap password** [**clear** | **encrypted**] *password*
4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp chap password** [**clear** | **encrypted**] *password* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp chap password clear xxxx`	指定したインターフェイスで CHAP 認証をイネーブルにし、インターフェイス固有の CHAP パスワードを定義します。 • **clear** を入力してクリア テキスト暗号化を選択するか、パスワードがすでに暗号化されている場合は **encrypted** を入力します。 • *password* 引数を、クリア テキストまたはすでに暗号化されているパスワードに置き換えます。このパスワードは、ルータのコレクション間のセキュアな通信の認証に使用されます。 • **ppp chap password** コマンドはリモート CHAP 認証のみに使用され（ピアに対するルータ認証の場合）、ローカルの CHAP 認証では有効になりません。このコマンドは、このコマンドをサポートしないピアを認証しようとする場合に使用すると便利です（古い Cisco IOS XR ソフトウェア イメージを実行しているルータなど）。 • CHAP シークレット パスワードは、不明なピアからのチャレンジに応答するためにルータによって使用されます。

	コマンドまたはアクション	目的

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

MS-CHAP 認証パスワードの設定

ここでは、MS-CHAP 認証をイネーブルにし、シリアル インターフェイスまたは POS インターフェイスで MS-CHAP パスワードを設定する手順について説明します。

前提条件

「PAP、CHAP、MS-CHAP 認証のイネーブル化」（P.320）の説明に従って、**ppp authentication** コマンドを使用し、インターフェイスで MS-CHAP 認証をイネーブルにする必要があります。

制約事項

両ホストのエンドポイントに同じ MS-CHAP パスワードを設定する必要があります。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp ms-chap password** [**clear** | **encrypted**] *password*

4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp ms-chap password** [**clear** | **encrypted**] *password* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password clear xxxx`	ルータのコレクションを呼び出すルータをイネーブルにし、共通の Microsoft チャレンジ ハンドシェイク 認証（MS-CHAP）シークレット パスワードを設定します。 MS-CHAP シークレット パスワードは、不明なピアからのチャレンジに応答するためにルータによって使用されます。

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

デフォルトの PPP 設定の変更方法

インターフェイスで初めて PPP をイネーブルにすると、次のデフォルト設定が適用されます。

- 認証が失敗すると、ただちに、インターフェイスは自身をリセットします。
- 応答がなくても許可される設定要求の最大数は 10 で、この数を超えるとすべての要求が停止されます。
- Negative Acknowledgment（CONFNAK; 否定応答）が連続して返される場合、それが許可される最大数は 5 で、この数を超えるとネゴシエーションが終了されます。
- 応答がなくても許可される Terminate Request（TermReq; 終了要求）の最大数は 2 で、この数を超えるとリンク制御プロトコル（LCP）またはネットワーク制御プロトコル（NCP）は終了されます。
- 認証パケットに対する応答の最大待機時間は 10 秒です。
- PPP ネゴシエーション中の応答の最大待機時間は 3 秒です。

ここでは、PPP カプセル化がイネーブルになっているシリアル インターフェイスまたは POS インターフェイスで基本的な PPP 設定を変更する手順について説明します。ここで使用するコマンドは、PPP（CHAP、MS-CHAP、PAP）によってサポートされるすべての種類の認証に適用されます。

前提条件

encapsulation ppp コマンドを使用し、インターフェイスで PPP カプセル化をイネーブルにする必要があります。

- POS インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでの POS インターフェイスの設定*」モジュールを参照してください。
- インターフェイスで POS のカプセル化をイネーブルにするには、このマニュアルの「*Cisco IOS XR ソフトウェアでのシリアル インターフェイスの設定*」モジュールを参照してください。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp max-bad-auth** *retries*
4. **ppp max-configure** *retries*
5. **ppp max-failure** *retries*
6. **ppp max-terminate** *number*
7. **ppp timeout authentication** *seconds*
8. **ppp timeout retry** *seconds*
9. **end**
   または
   commit
10. **show ppp interfaces** {*type interface-path-id* | **all** | **brief** {*type interface-path-id* | **all** | **location** *node-id*} | **detail** {*type interface-path-id* | **all** | **location** *node-id*} | **location** *node-id*}

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp max-bad-auth** *retries* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3`	（任意）PPP 認証が失敗した後、インターフェイスで許可する認証のリトライ回数を設定します。 • 許可する認証のリトライ回数を指定しない場合、認証が失敗すると、ただちに、ルータは自身をリセットします。 • *retries* 引数を、0 ～ 10 の範囲でリトライ回数に置き換えます。この回数を超えると、インターフェイスは自身をリセットします。 • デフォルトのリトライ回数は 0 回です。 • **ppp max-bad-auth** コマンドは、PPP カプセル化がイネーブルになっている任意のインターフェイスに適用できます。
ステップ 4	**ppp max-configure** *retries* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp max-configure 4`	（任意）（応答なしで）試行される設定要求の最大数を指定します。この数を超えると、要求は停止されます。 • *retries* 引数を、4 ～ 20 の範囲で設定要求がリトライする最大回数に置き換えます。 • デフォルトの設定要求の最大数は 10 です。 • 設定要求の最大回数分だけ送信されないうちに設定要求メッセージが応答を受け取った場合、以降の設定要求は放棄されます。
ステップ 5	**ppp max-failure** *retries* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp max-failure 3`	（任意）否定応答（CONFNAK）が連続して返される場合に、それが許可される最大数を設定します。この数を超えるとネゴシエーションは終了されます。 • *retries* 引数を、2 ～ 10 の範囲で CONFNAK の最大数に置き換えます。この数を超えるとネゴシエーションは終了されます。 • デフォルトの CONFNAK の最大数は 5 です。

	コマンドまたはアクション	目的
ステップ 6	**ppp max-terminate** *number* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp max-terminate 5`	（任意）応答がなくても送信される終了要求（TermReq）の最大数を設定します。この数を超えるとリンク制御プロトコル（LCP）またはネットワーク制御プロトコル（NCP）は終了されます。 • *number* 引数を、応答がなくても送信される TermReq の最大数に置き換えます。この数を超えると LCP または NCP は終了されます。範囲は 2 ～ 10 です。 • デフォルトの TermReq の最大数は 2 です。
ステップ 7	**ppp timeout authentication** *seconds* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp timeout authentication 20`	（任意）PPP 認証タイムアウト パラメータを設定します。 • *seconds* 引数を、認証パケットに対する応答を待機する最大時間（秒）に置き換えます。範囲は 3 ～ 30 秒です。 • デフォルトの認証タイムアウトは 10 秒です。この時間には、リモート ルータが接続を認証して許可し、応答するまでの時間を組み込む必要があります。ただし、この処理に 10 秒かからないこともあります。そのような場合は **ppp timeout authentication** コマンドを使用してタイムアウト時間を短くし、認証応答が失われる場合の接続時間を改善します。
ステップ 8	**ppp timeout retry** *seconds* **例：** `RP/0/RP0/CPU0:router(config-if)# ppp timeout retry 8`	（任意）PPP 認証タイムアウト リトライ パラメータを設定します。 • *seconds* 引数を、PPP ネゴシエーション時に応答を待機する最大時間（秒）に置き換えます。範囲は 1 ～ 10 秒です。 • デフォルトは 3 秒です。

	コマンドまたはアクション	目的

ステップ 9	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 10	**show ppp interfaces** {*type interface-path-id* | **all** | **brief** {*type interface-path-id* | **all** | **location** *node-id*} | **detail** {*type interface-path-id* | **all** | **location** *node-id*} | **location** *node-id*} **例：** `RP/0/RP0/CPU0:router# show ppp interfaces serial 0/2/0/0`	インターフェイスまたは PPP カプセル化がイネーブルになっているすべてのインターフェイスの PPP 設定を確認します。

認証プロトコルをディセーブルにする方法

ここでは、次の手順について説明します。

- 「インターフェイスでの PAP 認証のディセーブル化」（P.332）
- 「インターフェイスでの CHAP 認証のディセーブル化」（P.334）
- 「インターフェイスでの MS-CHAP 認証のディセーブル化」（P.336）

インターフェイスでの PAP 認証のディセーブル化

ここでは、シリアル インターフェイスまたは POS インターフェイスで PAP 認証をディセーブルにする手順について説明します。

手順の概要

1. **configure**

2. **interface** *type interface-path-id*
3. **ppp pap refuse**
4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp pap refuse** **例：** `RP/0/RP0/CPU0:router(config-if)# ppp pap refuse`	認証を要求するピアからのパスワード 認証プロトコル（PAP）認証を拒否します。 • 発信チャレンジ ハンドシェイク認証プロトコル（CHAP）が（**ppp authentication** コマンドを使用して）設定されている場合、拒否パケットでの認証方式として CHAP が提案されます。 • PAP 認証は、デフォルトではディセーブルに設定されています。

	コマンドまたはアクション	目的

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

インターフェイスでの CHAP 認証のディセーブル化

ここでは、シリアル インターフェイスまたは POS インターフェイスで CHAP 認証をディセーブルにする手順について説明します。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp chap refuse**
4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp chap refuse** **例：** `RP/0/RP0/CPU0:router(config-if)# ppp chap refuse`	認証を要求するピアからの CHAP 認証を拒否します。指定したインターフェイスで **ppp chap refuse** コマンドを入力すると、CHAP を使用してユーザー認証を強制しようとしたピアの試行はすべて拒否されます。 • CHAP 認証は、デフォルトではディセーブルに設定されています。 • 発信パスワード認証プロトコル（PAP）が（**ppp authentication** コマンドを使用して）設定されている場合、拒否パケットでの認証方式として PAP が提案されます。

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

インターフェイスでの MS-CHAP 認証のディセーブル化

ここでは、シリアル インターフェイスまたは POS インターフェイスで MS-CHAP 認証をディセーブルにする手順について説明します。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **ppp ms-chap refuse**
4. **end**
   または
   commit
5. **show running-config**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例：** `RP/0/RP0/CPU0:router(config)# interface serial 0/4/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ppp ms-chap refuse** **例：** `RP/0/RP0/CPU0:router(config-if)# ppp ms-chap refuse`	認証を要求するピアからの MS-CHAP 認証を拒否します。指定したインターフェイスで **ppp chap refuse** コマンドを入力すると、MS-CHAP を使用してユーザー認証を強制しようとしたピアの試行はすべて拒否されます。 • MS-CHAP 認証は、デフォルトではディセーブルに設定されています。 • 発信パスワード認証プロトコル（PAP）が（**ppp authentication** コマンドを使用して）設定されている場合、拒否パケットでの認証方式として PAP が提案されます。

	コマンドまたはアクション	目的

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show running-config** **例：** `RP/0/RP0/CPU0:router# show running-config`	PPP カプセル化がイネーブルになっているインターフェイスの PPP 認証情報を確認します。

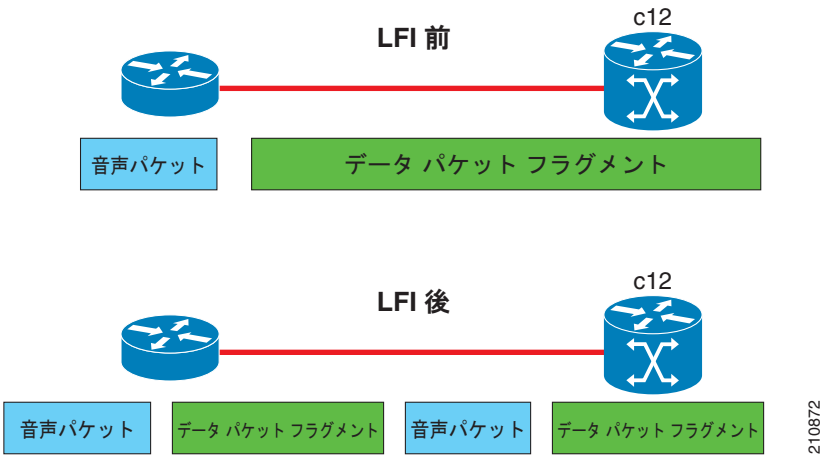
マルチリンク PPP について

Multilink Point-to-Point Protocol（MLPPP; マルチリンク ポイントツーポイント プロトコル）は、複数の物理リンクを組み合わせて 1 つの論理リンクを構成する機能を持ちます。Cisco XR 12000 シリーズ ルータ上に Cisco IOS XR を実装すると、複数の PPP インターフェイスが 1 つのマルチリンク インターフェイスに結合されます。MLPPP は、複数の PPP リンク間におけるデータグラムの分割、再構成、順序付けを行います。

Link Fragment Interleave（LFI; リンク フラグメンテーション/インターリーブ）は MLPPP インターフェイス用に設計されており、768 Kbps 未満の低速のインターフェイス上で音声とデータを統合する場合に必要になります。

LFI は、データと同じ回線上を移動する音声やビデオなど、遅延の影響を受けやすいトラフィックを安定させます。ネットワークが 768 Kbps 未満の低速のインターフェイス上で大きなパケットを処理しているときに遅延やジッタが生じると、音声は脆弱になります。LFI は、大きなデータグラムを分割（フラグメント）し、これらを低遅延のトラフィック パケットにインターリーブすることで、遅延やジッタを軽減します。

図 8　リンク フラグメンテーション/インターリーブ



サポートされるカード

MLPPP は、次のラインカードおよび SPA でサポートされています。

- Cisco XR 12000 マルチサービス ラインカード
- 2 ポートおよび 4 ポート チャネライズド T3 SPA（SPA-2XCT3/DS0、SPA-4XCT3/DS0）

LFI は、以下でサポートされています。

- Cisco 1 ポート チャネライズド STM-1/OC-3 共有ポート アダプタ

機能の概要

Cisco IOS XR での MLPPP は、PPP シリアル インターフェイスでサポートされているのと同じ機能（ただし、QoS を除きます）を提供します。加えて、次の機能も提供します。

- フラグメント サイズ（128、256、512 バイト）
- 長いシーケンス番号（24 ビット）
- 失われたフラグメントの検出タイムアウト時間（80 ミリ秒）
- 最小アクティブ リンク設定オプション
- マルチリンク インターフェイスでの LCP エコー要求/応答サポート
- Full T1 および E1 のフレーム化されたリンクとフレーム化されていないリンク

制限事項

Cisco IOS XR ソフトウェア対応の MLPPP には、以下の制限事項があります。

- サポートされるのはフル レート T1 のみです。
- バンドルのすべてのリンクは、同じ SPA に属します。
- バンドルのすべてのリンクは、同じ速度で動作する必要があります。
- バンドルごとの最大リンク数は 12 です。

- 2 ポート チャネライズド T3 SPA 上の最大バンドル数は 28 です。
- 4 ポート チャネライズド T3 SPA 上の最大バンドル数は 56 です。
- ラインカードごとの最大バンドル数は 224 です。
- MLPPP バンドルのすべてのシリアル リンクは、マルチリンク インターフェイスの **mtu** コマンドの値を継承します。そのため、MLPPP バンドルのメンバーとして設定する前に、シリアル インターフェイスで **mtu** コマンドを設定しないでください。Cisco IOS XR ソフトウェアは、以下をブロックします。
  - インターフェイスがデフォルト以外の MTU 値で設定されている場合、MLPPP バンドルのメンバーとしてシリアル インターフェイスを設定しようとする処理。
  - MLPPP バンドルのメンバーとして設定されているシリアル インターフェイスの **mtu** コマンド値を変更しようとする処理。

（注） PPP カプセル化を設定したインターフェイスで MTU 値を変更すると、回線プロトコルがフラップします。

Cisco IOS XR ソフトウェアでのマルチリンク処理は、マルチリンク コントローラと呼ばれるハードウェア モジュールによって制御されます。このコントローラは、ASIC、ネットワーク プロセッサ、CPU の連係動作で成り立ちます。MgmtMultilink コントローラにより、マルチリンク インターフェイスはチャネライズド SPA のシリアル インターフェイスのように動作します。

マルチリンク PPP の設定方法

ここでは、次の手順について説明します。

- 「コントローラの設定」（P.339）
- 「インターフェイスの設定」（P.342）
- 「MLPPP オプション機能の設定」（P.344）

コントローラの設定

コントローラを設定するには、次の作業を行います。

手順の概要

1. **configure**
2. **controller** *type interface-path-id*
3. **mode** *type*
4. **clock source** {**internal** | **line**}
5. **exit**
6. **controller t1** *interface-path-id*
7. **channel-group** *channel-group-number*
8. **timeslots** *range*
9. **exit**

10. **exit**
11. **controller mgmtmultilink** *interface-path-id*
12. **bundle** *bundle-id*
13. **end**
    または
    commit

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**controller** *type interface-path-id* **例：** `RP/0/0/CPU0:router(config)# controller t3 0/1/0/0`	コントローラ コンフィギュレーション サブモードを開始して、コントローラ名とインスタンス ID を *rack/slot/module/port* 表記で指定します。
ステップ 3	**mode** *type* **例：** `RP/0/0/CPU0:router# mode t1`	チャネライズするマルチリンクのタイプを設定します（たとえば、28 T1）。
ステップ 4	**clock source** {**internal** | **line**} **例：** `RP/0/0/CPU0:router(config-t3)# clock source internal`	（任意）ポートのクロッキングを設定します。 **（注）** デフォルトのクロック ソースは **internal** です。
ステップ 5	**exit** **例：** `RP/0/0/CPU0:router(config-t3)# exit`	コントローラのコンフィギュレーション モードを終了します。
ステップ 6	**controller t1** *interface-path-id* **例：** `RP/0/0/CPU0:router(config)# controller t1 0/1/0/0/0`	T1 コンフィギュレーション モードを開始します。
ステップ 7	**channel-group** *channel-group-number* **例：** `RP/0/0/CPU0:router(config-t1)# channel-group 0`	T1 チャネル グループを作成し、そのチャネル グループのチャネル グループ コンフィギュレーション モードを開始します。チャネル グループ番号は、0 ～ 23 の範囲で設定できます。

	コマンドまたはアクション	目的
ステップ 8	**timeslots** *range* **例：** `RP/0/0/CPU0:router(config-t1-channel_group)# timeslots 7-12`	1 つまたは複数の DS0 タイムスロットをチャネル グループに関連付け、関連付けたシリアル サブインターフェイスをそのチャネル グループに作成します。 • 範囲は 1 ～ 24 タイムスロットです。 • 24 タイムスロットすべてを単一のチャネル グループに割り当てることも、タイムスロットを複数のチャネル グループに分割することもできます。 **（注）** タイムスロットの範囲は、1 ～ 24 にする必要があります。これは、結果として構築されるシリアル インターフェイスが MLPPP バンドルに受け入れられるようにするためです。
ステップ 9	**exit** **例：** `RP/0/0/CPU0:router(config-t1-channel_group)# exit`	チャネル グループ コンフィギュレーション モードを終了します。
ステップ 10	**exit** **例：** RP/0/0/CPU0:router(config-t1)# exit	T1 コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 11	**controller mgmtmultilink** *interface-path-id* **例：** `RP/0/0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0`	マルチリンク インターフェイスの管理用にコントローラ コンフィギュレーション サブモードを開始します。コントローラ名とインスタンス ID を *rack/slot/module/port* 表記で指定します。

	コマンドまたはアクション	目的
ステップ 12	**bundle** *bundle-id* **例：** `RP/0/0/CPU0:router(config-mgmtmultilink)# bundle 20`	指定したバンドル ID でマルチリンク インターフェイスを作成します。

ステップ 13	**end**
	または
	commit
	
	例：
	`RP/0/0/CPU0:router(config-t3)# end`
	または
	`RP/0/0/CPU0:router(config-t3)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

インターフェイスの設定

インターフェイスを設定するには、次の作業を行います。

制約事項

- MLPPP バンドルのすべてのシリアル リンクは、マルチリンク インターフェイスの **mtu** コマンドの値を継承します。そのため、MLPPP バンドルのメンバーとして設定する前に、シリアル インターフェイスで **mtu** コマンドを設定しないでください。Cisco IOS XR ソフトウェアは、以下をブロックします。
  - インターフェイスがデフォルト以外の MTU 値で設定されている場合、MLPPP バンドルのメンバーとしてシリアル インターフェイスを設定しようとする処理。
  - MLPPP バンドルのメンバーとして設定されているシリアル インターフェイスの **mtu** コマンド値を変更しようとする処理。

（注） PPP カプセル化を設定したインターフェイスで MTU 値を変更すると、回線プロトコルがフラップします。

手順の概要

1. **configure**
2. **interface multilink** *interface-path-id*
3. **ipv4 address** *address/mask*
4. **multilink fragment-size** *size*
5. **keepalive** {*interval* | **disable**}
6. **exit**
7. **interface** *type interface-path-id*
8. **encapsulation** *type*
9. **multilink group** *group-id*
10. **end**
    または
    commit

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface multilink** *interface-path-id* **例：** `RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1`	マルチリンク インターフェイス名とインスタンス ID を *rack/slot/module/port/bundle-id* 表記で指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipv4 address** *ip-address* **例：** `RP/0/0/CPU0:router(config-if)# ipv4 address 80.170.0.1/24`	次の形式でインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。 *A.B.C.D/prefix or A.B.C.D/mask*
ステップ 4	**multilink fragment-size** *size* **例：** `RP/0/0/CPU0:router(config-if)# multilink fragment-size 128`	（任意）マルチリンク フラグメントのサイズを指定します（128 バイトなど）。フラグメント サイズによっては、サポートされない場合があります。 デフォルトは no fragments です。

ステップ 5	**keepalive** {*seconds* | **disable**}
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# keepalive 3`
	または
	`RP/0/RP0/CPU0:router(config-if)# keepalive disable`
		リンク制御プロトコル（LCP）がピアに ECHOREQ を送信する頻度（秒）を指定します。デフォルトのキープアライブ インターバルは 10 秒です。
		システムをデフォルトのキープアライブ インターバルに戻すには、**no keepalive** コマンドを使用します。
		キープアライブ タイマーをディセーブルにするには、**keepalive disable** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 6	**exit** **例：** `RP/0/0/CPU0:router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**interface** *type interface-path-id* **例：** `RP/0/0/CPU0:router(config)# interface serial 0/1/0/0/1:0`	インターフェイス名とインスタンス ID を *rack/slot/module/port/t1-number:channel-group* 表記で指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**encapsulation** *type* **例：** `RP/0/0/CPU0:router(config-if)# encapsulation ppp`	カプセル化のタイプを指定します。ここでは、PPP を指定します。 **（注）** PPP は、Cisco IOS XR リリース 3.4.1 以降でのみサポートされています。
ステップ 9	**multilink group** *group-id* **例：** `RP/0/0/CPU0:router(config-if)# multilink group 1`	このインターフェイスのマルチリンク グループ ID を指定します。

ステップ 10	**end**
	または
	commit
	
	例：
	`RP/0/0/CPU0:router(config-t3)# end`
	または
	`RP/0/0/CPU0:router(config-t3)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

MLPPP オプション機能の設定

次のいずれかのオプション機能を設定するには、次のタスクを実行します。

- アクティブ リンクの最大数
- マルチリンク インターリーブ

（注） アクティブ リンクの最大数は、両方のエンドポイントで設定する必要があります。

手順の概要

1. **configure**
2. **interface multilink** *interface-path-id*
3. **multilink**
4. **ppp multilink minimum-active links** *value*
5. **multilink interleave**
6. **no shutdown**
7. **end**
   または
   commit

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface multilink** *interface-path-id* **例：** `RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1`	マルチリンク インターフェイス名とインスタンス ID を *rack/slot/module/port/bundle-id* 表記で指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**multilink** **例：** `RP/0/0/CPU0:router(config-if)# multilink`	インターフェイス マルチリンク コンフィギュレーション モードを開始します。
ステップ 4	**ppp multilink minimum-active links** *value* **例：** `RP/0/0/CPU0:router(config-if-multilink)# ppp multilink minimum-active links 12`	（任意）マルチリンク インターフェイスのアクティブ リンクの最小数を指定します。
ステップ 5	**multilink interleave** **例：** `RP/0/0/CPU0:router(config-if-multilink)# multilink interleave`	（任意）マルチリンク インターフェイスでインターリーブをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**no shutdown** **例：** `RP/0/0/CPU0:router(config-if-mutlilink)# no shutdown`	shutdown 設定を削除します。 • shutdown 設定を削除すると、コントロールに強制された管理上のダウンが解除され、コントローラをアップ状態またはダウン状態に移行できるようになります。

ステップ 7	**end**
	または
	commit
	
	例：
	`RP/0/0/CPU0:router(config-t3)# end`
	または
	`RP/0/0/CPU0:router(config-t3)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

PPP の設定例

ここでは、次の設定例について説明します。

- 「POS インターフェイスでの PPP カプセル化の設定：例」（P.346）
- 「シリアル インターフェイスでの PPP カプセル化の設定：例」（P.347）
- 「マルチリンク PPP 設定の確認」（P.348）

POS インターフェイスでの PPP カプセル化の設定：例

次に、POS インターフェイスを作成し、PPP カプセル化を設定する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# ppp pap sent-username P1_CRS-8 password xxxx
RP/0/RP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access
RP/0/RP0/CPU0:router(config-if)# ppp chap password encrypted xxxx
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

次に、最初の認証が失敗した後に 2 回リトライできる（認証が失敗した場合に全部で 3 回リトライできる）ように POS インターフェイス 0/3/0/1 を設定する例を示します。

```
RP/0/RP0/CPU0:router# configuration
RP/0/RP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-if)# ppp max-bad-auth 3
```

シリアル インターフェイスでの PPP カプセル化の設定：例

次に、PPP MS-CHAP をカプセル化したシリアル インターフェイスを作成して設定する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface serial 0/3/0/0/0:0
RP/0/RP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RP0/CPU0:router(config-if)# no shutdown
RP/0/RP0/CPU0:router(config-if)# ppp authentication ms-chap MIS-access
RP/0/RP0/CPU0:router(config-if)# ppp ms-chap password encrypted xxxx
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

MLPPP の設定：例

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# controller t3 0/1/0/0
RP/0/0/CPU0:router# mode t1
RP/0/0/CPU0:router(config-t3)# clock source internal
RP/0/0/CPU0:router(config-t3)# exit
RP/0/0/CPU0:router(config)# controller t1 0/1/0/0/0
RP/0/0/CPU0:router(config-t1)# channel-group 0
RP/0/0/CPU0:router(config-t1-channel_group)# timeslots 7-12
RP/0/0/CPU0:router(config-t1-channel_group)# exit
RP/0/0/CPU0:router(config-t1)# exit
RP/0/0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0
RP/0/0/CPU0:router(config-mgmtmultilink)# bundle 20
RP/0/0/CPU0:router(config-t3)# commit
RP/0/0/CPU0:router(config-t3)# exit

RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# ipv4 address 80.170.0.1/24
RP/0/0/CPU0:router(config-if)# multilink fragment-size 128
RP/0/0/CPU0:router(config-if)# keepalive disable
RP/0/0/CPU0:router(config-if)# exit
RP/0/0/CPU0:router(config)# interface serial 0/1/0/0/1:0
RP/0/0/CPU0:router(config-if)# encapsulation ppp
RP/0/0/CPU0:router(config-if)# group 1
RP/0/0/CPU0:router(config-t3)# commit
RP/0/0/CPU0:router(config-t3)# exit

RP/0/0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/0/CPU0:router(config-if)# multilink
RP/0/0/CPU0:router(config-if-multilink)# ppp multilink minimum-active links 12
RP/0/0/CPU0:router(config-if-multilink)# multilink interleave
RP/0/0/CPU0:router(config-if-mutlilink)# no shutdown
RP/0/0/CPU0:router(config-t3)# commit
```

マルチリンク PPP 設定の確認

次のコマンドを使用して、マルチリンク設定を確認し、トラブルシューティングを行うことができます。

- 「show multilink interfaces：例」（P.348）
- 「show ppp interfaces multilink：例」（P.349）
- 「show ppp interface serial：例」（P.349）
- 「show imds interface multilink：例」（P.349）

show multilink interfaces：例

```
RP/0/0/CPU0:Router# show multilink interfaces multilink 0/3/1/0/301

Multilink0/3/1/0/301 is up, line protocol is up

     Fragmentation: disabled
     Member Links: 2 active, 0 inactive
      - Serial0/3/1/0/0:0: ACTIVE
      - Serial0/3/1/0/1:0: ACTIVE

RRP/0/0/CPU0:Router# show multilink interfaces

Multilink0/3/1/0/301 is up, line protocol is up

     Fragmentation: disabled
     Member Links: 2 active, 0 inactive
      - Serial0/3/1/0/0:0: ACTIVE
      - Serial0/3/1/0/1:0: ACTIVE

Multilink0/3/1/0/302 is up, line protocol is up

     Fragmentation: disabled
     Member Links: 2 active, 0 inactive
      - Serial0/3/1/1/1:0: ACTIVE
      - Serial0/3/1/1/0:0: ACTIVE

Serial0/3/1/0/0:0 is up, line protocol is up
     Multilink group id: 301
     Member status: ACTIVE

Serial0/3/1/1/0:0 is up, line protocol is up
     Multilink group id: 302
     Member status: ACTIVE

Serial0/3/1/0/1:0 is up, line protocol is up
     Multilink group id: 301
     Member status: ACTIVE

Serial0/3/1/1/1:0 is up, line protocol is up
     Multilink group id: 302
     Member status: ACTIVE
```

show ppp interfaces multilink：例

```
RP/0/0/CPU0:Router# show ppp interfaces multilink 0/3/1/0/1

Multilink 0/3/1/0/1 is up, line protocol is up
LCP: Open
     Keepalives disabled
  IPCP: Open
     Local IPv4 address: 1.1.1.2
     Peer IPv4 address:  1.1.1.1
  Multilink
     Member Links: 2 active, 1 inactive (min-active 1)
      - Serial0/3/1/0/0:0: ACTIVE
      - Serial0/3/1/0/1:0: ACTIVE
      - Serial0/3/1/0/2:0: INACTIVE : LCP has not been negotiated
```

show ppp interface serial：例

```
RP/0/0/CPU0:Router# show ppp interface Serial 0/3/1/0/0:0

Serial 0/3/1/0/0:0 is up, line protocol is up
  LCP: Open
     Keepalives disabled
     Local MRU: 1500 bytes
     Peer  MRU: 1500 bytes
     Local Bundle MRRU: 1596 bytes
     Peer  Bundle MRRU: 1500 bytes
     Local Endpoint Discriminator: 1b61950e3e9ce8172c8289df0000003900000001
     Peer  Endpoint Discriminator: 7d046cd8390a4519087aefb90000003900000001
  Authentication
     Of Peer: <None>
     Of Us:   <None>
  Multilink
     Multilink group id: 1
     Member status: ACTIVE
```

show imds interface multilink：例

```
RP/0/0/CPU0:Router# show imds interface Multilink 0/3/1/0/1

IMDS INTERFACE DATA (Node 0x0)

Multilink0_3_1_0_1 (0x04001200)
-----------------------
flags: 0x0001002f    type: 55 (IFT_MULTILINK)    encap: 52 (ppp)
state: 3 (up)     mtu: 1600    protocol count: 3
control parent: 0x04000800     data parent: 0x00000000
       protocol         capsulation           state        mtu
    --------------- -------------------- --------------- --------
    12 (ipv4)
                    26 (ipv4)            3 (up)          1500
                    47 (ipcp)            3 (up)          1500
    16 (ppp_ctrl)
                    53 (ppp_ctrl)        3 (up)          1500
    0 (Unknown)
                    139 (c_shim)         3 (up)          1600
                    52 (ppp)             3 (up)          1504
                    56 (queue_fifo)      3 (up)          1600
                    60 (txm_nopull)      3 (up)          1600
```

その他の参考資料

ここでは、PPP カプセル化に関する参考資料について説明します。

関連資料

内容	参照先
Cisco IOS XR マスター コマンド リファレンス	『*Cisco IOS XR Master Commands List*』
Cisco IOS XR インターフェイス コンフィギュレーション コマンド	『*Cisco IOS XR Interface and Hardware Component Command Reference*』
Cisco IOS XR ソフトウェアを使用した初期システム ブートアップとルータの設定情報	『*Cisco IOS XR Getting Started Guide*』
Cisco IOS XR AAA サービス構成情報	『*Cisco IOS XR System Security Configuration Guide*』および『*Cisco IOS XR System Security Command Reference*』
リモートの Craft Works Interface（CWI）クライアント管理アプリケーションからの、Cisco CRS-1 ルータ上のインターフェイスとその他のコンポーネントの設定に関する情報	『*Cisco Craft Works Interface Configuration Guide*』

規格

規格	タイトル
この機能によりサポートされた新規規格または改訂規格はありません。またこの機能による既存規格のサポートに変更はありません。	-

MIB

MIB	MIB リンク
この機能によりサポートされた新規 MIB または改訂 MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	Cisco IOS XR ソフトウェアを使用して選択したプラットフォームの MIB を検索およびダウンロードするには、次の URL の Cisco MIB Locator を使用します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC-1661	*The Point-to-Point Protocol (PPP)*
RFC- 1994	*PPP Challenge Handshake Authentication Protocol (CHAP)*

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、テクニカル ヒント、ツールへのリンクなど、さまざまな技術的コンテンツを検索可能な形で提供しています。Cisco.com に登録されている場合は、次のページからログインしてさらに多くのコンテンツにアクセスできます。	http://www.cisco.com/techsupport