



Cisco ASR 9000 シリーズ ルータ での PPP の設定

このモジュールでは、Cisco ASR 9000 シリーズ ルータでの POS およびシリアル 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) の設定について説明します。

PPP インターフェイス設定の機能履歴

リリース	変更内容
リリース 3.9.0	PPP、および PPP および MLPPP の ICSSO が Cisco ASR 9000 シリーズ ルータで導入されました。
リリース 3.9.1	T3 チャネライズド SONET のサポートが追加されました。
リリース 4.0.0	次の機能のサポートが、2 ポート チャネライズド OC-12c/DS0 SPA に対して追加されました。 <ul style="list-style-type: none">• IPHC over PPP、MLPPP、および MLPPP/LFI• NxDS0 シリアル インターフェイス PPP のサポートが次の SPA に対して導入されました。 <ul style="list-style-type: none">• 1 ポート チャネライズド OC-48/STM-16 SPA• 1 ポート OC-192c/STM-64 POS/RPR XFP SPA• 2 ポート OC-48c/STM-16 POS/RPR SPA• 8 ポート OC-12c/STM-4 POS SPA

リリース 4.0.1	<p>Cisco ASR 9000 シリーズ ルータでの PPP サポートが次の SPA に対して追加されました。</p> <ul style="list-style-type: none"> • Cisco 1 ポート チャネライズド OC-3/STM-1 SPA (MLPPP もサポート) • Cisco 2 ポートおよび 4 ポート クリア チャネル T3/E3 SPA • Cisco 4 ポート OC-3c/STM-1 SPA • Cisco 8 ポート OC-3c/STM-1 SPA
リリース 4.1.0	<p>ノイズ属性のサポートが PPP に対して追加されました。リンクにおいてリンク ノイズ モニタリング (LNM) しきい値を超えたときに MLPPP バンドル上のリンクを削除できるようにするためです。</p> <p>PPP のサポート (T1/E1 チャネルでの MLPPP のサポートなど) が、次の SPA で導入されました。</p> <ul style="list-style-type: none"> • Cisco 4 ポート チャネライズド T3 SPA • Cisco 8 ポート チャネライズド T1/E1 SPA

内容

- 「PPP の設定の前提条件」 (P.626)
- 「PPP について」 (P.627)
- 「PPP の設定方法」 (P.634)
- 「PPP の設定例」 (P.669)
- 「その他の関連資料」 (P.682)

PPP の設定の前提条件

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

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。

- 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 ASR 9000 シリーズ ルータでの 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 ASR 9000 シリーズ ルータでのシリアル 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 について

PPP および関連機能を設定するには、この項で説明する情報を理解する必要があります。

- 「PPP 認証」 (P.627)
- 「マルチリンク PPP」 (P.629)
- 「PPP および MLPPP の ICSSO」 (P.630)
- 「QoS を使用するマルチクラス MLPPP」 (P.632)
- 「T3 SONET チャネル」 (P.634)

PPP 認証

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、ローカル ルータがリモート デバイスに対して自身を認証しようとするには変わりありません。
- **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 デバイス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」および『Cisco IOS XR System Security Configuration Guide』の「Configuring AAA Services on Cisco IOS XR Software」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必要があります。

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必要があります。

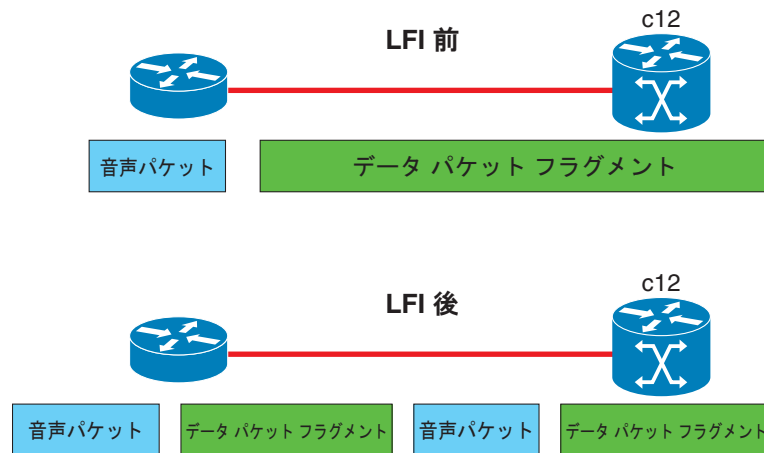
マルチリンク PPP

マルチリンク ポイントツーポイント プロトコル (MLPPP) は、複数の物理リンクを組み合わせることで 1 つの論理リンクを構成する機能を持ちます。実装によって、複数の PPP インターフェイスが結合されて 1 つのマルチリンク インターフェイスとなります。MLPPP は、複数の PPP リンクでデータグラムの断片化、再編成、および配列を行います。

リンク フラグメンテーション/インターリーブ (LFI) は、MLPPP インターフェイス用に設計されており、低速インターフェイス上の音声およびデータを統合するときに必要です。

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。ネットワークが低速インターフェイスの大きなパケットを処理しているとき、音声は増大した遅延およびジッターの影響を受けやすくなります。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、遅延やジッターを軽減します。

図 34 リンク フラグメンテーション/インターリーブ



MLPPP の機能概要

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。また、次の追加機能も提供します。

- 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期間 (1 秒)
- 最小アクティブ リンクの設定オプション。
- マルチリンク インターフェイスでの LCP エコー要求および応答のサポート。
- フル T1 および E1 フレームおよび非フレーム リンク。
- Cisco 2 ポート チャネライズド OC-12c/DS0 SPA での、T1/E1 リンクでのノイズ エラーのしきい値設定のサポート。これは、PPP にノイズ属性を通知して MLPPP バンドル リンクを削除させるために使用されます。LNM の詳細については、『Cisco ASR 9000 アグリゲーション サービス ルータ インターフェイスおよびハードウェア コンポーネント コンフィギュレーション ガイド』の「Cisco ASR 9000 シリーズ ルータでのクリア チャネル T3/E3 およびチャネライズド T3 および T1/E1 コントローラの設定」モジュールを参照してください。

IPHC Over MLPPP

2ポートチャネライズド OC-12c/DS0 SPA は、IPHC over PPP、MLPPP、および MLPPP/LFI をサポートします。IPHC の詳細と設定方法については、『Cisco ASR 9000 アグリゲーションサービスルータ インターフェイスおよびハードウェア コンポーネント コンフィギュレーションガイド』の「Cisco ASR 9000 シリーズルータでのシリアル 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 および MLPPP の ICSSO



(注) SR-APS および MR-APS は、Cisco 1 ポート チャネライズド OC-48/STM-16 SPA でサポートされません。

Cisco ASR 9000 シリーズ ルータでのシャーシ間ステートフル スイッチオーバー (ICSSO) の機能は、ポイントツーポイント プロトコル (PPP) やマルチリンク PPP (MLPPP) のセッションを、マルチルータ自動保護スイッチング (MR-APS) 現用ルータから MR-APS 保護ルータへの MR-APS スイッチオーバー時にも維持することです。

ICSSO によって、新しい MR-APS アクティブ ルータとリモート PPP/MLPPP ピア デバイス間のリンク制御プロトコル (LCP) または IP 制御プロトコル (IPCP) 再ネゴシエーションの必要なしに、MR-APS スイッチオーバーが可能になります。ICSSO の主な目的は、MR-APS スイッチオーバー中に加入者セッションおよびデータ損失を最小限に抑えることです。

ICSSO は、アクティブ ルータの PPP および MLPPP の状態情報とバックアップ ルータの状態情報を同期して、バックアップルータが MR-APS スイッチオーバーの後すぐにトラフィックを転送する準備が必ずできているようにします。

ICSSO は次に示す他のソフトウェア コンポーネントと連携します。

- 「マルチルータ自動保護スイッチング (MR-APS)」 (P.630)
- 「セッション状態冗長プロトコル (SSRP)」 (P.631)
- 「冗長グループ マネージャ (RG-MGR)」 (P.631)
- 「IP の高速再ルーティング (IP-FRR)」 (P.631)
- 「VPN ルーティングおよび転送 (VRF)」 (P.632)
- 「Open Shortest Path First (OSPF)」 (P.632)

マルチルータ自動保護スイッチング (MR-APS)

マルチルータ自動保護スイッチング (MR-APS) は、設備や機器の障害に対してレイヤ 1 を保護するためのシスコの機能です。この機能を使用するには、2 台のそれぞれ異なるルータに配置された SONET コントローラの保護のペアを設定します。冗長バックアップルータはアクティブルータと同じように設定されていて、MR-APS スイッチオーバー時にトラフィックをただちに転送する準備ができています。

保護ペアの通信には、SONET ダウンストリーム接続からのレイヤ 1 (k1/k2) シグナリング バイト (Bellcore 仕様 GR-253-CORE に従う) とレイヤ 3 シグナリング メッセージが使用されます。これには、Protect Group Protocol (PGP) が使用されます。MR-APS は、バックアップルート使用に切り替える IP-FRR アップデートを間接的にトリガーするような障害の原因の多くを検出します。

MR-APS の設定では、異なるルータ上の 2 台のインターフェイスは、現用インターフェイスまたは保護インターフェイスのロールを割り当てられます。これらのロールはオペレータによって設定されます。通常の状態では、現用インターフェイスがアクティブトラフィックを伝送します。現用インターフェイスに障害が発生した場合は、保護インターフェイスがただちにアクティブトラフィックを引き継ぐので、PPP トラフィックが失われることはありません。

セッション状態冗長プロトコル (SSRP)

MR-APS に設定された SONET コントローラのペアは、セッション状態冗長プロトコル (SSRP) 保護グループの一部です。SSRP は、アクティブとスタンバイのルータ間でインターフェイスとシステムの状態情報を伝達します。SSRP には、キープアライブプロトコルとしての役割もあります。

SSRP を設定するには、SONET コントローラにシャーシ間冗長グループを関連付け、MR-APS ピアルータによる各アクティブ SONET コントローラでの PPP セッションステート同期化をイネーブルにします。

PPP セッションは、次の 3 つの状態のいずれかになります。

- **Active** : PPP セッションがアクティブ状態となるのは、PPP セッションネゴシエーションが完了し、関連付けられたルートがインストール済みで、関連付けられた隣接関係が作成済みのおきです。Active 状態の PPP セッションは、スタンバイルータのピアにデータを複製します。
- **Standby Up** : スタンバイルータ上の PPP セッションが Standby Up 状態となるのは、複製された状態情報がアクティブルータから受信済みで、関連付けられた PPP ルートがインストール済みで、関連付けられた隣接関係が作成済みのおきです。Standby Up 状態の PPP セッションは、MR-APS スイッチオーバー直後からトラフィックを転送できる状態になっています。
- **Standby Down** : スタンバイルータ上の PPP セッションが Standby Down 状態となるのは、関連付けられたルートがインストール済みではなく、隣接関係も作成されていないおきです。

SSRP は MR-APS ピアルータ間で動作し、TCP/IP を使用します。1 つの SSRP セッションは、冗長 SONET コントローラの各ペアで実行されます。これは、複数の SSRP セッションが MR-APS 冗長ルータの 1 つのペアで実行できることを意味しています。



(注) SSRP は冗長性制御プロトコルではなく、状態情報同期プロトコルです。

冗長グループマネージャ (RG-MGR)

冗長グループマネージャ (RG-MGR) は保護インターフェイスのバックアップルートを設定します。RG-MGR は保護された SONET コントローラでのイベントを登録し、ルーティング情報ベース (RIB) コンポーネントに IP 高速再ルーティング (IP-FRR) 更新情報を渡します。

IP の高速再ルーティング (IP-FRR)



(注) IC-SSO で使用する場合、IP-FRR は PPP カプセル化だけでサポートされます。HDLC カプセル化との組み合わせではサポートされません。

IP 高速再ルーティング (IP-FRR) の特徴は、MR-APS スイッチオーバー後に、きわめて高速に PPP/MLPPP トラフィックの再ルーティングができることです。

IP-FRR はプライマリおよびバックアップルートを制御します。各ルートは、ルーティング情報ベース (RIB) 内でマッピングされます。MR-APS スイッチオーバー後にトラフィックを転送するためにどのバックアップパスが使用されるかは、IP-FRR によって制御されます。

MR-APS スイッチオーバーが発生すると、IP-FRR アップデートがトリガーされます。これによって、保護 SONET コントローラ上のバックアップ ルートがアクティブになります。現用 SONET コントローラが復元されると、別の IP-FRR アップデートがトリガーされ、トラフィックがプライマリ ルートに再ルーティングされます。

IP-FRR の詳細については、『*Cisco IOS XR MPLS Configuration Guide*』の「Implementing MPLS Traffic Engineering on Cisco IOS XR Software」モジュールを参照してください。

VPN ルーティングおよび転送 (VRF)

ICSSO は、VPN ルーティングおよび転送 (VRF) とともに使用できます。異なるサービス タイプごとにトラフィック ストリームを分離する場合、ユーザは VRF テクノロジーを使用して実行できます。VRF を利用すると、複数の独立したルーティングおよび転送データベースを作成して維持することができます。「[ICSSO で使用するマルチリンクの VRF の設定 : 例](#)」(P.674) および「[ICSSO で使用するためのイーサネットの VRF の設定 : 例](#)」(P.675) を参照してください。VRF の設定に関する詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*』を参照してください。

Open Shortest Path First (OSPF)

PPP セッションの終端がリモート ピアとなっている場合は、集約ルータはそのリモート ピアが使用可能かどうかを Open Shortest Path First (OSPF) を使用してネットワーク上でアダプタイズする必要があります。OSPF は、リモート PPP ピアが使用可能かどうかを ICSSO ピア ルータにアダプタイズするために必要です。「[ICSSO で使用する OSPF の設定 : 例](#)」(P.675) を参照してください。OSPF の設定方法の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*』を参照してください。

ICSSO の設定の概要

ICSSO は次のように設定されます。

- MR-APS の設定
- SSRP プロファイルを設定
- SSRP グループを設定
- PPP カプセル化のシリアル インターフェイスへの設定
- マルチリンク インターフェイスを設定
- ICSSO 設定を確認

このモジュールの「[PPP および MLPPP の ICSSO の設定](#)」(P.660) で、ICSSO を設定する手順を説明しています。

「[PPP および MLPPP の ICSSO の設定 : 例](#)」(P.670) では、ICSSO および関連コンポーネントの設定の具体的な例を示しています。

QoS を使用するマルチクラス MLPPP

マルチクラス マルチリンク ポイントツーポイント プロトコル (MLPPP) は、Quality of Service (QoS) と組み合わせて使用できます。設定するには、ポリシー マップ内の特定のクラスの下で `encap-sequence` コマンドを使用します。

encap-sequence コマンドは、MQC 定義クラス内のパケットの MLPPP MCMP クラス ID を指定します。

encap-sequence ID 番号の有効値は、**none**、0、1、2、3 です。**none** 値は、**priority level** が 1 のときだけ適用でき、MLPPP カプセル化がないことを示します。1、2、または 3 の値は、プライオリティ 1 もしくは 2 のクラスまたはキューイング アクションを含むその他のクラスで使用できます。

encap-sequence ID 番号の値のうち、0 はデフォルト クラス用に予約されており、他のクラスで指定することはできません。



(注) **encap-sequence** ID 番号は、番号順に設定する必要があります。たとえば、1 と 2 をすでに割り当てていない限り、ID 番号 3 は割り当てることができません。

encap-sequence ID 番号の数は、マルチリンク ヘッダーによってピア間でネゴシエーションされる MLPPP クラスの数未満でなければなりません。システムによってこれが確認されないため、ユーザは設定がこれに合っていることを確認する必要があります。

ppp multilink multiclass remote apply コマンドは、これを確認する方法を提供します。

encap-sequence ID 番号（デフォルト値の 0 を含む）を使用するクラスの数、**ppp multilink multiclass remote apply** コマンドの *min-number* 値よりも小さいことを確認します。たとえば、**ppp multilink multiclass remote apply** コマンドの *min-number* 値が 4 の場合は、**encap-sequence** ID 番号を持つクラスは 3 つ以下となります。

QoS ポリシーは、次の条件を検証します。これらの条件が満たされていない場合、ポリシーは拒否されます。

- **encap-sequence** ID 番号が 1～3 という許容値の範囲内である。
- **encap-sequence** がポリシー マップ内でいずれかのクラスに対して設定されている場合は、そのポリシー マップ内のクラスのうち、**プライオリティ レベル 1** のものすべてに **encap-sequence** ID 番号も指定されていることが必要になります。
- **encap-sequence** を **none** に設定できるのは、**プライオリティ レベル**が 1 のクラスに限定されます。
- **class-default** には **encap-sequence** 設定は含まれていません。
- キューイング アクションを含むクラスだけが **encap-sequence** 設定を持ちます。



(注) 同じ **encap-sequence** ID 番号を共有するクラスは、**プライオリティ**が同じである必要があります。

QoS ポリシー マップは、次のとおりに設定されます。

```
config
  policy-map type qos policy-name
    class class-name
      アクション
      アクション
      アクション
  ...
```

次に、MLPPP のポリシー マップを設定する例を示します。

```
config
  policy-map foo
    class ip-prec-1
      encap-sequence none
      police rate percent 10
      priority level 1
  !
  class ip-prec-2
```

```

        encap-sequence 1
        shape average percent 80
    !
    class ip-prec-3
        encap-sequence 1
        bandwidth percent 10
    !
    class class-default
    !
end-policy-map
!
```

QoS および QoS コマンド設定の詳細については、『*Cisco ASR 9000 Series Aggregation Services Routers Modular Quality of Service Configuration Guide*』および『*Cisco ASR 9000 Series Aggregation Services Routers Modular Quality of Service Command Reference*』を参照してください。

T3 SONET チャネル

Cisco ASR 9000 シリーズ ルータは、次のハードウェアで T3 チャネライズド SONET をサポートします。

- SIP 700 SPA インターフェイス プロセッサ
- 1 ポート チャネライズド OC-3/STM-1 SPA
- 2 ポート チャネライズド OC-12c/DS0 SPA
- 1 ポート チャネライズド OC-48/STM-16 SPA

チャネライズド SONET によって、複数の T3 チャネルを同じ物理リンク上で転送できるようになります。

チャネライズド SONET、T3 および T1 コントローラ、シリアル インターフェイス、および SONET APS の設定の詳細については、次の関連モジュールを参照してください。

- [「Cisco ASR 9000 シリーズ ルータ でのチャネライズド SONET/SDH の設定」](#)
- [「Cisco ASR 9000 シリーズ ルータ でのクリア チャネル SONET コントローラの設定」](#)
- [「Cisco ASR 9000 シリーズ ルータでのクリア チャネル T3/E3 およびチャネライズド T3 および T1/E1 コントローラの設定」](#)
- [「Cisco ASR 9000 シリーズ ルータでのシリアル インターフェイスの設定」](#)

PPP の設定方法

ここでは、次の手順について説明します。

- [「デフォルトの PPP 設定の変更」 \(P.635\)](#)
- [「PPP 認証の設定」 \(P.638\)](#)
- [「認証プロトコルのディセーブル化」 \(P.648\)](#)
- [「マルチリンク PPP の設定」 \(P.652\)](#)
- [「PPP および MLPPP の ICSSO の設定」 \(P.660\)](#)

デフォルトの PPP 設定の変更

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。
- 否定応答 (CONFNAK) 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終了要求 (TermReq) 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 ASR 9000 シリーズ ルータでの 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 ASR 9000 シリーズ ルータでのシリアル 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}**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： RP/0/RSP0/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	<code>interface type interface-path-id</code> 例： RP/0/RSP0/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	<code>ppp max-bad-auth retries</code> 例： RP/0/RSP0/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。 <ul style="list-style-type: none"> 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。 <code>retries</code> 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。 <code>ppp max-bad-auth</code> 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	<code>ppp max-configure retries</code> 例： RP/0/RSP0/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。 <ul style="list-style-type: none"> <code>retries</code> 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	<code>ppp max-failure retries</code> 例： RP/0/RSP0/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。 <ul style="list-style-type: none"> <code>retries</code> 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
<p>ステップ6 <code>ppp max-terminate number</code></p> <p>例: RP/0/RSP0/CPU0:router(config-if)# ppp max-terminate 5</p>	<p>(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。</p> <ul style="list-style-type: none"> <code>number</code> 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。
<p>ステップ7 <code>ppp timeout authentication seconds</code></p> <p>例: RP/0/RSP0/CPU0:router(config-if)# ppp timeout authentication 20</p>	<p>(任意) PPP 認証タイムアウト パラメータを設定します。</p> <ul style="list-style-type: none"> <code>seconds</code> 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 <code>ppp timeout authentication</code> 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。
<p>ステップ8 <code>ppp timeout retry seconds</code></p> <p>例: RP/0/RSP0/CPU0:router(config-if)# ppp timeout retry 8</p>	<p>(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。</p> <ul style="list-style-type: none"> <code>seconds</code> 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	<pre>end または commit</pre> <p>例: RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーションファイルに変更を保存し、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	<pre>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}</pre> <p>例: RP/0/RSP0/CPU0:router# show ppp interfaces serial 0/2/0/0</p>	<p>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。</p>

PPP 認証の設定

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.638)
- 「PAP 認証パスワードの設定」(P.642)
- 「CHAP 認証パスワードの設定」(P.644)
- 「MS-CHAP 認証パスワードの設定」(P.646)

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 ASR 9000 シリーズ ルータでの 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 ASR 9000 シリーズ ルータでのシリアル 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}**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例： RP/0/RSP0/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
<p>ステップ2 <code>interface type interface-path-id</code></p> <p>例 : RP/0/RSP0/CPU0:router(config)# interface serial 0/4/0/1</p>	<p>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。</p>
<p>ステップ3 <code>ppp authentication protocol [protocol [protocol]] [list-name default]</code></p> <p>例 : RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access</p>	<p>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。</p> <ul style="list-style-type: none"> • <i>protocol</i> 引数を、pap、chap、または ms-chap に置き換えます。 • <i>list name</i> 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。 • リスト名を指定しない場合は、デフォルト名が使用されます。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
<p>ステップ 4</p> <pre>end または commit</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</pre>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーション ファイルに変更を保存し、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。
<p>ステップ 5</p> <pre>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}</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router# show ppp interfaces serial 0/2/0/0</pre>	<p>インターフェイスの PPP ステート情報を表示します。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>

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.642) 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.644) 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.646) 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.638) 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`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： <code>RP/0/RSP0/CPU0:router# configure</code>	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
<p>ステップ 2 <code>interface type interface-path-id</code></p> <p>例 : RP/0/RSP0/CPU0:router(config)# interface serial 0/4/0/1</p>	<p>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。</p>
<p>ステップ 3 <code>ppp pap sent-username username password [clear encrypted] password</code></p> <p>例 : RP/0/RSP0/CPU0:router(config-if)# ppp pap sent-username xxxx password notified</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。

■ PPP の設定方法

	コマンドまたはアクション	目的
ステップ4	<pre>end または commit</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、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	<pre>show running-config</pre> <p>例 : RP/0/RSP0/CPU0:router# show running-config</p>	<p>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。</p>

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.638) 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

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<p><code>configure</code></p> <p>例： RP/0/RSP0/CPU0:router# <code>configure</code></p>	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	<p><code>interface type interface-path-id</code></p> <p>例： RP/0/RSP0/CPU0:router(config)# <code>interface serial 0/4/0/1</code></p>	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	<p><code>ppp chap password [clear encrypted] password</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# <code>ppp chap password clear xxxx</code></p>	<p>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。</p> <ul style="list-style-type: none"> • 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。 • <i>password</i> 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。

■ PPP の設定方法

	コマンドまたはアクション	目的
ステップ4	<pre>end または commit</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> - 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 - cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、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	<pre>show running-config</pre> <p>例 : RP/0/RSP0/CPU0:router# show running-config</p>	<p>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。</p>

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.638) 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

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： RP/0/RSP0/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	<code>interface type interface-path-id</code> 例： RP/0/RSP0/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	<code>ppp ms-chap password [clear encrypted] password</code> 例： RP/0/RSP0/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せん。
ステップ4	<code>end</code> または <code>commit</code> 例： RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit	設定変更を保存します。 <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 <ul style="list-style-type: none"> • 実行コンフィギュレーション ファイルに変更を保存し、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	<code>show running-config</code> 例： RP/0/RSP0/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。

認証プロトコルのディセーブル化

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.648)
- 「インターフェイスでの CHAP 認証のディセーブル化」 (P.649)
- 「インターフェイスでの MS-CHAP 認証のディセーブル化」 (P.651)

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例 : RP/0/RSP0/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/RSP0/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/RSP0/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。 <ul style="list-style-type: none"> • 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
<p>ステップ4</p> <pre>end または commit</pre> <p>例:</p> <pre>RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</pre>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> - 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 - cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、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。
<p>ステップ5</p> <pre>show running-config</pre> <p>例:</p> <pre>RP/0/RSP0/CPU0:router# show running-config</pre>	<p>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。</p>

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例 : RP/0/RSP0/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/RSP0/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/RSP0/CPU0:router(config-if)# ppp chap refuse	<p>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。</p> <ul style="list-style-type: none"> 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/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーション ファイルに変更を保存し、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/RSP0/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**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例： RP/0/RSP0/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/RSP0/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/RSP0/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。 <ul style="list-style-type: none"> • 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	<pre>end または commit</pre> <p>例: RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 - cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、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	<pre>show running-config</pre> <p>例: RP/0/RSP0/CPU0:router# show running-config</p>	<p>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。</p>

マルチリンク PPP の設定

ここでは、次の手順について説明します。

- 「前提条件」(P.652)
- 「制約事項」(P.652)
- 「コントローラの設定」(P.653)
- 「インターフェイスの設定」(P.656)
- 「MLPPP オプション機能の設定」(P.658)

前提条件

MLPPP および LFI は、1 ポート チャネライズド OC-3/STM-1 SPA および 2 ポート チャネライズド OC-12/DS0 SPA でサポートされます。

制約事項

Cisco IOS XR ソフトウェアの MLPPP には、次の制限があります。

- 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。
- バンドルごとに最大 10 のリンクがサポートされます。
- ラインカードごとに最大 700 のバンドルがサポートされます。
- システムごとに最大 2600 のバンドルがサポートされます。
- DS0 リンク メンバでは MLPPP インターフェイスはサポートされません。
- T3 チャネルをメンバとする場合、MLPPP インターフェイスはサポートされません。したがって、LFI も T3 チャネルではサポートされません。
- 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。

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。

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure</code> 例： RP/0/RSP0/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	<code>controller type interface-path-id</code> 例： RP/0/RSP0/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 <code>rack/slot/module/port</code> 表記で指定します。
ステップ 3	<code>mode type</code> 例： RP/0/RSP0/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	<code>clock source {internal line}</code> 例： RP/0/RSP0/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	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config-t3)# exit	コントローラ 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	<code>controller t1 interface-path-id</code> 例： RP/0/RSP0/CPU0:router(config)# controller t1 0/1/0/0/1	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	<code>channel-group channel-group-number</code> 例： RP/0/RSP0/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。
ステップ 8	<code>timeslots range</code> 例： RP/0/RSP0/CPU0:router(config-t1-channel_group)# timeslots 1-24	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。 <ul style="list-style-type: none">範囲は 1 ~ 24 タイムスロットです。 (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。

	コマンドまたはアクション	目的
ステップ 9	<p>exit</p> <p>例： RP/0/RSP0/CPU0:router(config-t1-channel_group)# exit</p>	<p>チャンネル グループ コンフィギュレーション モードを終了します。</p>
ステップ 10	<p>exit</p> <p>例： RP/0/RSP0/CPU0:router(config-t1)# exit</p>	<p>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。</p>
ステップ 11	<p>controller mgmtmultilink interface-path-id</p> <p>例： RP/0/RSP0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0</p>	<p>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 <i>rack/slot/module/port</i> 表記で指定します。</p>
ステップ 12	<p>bundle bundle-id</p> <p>例： RP/0/RSP0/CPU0:router(config-mgmtmultilink)# bundle 20</p>	<p>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。</p>
ステップ 13	<p>end または commit</p> <p>例： RP/0/RSP0/CPU0:router(config-t3)# end または RP/0/RSP0/CPU0:router(config-t3)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 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、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure 例： RP/0/RSP0/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/RSP0/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 <i>rack/slot/module/port/bundle-id</i> 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。

	コマンドまたはアクション	目的
ステップ3	<p><code>ipv4 address ip-address</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# ipv4 address 80.170.0.1/24</p>	<p>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。</p> <p><i>A.B.C.D/prefix</i> または <i>A.B.C.D/mask</i></p>
ステップ4	<p><code>multilink fragment-size bytes</code> または <code>multilink fragment delay delay-ms</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# multilink fragment-size 350 または RP/0/RSP0/CPU0:router(config-if)# multilink fragment delay 2</p>	<p>(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 <code>no fragments</code> です。</p> <p>または</p> <p>(任意) ミリ秒単位でのマルチリンク フラグメント遅延を指定します。これは、個々のメンバリンク (帯域幅 1536000bps/192000Bps の T1) の送信時間遅延と同じ長さになるように、MLPPP フラグメントサイズを設定します。</p> <p>ユーザが <code>fragment delay 2</code> を指定する場合、フラグメントサイズは $(192000 * 0.002) = 384B$ です。このコマンドの使用は <code>fragment size</code> での使用に限定されます。どちらのコマンドも、他方よりも優先されます。</p>
ステップ5	<p><code>keepalive {interval disable}[retry]</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# keepalive disable</p>	<p>チャンネルのキープアライブ タイマーを設定します。ここで、</p> <ul style="list-style-type: none"> <code>interval</code> : キープアライブ メッセージ間の秒数 (1 ~ 30)。デフォルトは 10 です。 <code>disable</code> : キープアライブ タイマーをオフにします。 <code>retry</code> : (任意) リンクがダウン状態に遷移する前に、応答なしでピアに送信できるキープアライブ メッセージの数 (1 ~ 255)。デフォルトは 3 です。 <p>(注) Cisco IOS デバイスによっては、そのデバイスに接続するにはマルチリンク キープアライブを両方のデバイスでディセーブルにする必要があります。</p>
ステップ6	<p><code>exit</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# exit</p>	<p>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 モードに入ります。</p>
ステップ7	<p><code>interface type interface-path-id</code></p> <p>例： RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/0/1:0</p>	<p>インターフェイス名とインスタンス ID を <code>rack/slot/module/port/t1-number:channel-group</code> 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。</p>
ステップ8	<p><code>encapsulation type</code></p> <p>例： RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp</p>	<p>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。</p>

コマンドまたはアクション	目的
ステップ9 <code>multilink group group-id</code> 例: <code>RP/0/RSP0/CPU0:router(config-if)# multilink group 20</code>	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 <code>end</code> または <code>commit</code> 例: <code>RP/0/RSP0/CPU0:router(config-t3)# end</code> または <code>RP/0/RSP0/CPU0:router(config-t3)# commit</code>	設定変更を保存します。 <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 <code>Uncommitted changes found, commit them before exiting (yes/no/cancel)?</code> <code>[cancel]:</code> <ul style="list-style-type: none"> - 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 - cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、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

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure</code> 例： RP/0/RSP0/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	<code>interface multilink interface-path-id</code> 例： RP/0/RSP0/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 <i>rack/slot/module/port/bundle-id</i> 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	<code>multilink</code> 例： RP/0/RSP0/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	<code>ppp multilink minimum-active links value</code> 例： RP/0/RSP0/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。 (注) リンクの LNM しきい値を超えたとき、MLPPP バンドルのリンクを削除するように PPP にシグナリングするようにノイズ属性のサポートが設定されている場合、リンクはこの <code>mimum-active</code> しきい値未満では削除されません。
ステップ5	<code>multilink interleave</code> 例： RP/0/RSP0/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	<p><code>no shutdown</code></p> <p>例: RP/0/RSP0/CPU0:router(config-if-mutlilink)# no shutdown</p>	<p>shutdown 設定を削除します。</p> <ul style="list-style-type: none"> 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	<p><code>end</code> または <code>commit</code></p> <p>例: RP/0/RSP0/CPU0:router(config-t3)# end または RP/0/RSP0/CPU0:router(config-t3)# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> 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、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーションファイルに変更を保存し、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 および MLPPP の ICSSO の設定

この項では、次の ICSSO の設定手順について説明します。

- 「前提条件」(P.660)
- 「制約事項」(P.661)
- 「基本 ICSSO 実装の設定」(P.661)
- 「MR-APS の設定」(P.662)
- 「シリアルおよびマルチリンク インターフェイスの SSRP の設定」(P.664)

前提条件

Cisco ASR 9000 シリーズ ルータは、次の MR-APS、最小装置、ハードウェア構成で ICSSO をサポートします。

- 6 スロットまたは 8 スロット シャーシ 2 台
- ルート/スイッチ プロセッサ (RSP) 4 台、シャーシあたり 2 台 (信頼性を高める)
- 2 つの 20G SIP、シャーシごとに 1 つ
- 次の SPA タイプのうち 2 つ、シャーシごとに 1 つ

- 2 ポート チャネライズド OC-12/DS0 SPA
- 4 ポート チャネライズド T3 SPA
- 8 ポート チャネライズド T1/E1 SPA
- 2 つの 40 ギガビット イーサネット ラインカード、シャーシごとに 2 つ
- 2 つの 4 ポート 10 ギガビット イーサネット ラインカード、シャーシごとに 1 つ
- 1 ポート チャネライズド OC-3/STM-1 SPA (SPA-1XCHSTM1/OC3)

制約事項

次の制約事項は、PPP および MLPPP の ICSSO に適用されます。

- ICSSO は 2 つの独立したルータだけでサポートされます。
同じルータ上の 2 枚のラインカードに対しては、ICSSO はサポートされません。
- ICSSO ピア ルータ間の IOS XR システム設定の自動同期または検証は利用できません。
- 次の制約事項は、2 ポート チャネライズド OC-12/DS0 SPA の ICSSO に適用されます。
 - ICSSO は、T1/T3 PPP および T1/MLPPP インターフェイスだけでサポートされます。
 - T1 メンバリンクは、同じ SPA で終端する必要があります。
 - MR-APS で保護されている MLPPP バンドルのメンバリンクはすべて、MR-APS 保護ペアの一部である同じ SONET ポートに含まれている必要があります。
 - OC-12 SONET インターフェイス上の T1/PPP、T3/PPP および MLPPP カプセル化されたインターフェイスは保護できます。
- 次の制約事項は、1 ポート チャネライズド T3 SPA の ICSSO に適用されます。
 - T3、T1、E1 チャネルだけの PPP でサポートされます。
 - E1 チャネルだけの MLPPP のメンバリンクでサポートされます。
- 次の制約事項は、8 ポート チャネライズド T1/E1 SPA の ICSSO に適用されます。
 - T1 および E1 チャネルだけの PPP でサポートされます。
 - E1 チャネルだけの MLPPP のメンバリンクでサポートされます。

基本 ICSSO 実装の設定

ICSSO の単純バージョンを設定するには、次の手順を使用します。

手順の概要

1. **config**
2. **redundancy**
3. **multi-router aps**
4. **group group_number**
5. **controller sonet path**
6. **member ipv4 address backup-interface**
7. **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	config 例： RP/0/RSP0/CPU0:router# config	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	redundancy 例： RP/0/RSP0/CPU0:router(config)# redundancy	冗長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	multi-router aps 例： RP/0/RSP0/CPU0:router(config-redundancy)# multi-router aps	Multi-Router APS 冗長を設定して、APS 冗長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	group group_number 例： RP/0/RSP0/CPU0:router(config-redundancy-aps)# group 1	APS 冗長グループを設定し、グループ番号を割り当てます。
ステップ5	controller sonet path 例： RP/0/RSP0/CPU0:router(config-redundancy-aps-group)# controller sonet 0/1/0/0	APS 冗長バックアップとして SONET コントローラを指定します。
ステップ6	member ipv4 address backup-interface type interface-path-id 例： RP/0/RSP0/CPU0:router(config-redundancy-group-controller)# member ipv4 10.10.10.10 backup-interface GigabitEthernet 0/6/0/1	IP-FRR で使用されるバックアップ インターフェイスの IP アドレスを指定します。
ステップ7	commit 例： RP/0/RSP0/CPU0:router(config-redundancy-group-controller)# commit	設定を保存します。
ステップ8	show running config 例： RP/0/RSP0/CPU0:router# show running config	設定を確認するために MR-APS、SONET コントローラおよび IP アドレス情報を含むルータの現在の設定を表示します。

MR-APS の設定

MR-APS を設定するには、次の手順に従います。

手順の概要

1. `config`
2. `aps group number`
3. `channel {0 | 1} remote ip-address`
4. `channel {0 | 1} local sonet interface-path-id`
5. `exit`
6. `aps rprplus`
7. `interface GigabitEthernet interface-path-id`
8. `description text`
9. `ipv4 address ipv4-address mask`
10. `commit`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>config</code> 例： RP/0/RSP0/CPU0:router# config	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	<code>aps group number</code> 例： RP/0/RSP0/CPU0:router(config)# aps group 1	自動保護スイッチング (APS) グループを追加して、APS グループ 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	<code>channel {0 1} remote ip-address</code> 例： RP/0/RSP0/CPU0:router(config-aps)# channel 0 remote 99.10.1.2	リモート ルータに物理的に配置されたポートとインターフェイスを SONET APS チャンネルとして割り当てます。 <ul style="list-style-type: none"> • 0 は保護チャンネルにチャンネルを指定します。 • 1 は現用チャンネルとしてチャンネルを指定します。
ステップ4	<code>channel {0 1} local sonet interface-path-id</code> 例： RP/0/RSP0/CPU0:router(config-aps)# channel 1 local SONET 0/1/0/0	ローカル SONET 物理ポートを SONET APS チャンネルとして割り当てます。 <ul style="list-style-type: none"> • 0 は保護チャンネルにチャンネルを指定します。 • 1 は現用チャンネルとしてチャンネルを指定します。
ステップ5	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config-aps)# exit	前のモードに戻ります。
ステップ6	<code>aps rprplus</code> 例： RP/0/RSP0/CPU0:router(config-aps)# aps rprplus	スイッチオーバーの APS ホールド タイマーを拡張します。

	コマンドまたはアクション	目的
ステップ7	<code>interface GigabitEthernet interface-path-id</code> 例: RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/6/0/0	ギガビットイーサネット インターフェイスを MR-APS ピアへのパスとして作成し、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	<code>description text</code> 例: RP/0/RSP0/CPU0:router(config-if)# description MR-APS PGP interface for aps group 1	このインターフェイスにテキスト説明を追加します。
ステップ9	<code>ipv4 address ipv4-address mask</code> 例: RP/0/RSP0/CPU0:router(config-if)# ipv4 address 99.10.1.1 255.255.255.0	インターフェイスのプライマリ IPv4 アドレスとサブネット マスクを設定します。
ステップ10	<code>commit</code> 例: RP/0/RSP0/CPU0:router(config-if)# commit	現在の設定を保存します。

シリアルおよびマルチリンク インターフェイスの SSRP の設定

シリアルおよびマルチリンク インターフェイスの SSRP を設定するには、次の手順を実行します。

手順の概要

1. `config`
2. `ssrp profile profile-name`
3. `peer ipv4 address A.B.C.D`
4. `exit`
5. `ssrp location node_id`
6. `group group-id profile profile_name`
7. `group group-id profile profile_name`
8. `exit`
9. `interface serial interface-path-id`
10. `ssrp group group-number id id-number ppp`
11. `encapsulation ppp`
12. `multilink`
13. `group group-id`
14. `exit`
15. `keepalive disable`
16. `exit`

17. `interface serial interface-path-id`
18. `ssrp group group-number id id-number ppp`
19. `encapsulation ppp`
20. `multilink`
21. `group group-id`
22. `exit`
23. `keepalive disable`
24. `exit`
25. `interface multilink interface-path-id`
26. `ipv4 address ipv4-address mask`
27. `ssrp group group-number id id-number ppp`
28. `encapsulation ppp`
29. `shutdown`
30. `keepalive disable`
31. `exit`
32. `controller MgmtMultilink interface-path-id`
33. `bundle bundleID`
34. `bundle bundleID`
35. `commit`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>config</code> 例： RP/0/RSP0/CPU0:router# config	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	<code>ssrp profile profile-name</code> 例： RP/0/RSP0/CPU0:router(config)# ssrp profile Profile_1	セッション状態冗長プロトコル (SSRP) プロファイルを設定し、SSRP 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	<code>peer ipv4 address A.B.C.D</code> 例： RP/0/RSP0/CPU0:router(config)# peer ipv4 address 10.10.10.10	セッション状態冗長プロトコル (SSRP) ピアの IPv4 アドレスを設定します。
ステップ4	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config-aps)# exit	前のモードに戻ります。

■ PPP の設定方法

	コマンドまたはアクション	目的
ステップ 5	<pre>ssrp location node_id</pre> <p>例 : RP/0/RSP0/CPU0:router(config)# ssrp location 0/1/CPU0</p>	セッション状態冗長プロトコル (SSRP) グループを作成するノードを指定し、SSRP ノード コンフィギュレーション モードを開始します。
ステップ 6	<pre>group group-id profile profile_name</pre> <p>例 : RP/0/RSP0/CPU0:router(config-ssrp)# group 1 profile Profile_1</p>	セッション状態冗長プロトコル (SSRP) グループを作成し、プロファイルに関連付けます。
ステップ 7	<pre>group group-id profile profile_name</pre> <p>例 : RP/0/RSP0/CPU0:router(config-ssrp-node)# group 2 profile Profile_2</p>	2 つ目のセッション状態冗長プロトコル (SSRP) グループを作成し、それをプロファイルに関連付けます。
ステップ 8	<pre>exit</pre> <p>例 : RP/0/RSP0/CPU0:router(config-ssrp-node)# exit</p>	前のモードに戻ります。
ステップ 9	<pre>interface serial interface-path-id[.subinterface]</pre> <p>例 : RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/0/1/1:0</p>	<p>物理インターフェイスまたは仮想インターフェイス。</p> <p>(注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、show interfaces コマンドを使用します。</p> <p>ルータ構文の詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。</p>
ステップ 10	<pre>ssrp group group-number id id-number ppp</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# ssrp group 1 id 1 ppp</p>	SSRP グループをインターフェイス上でアタッチします。
ステップ 11	<pre>encapsulation ppp</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp</p>	ポイントツーポイント プロトコル (PPP) を使用してルータと通信するためのカプセル化をイネーブルにします。
ステップ 12	<pre>multilink</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# multilink</p>	マルチリンク 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 13	<pre>group group-id</pre> <p>例 : RP/0/RSP0/CPU0:router(config-if)# group 1</p>	セッション状態冗長プロトコル (SSRP) グループをこのインターフェイスにアタッチします。

	コマンドまたはアクション	目的
ステップ 14	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config)# exit	前のモードに戻ります。
ステップ 15	<code>keepalive disable</code> 例： RP/0/RSP0/CPU0:router(config)# keepalive disable	このインターフェイスのキープアライブ タイマーをディセーブルにします。
ステップ 16	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config-if)# exit	前のモードに戻ります。
ステップ 17	<code>interface serial</code> <code>interface-path-id[.subinterface]</code> 例： RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/0/1/2:0	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータ構文の詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
ステップ 18	<code>ssrp group group-number id id-number ppp</code> 例： RP/0/RSP0/CPU0:router(config-if)# ssrp group 1 id 2 ppp	SSRP グループをインターフェイス上でアタッチします。
ステップ 19	<code>encapsulation ppp</code> 例： RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp	ポイントツーポイント プロトコル (PPP) を使用してルータと通信するためのカプセル化をイネーブルにします。
ステップ 20	<code>multilink</code> 例： RP/0/RSP0/CPU0:router(config-if)# multilink	マルチリンク 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 21	<code>group group-id</code> 例： RP/0/RSP0/CPU0:router(config-if)# group 1	セッション状態冗長プロトコル (SSRP) グループをこのインターフェイスにアタッチします。
ステップ 22	<code>exit</code> 例： RP/0/RSP0/CPU0:router(config-if)# exit	前のモードに戻ります。

■ PPP の設定方法

	コマンドまたはアクション	目的
ステップ 23	<pre>keepalive disable</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# keepalive disable</pre>	このインターフェイスのキープアライブ タイマーをディセーブルにします。
ステップ 24	<pre>exit</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# exit</pre>	前のモードに戻ります。
ステップ 25	<pre>interface multilink interface-path-id</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config)# interface Multilink 0/1/0/0/1</pre>	<p>物理インターフェイスまたは仮想インターフェイス。</p> <p>(注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、show interfaces コマンドを使用します。</p> <p>ルータ構文の詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。</p>
ステップ 26	<pre>ipv4 address ipv4-address mask</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.10.10.10 255.255.255.0</pre>	インターフェイスのプライマリ IPv4 アドレスとサブネット マスクを設定します。
ステップ 27	<pre>ssrp group group-number id id-number ppp</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# ssrp group 1 id 3 ppp</pre>	SSRP グループをインターフェイス上でアタッチします。
ステップ 28	<pre>encapsulation ppp</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp</pre>	ポイントツーポイント プロトコル (PPP) を使用してルータと通信するためのカプセル化をイネーブルにします。
ステップ 29	<pre>shutdown</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# shutdown</pre>	インターフェイスを設定のために管理上のダウン状態にします。
ステップ 30	<pre>keepalive disable</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# keepalive disable</pre>	このインターフェイスのキープアライブ タイマーをディセーブルにします。
ステップ 31	<pre>exit</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# exit</pre>	前のモードに戻ります。

	コマンドまたはアクション	目的
ステップ 32	controller <i>MgmtMultilink</i> <i>interface-path-id</i> 例： RP/0/RSP0/CPU0:router(config)# controller MgmtMultilink 0/1/0/0	汎用マルチリンク バンドルのコントローラを設定し、MgmtMultilink コンフィギュレーション モードを開始します。
ステップ 33	bundle <i>bundleID</i> 例： RP/0/RSP0/CPU0:router(config-mgmtmultilink)# bundle 1	マルチリンク インターフェイス バンドルを作成します。
ステップ 34	bundle <i>bundleID</i> 例： RP/0/RSP0/CPU0:router(config-mgmtmultilink)# bundle 2	マルチリンク インターフェイス バンドルを作成します。
ステップ 35	commit 例： RP/0/RSP0/CPU0:router(config-mgmtmultilink)# commit	現在の設定を保存します。

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.669)
- 「[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.670)
- 「[PPP および MLPPP の ICSSO の設定：例](#)」 (P.670)
- 「[マルチリンク PPP 設定の確認](#)」 (P.678)

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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# no shutdown
RP/0/RSP0/CPU0:router(config-if)# ppp pap sent-username Pl_TEST-8 password xxxx
RP/0/RSP0/CPU0:router(config-if)# ppp authentication chap pap MIS-access
RP/0/RSP0/CPU0:router(config-if)# ppp chap password encrypted xxxx
RP/0/RSP0/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/RSP0/CPU0:router# configure
```

■ PPP および MLPPP の ICSSO の設定 : 例

```
RP/0/RSP0/CPU0:router(config)# interface POS 0/3/0/1
RP/0/RSP0/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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface serial 0/3/0/0:0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.18.189.38 255.255.255.224
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# no shutdown
RP/0/RSP0/CPU0:router(config-if)# ppp authentication ms-chap MIS-access
RP/0/RSP0/CPU0:router(config-if)# ppp ms-chap password encrypted xxxx
RP/0/RSP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them? [yes]: yes
```

MLPPP の設定 : 例

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# controller t3 0/1/0/0/1
RP/0/RSP0/CPU0:router# mode t1
RP/0/RSP0/CPU0:router(config-t3)# clock source internal
RP/0/RSP0/CPU0:router(config-t3)# exit
RP/0/RSP0/CPU0:router(config)# controller t1 0/1/0/0/1/1
RP/0/RSP0/CPU0:router(config-t1)# channel-group 0
RP/0/RSP0/CPU0:router(config-t1-channel_group)# timeslots 1-24
RP/0/RSP0/CPU0:router(config-t1-channel_group)# exit
RP/0/RSP0/CPU0:router(config-t1)# exit
RP/0/RSP0/CPU0:router(config)# controller mgmtmultilink 0/1/0/0
RP/0/RSP0/CPU0:router(config-mgmtmultilink)# bundle 20
RP/0/RSP0/CPU0:router(config-t3)# commit
RP/0/RSP0/CPU0:router(config-t3)# exit

RP/0/RSP0/CPU0:router(config)# interface multilink 0/1/0/0/20
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 80.170.0.1/24
RP/0/RSP0/CPU0:router(config-if)# multilink fragment-size 128
RP/0/RSP0/CPU0:router(config-if)# keepalive disable
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# interface serial 0/1/0/0/1/1:0
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
RP/0/RSP0/CPU0:router(config-if)# multilink group 20
RP/0/RSP0/CPU0:router(config-t3)# commit
RP/0/RSP0/CPU0:router(config-t3)# exit

RP/0/RSP0/CPU0:router(config)# interface multilink 0/1/0/0/1
RP/0/RSP0/CPU0:router(config-if)# multilink
RP/0/RSP0/CPU0:router(config-if-multilink)# ppp multilink minimum-active links 10
RP/0/RSP0/CPU0:router(config-if-multilink)# multilink interleave
RP/0/RSP0/CPU0:router(config-if-multilink)# no shutdown
RP/0/RSP0/CPU0:router(config-t3)# commit
```

PPP および MLPPP の ICSSO の設定 : 例

ここでは ICSSO 設定および関連の設定に関する次の例を示します。

- 「ICSSO の設定 : 例」 (P.672)

- 「ICSSO とともに使用するためのチャネライズド SONET コントローラの設定 : 例」 (P.672)
- 「MR-APS の設定 : 例」 (P.672)
- 「シリアルおよびマルチリンク インターフェイスの SSRP の設定 : 例」 (P.673)
- 「ICSSO で使用するマルチリンクの VRF の設定 : 例」 (P.674)
- 「ICSSO で使用するためのイーサネットの VRF の設定 : 例」 (P.675)
- 「ICSSO で使用する OSPF の設定 : 例」 (P.675)
- 「ICSSO 設定の確認 : 例」 (P.675)

ICSSO の設定 : 例

次に、SONET コントローラで ICSSO を設定する例を示します。

```
config
  redundancy
    multi-router aps
    group 1
    controller sonet 0/1/0/0
      member ipv4 10.10.10.10 backup-interface GigabitEthernet 0/6/0/1
    commit
show running config
```

ICSSO とともに使用するためのチャネライズド SONET コントローラの設定 : 例

次の例では、ICSSO とともに使用するためのチャネライズド SONET コントローラの設定方法を示します。

```
config
  controller SONET0/7/1/0
    framing sonet
    sts 1
    mode t3
  !
    sts 2
    mode t3
  !
    sts 3
    mode t3
  !
  controller T3 0/7/0/1
    mode t1
    framing auto-detect
  !
  controller T1 0/7/0/1/1
    channel-group 0
    timeslots 1-24
```

MR-APS の設定 : 例

次に、MR-APS の設定例を示します。

```
config
  aps group 1
    channel 0 remote 99.10.1.2
    channel 1 local SONET0/1/0/0
  !
  aps rprplus
  !
  interface GigabitEthernet0/6/0/0
    description MR-APS PGP interface for aps group 1
    ipv4 address 99.10.1.1 255.255.255.0
```

次に、冗長グループ マネージャを設定する例を示します。

```
// mr-aps part:
aps group 1
  channel 0 remote 99.10.1.2
```



```

channel 1 local SONET0/1/0/0
!
// ssrp part:
ssrp location 0/1/CPU0
group 1 profile TEST
!
ssrp profile TEST
peer ipv4 address 99.10.1.2
!
// redundancy group manager part:
redundancy
multi-router aps
group 1
controller SONET0/1/0/0
member ipv4 99.30.1.2 backup-interface GigabitEthernet0/6/0/4
!

// ospf part:
router ospf 1
nsr
nsf ietf
redistribute connected instance IPCP
redistribute static
area 0
interface GigabitEthernet0/6/0/4
!
!
!

show redundancy-group multi-router aps

```

シリアルおよびマルチリンク インターフェイスの SSRP の設定 : 例

次の例では、SSRP をシリアルインターフェイス（PPP カプセル化あり）とマルチリンク インターフェイスで設定する方法を示します。

```

config
  ssrp profile TEST
    peer ipv4 address 99.10.1.2
  !
  ssrp location 0/1/CPU0
    group 1 profile TEST
  !
  interface Serial0/1/0/0/1/1:0
    ssrp group 1 id 1 ppp
    encapsulation ppp
    multilink
    group 1
  !
  keepalive disable
  !
  interface Serial0/1/0/0/1/2:0
    ssrp group 1 id 2 ppp
    encapsulation ppp
    multilink
    group 1
  !
  keepalive disable
  !
  interface Multilink0/1/0/0/1

```

```

    ipv4 address 51.1.1.1 255.255.255.0
    srrp group 1 id 3 ppp
    encapsulation ppp
    shutdown
!
keepalive disable
!
    controller MgmtMultilink0/1/0/0
    bundle 1

```



(注) シリアル インターフェイスの設定の詳細については、このマニュアルの『[Cisco ASR 9000 シリーズ ルータでのシリアル 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。



(注) マルチリンクの設定の詳細については、『[マルチリンク PPP の設定](#)』(P.652) を参照してください。

ICSSO で使用するマルチリンクの VRF の設定 : 例

次に、ICSSO で使用するためのマルチリンク インターフェイスの VPN ルーティングおよび転送 (VRF) を設定する例を示します。

```

config
  vrf EvDO-vrf
    address-family ipv4 unicast
!
  interface Multilink 0/0/0/0/1
    description To EvDO BTS Number 1
    vrf EvDO-vrf
    ipv4 address 150.0.1.3 255.255.255.0
    encapsulation ppp
!

```



(注) VRF の設定に関する詳細については、『[Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide](#)』を参照してください。マルチリンクの設定の詳細については、『[マルチリンク PPP の設定](#)』(P.652) を参照してください。

ICSSO で使用するためのイーサネットの VRF の設定 : 例

次に、ICSSO で使用するためのイーサネット インターフェイスの VPN ルーティングおよび転送 (VRF) を設定する例を示します。

```
config
  vrf EvDO-vrf
    address-family ipv4 unicast
  !
  interface GigabitEthernet 1/0/0/0.20
    description Inter-ASR9000 EvDO VLAN
    vrf EvDO-vrf
    encapsulation dot1q 20
```



(注) VRF の設定に関する詳細については、『Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide』を参照してください。イーサネットの設定の詳細については、このマニュアルの「Cisco ASR 9000 シリーズ ルータのイーサネット OAM の設定」モジュールを参照してください。

ICSSO で使用する OSPF の設定 : 例

一連のセル サイトで PPP セッションが終端する集約ルータは、Open Shortest Path First (OSPF) を使用して LAN スイッチに自身のアベイラビリティをアドバタイズします。次に、ICSSO で使用するために OSPF を設定する例を示します。

```
config
  router ospf 1
    nsr
    nsf ietf
    redistribute connected instance IPCP
    redistribute static
    area 0
  interface GigabitEthernet 0/6/0/1
  !
```



(注) OSPF の設定方法の詳細については、『Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide』を参照してください。

ICSSO 設定の確認 : 例

次に、ICSSO 設定を確認する例を示します。

- 「SSRP グループの確認 : 例」 (P.675)
- 「ICSSO ステータスの確認 : 例」 (P.676)
- 「MR-APS 設定の確認 : 例」 (P.676)
- 「OSPF 設定の確認 : 例」 (P.677)

SSRP グループの確認 : 例

次の例では、SSRP グループ設定を確認する方法を示します。

```
RP/0/RSP0/CPU0:Router# show ssrp groups all det loc 0/1/cpu0
```

■ PPP および MLPPP の ICSSO の設定 : 例

```

Tue Nov 10 16:57:55.911 UTC

Group ID: 1
Conn (ACT,SB): UP,UP
Profile: TEST
Peer: 99.10.1.2
Max-hops: 255
Sessions: 3
Channels Created
Client: PPP
  Active Init: TRUE
  Standby Init: TRUE
  Active State: IDT-End-Sent
  Standby State: IDT-End-Received
  Auth-Req Pending: FALSE
  Active ID Out: 93
  Active ID In: 93
  Active Last Reply In: 93
  Active Counter: 5

  Standby ID Out: 50
  Standby ID In: 50
  Standby Last Reply In: 50
  Standby Counter: 5

Session Interface
-----
1 Se0/1/0/0/1/1:0
2 Se0/1/0/0/1/2:0
3 Mu0/1/0/0/1

```

ICSSO ステータスの確認 : 例

次に、ICSSO ステータスを確認する例を示します。

```

RP/0/RSP0/CPU0:Router# show ppp sso sum loc 0/1/cpu0
Tue Nov 10 16:59:00.253 UTC

```

```

Not-Ready      : The session is not yet ready to run as Active or Standby
Stby-UnNegd    : In Standby mode, no replication state received yet
Act-Down       : In Active mode, lower layer not yet up
Deactivating   : Session was Active, now going Standby
Act-UnNegd     : In Active mode, not fully negotiated yet
Stby-Negd      : In Standby mode, replication state received and pre-programmed
Activating     : Session was Standby and pre-programmed, now going Active
Act-Negd       : In Active mode, fully negotiated and up
-              : This layer not running

```

Layer	Total	Not-Ready	Stby-UnNegd	Act-Down	Deactivating	Act-UnNegd	Stby-Negd	Activating	Act-Negd
LCP	6	0	0	0	0	0	0	0	6
of-us-auth	6	0	0	0	0	0	0	0	6
of-peer-auth	6	0	0	0	0	0	0	0	6
IPCP	2	0	0	0	0	0	0	0	2

MR-APS 設定の確認 : 例

次に、MR-APS の設定を確認する例を示します。

例 1 :

```
RP/0/RSP0/CPU0:Router# show redundancy-group multi-router aps all

Tue Nov 10 17:00:14.018 UTC

Interchassis Group: 1
    State: FRR ADD SENT
    Controller: SONET0/1/0/0                                0x2000080
    Backup Interface: GigabitEthernet0/6/0/1                0x10000180
    Next Hop IP Addr: 10.10.10.10

Interchassis Group: Not Configured
    State: WAIT CONFIG
    Controller: SONET0/1/0/1                                0x20003c0
    Backup Interface: None                                   0x0
    Next Hop IP Addr: 0.0.0.0
```

例 2 :

```
RP/0/RSP0/CPU0:Router# show cef adj rem loc 0/6/cpu0

Tue Nov 10 17:00:30.471 UTC
Display protocol is ipv4
Interface      Address                                     Type      Refcount

S00/1/0/0     Ifhandle: 0x2000080                        remote    2
Adjacency: PT:0xa47c9cf4
Interface: S00/1/0/0
Interface Type: 0x0, Base Flags: 0x110000 (0xa4a00494)
Nhinfo PT: 0xa4a00494, IdB PT: 0xa4cd60d8, If Handle: 0x2000080
Ancestor If Handle: 0x0

Protect FRR: 0xa4a8a040
Backup FRR: 0xa4a89f34
Backup NH: 0xa4a00a74
Backup IFH: 0x10000180
Backup Interface: Gi0/6/0/1
Backup IP: 10.10.10.10

FRR Active: 0
```

OSPF 設定の確認 : 例

次に、OSPF の設定を確認する例を示します。

例 1 :

```
RP/0/RSP0/CPU0:Router# show route back
Tue Nov 10 17:01:48.974 UTC

Codes: C - connected, S - static, R - RIP, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
        U - per-user static route, o - ODR, L - local, G - DAGR
        A - access/subscriber

C      51.1.1.2/32 is directly connected, 00:10:03, Multilink0/1/0/0/1
        Backup O E2 [110/20] via 10.10.10.10, GigabitEthernet0/6/0/1
```

■ PPP および MLPPP の ICSSO の設定 : 例

```

C   52.1.1.2/32 is directly connected, 00:11:47, Multilink0/1/0/0/2
      Backup  O E2 [110/20] via 10.10.10.10, GigabitEthernet0/6/0/1
S   110.0.0.2/32 [1/0] via 51.1.1.2, 00:11:40
      Backup  O E2 [110/20] via 10.10.10.10, GigabitEthernet0/6/0/1

```

例 2 :

```

RP/0/RSP0/CPU0:Router# show route 51.1.1.2
Tue Nov 10 17:02:26.507 UTC

```

```

Routing entry for 51.1.1.2/32
  Known via "connected IPCP", distance 0, metric 0 (connected)
  Installed Nov 10 16:51:45.703 for 00:10:40
  Routing Descriptor Blocks
    51.1.1.2 directly connected, via Multilink0/1/0/0/1
      Route metric is 0
  No advertising protos.

```

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.678)
- 「[show ppp interfaces multilink : 例](#)」 (P.681)
- 「[show ppp interface serial : 例](#)」 (P.681)
- 「[show imds interface multilink : 例](#)」 (P.681)

show multilink interfaces : 例

```

RP/0/RSP0/CPU0:Router# show multilink interfaces Serial 0/4/3/1/10:0
Mon Sep 21 09:24:19.604 UTC

```

```

Serial0/4/3/1/10:0 is up, line protocol is up
  Encapsulation: PPP
  Multilink group id: 6
  Member status: ACTIVE

```

```

RP/0/RSP0/CPU0:Router# show multilink interfaces Multilink 0/4/3/0/3
Mon Sep 21 09:17:12.131 UTC

```

```

Multilink0/4/3/0/3 is up, line protocol is up
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: PPP
  Member Links: 1 active, 1 inactive
    - Serial0/4/3/1/5:0 is up, line protocol is up
      Encapsulation: PPP
      Multilink group id: 3
      Member status: ACTIVE

    - Serial0/4/3/1/6:0 is administratively down, line protocol is administratively down
  Encapsulation: PPP
  Multilink group id: 3
  Member status: INACTIVE : LCP has not been negotiated

```

```

Fragmentation Statistics

```

```
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0          Output Fragmented bytes 0
Input Unfragmented packets 0         Input Unfragmented bytes 0
Output Unfragmented packets 0        Output Unfragmented bytes 0
Input Reassembled packets 0          Input Reassembled bytes 0
```

```
RP/0/5/CPU0:Mav-IOX-Rahul#sho multilink interfaces Serial 0/4/3/1/10:0
Mon Sep 21 09:24:19.604 UTC
```

```
Serial0/4/3/1/10:0 is up, line protocol is up
  Encapsulation: PPP
  Multilink group id: 6
  Member status: ACTIVE
```

```
RP/0/RSP0/CPU0:Router# show multilink interfaces
Mon Sep 21 09:15:10.679 UTC
```

```
Multilink0/4/3/0/1 is up, line protocol is up
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: FR
  Member Links: 1 active, 1 inactive
    - Serial0/4/3/1/2:0: INACTIVE : Down (Member link idle)
    - Serial0/4/3/1/1:0: ACTIVE : Up
```

```
Multilink0/4/3/0/10 is up, line protocol is down
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: PPP
  Member Links: 0 active, 0 inactive
  Fragmentation Statistics
    Input Fragmented packets 0          Input Fragmented bytes 0
    Output Fragmented packets 0          Output Fragmented bytes 0
    Input Unfragmented packets 0         Input Unfragmented bytes 0
    Output Unfragmented packets 0        Output Unfragmented bytes 0
    Input Reassembled packets 0          Input Reassembled bytes 0
```

```
Multilink0/4/3/0/100 is administratively down, line protocol is administratively down
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: PPP
  Member Links: 0 active, 0 inactive
  Fragmentation Statistics
    Input Fragmented packets 0          Input Fragmented bytes 0
    Output Fragmented packets 0          Output Fragmented bytes 0
    Input Unfragmented packets 0         Input Unfragmented bytes 0
    Output Unfragmented packets 0        Output Unfragmented bytes 0
    Input Reassembled packets 0          Input Reassembled bytes 0
```

```
Multilink0/4/3/0/2 is up, line protocol is up
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: FR
  Member Links: 2 active, 0 inactive
    - Serial0/4/3/1/4:0: ACTIVE : Up
    - Serial0/4/3/1/3:0: ACTIVE : Up
```

```
Multilink0/4/3/0/3 is up, line protocol is up
  Fragmentation: disabled
  Interleave: disabled
  Encapsulation: PPP
  Member Links: 1 active, 1 inactive
```

PPP および MLPPP の ICSSO の設定 : 例

```

- Serial0/4/3/1/5:0: ACTIVE
- Serial0/4/3/1/6:0: INACTIVE : LCP has not been negotiated
Fragmentation Statistics
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0        Output Fragmented bytes 0
Input Unfragmented packets 0       Input Unfragmented bytes 0
Output Unfragmented packets 0      Output Unfragmented bytes 0
Input Reassembled packets 0        Input Reassembled bytes 0

Multilink0/4/3/0/4 is up, line protocol is up
Fragmentation: disabled
Interleave: disabled
Encapsulation: PPP
Member Links: 2 active, 0 inactive
- Serial0/4/3/1/8:0: ACTIVE
- Serial0/4/3/1/7:0: ACTIVE
Fragmentation Statistics
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0        Output Fragmented bytes 0
Input Unfragmented packets 0       Input Unfragmented bytes 0
Output Unfragmented packets 0      Output Unfragmented bytes 0
Input Reassembled packets 0        Input Reassembled bytes 0

Multilink0/4/3/0/5 is up, line protocol is up
Fragmentation: disabled
Interleave: enabled
Encapsulation: PPP
Member Links: 1 active, 0 inactive
- Serial0/4/3/1/9:0: ACTIVE
Fragmentation Statistics
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0        Output Fragmented bytes 0
Input Unfragmented packets 0       Input Unfragmented bytes 0
Output Unfragmented packets 0      Output Unfragmented bytes 0
Input Reassembled packets 0        Input Reassembled bytes 0

Multilink0/4/3/0/6 is up, line protocol is up
Fragmentation: disabled
Interleave: enabled
Encapsulation: PPP
Member Links: 1 active, 0 inactive
- Serial0/4/3/1/10:0: ACTIVE
Fragmentation Statistics
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0        Output Fragmented bytes 0
Input Unfragmented packets 0       Input Unfragmented bytes 0
Output Unfragmented packets 0      Output Unfragmented bytes 0
Input Reassembled packets 0        Input Reassembled bytes 0

Multilink0/4/3/0/7 is up, line protocol is down
Fragmentation: disabled
Interleave: enabled
Encapsulation: PPP
Member Links: 0 active, 1 inactive
- Serial0/4/3/1/11:0: INACTIVE : LCP has not been negotiated
Fragmentation Statistics
Input Fragmented packets 0          Input Fragmented bytes 0
Output Fragmented packets 0        Output Fragmented bytes 0
Input Unfragmented packets 0       Input Unfragmented bytes 0
Output Unfragmented packets 0      Output Unfragmented bytes 0
Input Reassembled packets 0        Input Reassembled bytes 0

Multilink0/4/3/0/8 is up, line protocol is down
Fragmentation: disabled

```



```

Interleave: enabled
Encapsulation: PPP
Member Links: 0 active, 1 inactive
  - Serial0/4/3/1/12:0: INACTIVE : LCP has not been negotiated
Fragmentation Statistics
Input Fragmented packets 0           Input Fragmented bytes 0
Output Fragmented packets 0         Output Fragmented bytes 0
Input Unfragmented packets 0        Input Unfragmented bytes 0
Output Unfragmented packets 0       Output Unfragmented bytes 0
Input Reassembled packets 0         Input Reassembled bytes 0

```

show ppp interfaces multilink : 例

```

RP/0/RSP0/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/RSP0/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/RSP0/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

```

■ その他の関連資料

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

その他の関連資料

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

関連項目	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』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された 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、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

