PPP セッションのための ISG アクセスの設定

Intelligent Services Gateway（ISG）は、エッジ デバイスが柔軟で拡張性の高いサービスを加入者に提供できる、構造化フレームワークを提供する Cisco IOS ソフトウェアの機能セットです。このマニュアルでは、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）加入者のための ISG アクセスを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「PPP セッションのための ISG アクセスの機能情報」（P.65）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

PPP セッションのための ISG アクセスに関する前提条件

リリースおよびプラットフォーム サポートの詳細については、「PPP セッションのための ISG アクセスの機能情報」（P.65）を参照してください。

使用されるアクセス プロトコルは、インターフェイス上にプロビジョニングされている必要があります。

ローカル PPP 認証が必要な場合は、インターフェイスまたは仮想テンプレートで **ppp authentication** コマンドを設定する必要があります。

このマニュアル内の作業と例は、ISG 制御ポリシーの設定方法および使用方法に関する知識があることを前提としています。制御ポリシーの設定方法の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。

PPP セッションのための ISG アクセスに関する制約事項

Cisco 10000 シリーズ ルータ上の PPPoX セッションでは、Modular Quality of Service（QoS）Command Line Interface（MQC）ポリシーと ISG ポリシーを、同時に設定できません。たとえば、MQC ポリシーと ISG ポリシーは、PPPoX セッションの仮想テンプレート インターフェイスに適用できません（静的にも RADIUS からも）。

PPP セッションのための ISG アクセスの設定に関する情報

PPP セッションのためのアクセスを設定する前に、次の概念について理解しておく必要があります。

- 「PPP セッションのための ISG アクセスの概要」（P.54）
- 「PPP セッションのための ISG 加入者 IP アドレス管理」（P.55）
- 「PPP セッションのための ISG アクセスに対するデフォルト ポリシー」（P.55）
- 「PPP セッションのための ISG 制御ポリシーを使用する利点」（P.56）

PPP セッションのための ISG アクセスの概要

レイヤ 2 セッションは、ピア エンティティと ISG デバイスとの間で動作する制御プロトコルによって確立されます。通常、レイヤ 2 セッションは、同じ物理メディア上の他のセッションから隔離するためにカプセル化されます。

システムは、レイヤ 2 セッションにデフォルト処理を提供しますが、プロトコルを転送またはローカルで終端するためのポリシー、またはアクセス プロトコルから収集された ID データに基づいて、ローカルで加入者を認証するためのポリシーの設定が必要な場合があります。ISG 制御ポリシーは、アクセス プロトコルから、ピア エンティティの ID および資格情報を抽出するように設定できます。このメカニズムでは、プロトコルによって明示的に提供される ID、あるいは基盤となるメディアまたはアクセス ポートのネイティブな ID のいずれかの、セッションに関連する ID に基づいてレイヤ 2 セッションのサービスをプロビジョニングできます。

ISG は、次のレイヤ 2 アクセス プロトコルをサポートします。

- PPP
- PPP over Ethernet（PPPoE）
- PPP over ATM（PPPoA）

- Layer 2 Tunnel Protocol（L2TP）
- Layer 2 Forwarding（L2F）プロトコル

PPP セッションのための ISG 加入者 IP アドレス管理

ISG 加入者 IP アドレス管理は、ローカルで終端される IP セッションまたはレイヤ 2（PPP）セッションに適用されます。

加入者は、特定の IP サービス ドメイン内でルーティングを受けるためには、ドメイン固有の IP アドレスをネットワークに知らせる必要があります。加入者が IP サービス ドメイン（アクセス プロバイダーによって管理される任意のプライベート ドメインを含む）間を移動する場合は、ネットワークに知らせる IP アドレスを、新しいドメインを反映して変更する必要があります。ローカルで終端される PPP セッションについては、ISG は、次の IP アドレスの割り当て方法をサポートします。

- ユーザ プロファイル内の IP アドレス
- ユーザ プロファイル内の IP サブネット
- ユーザ プロファイル内の名前付きアドレス プール
- ローカル アドレス プール
- PPP のための IP アドレス管理の標準的方法（PPP セッションのための IP アドレス管理サポートの詳細は『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.2』を参照）

ローカルで終端された PPP セッションが、ある Virtual Routing and Forwarding（VRF）インスタンスから別の VRF に転送される場合、IPCP を使用して、ピア IP アドレスが再ネゴシエーションされます。

PPP セッションの VRF 転送

VRF 転送では、新しいプライマリ サービスの選択に従って、ISG 加入者セッションをある VRF から別の VRF に移動できます。Network Access Point（NAP; ネットワーク アクセス ポイント）からの IP アドレスで PPP セッションが確立されると、加入者は Web ポータルへのアクセス、およびサービス プロバイダーの選択が可能になります。PPP セッションの VRF 転送では、ISG は、IP アドレスを新しいドメインから PPP セッションに再度割り当てる必要があります。PPP セッションでは、IP Control Protocol（IPCP）再ネゴシエーションによって、IP アドレスが再度割り当てられます。

PPP 再ネゴシエーションなしでは、PPP セッションの VRF 転送はサポートされません。

PPP セッションのための ISG アクセスに対するデフォルト ポリシー

ISG は、制御ポリシーが設定されいない場合のレイヤ 2 セッションのデフォルト処理を提供します。**vpdn enable** コマンドが設定されている場合で、ユーザ名にドメイン名が指定されている（たとえば、user@domain）か、または Dialed Number Identification Service（DNIS; 着信番号識別サービス）番号が提供されている場合、システムはこの情報に基づいて認可を行います。Virtual Private Dialup Network（VPDN）トンネル情報が検出されると、セッションは L2TP Network Server（LNS; L2TP ネットワーク サーバ）での処理のために転送されます。リモート LNS で認証が要求されている場合、**ppp authentication** コマンドを PPP インターフェイスまたは仮想テンプレートで設定する必要があります。**vpdn authen-before-forward** コマンドが設定されている場合、PPP セッションを LNS に転送する前に、PPP セッションの認証がローカルで試行されます。

ドメイン名または DNIS のトンネル情報が検出されていない場合、または **vpdn enable** コマンドが設定されていない場合は、Stack Group Bidding Protocol（SGBP）認可が試行されます（SGBP が設定されている場合）。SGBP を使用して認可情報を取得できない場合、PPP セッションはローカルで終端され

ます。ローカル終端は、ピアと ISG デバイスの間で PPP セッションが確立され、IP ペイロードがルーティングされることを意味しています。後者の場合、**ppp authentication** コマンドが PPP インターフェイスまたは仮想テンプレートで設定されている場合のみ、認証が行われます。

セッション開始イベントに ISG 制御ポリシーが定義されている場合、デフォルト処理ではなく、そのポリシーが優先されます。

PPP セッションのための ISG 制御ポリシーを使用する利点

ISG は、アクセス プロトコルを介してピア エンティティからの ID 情報と資格情報の抽出を制御することによって、レイヤ 2 セッションのサービス決定に柔軟なアプローチを提供します。たとえば、コール要求が着信する ATM Permanent Virtual Circuit（PVC; 相手先固定接続）に基づいてサービスが決定される場合、セッションの確立およびサービスの提供の前に、制御プロトコルの実行が完了している必要はありません。この方法では、ローカル リソースを節約し、コール セットアップ時間を改善できます。

制御ポリシーを使用した PPP セッションのための ISG アクセスの設定方法

ISG レイヤ 2 アクセスを設定するには、次の手順を実行します。

1. 加入者 ID が、レイヤ 2 セッション処理にどのように影響するかを決定します。具体的には、プロトコルを転送するのか。ローカルで終端するのか、および加入者をローカルで認証するかどうかを決定します。
2. レイヤ 2 セッション処理を提供するため、制御ポリシーを設定します。制御ポリシーの設定方法の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。レイヤ 2 アクセスの制御ポリシーの例については、「PPP セッションのための ISG アクセスの設定例」（P.61）を参照してください。
3. PPP セッションの ISG VRF 転送をイネーブルにします。
4. 必要に応じて、設定の確認とトラブルシューティングを行います。

ここでは、次の作業について説明します。

- 「PPP セッションのための ISG VRF 転送のイネーブル化」（P.56）
- 「PPP セッションのための ISG アクセスのトラブルシューティング」（P.59）

PPP セッションのための ISG VRF 転送のイネーブル化

VRF 転送では、新しいプライマリ サービスの選択に従って、ISG 加入者セッションをある VRF から別の VRF に移動できます。この手順は、次のセクションから構成されます。

- 「前提条件」（P.57）
- 「サービス ポリシー マップでの VRF の指定」（P.57）
- 「PPP セッションの VRF 転送の確認」

前提条件

この手順は、仮想テンプレートおよび IP アドレスの割り当て方法を設定することによって、PPP セッションのサポートが設定されていることを前提としています。VRF 転送が機能するためには、元の VRF、ループバック インターフェイス、および IP アドレス プールを、ユーザ プロファイルではなく、仮想テンプレートで指定する必要があることに注意してください。仮想テンプレートおよび PPP セッションのサポートの設定方法については、『*Cisco IOS Dial Technologies Configuration Guide*』を参照してください。

サービス ポリシー マップでの VRF の指定

VRF 転送は、新しいプライマリ サービスがセッションに対してアクティブな場合に発生し、セッションが 1 つの VRF から別の VRF に転送されます。サービスは、外部 Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ上のサービス プロファイル内、または ISG デバイス上のサービス ポリシー マップに設定できます。ISG デバイス上のサービス ポリシー マップに VRF を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**policy-map type service** *policy-map-name* 例： `Router(config)# policy-map type service service1`	ISG サービスの定義に使用されるサービス ポリシー マップを作成または変更し、サービス ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**ip vrf forwarding** *name-of-vrf* 例： `Router(config-service-policymap)# ip vrf forwarding blue`	サービスを VRF に関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**sg-service-type primary** 例： `Router(config-service-policymap)# sg-service-type primary`	サービスをプライマリ サービスとして定義します。 • プライマリ サービスは、ネットワーク転送ポリシーが含まれるサービスです。プライマリ サービスは、**sg-service-type primary** コマンドを使用してプライマリ サービスとして定義する必要があります。プライマリ サービスではないサービスは、デフォルトではセカンダリ サービスとして定義されます。
ステップ 6	**sg-service-group** *service-group-name* 例： `Router(config-service-policymap)# sg-service-group group1`	（任意）ISG サービスをサービス グループに関連付けます。 • サービス グループとは、特定のセッションに対して同時にアクティブにできるサービスをグループ化したものです。一般的なサービス グループには、1 つのプライマリ サービスと 1 つ以上のセカンダリ サービスが含まれます。

PPP セッションの VRF 転送の確認

PPP セッションの VRF 転送を確認するには、次の作業を実行します。**show** のすべての手順はオプションで、任意の順序で実行できます。

手順の概要

1. **enable**
2. **show subscriber session all**
3. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
4. **show ip route** [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show subscriber session all** 例： `Router# show subscriber session all`	加入者が選択したサービスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} 例： `Router# show idmgr session key session-handle 48000002`	ISG セッションおよびサービス ID に関する情報を表示します。
ステップ 4	**show ip route** [**vrf** *vrf-name*] 例： `Router# show ip route`	ルーティング テーブルの現在のステータスを表示します。

PPP セッションのための ISG アクセスのトラブルシューティング

この作業のコマンドを使用すると、レイヤ 2 セッションのモニタとトラブルシューティングを行えます。これらのコマンドはすべてオプションで、特定の順序で入力する必要はありません。

手順の概要

1. **enable**
2. **show subscriber session detailed**
3. **debug condition**
4. **debug subscriber packet** [**event** | **full** | **detail**]
5. **debug subscriber error**
6. **debug subscriber event**
7. **debug subscriber fsm**
8. **debug pppatm** {**event** | **error** | **state**} [**interface atm** *interface-number*[**.***subinterface-number*]] **vc** {[*vpi*/*vci*]*vci* | *virtual-circuit-name*}
9. **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show subscriber session detailed** 例： `Router# show subscriber session detailed`	ISG 加入者セッションに関する情報を表示します。
ステップ 3	**debug condition** *condition* 例： `Router# debug condition username user5@example.com`	指定された条件に基づいて、デバッグ出力をフィルタリングします。 **（注）** 条件付きデバッグの詳細については、「Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging」モジュールを参照してください。
ステップ 4	**debug subscriber packet** [**event** | **full** | **detail**] 例： `Router# debug subscriber packet event`	Subscriber Service Switch（SSS）コールのセットアップ中のパケットに関する診断情報を表示します。
ステップ 5	**debug subscriber error** 例： `Router# debug subscriber error`	SSS コールのセットアップ中に発生する可能性のあるエラーに関する診断情報を表示します。
ステップ 6	**debug subscriber event** 例： `Router# debug subscriber event`	SSS コールのセットアップ イベントに関する診断情報を表示します。
ステップ 7	**debug subscriber fsm** 例： `Router# debug subscriber fsm`	SSS コール セットアップ状態に関する診断情報を表示します。
ステップ 8	**debug pppatm** {**event** | **error** | **state**} [**interface atm** *interface-number*[*.subinterface-number*]] **vc** {[*vpi*/*vci*]*vci* | *virtual-circuit-name*} 例： `Router# debug pppatm error`	インターフェイス上または Virtual Circuit（VC; 仮想回線）上での PPP over ATM（PPPoA）イベント、エラー、および状態に関する診断情報を、グローバルまたは条件付きで表示します。
ステップ 9	**debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**} 例： `Router# debug ppp packet`	PPP を実装しているインターネットワーク内での、トラフィックおよび対話に関する情報を表示します。

例

次の例では、ユーザ名「cpe6_1@example.com」に基づいて、**debug subscriber packet detail** コマンドの出力がフィルタリングされます。

```
Router# debug condition username cpe6_1@example.com
Condition 1 set

Router# show debug
Condition 1: username cpe6_1@example.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on

Router# show debug
SSS:
  SSS packet detail debugging is on
Condition 1: username cpe6_1@example.com (0 flags triggered)

Router#
```

PPP セッションのための ISG アクセスの設定例

ここでは、次の例について説明します。

- 「PPP セッションのための ISG アクセスの設定：例」（P.61）
- 「再ネゴシエーションを使用した PPP セッションの VRF 転送：例」（P.63）

PPP セッションのための ISG アクセスの設定：例

次に、PPP 加入者にサービスを提供する ISG ポリシーの設定例を示します。この例では、次のアクションを実行するための ISG を設定します。

- ATM Virtual Path Identifier/Virtual Channel Identifier（VPI/VCI; 仮想パス ID/ 仮想チャンネル ID）に基づく PPP 転送

  ISG は、VPI が 200 未満および VCI が 100 未満のすべての加入者に対して、転送サービス「xconnect」をアクティブにします。このポリシー ルールにより、ISG は PPP プロトコル全体を実行することなく、関連付けられた加入者にサービスを提供できます。その他すべての加入者は、ユーザ名で指定されるドメインに基づいてサービスを取得します。ISG は、ユーザ名をプロトコルから取得する必要があります。

- PPP ローカル終端

  ISG は、「ispa」ドメインと一致する加入者に対して、「ispa」サービスをアクティブすることによって、ローカル終端を提供します。システムは、方式リスト「list1」を使用して、加入者の認証を行います。ローカル終端サービスについては、サービス プロファイル、インターフェイス、または仮想テンプレートで他の VRF が指定されない限り、グローバル VRF がデフォルトで適用されます。

- 転送前 PPP 認証

  ISG は、セッションを LNS に転送する前に、「ispb」ドメインと一致する加入者をローカル認証します（サービス ポリシー マップ「ispb」は VPDN グループを指定しているため、セッションは LNS に転送されます）。加入者は、方式リスト「list2」を使用して認証されます。

- ローカル認証なしの PPP 転送

  ISG は、「ispc」ドメインと一致する加入者に対して、ローカル認証なしでセッションを LNS に転送します。

- PPP ドメインの除外

  ISG は、「ispd」ドメインと一致する加入者のセッションに対するサービスを拒否し、接続を解除します。

- PPP ドメインに基づくサービスのアクティベーション

  その他のドメインと一致する加入者に対して、ISG は指定されたドメインと同じ名前を持つサービスをアクティブにします。

制御クラス マップを設定することで、制御ポリシー ルールを実行するために適合すべき条件を定義します。

```
class-map type control match-all PPP_SESSION
  match identifier protocol ppp

class-map type control match-all NAS_PORT_CONDITION
  class type control match identifier name PPP_SESSION
  less-than identifier nas-port type atm vpi 200 vci 100

class-map type control match-all ISPA
  match identifier unauthenticated-domain ispa

class-map type control match-all ISPB
  match identifier unauthenticated-domain ispb

class-map type control match-all ISPC
  match identifier unauthenticated-domain ispc

class-map type control match-all ISPD
  match identifier unauthenticated-domain ispd
```

トップレベル制御ポリシー マップを定義します。

```
policy-map type control L2_ACCESS
```

コールが着信する ATM VPI/VCI に基づいて転送サービスをアクティブにする、制御ポリシー ルールを定義します。

```
 class type control NAS_PORT_CONDITION event session-start
  1 service-policy type service xconnect
```

プロトコルからドメイン名を収集する、制御ポリシー ルールを定義します。ドメイン名は、構造化されたユーザ名から入手できます（たとえば、user@domain）。

```
 class type control PPP_SESSION event session-start
  1 collect identifier unauthenticated-domain
  2 service-policy type control DOMAIN_BASED_ACCESS
```

ネストされた制御ポリシーを定義します。

```
policy-map type control DOMAIN_BASED_ACCESS
```

サービス「ispa」のアクティブ化によってローカル終端を提供する、制御ポリシー ルールを定義します。

```
 class type control ISPA event session-start
  1 authenticate aaa list list1
  2 service-policy type service ispa
```

サービス「ispb」をアクティブ化する前に、ローカルで加入者を認証するシステムを設定する、制御ポリシー ルールを定義します。サービス「ispb」は、セッションを LNS に転送するよう指定します。

```
 class type control ISPB event session-start
  1 authenticate aaa list list2
  2 service-policy type service ispb
```

サービス「ispc」をアクティブにする制御ポリシー ルールを定義して、転送を指定します。

```
 class type control ISPC event session-start
  1 service-policy type service ispc
```

サービス「ispd」と一致する加入者に対して、セッションの接続解除を行う制御ポリシー ルールを定義します。

```
 class type control ISPD event session-start
  service disconnect
```

その他すべてのドメインに対してデフォルトを定義する制御ポリシー ルールを定義します。これにより、指定されたドメインと同じ名前を持つサービスがアクティブになります。

```
 class type control always event session-start
    service-policy type service identifier unauthenticated-domain
```

サービス ポリシー マップを設定します。

```
policy-map type service xconnect
  service vpdn group 1

policy-map type service ispa
  service local
  ip vrf forwarding red

policy-map type service ispb
  service vpdn group 2

policy-map type service ispc
  service vpdn group 3
```

制御ポリシー マップをグローバルに適用します。

```
service-policy type control L2_ACCESS
```

再ネゴシエーションを使用した PPP セッションの VRF 転送：例

次に、PPPoE を使用してセッションを確立するコンフィギュレーション、および VRF を関連付けるために作成される RADIUS サービス プロファイルの例を示します。この例では、PPP セッションは、最初に実行されるときにはデフォルトのルーティング テーブルに属し、IP アドレスがデフォルト IP アドレス プール「DEF-POOL」から割り当てられます。加入者が「ISP-RED」サービスを選択すると、ISG は「ISP-RED」サービス プロファイルをダウンロードし、セッションに適用します。その後、PPP セッションは VRF「RED」に転送されます。クライアント デバイスと ISG デバイスの間で IPCP 再ネゴシエーションが実行され、加入者はプール「POOL-RED」から新しい IP アドレスを割り当てられます。

```
ip vrf RED
 rd 1:1

interface Loopback0
 ip address 10.0.0.1 255.255.255.0

interface Loopback1
 ip address 10.0.1.0 255.255.255.0
 ip vrf forwarding RED
!
interface Ethernet0/0
  pppoe enable

interface Virtual-Template1
 ip unnumbered Loopback0
 service-policy control RULE2
 peer default ip address pool DEF-POOL
 ppp authentication chap

ip local pool DEF-POOL 172.16.5.1 172.16.5.250
ip local pool POOL-RED 172.20.5.1 172.20.5.250
```

ISP RED のサービス プロファイル

```
Cisco-AVpair = ip:vrf-id=RED
Cisco-AVpair = "ip:ip-unnumbered=loopback 1"
Cisco-AVpair = ip:addr-pool=POOL-RED
Cisco-AVpair = subscriber:sg-service-type=primary
Cisco-AVpair = subscriber:sg-service-group=RED-GROUP
Cisco-SSG-Service-Info = IPPPOE-RED
Cisco-SSG-Service-Info = R10.1.1.0;255.255.255.0
Framed-Protocol = PPP
Service-Type = Framed
```

その他の参考資料

ここでは、PPP セッションのための ISG アクセスに関する関連資料について説明します。

関連資料

内容	参照先
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』
AAA 設定作業	『*Cisco IOS Security Configuration Guide*』の「Authentication」の項
AAA コマンド	『*Cisco IOS Security Command Reference*』の「Authentication, Authorization, and Accounting (AAA)」の項
PPP 設定作業	『*Cisco IOS Dial Services Configuration Guide*』の「PPP Configuration」の項
PPP コマンド	『*Cisco IOS Dial Services Command Reference*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/public/support/tac/home.shtml

PPP セッションのための ISG アクセスの機能情報

表 4 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(28)SB 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「Intelligent Services Gateway Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームおよびソフトウェア イメージのサポート情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 4　ISG レイヤ 2 アクセスの機能情報

機能名	リリース	機能設定情報
ISG：セッション：作成：P2P セッション（PPPoE、PPPoXoX）	12.2(28)SB 12.2(33)SRC	ISG セッションとは、特定のデータ フロー間でサービスとポリシーが関連付けられる主要なコンテキストです。Point-to-Point（P2P; ポイントツーポイント）セッションは、シグナリング プロトコルを通じて確立されます。ISG は、PPP、PPPoE、および PPPoA など各種の P2P カプセル化を処理します。 この機能に関する詳細については、次の各項を参照してください。 • 「PPP セッションのための ISG アクセスの設定に関する情報」（P.54） • 「制御ポリシーを使用した PPP セッションのための ISG アクセスの設定方法」（P.56） Cisco IOS Release 12.2(33)SRC では、サポートには Cisco 7600 ルータのサポートが追加されました。