IP 加入者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。ISG は、ルーテッド レイヤ 2 またはレイヤ 3 アクセス ネットワークから ISG に接続する加入者の IP セッションをサポートします。このモジュールでは、IP 加入者セッションの確立、加入者 IP アドレッシングの管理、およびダイナミック Virtual Private Network（VPN; バーチャル プライベート ネットワーク）選択の設定のために、ISG を設定する方法について説明します。

（注） このマニュアルで説明する各項と設定手順は、Network Address Translation（NAT; ネットワーク アドレス変換）が ISG 以外のレイヤ 3 ゲートウェイで実行されていることを前提としています。

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、「IP 加入者セッションのための ISG アクセスの機能情報」（P.114）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。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。

目次

IP 加入者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の要件の詳細については、「IP 加入者セッションのための ISG アクセス の機能情報」（P.114）を参照してください。

Dynamic Host Configuration Protocol（DHCP）サーバが、DHCP リース プロトコルをサポートしている必要があります。

IP 加入者セッションのための ISG アクセスに関する制約事項

重複する IP アドレスに関する制約事項

同じ Virtual Routing and Forwarding（VRF; 仮想経路フォワーディング）インスタンス内で重複する IP アドレスは、サポートされていません。

異なる VRF 内の重複する IP 加入者は、スタティック IP 加入者セッションおよびルーテッド IP 加入者セッションに対する同じインターフェイス上ではサポートされていません。異なる VRF 内の重複する IP 加入者は、レイヤ 2 接続された DHCP 加入者セッションに対する同じインターフェイス上でサポートされています。

IP サブネット セッションに関する制約事項

IP サブネット セッションは、**ip subscriber l2-connected** コマンドで設定されたインターフェイス上ではサポートされていません。IP サブネット セッションは、インターフェイス上で **ip subscriber routed** コマンドが設定されている場合のみサポートされます。

ISG DHCP に関する制約事項

レイヤ 3 DHCP リレー エージェントが ISG デバイスと加入者デバイスの間に存在する場合、ISG は DHCP 要求をリレーできません。

DHCP リース クエリーでは、Cisco 7600 および 7200 シリーズ ルータ、および Cisco 10000 シリーズ ルータがサポートされます。

ダイナミック VPN 選択に関する制約事項

ダイナミック VPN 選択は、IP インターフェイス セッション、IP サブネット セッション、およびグローバルではない VRF インターフェイスから入る加入者に対しては、サポートされていません。

ダイナミック VPN 選択は、アクセス インターフェイス上で静的な VPN コンフィギュレーションを持つ加入者に対しては、サポートされていません。

アドレス再割り当ての行われたダイナミック VPN 選択は、DHCP によって開始されたルーテッド IP 加入者セッションに対してはサポートされていません。ルーテッド IP 加入者の IP アドレスは、アクセス ネットワーク内でルーティング可能になっている必要があります。Internet Service Provider（ISP; インターネット サービス プロバイダー）または VRF の所有するプライベート アドレスは、重複していたり、加入者と ISG デバイスとの間のネットワークでルーティングできないことがあるため、このような加入者には IP アドレスを割り当てられません。

IP セッション全般に関する制約事項

Packet of Disconnect（PoD; パケット オブ ディスコネクト）は、IP 加入者セッションではサポートされていません。

IP 加入者セッションは、ambiguous IEEE 802.1QinQ（QinQ）または IEEE 802.1Q（Dot1Q）サブインターフェイスではサポートされていません。

IP 加入者セッションは、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）パケットを受信するインターフェイスではサポートされていません。

Modular Quality of Service（QoS）Command-Line Interface（CLI; コマンドライン インターフェイス）（MQC）に基づくシェーピングとキューイングは、IP 加入者セッションではデフォルト クラスの出力方向でサポートされています。

スタティック IP セッション上での機能の設定はサポートされていません。

Cisco 10000 シリーズ インターネット ルータに関する制約事項

ISG は、Cisco 10000 シリーズ インターネット ルータ上では、RADIUS パケットによって開始された IP 加入者セッションをサポートしていません。

IP インターフェイス セッションは、Cisco 10000 シリーズ インターネット ルータ上の ATM メイン インターフェイスと ATM マルチポイント サブインターフェイス上ではサポートされません。

IP 加入者セッションと PPP over ATM または PPP over Ethernet（PPPoX）セッションは、同じ ATM メイン インターフェイスまたはサブインターフェイス上ではサポートされません。複数の IP 加入者セッションまたは複数の PPPoX セッションのいずれかを、ATM メイン インターフェイスまたはサブインターフェイスで一度に設定できます。

IP 加入者セッションは、次のインターフェイス上ではサポートされません。

- マルチリンク インターフェイス
- トンネル インターフェイス
- 仮想テンプレート インターフェイス
- IPsec トンネル

DHCP が開始した IP セッションでは、DHCP 制御パケット（bootps パケットと bootpc パケット）を許可するためのアクセス リストを明示的に設定する必要があります。DHCP 制御パケットを許可するようにアクセス リストが設定されていない場合、IP セッションに適用される ISG 機能がこれらのパケットをドロップする場合があるため、予期しないまたは誤った ISG 動作が発生する可能性があります。たとえば、DHCP が開始した IP セッションを維持する DHCP 更新パケットが、IP セッションに適用されるセキュリティ アクセス リストによってドロップされる可能性があります。

Cisco 10000 シリーズ ルータでは、同じインターフェイス上で ISG も設定されている場合、Parallel eXpress Forwarding（PXF）パス内で unicast Reverse Path Forwarding（uRPF）がサポートされません。たとえば、次の構成では PXF パス内で uRPF がサポートされます。

```
interface GigabitEthernet7/0/0
 ip address 10.10.10.1 255.255.255.252
 ip verify unicast reverse-path
```

ところが、次の構成では PXF パス内で uRPF がサポートされません。

```
interface GigabitEthernet7/0/0
 ip address 10.10.10.1 255.255.255.252
 ip verify unicast reverse-path
 service-policy type control isg-control
 ip subscriber routed
 initiator unclassified ip-address
```

この構成では、ルータが受信するすべての IP パケットのうち、その発信元 IP アドレスが既存の ISG IP セッションと一致しないものは、Cisco 10000 Route Processor（RP）にパントされ、uRPF 処理が行われます。これにより、Cisco 10000 RP 上での割り込みレベル CPU 使用率が増大する場合があります。IP スプーフィングの問題を防止するため、すべての正当な IP ネットワークを発信元として指定する入力 Access Control List（ACL; アクセス コントロール リスト）の実装を検討してください。Cisco 10000 シリーズ ルータは、ISG 処理を実行する前に PXF 内の入力 ACL を処理します。

ISG インターフェイスに適用されるアクセス リストは、既存の ISG セッションに属する IP トラフィックに対しては、その ISG セッションがクリアされて再導入されるまで有効になりません。したがって、ACL を適用して ISG-enabled インターフェイス上のトラフィックをフィルタリングするには、ACL を適用した後、必ず ISG をクリアしてください。

Cisco 10000 シリーズ ルータでは、アクセス インターフェイス上で VRF インスタンスが変更されたときに、既存のセッションが終了されます。

Cisco 7600 ルータに関する制約事項

Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータは、次のアクセス インターフェイス上で IP 加入者セッションをサポートしません。

- Gigabit EtherChannel（ポート チャネル）
- スイッチ仮想インターフェイス
- Generic Routing Encapsulation（GRE）
- PPP
- Layer 2 Tunnel Protocol（L2TP）

Shared Port Adapter Interface Processor（SIP2）Network Processor（NWP）は、アクセス インターフェイス、ネットワーク インターフェイス、およびマルチサービス インターフェイス上で ISG 加入者トラフィック用に設定された IP 機能をサポートしません。

加入者冗長性とロード バランシングは、IP 加入者に対してはサポートされません。

Cisco IOS Release 12.2(33)SRE 以降のリリースでは、Cisco 7600 ルータは、SIP400 および ES+ ラインカード上でのみ、および次のインターフェイス上でのみ IP 加入者セッションをサポートします。

- SIP400 ラインカード上のメイン インターフェイスとアクセスタイプ サブインターフェイス
- Ethernet Services Plus（ES+）ラインカード上のメイン インターフェイスとすべてのタイプのサブインターフェイス
- ES+ ラインカード上のポートチャネル インターフェイス

Cisco 7600 ルータには、ラインカード単位およびルータ シャーシ単位の IP 加入者セッション数に制限があります。アクティブなセッション数が次の制限を超えると、エラー メッセージが表示されます。

- Cisco 7600 シャーシ：32,000 加入者セッション（Cisco IOS Release 12.2(33)SRE1 以降のリリースでサポート）
- ES+ ラインカード：ポート グループごとに 4000 加入者セッション、ラインカードごとに 16,000 セッション（Cisco IOS Release 12.2(33)SRE 以降のリリースでサポート）
- SIP400 ラインカード：8000 加入者セッション（Cisco IOS Release 12.2(33)SRD4 以降のリリースでサポート）

IP 加入者セッションのための ISG アクセスに関する情報

IP 加入者セッションのタイプ

ISG は、次の 3 タイプの IP 加入者セッションをサポートします。

IP セッション

IP セッションには、単一の加入者 IP アドレスに関連付けられたすべてのトラフィックが含まれます。IP アドレスがシステムに固有でない場合は、VRF や MAC アドレスなど、他の識別特性によってセッションの ID の一部が形成されます。ISG は、DHCP パケット、未分類の IP アドレスまたは MAC アドレスを持つパケット、または RADIUS パケットの受信時に、IP セッションを作成するように設定できます。詳細については、「IP 加入者セッションの開始」（P.73）を参照してください。

IP セッションは、接続されている加入者デバイス（ISG から 1 ルーティング ホップ）、またはゲートウェイから 2 ホップ以上の加入者デバイスに対してホストされます。

IP インターフェイス セッション

IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成され、インターフェイスがシャットダウンされてもセッションを継続します。デフォルトでは、IP インターフェイス セッションは、完全なネットワーク アクセス権を持つ「unauthenticated」状態で開始します。

IP インターフェイス セッションは、加入者がインターフェイスで表現され（PPP を除く）、複数の IP アドレスを使用して通信する状況で使用される場合があります。たとえば、Routed Bridge Encapsulation（RBE; ルーテッド ブリッジ エンカプセレーション）を使用する加入者は、複数の PC をサポートする家庭用 Customer Premises Equipment（CPE; 顧客宅内機器）への専用の ATM Virtual Circuit（VC; 仮想回線）を持っている場合があります。

IP サブネット セッション

IP サブネット セッションは、単一の IP サブネットに関連付けられているすべてのトラフィックを表します。IP サブネット セッションは、特定の IP サブネットに関連付けられているパケットへの均一なエッジ処理の適用に使用されます。IP サブネット セッションが設定されている場合、ISG は、そのサブネットを単一の加入者として取り扱います。これは、ISG の機能および機能性が、サブネット トラフィックに集約として適用されることを意味しています。

IP サブネット セッションは、ルーテッド IP 加入者トラフィック用にサポートされています。

IP サブネット セッションは IP セッションと同じ方法で作成されますが、加入者が認可または認証されていて、Framed-IP-Netmask アトリビュートがユーザ プロファイルまたはサービス プロファイルに存在する場合に、ISG が発信元 IP に基づくセッションを、Framed-IP-Netmask アトリビュート内にサブネット値を持つサブネット セッションに変換する点が異なります。

(注) 入力インターフェイスが単一のサブネットにマップされる場合、サブネットは、IP インターフェイス セッションで調整される場合があります。ただし、ISG が加入者から 2 ホップ以上離れている場合、および同じインターフェイスを通して複数のサブネットにアクセスする可能性がある場合には、トラフィックを識別し、各サブネットに適切なエッジ機能性を適用するように IP サブネット セッションを定義できます。

マルチキャスト セッションと IP セッションの共存

ISG セッション マルチキャスト共存機能では、Cisco 7600 シリーズ ルータの同じサブインターフェイス上でマルチキャストおよび IP セッションが共存できるようにして、同じ VLAN 上ですべての加入者とサービス（データとマルチキャスト）をホストする機能が導入されます。ISG IP セッションは、非アクセスタイプのサブインターフェイスでサポートされます。既存のセッションがある場合、またはセッションが存在しない場合であっても、このサポートがあると、IP セッション用に設定されたインターフェイスをマルチキャスト トラフィックが、セッションを作成することなくアップストリームとダウンストリームの両方向で通過し易くなります。

IP 加入者の接続

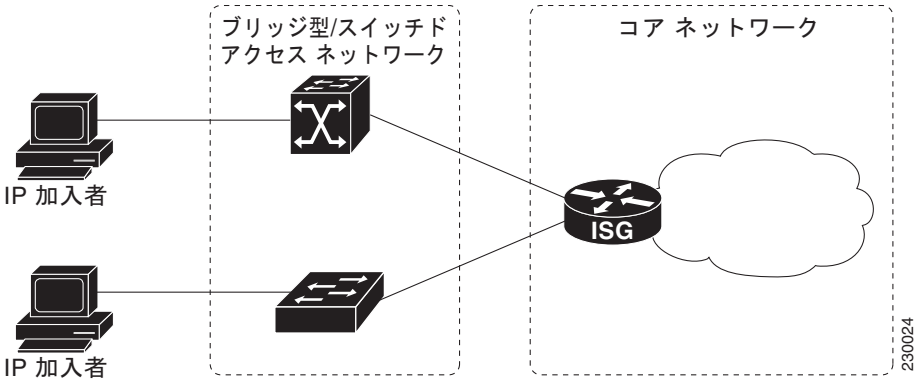
IP 加入者は、レイヤ 2 接続されたアクセス ネットワークまたはルーテッド アクセス ネットワークのいずれかを通して ISG に接続します。ここでは、次のタイプの IP 加入者接続について説明します。

- 「レイヤ 2 接続されたアクセス ネットワーク」（P.72）
- 「ルーテッド アクセス ネットワーク」（P.73）

レイヤ 2 接続されたアクセス ネットワーク

レイヤ 2 接続された加入者は、ISG の物理インターフェイスに直接接続されるか、またはブリッジ型ネットワークやスイッチド ネットワークなどのレイヤ 2 アクセス ネットワークを通して ISG に接続されます。レイヤ 3 フォワーディングは存在しないか、または加入者トラフィックをレイヤ 2 アクセス ネットワーク内で誘導するためには使用されません。加入者の IP アドレスは、レイヤ 2 接続された物理インターフェイスと同じサブネット内に存在する場合も、また存在しない場合もあります。図 2 に、レイヤ 2 接続されたアクセス ネットワークの例を示します。

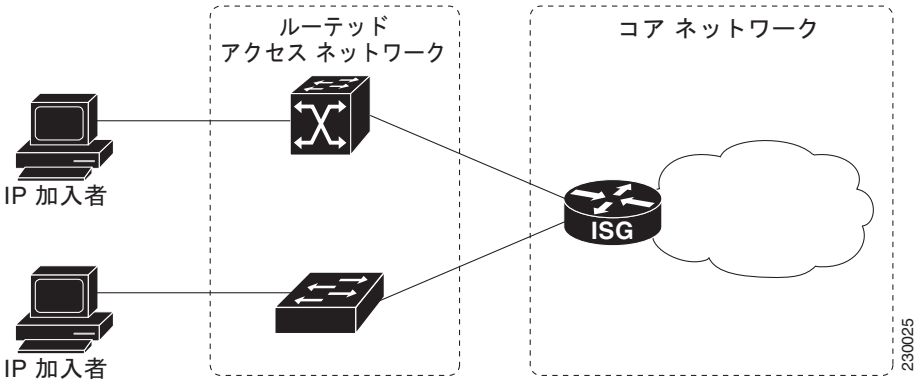
図 2　レイヤ 2 接続されたアクセス ネットワーク



ルーテッド アクセス ネットワーク

ルーテッド加入者トラフィックは、ISG に到達する前に、少なくとも 1 台の中継ルータがあるレイヤ 3 アクセス ネットワークを通してルーティングされます。加入者の IP アドレスは、少なくともレイヤ 3 アクセス ネットワーク内でルーティング可能です。レイヤ 3 アクセス ネットワークには、単一のルーティング ドメインが含まれており、したがって重複する IP アドレスをサポートしません。図 3 に、ルーテッド アクセス ネットワークの例を示します。

図 3　ルーテッド アクセス ネットワーク



IP 加入者セッションの開始

ISG は、インターフェイス上の IP セッションまたは IP サブネット セッションの開始を表す、次のイベントの 1 つ以上を許可するよう設定できます。

- DHCP DISCOVER パケット

  次の条件と一致する場合、DHCP DISCOVER パケットを受信すると、IP セッションの作成がトリガーされます。

  - ISG は、新しい IP アドレスの割り当てに関して DHCP リレーまたはサーバとして機能します。
  - 加入者は、DHCP 用に設定されます。
  - DHCP DISCOVER パケットは、加入者から受信する最初の DHCP 要求です。

- 未分類の発信元 IP アドレス

  ルーテッド IP 加入者に関しては、未分類の発信元 IP アドレスを持つ IP パケットが出現することにより、新しい IP セッションがトリガーされます（その IP アドレスに対して、IP セッションがまだ存在しないことを意味しています）。

- 未分類の発信元 MAC アドレス

  レイヤ 2 接続された IP 加入者に関しては、未分類の発信元 MAC アドレスを持つ IP パケットが出現することにより、新しい IP セッションがトリガーされます（その MAC アドレスに対して、IP セッションがまだ存在しないことを意味しています）。

- RADIUS Access-Request パケット

  ルーテッド アクセスまたはレイヤ 2 接続されたアクセスに関しては、ISG が RADIUS プロキシとして機能しているときに RADIUS Access-Request パケットが出現することにより、新しい IP セッションがトリガーされます。

IP 加入者のアドレッシング

ISG が IP 加入者の IP アドレッシングを処理する方法については、次の項を参照してください。

- 「ISG 加入者 IP アドレスの割り当て方法」（P.74）
- 「パブリック IP アドレスとプライベート IP アドレス」（P.75）
- 「IP アドレスの重複」（P.76）
- 「DHCP を使用した ISG 加入者 IP アドレスの割り当て」（P.76）

ISG 加入者 IP アドレスの割り当て方法

IP 加入者は、IP アドレスを静的に設定するか、または IP アドレスを割り当てる機能を持つ何らかのネットワーク プロトコルで動的に取得します。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。

ここでは、ISG が各タイプのレイヤ 3 セッション用にサポートする IP アドレスの割り当て方法について説明します。

- 「IP インターフェイス セッション」（P.74）
- 「IP セッション」（P.75）
- 「IP サブネット セッション」（P.75）

IP インターフェイス セッション

IP インターフェイス セッションに関しては、ISG は、加入者 IP アドレスの割り当てに関与（または認識）しません。

IP セッション

IP セッションに関して、ISG は、次の IP アドレスの割り当て方法をサポートします。

- スタティック IP アドレス

  加入者のスタティック IP アドレスがサービス ドメインに対して正しく設定されている場合、ISG は、その加入者の IP アドレスを割り当てる必要がありません。

- DHCP

  IP アドレスの割り当てに DHCP が使用されている場合で、DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しい場合、ISG は、その加入者の IP アドレスを割り当てる必要がありません。

  DHCP によって割り当てられた IP アドレスがサービス ドメインに対して正しくない場合、または VRF 転送によってドメインが変更された場合、ISG は、DHCP IP アドレスの割り当てに関与するように設定できます。

  ISG が DHCP IP アドレスの割り当てに関与するためには、次の条件を満たす必要があります。

  - 加入者が、レイヤ 2 接続されている。
  - ISG デバイスが、DHCP サーバまたはリレーとして機能することにより、DHCP 要求のパス内に存在する。
  - 加入者が、静的に設定された IP アドレスを持つ。

  これをサポートした展開では、推奨される IP アドレスの割り当て方法が DHCP になります。

IP サブネット セッション

IP サブネット セッションでは、ユーザ プロファイルに IP サブネットが指定されます。

パブリック IP アドレスとプライベート IP アドレス

IP 加入者にどのように IP アドレスが割り当てられても、その IP アドレスは、パブリック IP アドレスか、プライベート IP アドレスのカテゴリに入ります。IP 加入者にプライベート IP アドレスが割り当てられ、加入者がインターネットに到達する必要がある場合、加入者とインターネットの間にある ISG やファイアウォールなどのレイヤ 3 ゲートウェイは、加入者のプライベート IP アドレスに対して NAT を実行する必要があります。

アクセス ネットワークがレイヤ 2 接続されたネットワークの場合、加入者 IP アドレスは、アクセス インターフェイスに対してネイティブでも外部でもかまいません。ネイティブ加入者 IP アドレスは、アクセス インターフェイス上でプロビジョニングされたサブネットに属するアドレスです。外部加入者 IP アドレスは、アクセス インターフェイス上でプロビジョニングされたサブネットに属さないアドレスです。リテール ISP が自分の IP アドレス割り当てから IP アドレスを IP 加入者に割り当てたが、それがホールセール ISP とは異なる場合、またはホーム アクセス ネットワーク内でネイティブなスタティック IP アドレスを持つ IP 加入者が外部アクセス ネットワークに移動した場合、外部加入者 IP アドレスになる可能性があります。外部 IP アドレスを持つ外部 IP 加入者をサポートするには、ISG は、ISG 自身の MAC アドレスを持つ外部 IP アドレスから送信される Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に応答する必要があります。アクセス ネットワークはレイヤ 2 接続されているため、ISG は、すべての加入者との隣接関係を維持します。

アクセス ネットワークがルーテッド ネットワークの場合、加入者 IP アドレスは、アクセス ネットワーク内でルーティング可能になっている必要があります。ルーティングできない場合、加入者トラフィックは ISG に到達できません。この場合、ISG は各加入者と隣接関係を持てませんが、登録者へのネクストホップという隣接関係を持ちます。ネクストホップは、ISG 上のルーティング プロセスによって決定されます。

IP アドレスの重複

アクセス ネットワークが VPN 機能なしで展開されている場合、アクセス ネットワーク内の IP アドレス空間は、すべての IP 加入者に共有されます。IP アドレスが動的に割り当てられる場合、これらのアドレスが重複しないように注意する必要があります。重複する IP アドレスが意図的に IP 加入者に割り当てられた場合、アクセス ネットワークは、レイヤ 2 分離メカニズムを使用して IP アドレス空間を区別する必要があります。たとえば、アクセス ネットワークは、各 IP アドレス空間を別々の VLAN に置くことができます。

アクセス ネットワークがローカル IP 加入者とローミング ユーザの両方に対して処理を行う場合、ローミング加入者のスタティック プライベート IP アドレスが、別の加入者のネイティブ プライベート IP アドレスと重複する可能性があります。たとえば、一般にはダイナミック IP アドレスを割り当てるパブリック ワイヤレス ホット スポットが、一時的なローミング ユーザに、静的に設定された IP アドレスでアクセスを提供する場合があります。この特殊な重複状態をサポートするには、すべての IP 加入者は、重複する MAC アドレスの存在しない、レイヤ 2 接続されたアクセス ネットワークに属している必要があります。この場合、IP 加入者は、MAC アドレスを使用して区別できます。

DHCP を使用した ISG 加入者 IP アドレスの割り当て

ISG が（DHCP サーバまたは DHCP リレーのどちらかとして）DHCP 要求のパス内にある場合、ISG が、加入者 IP アドレスの割り当てに使用される IP アドレス プールと DHCP サーバに影響を与えることがあります。加入者に割り当てられている IP アドレスに影響する ISG をイネーブルするには、DHCP アドレス プール クラスをアドレス ドメインに関連付けます。DHCP アドレス プール クラスも、加入者に関連付けられたサービス ポリシー マップ、サービス プロファイル、またはユーザ プロファイルで設定する必要があります。加入者から DHCP 要求を受信すると、DHCP は、加入者に関連付けられたアドレス プール クラスを使用して、要求に対するサービスに使用する DHCP アドレス プールを決定します。その結果、IP アドレスは、要求単位で、ローカル DHCP サーバによって提供されるか、または選択されたプールに定義されたリモート DHCP サーバにリレーされます。

IP 加入者 ID

ISG は、IP セッションの作成時に IP 加入者を一意に識別する必要があるため、IP 加入者 ID は、IP セッションの開始と密接に関連しています。ただし、IP 加入者を識別する必要性は、セッションの開始フェーズの後で発生します。ここでは、ISG が IP 加入者を一意に識別する方法について説明します。

- 「ルーテッド IP 加入者 ID」（P.76）
- 「セカンダリ ID としての MAC アドレス」（P.77）
- 「DHCP リース クエリーのサポート」（P.77）
- 「レイヤ 2 接続された IP 加入者 ID」（P.78）
- 「インターフェイス IP 加入者 ID」（P.78）

ルーテッド IP 加入者 ID

定義により、加入者 IP アドレスは少なくともアクセス ネットワーク内でルーティング可能になっている必要があるため、アクセス ネットワークがルーテッド ネットワークの場合、加入者 IP アドレスを使用して IP 加入者を一意に識別できます。

加入者 IP アドレスを識別方法として使用する場合、ISG は加入者 IP アドレスが一意であると見なします。また、アクセス ネットワークがレイヤ 3 ロード バランシング、冗長性、または非対称ルーティングで展開されている場合、ISG は、同じ IP 加入者からの IP トラフィックが異なるアクセス インター

フェイスに到着すると見なします。このタイプの展開をサポートするため、ISG は、同じアクセス ネットワークに接続されているすべてのアクセス インターフェイス用として、単一の IP アドレス空間を想定します。

単一の物理アクセス ネットワーク上で、複数の IP アドレス空間をサポートする必要がある場合、アクセス ネットワークは、何らかのレイヤ 2 カプセル化を使用して、各 IP アドレス空間に個別の論理アクセス ネットワークを作成する必要があります。この場合でも、ISG は、論理アクセス ネットワークに接続するすべての論理アクセス インターフェイスに対して、単一の IP アドレス空間を持つことができます。

加入者 IP アドレスがプライベート IP アドレスの場合、アクセス ネットワークは、それらの加入者トラフィックをルーティング可能になっている必要があります。加入者トラフィックがインターネット宛ての場合は、NAT を実行する必要があります。

ルーテッド IP 加入者に関して、加入者 IP アドレスは IP セッションのキーとして機能します。ISG は、IP トラフィックを次のように IP セッションに関連付けます。

- アップストリーム方向では、IP パケットの発信元 IP アドレスが IP セッションの識別に使用されます。発信元 IP アドレスは、加入者 IP アドレスです。
- ダウンストリーム方向では、IP パケットの宛先 IP アドレスが IP セッションの識別に使用されます。宛先 IP アドレスは、加入者 IP アドレスです。

IP 加入者が VPN ユーザの場合、加入者 IP アドレスは ISG 上のグローバル ルーティング テーブルおよび VPN ルーティング テーブルの両方でルーティング可能になっている必要があります。

IP サブネット加入者の場合、加入者 IP アドレスは、/32 の IP ホスト アドレスではなく、IP プレフィクス アドレスとして定義されます。この IP プレフィクスは、エンド ユーザが使用する IP アドレス範囲をカバーしますが、ISG から見ると単一の論理 IP 加入者を表しています。この展開では、すべてのエンド ユーザが、ISG から提供される同じ接続およびサービスを共有します。

異なるネットワーク マスクを持つ IP 加入者の分類を正規化するため、ISG は、ネットワーク マスクとルーテッド IP 加入者の加入者 IP アドレスを組み合せて使用します。

セカンダリ ID としての MAC アドレス

セッションの開始時に、**collect identifier mac-address** コマンドを設定する必要があります。このコマンドは、ISG デバイスに対して、MAC アドレスをセッション ID の一部として格納するよう指示します。ルーテッド IP 加入者セッションに関して、MAC アドレスは、DHCP リース クエリー プロトコルを使用して、DHCP サーバから収集されます。コマンドの設定の詳細については、「*Configuring ISG Control Policies*」モジュールを参照してください。

DHCP リース クエリーのサポート

DHCP リース クエリー メッセージは、DHCP リレー エージェントから DHCP サーバに送信される DHCP メッセージ タイプです。DHCP リース クエリー対応リレー エージェントは、IP エンドポイントの場所を DHCP リース クエリー メッセージに送信します。

DHCP リース クエリー トランザクションは、特別なメッセージ タイプを持つ DHCP トランザクションです。これにより、クライアントは、IP アドレスのオーナーおよびリースの有効期限に関して、DHCP サーバに問い合わせることができます。リース クエリーのための DHCP サーバの設定の詳細については、「DHCP サーバの IP アドレスの設定」（P.102）を参照してください。

レイヤ 2 接続された IP 加入者 ID

レイヤ 2 接続されたアクセス ネットワークは、ネイティブ IP アドレスを持つ IP 加入者に加えて、外部 IP アドレスおよび重複する IP アドレスを持つ IP 加入者に対して IP 接続を提供できます。そのようなアクセス ネットワークでは、加入者 IP アドレスが一意ではない可能性があり、ISG は加入者がどの種類の IP アドレスを持っているかにかかわらず、加入者 MAC アドレスを使用してレイヤ 2 接続された IP 加入者を識別します。

プライベート IP アドレスまたは重複する IP アドレスを持つ、IP 加入者のインターネット宛てのトラフィックは、NAT の対象となります。

レイヤ 2 接続された IP 加入者に関して、加入者 MAC アドレス（VLAN 内で一意）および IP アドレスの両方が IP セッションのキーとして使用されますが、それらのキーは使用される方向が異なります。

- アップストリーム方向では、IP パケットの VLAN ID と発信元 MAC アドレスが IP セッションの識別に使用されます。
- ダウンストリーム方向では、IP パケットの宛先 IP アドレスと VLAN ID の両方が、IP 加入者コンテキストの識別に使用されます。

インターフェイス IP 加入者 ID

アクセス インターフェイスが IP 加入者の識別に使用されると、各アクセス インターフェイスが単一の IP 加入者に対応します。アクセス インターフェイスが利用可能になり次第、ISG は、インターフェイスをキーとして使用して IP セッションを作成し、このインターフェイスのすべての送受信 IP トラフィックを IP セッションに関連付けます。

IP トラフィックと IP 加入者を正確に関連付けるため、ISG は、IP 加入者を識別する方法としてインターフェイスを使用するように設定する必要があります。その後 ISG は、次のように IP トラフィックを分類します。

- アクセス ネットワーク（アップストリーム方向）から IP トラフィックを受信すると、ISG は入力インターフェイスを使用して IP セッションを識別します。
- コア ネットワーク（ダウンストリーム方向）から IP トラフィックを受信すると、ISG は、出力インターフェイスを使用して IP セッションを識別します。

IP 加入者の VPN 接続とサービス

ここでは、ISG IP 加入者の VPN 接続とサービスについて説明します。

加入者 VPN メンバシップ

IP 加入者は、展開要件に基づいて VPN サービスを持つ場合と持たない場合があります。VPN サービスを持たない場合、IP 加入者は、常に 1 つの VPN ドメインにのみ属している可能性があります。IP 加入者は、次のいずれかの方法で VPN ドメインに関連付けられています。

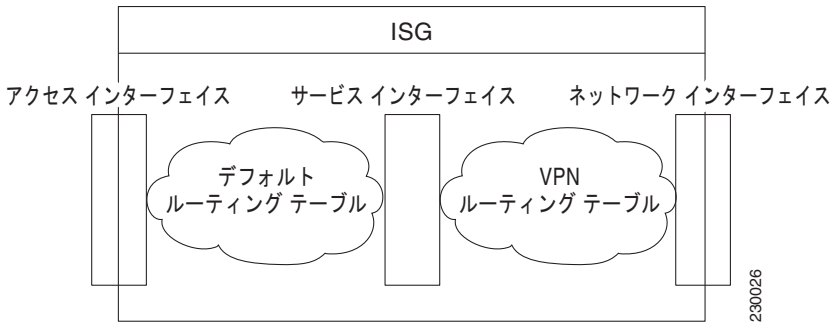
- スタティック VPN 割り当て : VPN IP 加入者はスタティック VPN ドメインに属しています。IP 加入者は、ISG に接続すると、事前に割り当てられた VPN ドメインに配置されます。
- ダイナミック VPN 選択 : VPN IP 加入者は、ダイナミック サービス ログインを通して、異なる VPN ドメインの中からドメインを選択および切り換え可能です。新しい VPN ドメインが選択されると、新しい VPN ドメインの VPN サービスが IP 加入者に適用される前に、現在の VPN ドメインの VPN サービスを削除する必要があります。

  ダイナミック VPN 選択は、セッションの開始時に VRF がダウンロードされ加入者セッションに適用される自動サービス ログインを通して開始するか、または選択されたサービスに対応する VRF に加入者が転送される Web ポータルの加入者サービス選択を通して開始できます。

マルチサービス インターフェイス モデル

スタティック VPN 設定を持たない加入者に関しては、ISG デバイス上でマルチサービス インターフェイスが VRF に IP セッションをマップするように設定する必要があります。マルチサービス インターフェイスは、VPN ルーティング ドメインとデフォルト ルーティング ドメインの間の境界を表します。IP 加入者が接続期間全体を通じて複数のルーティング ドメインに関連付けられる可能性がある場合、マルチサービス インターフェイスは、1 つの VPN ドメインから別の VPN ドメインに切り換える IP 加入者の境界ポイントとして機能します。1 つのマルチサービス インターフェイスが、各ルーティング ドメイン用に設定されている必要があります。図 4 に、マルチサービス インターフェイス モデルを示します。

図 4　　マルチサービス インターフェイス モデル



VPN アドレッシング

加入者セッションがある VPN ドメインから別のドメインに転送されると、そのセッションは実質的に新しいアドレッシング ドメインに属します。このドメインは、加入者の以前のドメインと重複する場合も、重複しない場合もあります。それに従って、パケットがサービス ドメイン内から正しくルーティング バックされるように、加入者のネットワーク側アドレスを変更する必要があります。

Web ポータルとの対話なしでは加入者の ID および加入サービスを判断できない場合は、VRF 転送が必要です。IP パケットがポータル サーバとの間でルーティングされるためには、少なくとも開始時にローカル ルーティング コンテキストが必要です。ポータルベース サービスの選択に従い、加入者は、

通常、選択されたサービス ドメインに関連付けられている VRF に転送される必要があります。また、VRF 転送に従い、加入者は、新しいドメイン内でルーティング可能なアドレスを受け取る必要があります。

ISG が加入者デバイスと隣接し、DHCP リレーまたはサーバとして機能している場合は、DHCP を使用して加入者にドメイン固有のアドレスを割り当てられます。

VRF 転送をサポートするには、DHCP を短い初期リースで設定するよう強く推奨します（既存の加入者アドレスを変更できるのは、現在のリース期限が切れたときだけです）。加入者は、次の DHCP の更新要求を受信するまで、選択したドメインにアクセスできません。短い初期リース期間を使用することにより、VRF の変更と DHCP の更新の間隔が最小になります。長いリース期間を使用する場合、IP アドレス変更は、アウトオブバンド方式を実装して開始する必要があります。

加入者デバイスで、新しいアドレスの割り当てに DHCP を使用できる場合は、転送の実行にサブネットベース VRF 選択を使用できます。サブネットベース VRF 選択（*VRF の自動分類* とも呼ばれる）は、発信元 IP サブネット アドレスに基づいて、入力ポートで VRF を選択する機能です。

サービス プロバイダーおよび組織は、元々重複していないパブリック IP アドレス ブロックを割り当てています。したがって、パブリック IP アドレスが割り当てられる場合、VPN IP 加入者の IP アドレスは重複しません。異なる VPN ドメインの VPN IP 加入者にプライベート IP アドレスが割り当てられると、アクセス ネットワークでアドレスの重複が起こる場合があります。

異なる VPN ドメインの VPN IP 加入者を分割するレイヤ 2 カプセル化が行われない場合、アクセス ネットワークは単一の IP アドレス空間です。したがって、VPN IP 加入者を展開する場合、ISG は、重複する IP アドレスを処理できる必要があります。重複する IP アドレスを持つ VPN IP 加入者による IP 接続は、レイヤ 2 接続されたアクセス ネットワークを介して、ISG に接続された場合のみ可能です。

VPN IP 加入者 ID

ISG は、非 VPN IP 加入者の識別と同じ方法で、VPN IP 加入者を識別します。アップストリーム IP トラフィックは、アクセス ネットワークから VPN に流れる加入者 IP トラフィックとして定義されます（サービス プロバイダー コア ネットワークの最上位に位置）。ダウンストリーム IP トラフィックは、VPN からアクセス ネットワークに送信される加入者 IP トラフィックとして定義されます。

VRF 転送のサービス モデル

プライマリ サービスとは、そのサービス定義にネットワーク転送ポリシー（VRF など）を含むサービスです。1 つのセッションに対して、一度に 1 つのプライマリ サービスだけをアクティブにできます。*セカンダリ* サービスとは、ネットワーク転送ポリシーを含まないすべてのサービスです。

すでにアクティブ化されたプライマリ サービスを持つ加入者が、他のプライマリ サービスを選択しようとすると、ISG は現在のすべてのサービス（現在のプライマリ サービスを含む）を非アクティブ化し、新しいプライマリ サービスをアクティブにすることで、VRF を切り換えます。

すでにアクティブ化されたプライマリ サービスを持つ加入者が、セカンダリ サービスを選択しようとすると、ISG のアクションは、そのセカンダリ サービスがサービス グループの一部かどうかによって異なります。*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。表 5 は、加入者がセカンダリ サービスを選択した場合に、ISG が実行するアクションを示しています。

表 5　セカンダリ サービスの ISG アクティベーション ポリシー

プライマリ サービスの特性	セカンダリ サービスの特性	ISG で行われる動作
サービス グループ アトリビュートのないプライマリ サービス	サービス グループのあるセカンダリ サービス	セカンダリ サービスを起動しない。
	サービス グループのないセカンダリ サービス	セカンダリ サービスを起動する。
サービス グループ アトリビュートのあるプライマリ サービス	異なるサービス グループのあるセカンダリ サービス	セカンダリ サービスを起動しない。
	同じサービス グループのあるセカンダリ サービス	セカンダリ サービスを起動する。
	サービス グループのないセカンダリ サービス	セカンダリ サービスを起動する。

ダイナミック VPN 選択の利点

いわゆる*公平なアクセス ネットワーキング*をサポートする必要がある市場において、ルーティングと転送ドメイン（*ネットワーク サービス*とも呼ばれる）の間で、加入者セッションの切り換えが必要になることがよくあります。公平なアクセス ネットワーキングは、サービス プロバイダーによるリテール加入者ネットワークへの公平なアクセスを、アクセス プロバイダーが可能にしなければならないことを定めた取締規則でしばしば要求されます。ISG ダイナミック VPN 選択は、ネットワーク サービス間での加入者の転送を可能にすることで、公平なアクセス ネットワーキングを促進します。

CoA クライアントに対する VRF-Aware サポート

- ISG は、CoA クライアント（RADIUS サーバ）に対する VRF-aware 機能をサポートしているため、1 台の CoA クライアントが複数の VRF の加入者を処理できます。加入者セッションは、CoA クライアントが設定されているものとは別の VRF 内に存在することも可能です。IP 加入者セッションが別の VRF 内に存在する場合に CoA メッセージを ISG に送信するには、表 6 に示す Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）をセッション ID で使用する必要があります。

表 6　VRF ID VSA の説明

サブアトリビュート ID	アトリビュート タイプ	値	例
250	account-info	S<*subscriber-ip-address*[:vrf-id=*vrf-name*]> • S：加入者 IP のコード • *vrf-name*：Network Access Server（NAS; ネットワーク アクセス サーバ）が加入者 IP アドレスを検索する VRF	Cisco-Account-Info=S10.0.0.3:vrf-id=subscriber_VRF1

次に、VRF の設定例を示します。

RADIUS ユーザ プロファイル

```
simulator radius subscriber 401
 authentication smith pap smith
 vsa cisco 250 S10.0.0.3:vrf-id=subscriber_VRF1
 vsa cisco generic 252 binary 015042484b
```

加入者セッションの検索は、VRF を提供する方式に基づいて行われます。加入者 IP アドレスの検索に使用する VRF を決定する優先順位は、次のとおりです。

1. セッション ID の一部として CoA メッセージ内にある VRF
2. クライアント コンフィギュレーション内にある VRF
3. CoA クライアントが属する VRF

表 7 に、クライアントがサーバに CoA メッセージを送信した場合の、予想される動作を示します。

表 7　　vrf-id アトリビュートを使用した予想される動作

vrf-id がある場所		
CoA メッセージ	**CoA クライアント コンフィギュレーション**	**加入者 IP アドレスが検索される VRF**
あり	あり	CoA メッセージ内の VRF
あり	なし	CoA メッセージ内の VRF
なし	あり	クライアント コンフィギュレーション内の VRF
なし	なし	クライアント側インターフェイスのコンフィギュレーション内の VRF
vrf-id=global	なし	サーバ上のグローバル ルーティング テーブル内の VRF

IP セッションの終了

IP セッションは次のいずれかの方法で終了されます。

- DHCP リースの期限切れまたはクライアントからの DHCP 解除

  DHCP を使用して新しいセッションが検出される場合、その分離も DHCP イベントによって通知されることがあります。

- application stop

  セッションを終了するために使用されるアプリケーション コマンドです。**application stop** コマンドは、通常、加入者が Web ポータルからアカウント ログオフを開始する場合に、セッションを終了するために使用されます。アプリケーションの停止は、管理者が加入者の悪質な行動に対応するために起こすアクションなど、管理者のアクションによって引き起こされる可能性もあります。

- アイドル タイムアウトとセッション タイムアウト

  アイドル タイムアウトとセッション タイムアウトは、IP セッションの終了を検出または強制するために使用できます。

- 制御ポリシー

  「サービス切断」アクションを含む制御ポリシーは、セッションを終了するために使用できます。

DHCP-Initiated IP セッションの IP セッション回復

IP セッションが終了した場合（アカウントのログオフまたはセッションのタイムアウトなど）、または IP セッションが失われた場合（ルータのリロードなど）、クライアントは引き続き有効期限内の DHCP リースを保持できます。この場合 ISG はセッションの再起動を実行し、DHCP のリース期限が切れるまでクライアントの IP 接続の停止を防止します。セッションの再起動イベントが発生した場合、ISG が実行するアクションの定義する制御ポリシーを設定できます。ポリシーが定義されていない場合は、デフォルトのポリシーが有効になります。デフォルトのポリシーでは、ISG はセッションの再起動の 60 秒後にセッションを接続解除し、次の設定に相当します。

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

このデフォルト ポリシーは、次の **show subscriber policy rules** コマンドの出力に表示されます。

```
Rule: internal-rule-session-restart
 Class-map: always event session-restart
  Action: 1 service disconnect delay 60
  Executed: 0
```

IP 加入者セッションのデフォルト サービス

IP セッションは、後続の加入者パケットを適切に処理するために、デフォルト サービスを必要とする場合があります。たとえば、メニュー駆動の認証やサービス選択を実行可能なキャプティブ ポータルに対して、TCP パケットを許可または強制する場合などがあります。IP セッションに対してデフォルトのサービス ポリシー マップまたはサービス プロファイルを設定して、トラフィックをリダイレクトしたり、セッション ID のための Port-Bundle ホストキー機能をイネーブルにしたり、透過的な自動ログインをイネーブルにできます。

また、デフォルト サービスにはネットワーク サービスも含まれることがあり、加入者が Web ポータルにアクセスし、認証とサービス選択を行えるようになります。

IP 加入者セッションのための ISG の設定方法

ISG レイヤ 3 アクセスを設定するには、次の作業を実行します。

- 「IP 加入者用の ISG セッションの作成」（P.83）（必須）
- 「DHCP を使用した ISG 加入者 IP アドレスの管理」（P.95）（必須）
- 「ISG ダイナミック VPN 選択の設定」（P.103）（必須）
- 「DHCP サーバの IP アドレスの設定」（P.102）（必須）

IP 加入者用の ISG セッションの作成

ISG は、加入者側インターフェイスの IP トラフィック用の IP セッションを作成します。

（注） Cisco 7600 ルータの場合、ISG IP セッションは、アクセス サブインターフェイス上と非アクセス サブインターフェイス上の両方で設定できます。

次の作業では、インターフェイス上で IP セッションをイネーブルにし、セッションを識別する方法を示します。

- 「ルーテッド ISG 加入者用の IP 加入者セッションの作成」（P.84）（必須）
- 「レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成」（P.86）（必須）
- 「ISG IP インターフェイス セッションの作成」（P.87）（必須）
- 「ISG スタティック セッションの作成」（P.88）（必須）
- 「ISG IP サブネット セッションの作成」（P.90）（必須）
- 「DHCP-Initiated IP セッションのための IP セッション回復の設定」（P.91）（必須）
- 「ISG IP 加入者セッションの確認」（P.93）（任意）
- 「ISG IP 加入者セッションのクリア」（P.94）（任意）

ルーテッド ISG 加入者用の IP 加入者セッションの作成

ルーテッド IP 加入者とは、ISG に達する前に、少なくとも 1 台の中継ルータがあるレイヤ 3 アクセス ネットワークを通じてルーティングされる加入者です。ルーテッド IP 加入者用の IP セッションを作成するよう ISG 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. **interface** *type number*

   または

   interface *type number* **access**
4. **ip subscriber routed**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**}
6. **end**

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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	インターフェイスを指定し、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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber routed** 例： `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。
ステップ 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address**} 例： `Router(config-subscriber)# initiator dhcp class-aware`	指定されたパケット タイプの受信時に IP 加入者セッションを作成するよう、ISG を設定します。 • **dhcp**：ISG は、DHCP DISCOVER パケットを受信すると IP セッションを開始します。**class-aware** キーワードで DHCP にクラス名を提供することにより、ISG は、HDCP によって割り当てられる IP アドレスに影響を与えることができます。 • **radius-proxy**：ISG は、RADIUS Access-Request パケットを受信すると IP セッションを開始します。 **（注）** RADIUS プロキシ機能は、Cisco 7600 ルータ上ではサポートされません。 • **unclassified ip-address**：ISG は、未分類の IP 発信元アドレスを持つ最初の IP パケットを受信すると IP セッションを開始します。 • このコマンドを複数回入力すると、IP セッションの開始方法を複数指定できます。 **（注）** クライアント IP アドレスの割り当てで、ISG デバイスが DHCP リレーまたは DHCP サーバのどちらかとして機能する場合は、DHCP DISCOVER パケットの受信時に IP セッションを開始するよう、ISG を設定する必要があります。**initiator unclassified ip** コマンド、または **initiator unclassified mac** コマンドではなく、**initiator dhcp** コマンドを設定する必要があります。
ステップ 6	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成

レイヤ 2 接続された加入者は、ISG の物理インターフェイスに直接接続されるか、またはブリッジ型ネットワークやスイッチド ネットワークなどのレイヤ 2 アクセス ネットワークを通して ISG に接続されます。レイヤ 2 接続された IP 加入者用の IP セッションを作成するよう ISG 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. **interface** *type number*
   または
   interface *type number* **access**
4. **ip subscriber l2-connected**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
6. **arp ignore local**
7. **end**

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	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	インターフェイスを指定し、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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber l2-connected** 例： `Router(config-if)# ip subscriber l2-connected`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。 **（注）** レイヤ 2 接続された加入者用の IP セッションの設定には、**ip subscriber l2-connected** コマンドの使用を推奨します。加入者 IP アドレスがアクセス ドメインでルーティング可能な場合、**ip subscriber routed** コマンドを使用することもできます。

	コマンドまたはアクション	目的
ステップ 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**} 例： `Router(config-subscriber)# initiator unclassified mac-address`	指定されたパケット タイプの受信時に IP 加入者セッションを作成するよう、ISG を設定します。 • **dhcp**：ISG は、DHCP DISCOVER パケットを受信すると IP セッションを開始します。**dhcp** キーワードを使用する場合は **class-aware** キーワードが必要です。 • **radius-proxy**：ISG は、RADIUS パケットを受信すると IP セッションを開始します。 （注） RADIUS プロキシ機能は、Cisco 7600 ルータ上ではサポートされません。 • **unclassified mac-address**：ISG は、未分類の MAC 発信元アドレスを持つ最初の IP パケットを受信すると IP セッションを開始します。 • このコマンドを複数回入力すると、IP セッションの開始方法を複数指定できます。 （注） クライアント IP アドレスの割り当てで、ISG デバイスが DHCP リレーまたは DHCP サーバのどちらかとして機能する場合は、DHCP DISCOVER パケットの受信時に IP セッションを開始するよう、ISG を設定する必要があります。**initiator unclassified ip** コマンド、または **initiator unclassified mac** コマンドではなく、**initiator dhcp** コマンドを設定する必要があります。
ステップ 6	**arp ignore local** 例： `Router(config-subscriber)# arp ignore local`	（任意）同じインターフェイス上で、ISG が、宛先の着信 Address Resolution Protocol（ARP; アドレス解決プロトコル）要求に応答しないようにします。
ステップ 7	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP インターフェイス セッションの作成

ISG IP インターフェイス セッションは、指定されたインターフェイスまたは指定されたサブインターフェイスを通るすべての IP パケットを対象とします。ISG IP インターフェイス セッションを作成するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*[**.***subinterface-number*]
4. **ip subscriber interface**
5. **end**

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	**interface** *type number*[*.subinterface-number*] 例： `Router(config)# interface ethernet 0/0.1`	インターフェイスまたはサブインターフェイスを指定し、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 4	**ip subscriber interface** 例： `Router(config-if)# ip subscriber interface`	インターフェイス上でホストされる IP 加入者のタイプを指定します。
ステップ 5	**end** 例： `Router(config-if)# exit`	（任意）特権 EXEC モードに戻ります。

ISG スタティック セッションの作成

ISG スタティック セッション作成機能では、管理者が開始したスタティック IP セッションが可能になります。ISG スタティック セッションでは、CLI からスタティック IP セッションを設定できます。スタティック IP セッションは、サーバ アドレスのグループを設定することによって作成できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ip source** *ipaddress* **mac** *macaddress*
   または
   ip source *ipaddress* **mask** *subnetmask*
5. **exit**
6. **interface** *type number* または
   interface *type number* **access**
7. **ip subscriber l2-connected**
   または
   ip subscriber routed
8. **initiator static ip subscriber list** *list-name*
9. **end**

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	**ip subscriber list** *list-name* **例：** `Router(config)# ip subscriber list mylist`	IP 加入者リスト名を指定し、サーバ リスト 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 source** *ipaddress* **mac** *macaddress* または **ip source** *ipaddress* **mask** *subnetmask* **例：** `Router(config-server-list)# ip source 209.165.200.225 mac 0.7.f` または `Router(config-server-list)# ip source 209.165.200.225 mask 255.255.255.224`	スタティック サーバ IP アドレスおよび MAC アドレス（L2-connected の場合）、またはサブネット マスク（ルーテッドの場合）を指定します。
ステップ 5	**exit** **例：** `Router(config-server-list)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *type number* または **interface** *type number* **access** **例：** `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	インターフェイスを指定し、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。 • **access**：サブインターフェイスを指定します。
ステップ 7	**ip subscriber l2-connected** または **ip subscriber routed** **例：** `Router(config-if)# ip subscriber l2-connected` または `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。 **（注）** レイヤ 2 接続された加入者用の IP セッションの設定には、**ip subscriber l2-connected** コマンドの使用を推奨します。ただし、加入者 IP アドレスがアクセス ドメインでルーティング可能な場合、**ip subscriber routed** コマンドを使用することもできます。

	コマンドまたはアクション	目的
ステップ 8	**initiator static ip subscriber list list-name** 例： `Router(config-subscriber)# initiator static ip subscriber list mylist`	パケット タイプとして static を指定して IP 加入者セッションを作成し、セッションをリストに追加します。
ステップ 9	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP サブネット セッションの作成

IP サブネット セッションは、単一の IP サブネットに関連付けられているすべてのトラフィックを表します。IP サブネット セッションは、特定の IP サブネットに関連付けられているパケットへの均一なエッジ処理の適用に使用されます。IP サブネット セッションが設定されている場合、ISG は、そのサブネットを単一の加入者として取り扱います。これは、ISG の機能および機能性が、サブネット トラフィックに集約として適用されることを意味しています。IP サブネット セッションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
   または
   interface *type number* **access**
4. **ip subscriber routed**
5. **initiator unclassified ip-address**
6. **end**
7. Framed-IP-Netmask アトリビュートをサービスまたはユーザ プロファイルに追加します。

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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	インターフェイスを指定し、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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip subscriber routed** 例： `Router(config-if)# ip subscriber routed`	インターフェイス上でホストされる IP 加入者のタイプを指定し、ISG IP 加入者コンフィギュレーション モードを開始します。
ステップ 5	**initiator unclassified ip-address** 例： `Router(config-subscriber)# initiator unclassified ip-address`	未分類の IP 発信元アドレスを持つ IP パケットを受信すると IP 加入者セッションを作成するように、ISG を設定します。
ステップ 6	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 7	Framed-IP-Netmask アトリビュートをサービスまたはユーザ プロファイルに追加します。	加入者の IP サブネット セッションをイネーブルにします。 • 加入者が認可または認証されていて、Framed-IP-Netmask アトリビュートがユーザ プロファイルまたはサービス プロファイルに存在する場合、ISG は発信元 IP に基づくセッションを、Framed-IP-Netmask アトリビュート内のサブネット値を持つサブネット セッションに変換します。

DHCP-Initiated IP セッションのための IP セッション回復の設定

ISG がセッションを終了またはリロードした後、IP セッションの回復時に特定のアクションを実行するように ISG を設定するには、次の作業を実行します。この作業は、DHCP-Initiated IP セッションにのみ適用されます。

セッション回復のためのポリシーが設定されていない場合、ISG は次のデフォルト ポリシーを適用します。

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **end**

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 control** *policy-map-name* 例： `Router(config)# policy-map type control MY-POLICY`	制御ポリシーの定義に使用される制御ポリシー マップを作成または変更し、制御ポリシー 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	**class type control** {*control-class-name* | **always**} **event session-restart** 例： `Router(config-control-policymap)# class type control always event session-restart`	セッションの再起動時に評価される制御クラスを指定し、ポリシー マップ クラス制御コンフィギュレーション モードを開始します。 • 制御クラスが **always** のポリシー ルールは、常に制御ポリシー マップ内でプライオリティが最も低いルールとして扱われます。

	コマンドまたはアクション	目的
ステップ 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **例：** `Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`	（任意）指定された ID に基づいて、認可の要求を開始します。
ステップ 6	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}} **例：** `Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`	（任意）ISG サービスをアクティブ化します。 • サービス名の代わりに ID を指定すると、指定された ID と同じ名前のサービスがアクティブ化されます。
ステップ 7	*action-number* **set-timer** *name-of-timer minutes* **例：** `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	（任意）名前付きのポリシー タイマーを開始します。 • タイマーの期限切れによって、イベント timed-policy-expiry が生成されます。
ステップ 8	**end** **例：** `Router(config-control-policymap-class-control)# end`	（任意）特権 EXEC モードに戻ります。

ISG IP 加入者セッションの確認

IP 加入者セッションの設定と作成を確認するには、次の作業を実行します。コマンドはどの順序で実行してもかまいません。

手順の概要

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]
3. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
4. **show platform isg session-count** {**all** | *slot*}

5. **exit**

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**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **例：** `Router# show subscriber session detailed`	加入者セッションの ISG ポリシーおよび ISG 機能に関する情報を表示します。
ステップ 3	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **例：** `Router# show ip subscriber ip 10.10.10.10`	ISG IP 加入者セッションに関する情報を表示します。
ステップ 4	**show platform isg session-count** {**all** | *slot*} **例：** `Router# show platform isg session-count all`	アクティブな ISG 加入者セッション数をライン カードごとに表示します。
ステップ 5	**exit** **例：** `Router# exit`	（任意）特権 EXEC モードを終了します。

ISG IP 加入者セッションのクリア

IP 加入者セッションをクリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]
4. **exit**

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 ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **例：** `Router# show ip subscriber ip 10.10.10.10`	（任意）ISG 加入者 IP セッションに関する情報を表示します。
ステップ 3	**clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **例：** `Router# clear ip subscriber ip 10.10.10.10`	ISG IP 加入者セッションをクリアします。
ステップ 4	**exit** **例：** `Router# exit`	特権 EXEC モードを終了します。

トラブルシューティングのヒント

ISG IP 加入者セッションをトラブルシューティングするには、次のコマンドを使用します。

- **debug ip subscriber**
- **debug condition**

DHCP を使用した ISG 加入者 IP アドレスの管理

この作業を実行するには、その前に次の概念について理解しておく必要があります。

- 「DHCP を使用した ISG 加入者 IP アドレスの割り当て」（P.76）

DHCP を使用して ISG 加入者 IP アドレスを管理するには、次の作業を実行します。

- 「ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定」（P.96）（必須）
- 「DHCP サーバ ユーザ認証の設定」（P.97）（必須）
- 「サービス ポリシー マップ内の DHCP クラスの設定」（P.100）（必須）
- 「サービス プロファイルまたはユーザ プロファイル内の DHCP クラスの設定」（P.101）（必須）
- 「DHCP サーバの IP アドレスの設定」（P.102）（必須）

前提条件

ISG が DHCP を使用して IP アドレスを割り当てるためには、次の前提条件があります。

- 加入者が、レイヤ 2 接続されている。
- ISG が DHCP 要求のパス内にあり、DHCP サーバまたはリレーとして機能している。
- 該当する IP サブネットが加入者インターフェイス上で設定されている。

この作業は、ネットワーク内で DHCP が設定されていることを前提としています。

ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定

クラス名を持つローカル DHCP コンポーネントを提供することで、インターフェイス上の加入者への IP アドレスの割り当てに、ISG が影響を与えられるようにするには、次の作業を実行します。クラス名とは、**ip dhcp pool** コマンドを使用して設定されたクラスのことで、アドレスのプールまたはリレーの宛先を参照していてもかまいません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*

   または

   interface *type number* **access**
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** {**l2-connected** | **routed**}
6. **initiator dhcp class-aware**
7. **end**

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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* または **interface** *type number* **access** 例： `Router(config)# interface GigabitEthernet 1/0/0` または `Router(config)# interface GigabitEthernet 1/0/0.100 access`	設定用のインターフェイスを指定し、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。 • **access**：サブインターフェイスを指定します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 209.165.200.225 255.255.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip subscriber** {**l2-connected** | **routed**} 例： `Router(config-if)# ip subscriber l2-connected`	ISG IP 加入者コンフィギュレーション モードをイネーブルにします。
ステップ 6	**initiator dhcp class-aware** 例： `Router(config-subscriber) initiator dhcp class-aware`	DHCP DISCOVER パケットを受信したときに IP セッションを作成するよう、ISG を設定します。 • **class-aware**：DHCP にクラス名を提供することにより、ISG は、HDCP によって割り当てられる IP アドレスに影響を与えることができます。
ステップ 7	**end** 例： `Router(config-subscriber)# end`	（任意）特権 EXEC モードに戻ります。

DHCP サーバ ユーザ認証の設定

サーバ上で DHCP クライアントを認証するには、次の作業を実行します。

前提条件

DHCP サーバ ユーザ認証をイネーブルにするには、ISG フレームワークを使用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*

7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp class-aware**
11. **end**

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	**aaa new-model** 例： `Router(config)# aaa new model`	Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）をイネーブルにします。
ステップ 4	**aaa authentication login** *list-name* **local** 例： `Router(config)# aaa authentication login mylist local`	ログイン時の AAA 認証を設定します。
ステップ 5	**ip dhcp pool** *pool-name* 例： `Router(config)# ip dhcp pool testpool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。
ステップ 6	**network** *network-number mask* 例： `Router(dhcp-config)# network 172.16.0.0 255.240.0.0`	Cisco IOS DHCP サーバ上の DHCP アドレス プールのプライマリまたはセカンダリ サブネットに、ネットワーク番号とマスクを設定します。
ステップ 7	**exit** 例： `Router(dhcp-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* 例： `Router(config)# interface Ethernet 0/0`	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 9	**ip subscriber l2-connected** 例： `Router(config-if)# ip subscriber l2-connected`	インターフェイス上でレイヤ 2 接続された IP セッションを設定し、IP 加入者コンフィギュレーション モードを開始します。
ステップ 10	**initiator dhcp class-aware** 例： `Router(config-subscriber)# initiator dhcp class-aware`	DHCP によって開始された IP セッション用の、DHCP のクラスを開始します。
ステップ 11	**end** 例： `Router(config-subscriber)# end`	特権 EXEC モードに戻ります。

トラブルシューティングのヒント

debug ip dhcp server events コマンド、**debug ip dhcp server packet** コマンド、および **debug subscriber policy dpm event** コマンドを使用すると、DHCP 認証を確認できます。次に、**debug subscriber policy dpm event** コマンドの出力例を示します。

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address =
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the
SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address =
001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

また、**show subscriber session detailed** コマンドおよび **show ip dhcp binding** コマンドを使用すると、加入者情報と DHCP プール情報を表示できます。次に、**show ip dhcp binding** コマンドの出力例を示します。

```
Router# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

サービス ポリシー マップ内の DHCP クラスの設定

サービス ポリシー マップに DHCP クラスを割り当てるには、次の作業を実行します。このサービス ポリシー マップがアクティブな加入者には、DHCP プールまたはクラスに関連付けられたリモート サーバから、IP アドレスが割り当てられます。

前提条件

DHCP プールが設定されている。DHCP プール内で設定されたクラスと、サービス ポリシー マップ内で設定された DHCP クラスが一致している。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **show policy-map type service**

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-name* 例： `Router(config)# policy-map type service service1`	設定用にサービス ポリシー マップを作成するか、既存のサービス ポリシー マップを指定して、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	**classname** *class-name* 例： `Router(config-service-policymap)# classname class1`	DHCP プールをサービス ポリシー マップに関連付けます。
ステップ 5	**end** 例： `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 6	**show policy-map type service** 例： `Router# show policy-map type service`	（任意）すべてのサービス ポリシー マップの内容を表示します。 • このコマンドを使用して、DHCP クラスがサービス ポリシー マップに関連付けられていることを確認します。

次の作業

サービス ポリシー マップに DHCP アドレス プール クラスを設定後は、制御ポリシーを使用してサービスをアクティブにするなど、サービス ポリシー マップをアクティブにする方法を設定することがあります。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

サービス プロファイルまたはユーザ プロファイル内の DHCP クラスの設定

ユーザ プロファイルまたはサービス プロファイルに DHCP クラスの Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）を追加するには、次の作業を実行します。ユーザ プロファイルまたはサービス プロファイルがアクティブな加入者には、DHCP プールまたはクラスに関連付けられたリモート サーバから、IP アドレスが割り当てられます。

前提条件

DHCP アドレス プールが設定されている。DHCP アドレス プール内で設定されたクラスと、サービス プロファイルまたはユーザ プロファイル内で設定された DHCP アドレス プール クラスが一致している。

手順の概要

1. DHCP クラス アトリビュートを、ユーザ プロファイルまたはサービス プロファイルに追加します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	DHCP クラス アトリビュートを、ユーザ プロファイルまたはサービス プロファイルに追加します。 例： `26,9,1 = "subscriber:classname=class-name"`	DHCP アドレス プールをサービスまたは特定の加入者に関連付けます。

次の作業

サービス ポリシー マップまたはサービス プロファイルのアクティブ化の方法を設定できます。たとえば、サービスのアクティブ化に制御ポリシーを使用できます。サービスをアクティブにする方法については、「Configuring ISG Subscriber Services」モジュールを参照してください。

DHCP サーバの IP アドレスの設定

ネットワーク上で使用する DHCP サーバの指定、またはネットワーク上で利用可能な複数の DHCP サーバの IP アドレスの設定、およびルーテッド IP セッションの DHCP リース クエリーの指定を行うには、次の作業を実行します。

（注） DHCP リース クエリーが実行される場合、ルーテッド IP セッションに対して DHCP サーバ IP アドレスを設定する必要があります。

前提条件

- DHCP サーバが DHCP リース プロトコルをサポートしている。
- 電話機の IP アドレスが DHCP アドレス割り当てによって割り当てられている。
- トラフィックがレイヤ 3 として分類されている。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}
4. **end**

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	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}} 例： `Router(config)# ip dhcp-server query lease retries 3`	ネットワーク上で利用可能な 1 つまたは複数の DHCP サーバの IP アドレスを設定し、ルーテッド IP セッションの DHCP リース クエリーを指定します。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了します。

ISG ダイナミック VPN 選択の設定

ISG ダイナミック VPN 選択を設定するには、次の手順を実行します。

- 「マルチサービス インターフェイスの設定」（P.103）（必須）
- 「サービス ポリシー マップでの VRF の指定」（P.104）（必須）
- 「IP セッションの VRF 転送の確認」（P.105）（任意）
- 「IP セッションの VRF 転送のトラブルシューティング」（P.107）（任意）

マルチサービス インターフェイスの設定

マルチサービス インターフェイスを設定するには、次の手順を実行します。

制約事項

IP インターフェイス機能（QoS およびアクセス リストなど）は、マルチサービス インターフェイス上でサポートされません。

1 つのマルチサービス インターフェイスは、1 つの VRF だけに属すことができます。たとえば、次のような設定は機能しません。

```
interface multiservice 1
 ip vrf forwarding VRF_A
!
interface multiservice 2
 ip vrf forwarding VRF_A
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**

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。

	コマンドまたはアクション	目的
ステップ 3	**interface multiservice** *interface-number* 例： `Router(config)# interface multiservice 1`	ダイナミック VPN 選択をイネーブルにするマルチサービス インターフェイスを作成し、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 4	**ip vrf forwarding** *vrf-name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VPN VRF をインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.0.0 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。 • VPN の IP アドレスを指定します。
ステップ 6	**end** 例： `Router(config-if)# end`	（任意）特権 EXEC モードに戻ります。

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 AAA 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*
7. **end**

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。

	コマンドまたはアクション	目的
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 vrf1`	サービスを VRF に関連付けます。
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。
ステップ 7	**end** 例： `Router(config-service-policymap)# end`	（任意）特権 EXEC モードに戻ります。

IP セッションの VRF 転送の確認

IP セッションの VRF 転送を確認するには、必要に応じて次の作業手順を実行します。

手順の概要

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]]
4. **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**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]
7. **exit**

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 uid** *session-identifier* **detail** 例： Router# show subscriber session uid 4 detail	特定のセッション ID を持つ 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	**show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]] 例： Router# show ip subscriber vrf vrf1	ISG IP 加入者セッションに関する情報を表示します。
ステップ 4	**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 nativeip-vrf ip-address 209.165.200.225	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 5	**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。
ステップ 6	**show ip dhcp binding** [**ip-address**] 例： Router# show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。
ステップ 7	**exit** 例： Router# exit	特権 EXEC モードを終了します。

IP セッションの VRF 転送のトラブルシューティング

この手順のコマンドを使用すると、IP セッションの VRF 転送をトラブルシューティングできます。コマンドはどの順序で入力してもかまいません。

手順の概要

1. **debug subscriber** {**event** | **error** | **packet** | **policy** | **service**}
2. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
3. **debug subscriber policy dpm** {**error** | **event**}
4. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**debug subscriber** {**event** | **error** | **packet** | **policy** | **service**} 例： `Router# debug subscriber service`	加入者ポリシー、ポリシー サーバ イベント、およびサービスの変更に関するデバッグ メッセージを表示します。
ステップ 2	**debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**} 例： `Router# debug ip subscriber error`	サービス ゲートウェイ上で作成される IP セッションに関するデバッグ メッセージを表示します。
ステップ 3	**debug subscriber policy dpm** {**error** | **event**} 例： `Router# debug subscriber policy dpm event`	DHCP イベントに関連する、ポリシー実行についての診断情報を表示します。
ステップ 4	**debug ip dhcp server** {**events** | **packets** | **linkage** | **class**} 例： `Router# debug dhcp ip dhcp server events`	Cisco IOS DHCP サーバのデバッグをイネーブルにします。

次の作業

レイヤ 3 セッションを起動するよう ISG を設定後は、Port-Bundle Host Key 機能、未認証の加入者トラフィックのリダイレクト、または自動加入者ログインなど、加入者 ID および認可のためのポリシーを設定することがあります。ここでは、これらのポリシーを設定する手順について説明します。

- *『Configuring ISG Port-Bundle Host Key』*
- *『Redirecting Subscriber Traffic Using ISG Layer 4 Redirect』*
- *『Configuring ISG Policies for Automatic Subscriber Logon』*

IP 加入者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。

例：ISG IP インターフェイス加入者

次の例は、イーサネット インターフェイス 0/0 で IP インターフェイス セッションを設定する手順を示しています。

```
interface ethernet 0/0
 ip subscriber interface
```

例：ISG ルーテッド IP 加入者

次の例は、ルーテッド アクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/1.401 上で ISG に接続する加入者の IP セッションを作成するための、ISG の設定方法を示しています。ISG は、DHCP DISCOVER パケット、有効な着信 IP パケット、および RADIUS Access-Request パケットを受信すると、IP セッションを作成します。

```
interface GigabitEthernet 0/1.401
 ip subscriber routed
  initiator dhcp class-aware
  initiator unclassified ip-address
  initiator radius-proxy
```

例：ISG レイヤ 2 接続された IP 加入者

次の例は、レイヤ 2 接続されたアクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/1.401 上で ISG に接続する加入者用の IP セッションを作成するための、ISG の設定方法を示しています。ISG は、有効な発信元 MAC アドレスを持つ任意のフレームを受信すると、IP セッションを作成します。

```
interface Ethernet 0/0.1
 encapsulation dot1Q 100
 ip unnumbered Loopback1
 ip subscriber l2-connected
  initiator unclassified mac-address
  arp ignore local
```

例：ISG スタティック セッションの作成

次の例は、レイヤ 2 接続されたアクセス ネットワークを通じて、ギガビット イーサネット インターフェイス 0/4 で ISG に接続する加入者用のサーバ 209.165.200.225 に対して、ISG スタティック セッションを作成する方法を示しています。ISG は、有効な発信元 IP アドレスを受信するとスタティック セッションを作成します。

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 2/0/0
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

例：DHCP-Initiated セッションの回復

次の例は、VRF「FIRST」に属する加入者のセッションの再起動時に、「FIRST-SERVICE」と呼ばれるサービスに適用する ISG ポリシーを設定する方法を示しています。

```
class-map type control TEST
 match vrf FIRST

policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

例：DHCP クラス対応機能を持つ ISG インターフェイス

次の例は、DHCP Class-Aware 機能を持つギガビット イーサネット インターフェイス 1/0/0.400 を設定する方法を示しています。これで、ISG は、DHCP IP アドレス割り当てに影響を与えることができます。「SERVICE_DHCP」サービスがアクティブな場合、DHCP プール「DHCP_POOL2」がアドレスの割り当てに使用されます。その他の場合には、デフォルトのプール「DHCP_POOL1」が使用されます。

```
interface GigabitEthernet1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP_POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
```

```
ip dhcp class DHCP_CLASS2
!
policy-map type service SERVICE_DHCP
 classname DHCP_CLASS2
!
```

例：ISG の DHCP アドレス プール クラスおよびリレー動作

ここでは、ISG の DHCP アドレス プール コンフィギュレーションおよびリレー動作の例を示します。

ISG 設定と DHCP サーバの共存

次の設定例で、ISP1 社と ISP2 社は ISP です。ISP1 社は、On-Demand Address Pools（ODAP）を使用して動的に割り当てられたアドレス プールからアドレスを割り当てます。ISP2 社の顧客アドレスは、アドレス プール 10.100.0.0/16 から割り当てられます。どの ISP にも関連付けられていない顧客は、アドレス プール 10.1.0.0/16 から割り当てられたアドレスを持ち、リース時間は 10 分間に設定されます。

```
!Address pool for ISP1 customers

ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool def-pool
 network 10.100.0.0 255.255.0.0
 class isp2
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

ISG 設定と DHCP リレー エージェントの共存

次の設定例には、「poolA」と「poolB」という 2 つの ISP があります。「poolA」ISP とその顧客は、10.1.0.0/16 から 10.3.0.0/16 の範囲のアドレスを持つことができ、10.55.10.1 の DHCP サーバにリレーされます。「poolB」ISP とそのカスタマーは、10.2.0.0/16 から 10.4.0.0/16 の範囲のアドレスを持つことができ、10.10.2.1 の DHCP サーバにリレーされます。

```
!Address ranges:

interface ethernet1
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary

interface ethernet2
 ip address 10.3.0.0 255.255.0.0
 ip address 10.4.0.0 255.255.0.0

!Address pools for poolA1 and poolA2:
 ip dhcp pool poolA1
 relay source 10.1.0.0 255.255.0.0
 class poolA1
 relay target 10.55.10.1

!Address pool for poolA2:
```

```
ip dhcp pool poolA2
 relay source 10.3.0.0 255.255.0.0
 class poolA2
 relay target 10.55.10.1

!Address pools for poolB1 and poolB2:

ip dhcp pool poolB1
 relay source 10.2.0.0 255.255.0.0
 class poolB1
 relay target 10.10.2.1

ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

リレー用のセキュア ARP の設定では、アドレス プール コンフィギュレーション モードで **update arp** コマンドを使用して、セキュア ARP がすでに DHCP サーバ上で使用したものと同じコンフィギュレーション コマンドが使用されます。システムがこのアドレス プールからアドレスを割り当てる場合は、セキュア ARP が追加されます。システムがこのアドレス プールを使用してパケットをリレーする場合も、セキュア ARP が追加されます。

例：ダイナミック VPN 選択

次の例は、加入者が DHCP グローバル プール「DHCP_POOL1」から、IP アドレスを最初に割り当てられる場合の設定を示しています。加入者が Web ポータルにアクセスして「CorporateVPN」サービスを選択後、ISG が VRF 転送を実行し、加入者は DHCP プール「VPN_POOL1」から新しい IP アドレスを割り当てられます。この場合、単一のマルチサービス インターフェイスが必要です。

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP_POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
 class default
!
ip dhcp class default
!
!
```

```
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN_POOL1
 vrf VPN_406_1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30

class DHCP_CLASS_VPN_406_1001

!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

その他の参考資料

ここでは、IP 加入者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
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
ISG コマンド	『*Cisco IOS Intelligent Services Gateway Command Reference*』
DHCP の設定	『*Cisco IOS IP Addressing Configuration Guide*』の「*DHCP*」
ISG 制御ポリシー	『*Cisco IOS Intelligent Services Gateway Configuration Guide*』の「Configuring ISG Control Policies」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

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/cisco/web/support/index.html

IP 加入者セッションのための ISG アクセス の機能情報

表 8 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。

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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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 8 には、一連のソフトウェア 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 8　IP 加入者セッションのための ISG アクセスの機能情報

機能名	リリース	機能情報
DHCP サーバ ユーザ認証	12.2(33)SRE 15.0(1)S	DHCP サーバ ユーザ認証機能は、DHCP クライアントを認証するために使用されます。 Cisco IOS Release 12.2(33)SRE では、サポートに Cisco 7600 ルータのサポートが追加されました。 この機能に関する詳細については、次の項を参照してください。 • 「DHCP サーバ ユーザ認証の設定」（P.97）
DHCP-Initiated IP セッションの IP セッション回復	12.2(31)SB 12.2(33)SRC2	ISG によって、デフォルト ポリシーが提供され、DHCP-Initiated IP セッションの回復後のセッション再起動時に、ISG が行うアクションを決定するポリシーを設定できるようになります。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「DHCP-Initiated IP セッションの IP セッション回復」（P.83） • 「DHCP-Initiated IP セッションのための IP セッション回復の設定」（P.91） この機能によって、次のコマンドが導入または変更されました。**class type control**、**match vrf**

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
IP 加入者セッションの CLI アップデート	12.2(31)SB2 12.2(33)SRC	ISG IP 加入者セッションを設定するために使用するコマンドの一部が、変更または置き換えられました。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 この機能に関する詳細については、次の項を参照してください。 • 「IP 加入者セッションのための ISG の設定方法」（P.83） この機能によって、次のコマンドが導入または変更されました。**clear ip subscriber**、**debug ip subscriber**、**identifier interface**、**identifier ip src-addr**、**initiator**、**interface multiservice**、**ip subscriber interface**、**ip subscriber**、**show ip subscriber**
ISG：装置：DHCP リース クエリー サポート	12.2(33)SRE 12.2(33)XNE	DHCP リース クエリー トランザクションとは、特殊なメッセージ タイプがある DHCP トランザクションです。これにより、クライアントは、IP アドレスの所有者とリース有効期間に関して DHCP サーバに問い合わせることなどができます。 Cisco IOS Release 12.2(33)XNE では、Cisco 10000 シリーズ ルータのサポートが追加されました。 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。 • 「IP 加入者 ID」（P.76） • 「DHCP サーバの IP アドレスの設定」（P.102）
ISG：セッション：作成：インターフェイス IP セッション：L2	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「ISG IP インターフェイス セッションの作成」（P.87）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：作成：インターフェイス IP セッション：L3	12.2(28)SB 12.2(33)SRC 12.2SRE	ISG IP インターフェイス セッションには、特定の物理インターフェイスまたは仮想インターフェイスで受信されるすべての IP トラフィックが含まれます。IP インターフェイス セッションは、CLI を通じてプロビジョニングされるため、セッションは、IP インターフェイス セッション コマンドを入力したときに作成されます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「ISG IP インターフェイス セッションの作成」（P.87）
ISG：セッション：作成：IP セッション：プロトコル イベント（DHCP）	12.2(28)SB 12.2(33)SRC	ほとんどの ISG セッションは、すでにアクティブなセッションに関連付けられないデータ フローの検出時に作成されます。ISG は、加入者から最初の DHCP DISCOVER パケットを受信したときに、IP セッションを作成するように設定できます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L2	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：作成：IP セッション：サブネットおよび発信元 IP：L3	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フロー間でサービスとポリシーを関連付けるために使用される主要なコンポーネントです。IP サブネット セッションとは、単一の IP サブネットからの IP トラフィックを含む ISG セッションです。発信元 IP セッションには、単一の発信元 IP アドレスからのトラフィックが含まれます。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：セッション：マルチキャスト：共存	12.2(33)SRE	ISG セッション マルチキャスト共存機能では、Cisco 7600 シリーズ ルータの同じサブインターフェイス上でマルチキャストおよび IP セッションが共存できるようにして、同じ VLAN 上ですべての加入者とサービス（データとマルチキャスト）をホストする機能が導入されます。 Cisco IOS Release 12.2(33)SRE では、サポートに Cisco 7600 ルータのサポートが追加されました。 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。 • 「マルチキャスト セッションと IP セッションの共存」（P.72） • 「ルーテッド ISG 加入者用の IP 加入者セッションの作成」（P.84） • 「レイヤ 2 接続された ISG 加入者用の IP 加入者セッションの作成」（P.86） • 「ISG IP サブネット セッションの作成」（P.90） • 「ダイナミック DHCP クラス アソシエーションのための ISG インターフェイスの設定」（P.96）

表 8　IP 加入者セッションのための ISG アクセスの機能情報 （続き）

機能名	リリース	機能情報
ISG：セッション：VRF 転送：	12.2(28)SB 12.2(33)SRC	ISG セッションは、特定のデータ フローでサービスとポリシーを関連付けるために使用される主要なコンポーネントです。ネットワーク サービスのためにルーティングが必要な場合、ISG セッションは、Virtual Routing and Forwarding（VRF）インスタンスに関連付けられます。ISG VRF 転送は、仮想ルーティング ドメイン間でアクティブ セッションを動的に切り替える手段を提供します。 Cisco IOS Release 12.2(33)SRC では、Cisco 7600 ルータのサポートが追加されました。 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。 • 「IP 加入者セッションのための ISG アクセスに関する情報」（P.71） • 「IP 加入者セッションのための ISG の設定方法」（P.83）
ISG：スタティック セッションの作成	12.2(33)SRE 12.2(33)XNE	ISG スタティック セッション作成機能では、管理者が開始したスタティック IP セッションが可能になります。 Cisco IOS Release 12.2(33)SRE では、サポートに Cisco 7600 ルータのサポートが追加されました。 Cisco IOS Release 12.2(33)XNE では、Cisco 10000 シリーズ ルータのサポートが追加されました。 この機能に関する詳細については、次の項を参照してください。 • 「ISG スタティック セッションの作成」（P.88） この機能によって、次のコマンドが導入または変更されました。**initiator static subscriber list**、**ip source**、**ip subscriber list**、**show ip subscriber static list**
CoA クライアントに対する VRF-Aware サポート	12.2(31)SB12	1 台の CoA クライアントが、異なる VRF の ISG 加入者をサポートできます。