Per VRF AAA

Per VRF AAA 機能により、ISP は、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サービスを Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスに基づいて区分して、カスタマーに独自の AAA サービスの一部を制御させることができます。

サーバ グループのサーバ リストは、グローバル コンフィギュレーションでのホストへの参照に加えて、プライベート サーバの定義を含めるために拡張されています。このため、カスタマー サーバとグローバル サービス プロバイダーのサーバに同時にアクセスできます。

Cisco IOS Release 12.2(15)T 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。この機能は、Dynamic Per VRF AAA 機能とも呼ばれていました。

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、「Per VRF AAA の機能情報」（P.33）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。

この章の構成

Per VRF AAA の前提条件

Per VRF AAA 機能を設定する前に、AAA をイネーブルにする必要があります。詳細については、「Per VRF AAA の設定方法」（P.6）を参照してください。

Per VRF AAA の制約事項

- この機能は、RADIUS サーバについてのみサポートされています。
- すべての機能について、Network Access Server（NAS; ネットワーク アクセス サーバ）と AAA サーバとの間で一貫性が必要なため、サーバ グループごとの設定ではなく、Per VRF を設定したら、動作パラメータを定義する必要があります。
- ローカルまたはリモートでカスタマー テンプレートを設定する機能は、Cisco IOS Release 12.2(15)T 以降のリリースでのみ使用できます。

Per VRF AAA について

Per VRF AAA 機能を使用する場合、AAA サービスを VRF インスタンスに基づいたものにできます。この機能により、Provider Edge（PE; プロバイダー エッジ）または Virtual Home Gateway（VHG; 仮想ホーム ゲートウェイ）で、カスタマーの Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に関連付けられたカスタマーの RADIUS サーバと RADIUS プロキシを経由せずに直接通信できます。RADIUS プロキシを使用する必要がないため、ISP は、VPN による提供サービスをより効率的に拡張でき、カスタマーにさらに柔軟性を提供できます。

Per VRF AAA の機能

カスタマーごとに AAA をサポートするには、一部の AAA 機能をで VRF を認識させる必要があります。つまり、ISP は、AAA サーバ グループ、方式リスト、システム アカウンティング、およびプロトコル固有のパラメータなどの動作パラメータを定義し、これらのパラメータを特定の VRF インスタンスにバインドできる必要があります。動作パラメータの定義とバインディングには、次の 1 つ以上の方式が使用できます。

- Virtual Private Dial-up Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）：特定のカスタマーに設定されたに仮想テンプレートまたはダイヤラ インターフェイス。

- ローカルで定義されたカスタマー テンプレート：カスタマーの定義による Per VPN。カスタマー テンプレートは、ローカルで VHG に保存されます。この方式は、ドメイン名または Dialed Number Identification Service（DNIS; 着信番号識別サービス）に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。
- リモートで定義されたカスタマー テンプレート：RADIUS プロファイルでサービス プロバイダーの AAA サーバに保存された、カスタマーの定義による Per VPN。この方式は、ドメイン名または DNIS に基づいて、リモート ユーザを特定の VPN に関連付け、カスタマーの AAA サーバに対する仮想アクセス インターフェイスおよびすべての動作パラメータに VPN 固有の設定を提供する場合に使用できます。

（注） ローカルまたはリモートで定義されたカスタマー テンプレートを設定する機能は、Cisco IOS Release 12.2(15)T 以降のリリースでのみ使用できます。

AAA アカウンティング レコード

シスコが採用している AAA アカウンティングでは、ユーザ認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。開始レコードと終了レコードは、ユーザがアカウンティング レコードを使用してネットワークを管理およびモニタするために必要です。

新しいベンダー固有アトリビュート

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）アトリビュート 26 を使用してベンダー固有の情報を伝達する方法が規定されています。アトリビュート 26 は VSA をカプセル化します。このため、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。

シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は「cisco-av-pair」です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

「Protocol」は、特定の認可タイプを表すシスコの「protocol」アトリビュートです。「Attribute」と「value」は、シスコの TACACS+ 仕様に定義されている適切なアトリビュート値（AV）ペアで、「sep」は必須アトリビュートの場合には「=」、オプションのアトリビュートの場合に「*」を使用します。これにより、TACACS+ 認可で使用できるすべての機能を RADIUS にも使用できるようになります。

表 1 に、現在 Per VRF AAA でサポートされている VSA の概要を示します。

表 1　Per VRF AAA でサポートされる VSA

VSA 名	値の種類	説明
（注）　別の拡張子が明示的に記述されている場合を除き、各 VSA には VSA 名の前に拡張子「template:」が必要です。		
account-delay	string	この VSA は「on」にする必要があります。この VSA の機能は、カスタマー テンプレートの **aaa accounting delay-start** コマンドと同じです。
account-send-stop	string	この VSA は「on」にする必要があります。この VSA の機能は、**failure** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
account-send-success-remote	string	この VSA は「on」にする必要があります。この VSA の機能は、**success** キーワードを指定した **aaa accounting send stop-record authentication** コマンドと同じです。
attr-44	string	この VSA は「access-req」にする必要があります。この VSA の機能は、**radius-server attribute 44 include-in-access-req** コマンドと同じです。
ip-addr	string	この VSA は、IP アドレスを指定します。その後に、ルータが独自の IP アドレスを示すために使用するマスク、およびクライアントとのネゴシエーションのマスクが続きます。例：ip-addr=192.168.202.169 255.255.255.255。
ip-unnumbered	string	この VSA は、ルータ上のインターフェイスの名前を指定します。この VSA の機能は、「Loopback 0」などのインターフェイス名を指定する **ip unnumbered** コマンドと同じです。
ip-vrf	string	この VSA は､エンド ユーザのパケットに使用する VRF を指定します。この VRF 名は、**ip vrf forwarding** コマンドを使用してルータに使用する名前に一致させる必要があります。
peer-ip-pool	string	この VSA は、ピアに割り当てられるアドレスの IP アドレス プールの名前を指定します。このプールは、**ip local pool** コマンドを使用して設定するか、RADIUS 経由で自動的にダウンロード可能にする必要があります。

VSA 名	値の種類	説明
ppp-acct-list	string	この VSA は、PPP セッションに使用するアカウンティング方式リストを定義します。 VSA 構文は次のとおりです。「ppp-acct-list=[start-stop | stop-only | none] group X [group Y] [broadcast]」これは、**aaa accounting network mylist** コマンド機能と等しくなります。 ユーザは、start-stop、stop-only、または none オプションを少なくとも 1 つ指定する必要があります。start-stop または stop-only を指定した場合、ユーザは少なくとも 1 つ、ただし 4 つ以内のグループ引数を指定する必要があります。各グループ名は、整数で構成する必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。各グループが指定されると、ユーザはブロードキャストオプションを指定できます。
ppp-authen-list	string	この VSA は、PPP セッションで使用する認証方式リスト、および複数の方式が指定されている場合は、方式を使用する順序を定義します。 VSA 構文は次のとおりです。「ppp-authen-list=[groupX | local | local-case | none | if-needed]」これは、**aaa authentication ppp mylist** コマンド機能と等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認証方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。
ppp-authen-type	string	この VSA を使用すると、エンド ユーザは、pap、chap、eap、ms-chap、ms-chap-v2、any のいずれかの認証タイプ、または使用可能なタイプをスペースで区切って、少なくとも 1 つの認証タイプを指定できます。 エンド ユーザは、この VSA で指定された方式のみを使用して、ログインが許可されます。 PPP はアトリビュートで提示された順序で、これらの認証方式を試行します。
ppp-author-list	string	この VSA は、PPP セッションに使用する認可方式リストを定義します。使用する方式と順序を示します。 VSA 構文は次のとおりです。「ppp-author-list=[groupX] [local] [if-authenticated] [none]」これは、**aaa authorization network mylist** コマンド機能に等しくなります。 ユーザは少なくとも 1 つ、ただし 4 つ以内の認可方式を指定する必要があります。サーバ グループが指定されている場合、グループ名は整数である必要があります。グループ内のサーバは、VSA「rad-serv」を経由して、access-accept で識別されている必要があります。

VSA 名	値の種類	説明
（注） RADIUS VSAs—rad-serv、rad-server-filter、rad-serv-source-if、および rad-serv-vrf : VSA 名の前に拡張子「aaa:」が必要です。		
rad-serv	string	この VSA は、サーバのグループとともに、IP アドレス、キー、タイムアウト、およびサーバの再送信回数を示します。 VSA 構文は次のとおりです。「rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W]」IP アドレス以外、すべてのパラメータはオプションで、任意の順序で発行できます。オプションのパラメータが指定されていない場合、デフォルト値が使用されます。 キーにスペースを含めることはできません。「retransmit V」では「V」は、1 ～ 100 の範囲、「timeout W」では「W」は、1 ～ 1000 の範囲で指定できます。
rad-serv-filter	string	VSA 構文は次のとおりです。「rad-serv-filter=authorization | accounting-request | reply-accept | reject-filtername」フィルタ名は、**radius-server attribute list filtername** コマンドを使用して定義する必要があります。
rad-serv-source-if	string	この VSA は、RADIUS パケットの送信に使用するインターフェイスの名前を指定します。指定されたインターフェイスは、ルータ上に設定されたインターフェイスと一致する必要があります。
rad-serv-vrf	string	この VSA は、RADIUS パケットの送信に使用する VRF の名前を指定します。VRF 名は、**ip vrf forwarding** コマンドを使用して指定された名前と一致する必要があります。

Per VRF AAA の設定方法

ここでは、Per VRF AAA 機能を使用して考えられる導入シナリオに関する手順について説明します。

- 「Per VRF AAA の設定」（P.6）（必須）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の設定」（P.13）（任意）
- 「リモート カスタマー テンプレートを使用した Per VRF AAA の設定」（P.17）（任意）
- 「VRF ルーティングの設定確認」（P.20）（任意）
- 「Per VRF AAA 設定のトラブルシューティング」（P.21）（任意）

Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「AAA の設定」（P.7）
- 「サーバ グループの設定」（P.7）
- 「Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.8）

- 「Per VRF AAA の RADIUS 固有のコマンドの設定」（P.11）
- 「Per VRF AAA のインターフェイス固有のコマンドの設定」（P.12）

AAA の設定

AAA をイネーブルにするには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ip vrf default**

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`	AAA をグローバルにイネーブルにします。
ステップ 4	**ip vrf default** **例：** `Router(config)# ip vrf default`	デフォルトの VRF 名が設定されるまで、デフォルトの VRF 名がヌル値になるように、このコマンドは、**radius-server domain-stripping** コマンドなどの VRF 関連の AAA コマンドを設定する前に設定する必要があります。

サーバ グループの設定

サーバ グループを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *groupname*
5. **server-private** *ip-address* [**auth-port port-number** | **acct-port port-number**] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

6. **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	**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`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa group server radius** *groupname* **例：** `Router(config)# aaa group server radius v2.44.com`	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。server-group 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	**server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **例：** `Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 **（注）** プライベート サーバ パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。
ステップ 6	**exit** **例：** `Router(config-sg-radius)# exit`	server-group 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 モードに戻ります。

Per VRF AAA の認証、認可、およびアカウンティングの設定

Per VRF AAA の認証、認可、およびアカウンティングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2...*]
6. **aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*

7. **aaa accounting delay-start** [**vrf** *vrf-name*]
8. **aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**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	**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`	AAA をグローバルにイネーブルにします。
ステップ 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...] **例：** `Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com`	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の AAA 認証方式を指定します。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} *method1* [*method2*...] **例：** `Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 6	**aaa accounting system default** [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **例：** `Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com`	課金、または RADIUS を使用する際のセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。 **（注）** **stop-only** キーワードは、Cisco IOS Release 12.4(24)T 以降のリリースでは使用できません。

	コマンドまたはアクション	目的
ステップ 7	**aaa accounting delay-start** [**vrf** *vrf-name*] **例：** `Router(config)# aaa acounting delay-start vrf v2.44.com`	ユーザの IP アドレスが確立されるまで、アカウンティング開始レコードの生成を表示します。
ステップ 8	**aaa accounting send stop-record authentication** {**failure** | **success remote-server**} [**vrf** *vrf-name*] **例：** `Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com`	アカウンティング終了レコードを生成します。 **failure** キーワードを使用すると、認証中に拒否されたコールに対する「終了」レコードが送信されます。 **success** キーワードを使用すると、次のいずれかの基準を満たすコールに対して、「終了」レコードが送信されます。 • コールが終了したときに、リモート AAA サーバによって認証されるコール。 • リモート AAA サーバによって認証されず、開始レコードが送信されたコール。 • 正常に確立され、「stop-only」**aaa accounting** 設定で終了したコール。 **（注）** **success** および **remote-server** キーワードは、Cisco IOS Release 12.4(2)T 以降のリリースで使用できます。 **（注）** **success** および **remote-server** キーワードは、Cisco IOS Release 12.2SX では使用できません。

Per VRF AAA の RADIUS 固有のコマンドの設定

Per VRF AAA の RADIUS 固有のコマンドを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**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	**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 radius source-interface** *subinterface-name* [**vrf** *vrf-name*] **例：** `Router(config)# ip radius source-interface loopback55`	すべての発信 RADIUS パケットに対して、RADIUS に指定されたインターフェイスの IP アドレスを強制的に使用させ、Per VRF に基づいて仕様をイネーブルにします。
ステップ 4	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] **例：** `Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com`	ユーザ認証前に、アクセス要求パケットで、RADIUS アトリビュート 44 を送信し、Per VRF に基づいて仕様を有効にします。

Per VRF AAA のインターフェイス固有のコマンドの設定

Per VRF AAA でインターフェイス固有のコマンドを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2...*]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
8. **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	**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* [*name-tag*] **例：** `Router(config)# interface loopback11`	インターフェイス タイプを設定し、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 vrf forwarding** *vrf-name* **例：** `Router(config-if)# ip vrf forwarding v2.44.com`	インターフェイスと VRF を関連付けます。
ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]} *listname* **例：** `Router(config-if)# ppp authentication chap callin V2_44_com`	Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）および Password Authentication Protocol（PAP; パスワード認証プロトコル）または両方をイネーブルにし、インターフェイス上で、CHAP または PAP 認証が選択される順序を指定します。
ステップ 6	**ppp authorization** *list-name* **例：** `Router(config-if)# ppp authorization V2_44_com`	選択したインターフェイスで、AAA 認可をイネーブルにします。
ステップ 7	**ppp accounting default** **例：** `Router(config-if)# ppp accounting default`	選択したインターフェイスで、AAA アカウンティング サービスをイネーブルにします。
ステップ 8	**exit** **例：** `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「ローカル カスタマー テンプレートを使用した AAA の設定」（P.14）
- 「ローカル カスタマー テンプレートを使用したサーバ グループの設定」（P.14）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.14）
- 「ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定」（P.14）
- 「ローカル カスタマー テンプレートの設定」（P.14）

ローカル カスタマー テンプレートを使用した AAA の設定

「AAA の設定」（P.7）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用したサーバ グループの設定

「サーバ グループの設定」（P.7）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認証、認可、およびアカウンティングの設定

「Per VRF AAA の認証、認可、およびアカウンティングの設定」（P.8）で説明する作業を実行します。

ローカル カスタマー テンプレートを使用した Per VRF AAA の認可の設定

ローカル テンプレートを使用して Per VRF AAA の認可を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

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 authorization template** **例：** `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization network default local** **例：** `Router(config)# aaa authorization network default local`	ローカルを認可のデフォルト方式として指定します。

ローカル カスタマー テンプレートの設定

ローカル カスタマー テンプレートを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**]
5. **peer default ip address pool** *pool-name*
6. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **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	**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	**vpdn search-order domain** **例：** `Router (config)# vpdn search-order domain`	ドメインに基づいてプロファイルを検索します。
ステップ 4	**template** *name* [**default** | **exit** | **multilink** | **no** | **peer** | **ppp**] **例：** `Router (config)# template v2.44.com`	カスタマー プロファイル テンプレートを作成し、受信先のカスタマーに関連する一意の名前を割り当てます。 テンプレート コンフィギュレーション モードを開始します。 **（注）** ステップ 5、6、および 7 はオプションです。カスタマー アプリケーション要件に適した **multilink**、**peer**、および **ppp** キーワードを入力します。
ステップ 5	**peer default ip address pool** *pool-name* **例：** `Router(config-template)# peer default ip address pool v2_44_com_pool`	（任意）このテンプレートの添付先のカスタマー プロファイルが、指定した名前のローカル IP アドレス プールを使用するように指定します。
ステップ 6	**ppp authentication** {*protocol1* [*protocol2*...]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **例：** `Router(config-template)# ppp authentication chap`	（任意）PPP リンク認証方式を設定します。
ステップ 7	**ppp authorization** [**default** | *list-name*] **例：** `Router(config-template)# ppp authorization v2_44_com`	（任意）PPP リンク認可方式を設定します。

	コマンドまたはアクション	目的
ステップ 8	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **例：** `Router(config-template)# aaa accounting v2_44_com`	（任意）指定したカスタマー プロファイルで、AAA 動作パラメータをイネーブルにします。
ステップ 9	**exit** **例：** `Router(config-template)# exit`	テンプレート 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 モードに戻ります。

リモート カスタマー テンプレートを使用した Per VRF AAA の設定

ここでは、次の各手順について説明します。

- 「リモート カスタマー テンプレートを使用した AAA の設定」（P.18）
- 「サーバ グループの設定」（P.18）

リモート カスタマー テンプレートを使用した AAA の設定

「AAA の設定」（P.7）で説明する作業を実行します。

サーバ グループの設定

「サーバ グループの設定」（P.7）で説明する作業を実行します。

リモート カスタマー テンプレートを使用した Per VRF AAA の認証の設定

リモート カスタマー テンプレートを使用して Per VRF AAA の認証を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

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 authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **例：** `Router(config)# ppp authentication ppp default group radius`	PPP を実行するシリアル インターフェイス上で使用する 1 つ以上の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）認証方式を指定します。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*] **例：** `Router(config)# aaa authorization network default group sp`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。

リモート カスタマー テンプレートを使用した Per VRF AAA の認可の設定

リモート カスタマー テンプレートを使用して Per VRF AAA の認可を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]

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 authorization template** **例：** `Router(config)# aaa authorization template`	ローカルまたはリモート テンプレートの使用をイネーブルにします。
ステップ 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2*...] **例：** `Router(config)# aaa authorization network default sp`	認可のデフォルト方式として指定されたサーバ グループを指定します。

SP RADIUS サーバ上の RADIUS プロファイルの設定

RADIUS プロファイルのアップデート方法の例については、「リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA：例」（P.23）を参照してください。

VRF ルーティングの設定確認

VRF ルーティングの設定確認には、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **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	**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	**show ip route vrf** *vrf-name* **例：** `Router(config)# show ip route vrf northvrf`	VRF に関連付けられた IP ルーティング テーブルを表示します。

Per VRF AAA 設定のトラブルシューティング

Per VRF AAA 機能のトラブルシューティングを行う場合は、EXEC モードで次のコマンドを少なくとも 1 つ使用します。

コマンド	目的
`Router#` **debug aaa accounting**	説明の義務があるイベントが発生したときに、その情報を表示します。
`Router#` **debug aaa authentication**	AAA 認証に関する情報を表示します。
`Router#` **debug aaa authorization**	AAA 認証に関する情報を表示します。
`Router#` **debug ppp negotiation**	PPP を実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
`Router#` **debug radius**	RADIUS 関連の情報を表示します。
`Router#` **debug vpdn event**	VPN の通常のトンネルの確立、またはシャットダウンの一部である Layer 2 Transport Protocol（L2TP; レイヤ 2 プロトコル）のエラーおよびイベントを表示します。
`Router#` **debug vpdn error**	VPN のデバッグ トレースを表示します。

Per VRF AAA の設定例

ここでは、次の設定例について説明します。

- 「Per VRF の設定：例」（P.22）
- 「カスタマー テンプレート：例」（P.23）
- 「AAA アカウンティング終了レコード：例」（P.25）

Per VRF の設定：例

ここでは、次の設定例について説明します。

Per VRF AAA：例

次に、関連付けられたプライベート サーバで AAA サーバ グループを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model

aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com

aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com

ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

ローカルで定義されたカスタマー テンプレートを使用した Per VRF AAA：例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、ローカルで定義されたカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com

aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
  ip vrf forwarding V1.55.com

template V1.55.com
  peer default ip address pool V1_55_com_pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req
  ip vrf forwarding v1.55.com
  ip radius source-interface Loopback55
```

リモート RADIUS カスタマー テンプレートを使用した Per VRF AAA：例

次に、関連付けられたプライベート サーバのある AAA サーバ グループで、SP RADIUS サーバ上にリモートで定義したカスタマー テンプレートを使用して Per VRF AAA 機能を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp

aaa group server radius sp
   server 10.3.3.3

radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

次の RADIUS サーバ プロファイルは、SP RADIUS サーバ上で設定されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

カスタマー テンプレート：例

ここでは、次の設定例について説明します。

- 「RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレート：例」（P.23）
- 「RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレート：例」（P.24）

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してローカルで設定されたカスタマー テンプレート：例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにローカルで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server

aaa group server radius SP_AAA_server
 server 10.10.100.7 auth-port 1645 acct-port 1646
```

```
aaa group server radius V1_55_com
 server-private 10.10.132.4 auth-port 1645 acct-port 1646
 authorization accept min-author
 accounting accept usage-only
 ip vrf forwarding V1.55.com

ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55

template V1.55.com
 peer default ip address pool V1.55-pool
 ppp authentication chap callin V1_55_com
 ppp authorization V1_55_com
 ppp accounting V1_55_com
 aaa accounting delay-start
 aaa accounting send stop-record authentication failure
 radius-server attribute 44 include-in-access-req

vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41

interface Virtual-Template13
 ip vrf forwarding V1.55.com
 ip unnumbered Loopback55
 ppp authentication chap callin
 ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com

radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46

radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww
```

RADIUS Attribute Screening およびブロードキャスト アカウンティングを使用してリモートで設定されたカスタマー テンプレート：例

次に、RADIUS Attribute Screening およびブロードキャスト アカウンティングを含む追加機能を設定する、単一のカスタマー向けにリモートで設定されたテンプレートを作成する方法の例を示します。

```
aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius

ip vrf V1.55.com
 rd 1:55
 route-target export 1:55
 route-target import 1:55
```

```
vpdn-group V1.55
 accept-dialin
  protocol l2tp
  virtual-template 13
 terminate-from hostname lac-lb-V1.55
 source-ip 10.10.104.12
 lcp renegotiation always
 l2tp tunnel password 7 060506324F41

interface Virtual-Template13
 no ip address
 ppp authentication chap callin
 ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

radius-server attribute list min-author
 attribute 6-7,22,27-28,242
radius-server attribute list usage-only
 attribute 1,40,42-43,46
```

カスタマー テンプレートは、v1.55.com の RADIUS サーバ プロファイルとして保存されます。

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

AAA アカウンティング終了レコード：例

次に、**start-stop** または **stop-only** キーワードを指定して **aaa accounting** コマンドを発行したときに、「終了」レコードの生成を制御する **aaa accounting send stop-record authentication** コマンドを設定する方法を示す、AAA アカウンティング終了レコードの例を示します。

（注） **success** および **remote-server** キーワードは、Cisco IOS Release 12.4(2)T 以降のリリースで使用できます。

ここでは、次の設定例について説明します。

- 「AAA アカウンティング終了レコードと成功したコール：例」（P.26）
- 「AAA アカウンティング終了レコードと拒否されたコール：例」（P.28）

AAA アカウンティング終了レコードと成功したコール：例

次に、**aaa accounting send stop-record authentication** コマンドを **failure** キーワードを指定して発行した場合に、成功したコールに関する「開始」および「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
```

```
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
```

```
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

AAA アカウンティング終了レコードと拒否されたコール：例

次に、**aaa accounting send stop-record authentication** コマンドを **success** キーワードを指定して発行した場合に、認証中に拒否されたコールに関する「終了」レコードが送信されている例を示します。

```
Router# show running-config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius

Router#

*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
```

```
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=10.0.0.2"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
```

```
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "10.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "10.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@example.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                    [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                  [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

その他の参考資料

ここでは、Per VRF AAA 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
AAA：サーバ グループの設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Cisco IOS Switching Services コマンド	『*Cisco IOS IP Switching Command Reference*』
Multiprotocol Label Switching の設定	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4T』
仮想テンプレートの設定	『*Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T』の「Virtual Templates, Profiles, and Networks」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によ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。	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
この機能によってサポートされる新しい RFC や変更された RFC はありません。	—

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/techsupport

Per VRF AAA の機能情報

表 2 に、この機能のリリース履歴を示します。

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。

Cisco Feature Navigator を使用すると、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できます。Cisco Feature Navigator を使用すると、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サポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 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 2　Per VRF AAA の機能情報

機能名	リリース	機能情報
Per VRF AAA Dynamic Per VRF AAA Attribute Filtering Per-Domain and VRF Aware Framed-Routes RADIUS Per-VRF サーバ グループ	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(13)T 12.2(15)T 12.4(2)T 12.2(28)SB 12.2(33)SR 12.2(33)SXI 12.2(33)SXH4	Per VRF AAA 機能により、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスに基づいた、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）が行えます。Cisco IOS Release 12.2(15)T 以降のリリースでは、ローカルまたはリモートで保存したカスタマー テンプレートを使用し、カスタマー テンプレートに保存された情報に基づいて、AAA サービスを実行できます。 12.2(1)DX には、Cisco 7200 シリーズおよび Cisco 7401ASR に Per VRF AAA 機能が導入されています。 12.2(2)DD には、**ip vrf forwarding（server-group）**および **radius-server domain-stripping** コマンドが追加されています。 Per VRF AAA、Dynamic Per VRF AAA、および Attribute Filtering Per-Domain and VRF Aware Framed-Routes 機能は、Cisco IOS Release 12.2(15)T に導入されています。このリリースには、**aaa authorization template** コマンドも追加されています。 12.4(2)T では、**aaa accounting send stop-record authentication** コマンドが AAA アカウンティング終了レコードへの追加サポートでアップデートされました。 12.2(33)SRC には、RADIUS Per-VRF Server Group 機能が追加されました。 Cisco IOS Release 12.2(33)SXI には、これらの機能が導入されました。 Cisco IOS Release 12.2(33)SXH4 には、これらの機能が導入されました。 この機能により、次のコマンドが導入または変更されました。**aaa accounting**、**aaa accounting delay-start**、**ip radius source-interface**、**radius-server attribute 44 include-in-access-req**、**server-private（RADIUS）**

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモート アクセス コントロール（認可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

L2TP：Layer 2 Tunnel Protocol（レイヤ 2 トンネル プロトコル）。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

PE：プロバイダー エッジ。サービス プロバイダー ネットワークのエッジ上のネットワーキング デバイス。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：Virtual Private Network（VPN; バーチャル プライベート ネットワーク）。リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。

VRF：Virtual Route Forwarding。最初は、ルータにグローバルのデフォルト ルーティング / フォワーディング テーブルは 1 つしかありません。VRF は、複数の分離されたルーティング / フォワーディング テーブルとして表示でき、ユーザのルートには別のユーザのルートとの相互関係はありません。
