



DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 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。DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon 機能を使用すると、サービス プロバイダーは Dynamic Host Configuration Protocol (DHCP) オプション 60 およびオプション 82 によって Transparent Automatic Logon (TAL) をサポートでき、オプション 82 への Virtual Private Network (VPN; バーチャル プライベート ネットワーク) ID 拡張によってホールセール型の IP セッションをサポートできるため、家庭向けのトリプルプレイ サービスをプロビジョニングできるようになります。

この機能はプラットフォームに依存せず、Cisco 7600 ルータ、Cisco 7200 ルータ、および Cisco 7301 ルータでサポートされます。

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、「[DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の機能情報](#)」(P.197) 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

- 「[DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の前提条件](#)」(P.190)
- 「[DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の制約事項](#)」(P.190)

- 「DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定方法」 (P.191)
- 「DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定例」 (P.195)
- 「その他の参考資料」 (P.195)
- 「DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の機能情報」 (P.197)

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の前提条件

認可に使用されるベンダー クラス ID (オプション 60) には、カスタマーのアプライアンス (PC、電話機、またはセットトップ ボックス) によってベンダー クラス ID を DHCP オプション 60 の情報に挿入する必要があります。

ホールセール型 IP セッションのプロビジョニングでは、VPN-ID を回線 ID およびリモート ID と一緒に DHCP オプション 82 の情報に挿入する必要があります。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の制約事項

RADIUS プロキシ ユーザは、この機能でサポートされません。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon に関する情報

- 「ISA Automatic Subscriber Logon」 (P.190)
- 「オプション 60 およびオプション 82 に基づく認可」 (P.191)
- 「DHCP オプション 82 および VPN-ID サブオプション」 (P.191)

ISA Automatic Subscriber Logon

TAL を使用すると、指定された ID を認可要求でユーザ名の代わりに使用できます。Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) サーバによる指定された IP に基づく加入者の認可をイネーブるにすると、加入者からのパケットが受信されるとすぐに、AAA サーバから加入者のプロフィールをダウンロードできます。

セッションの開始は、TAL をトリガーするイベントです。DHCP で開始された IP セッションの場合、DHCP DISCOVER 要求の受信時にセッションが開始されます。

オプション 60 およびオプション 82 に基づく認可

回線 ID およびリモート ID フィールド (オプション 82) は、DHCP リレー エージェント情報オプションの一部です。Digital Subscriber Line Access Multiplexer (DSLAM; デジタル加入者線アクセス マルチプレクサ) は、オプション 82 のフィールドを DHCP メッセージに挿入し、カスタマーのアプライアンスはオプション 60 のフィールドを挿入します。

認可要求でユーザ名として回線 ID、リモート ID、またはベンダー クラス ID、あるいはこれらの組み合わせを使用するように ISG ポリシーを設定できます。また、NAS-Port-ID を認可の ID として使用するように ISG ポリシーを設定することもできます。NAS-Port-ID を ID として使用する場合、回線 ID、リモート ID、およびベンダー クラス ID の組み合わせを含めるように設定できます。

デフォルトでは、ISG でレイヤ 2 エッジ アクセス デバイスによって認可のために指定される回線 ID とリモート ID を使用します。ip dhcp relay information option コマンドの設定によって、ISG が受信したオプション 82 の情報を使用して独自に情報を生成するか、または (encapsulate キーワードが指定されている場合に) 以前のオプション 82 を独自のオプション 82 と一緒にカプセル化するかが指定されます。詳細については、『Cisco IOS IP Addressing Services Configuration Guide』の「Configuring the Cisco IOS DHCP Relay Agent」を参照してください。

オプション 60 およびオプション 82 を含めるように NAS-Port-ID が設定されていない場合、NAS-Port-ID が DHCP リレー エージェント情報パケットを受信した ISG インターフェイス (たとえば、Ethernet1/0) で入力されます。

DHCP オプション 82 および VPN-ID サブオプション

IP セッションのホールセール サービスをサポートするには、認可要求で VPN-ID を回線 ID およびリモート ID と一緒に指定する必要があります。Transparent Automatic Logon 機能用の VPN-ID サポート付き DHCP オプション 60 およびオプション 82 では、家庭内のデバイスを差別化できるように、2 セットのオプション 82 の情報を 1 つのメッセージに含めることができます。

- オプション 82 の情報の 1 番目のセットには、家庭内のデバイスに関連付ける家庭の情報とオプション 60 が含まれます。
- オプション 82 の情報の 2 番目のセットには、VPN-ID が設定されている場合、家庭の VPN 情報が含まれます。

DHCP サーバは、VPN-ID、リモート ID、回線 ID、およびアドレスを割り当てるためのオプション 60 の情報とともに、リレーによって転送されたオプション 82 の情報を処理します。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定方法

認可のためのユーザ名または NAS-Port-ID を使用して、TAL 用の ISG ポリシーを設定できます。

- 「オプション 60 およびオプション 82 を使用した ISG 制御ポリシーの設定」 (P.192)
- 「NAS-Port-ID を使用した ISG 制御ポリシーの設定」 (P.193)
- 「オプション 60 およびオプション 82 を含む NAS-Port-ID の設定」 (P.194)

オプション 60 およびオプション 82 を使用した ISG 制御ポリシーの設定

認可要求のユーザ名フィールドに指定された ID を挿入する ISG 制御ポリシーを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type control *policy-map-name***
4. **class type control {*class-map-name* | **always**} event session-start**
5. ***action-number* authorize [aaa {*list-name* | **list** {*list-name* | **default**}}] [**password** *password*]]**
[upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier****
***identifier-type* [**plus** *identifier-type*]**
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。 <ul style="list-style-type: none">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 <i>policy-map-name</i> 例： Router(config)# policy-map type control TAL	制御ポリシー マップ コンフィギュレーション モードを開始して、制御ポリシーを定義します。
ステップ 4	class type control {<i>class-map-name</i> always} event session-start 例： Router(config-control-policymap)# class type control TAL-subscribers event session-start	制御ポリシー マップ クラス コンフィギュレーション モードを開始して、関連付けられた実行するアクションのセットと一致させる必要のある条件を定義します。 <ul style="list-style-type: none">「Identifying Traffic for Automatic Logon in a Control Policy Class Map」 の項で設定された制御クラス マップを指定します。
ステップ 5	<i>action-number</i> authorize [aaa {<i>list-name</i> list {<i>list-name</i> default}}] [password <i>password</i>]] [upon network-service-found {continue stop}] [use method <i>authorization-type</i>] identifier <i>identifier-type</i> [plus <i>identifier-type</i>] 例： Router(config-control-policymap-class-contr ol)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address vendor-class-id plus circuit-id plus remote-id	指定された ID を認可要求のユーザ名フィールドに挿入します。

	コマンドまたはアクション	目的
ステップ 6	<pre>end</pre> <p>例 :</p> <pre>Router(config-control-policymap-class-control)# end</pre>	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NAS-Port-ID を使用した ISG 制御ポリシーの設定

認可要求の NAS-Port-ID で使用する ISG 制御ポリシーを設定するには、次の作業を実行します。

手順の概要

1. `enable`
2. `configure terminal`
3. `policy-map type control policy-map-name`
4. `class type control {class-map-name | always} event session-start`
5. `action-number authorize [aaa {list-name | list {list-name | default}}] [password password]]`
`[upon network-service-found {continue | stop}] [use method authorization-type] identifier nas-port`
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	<pre>enable</pre> <p>例 :</p> <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • 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	<pre>configure terminal</pre> <p>例 :</p> <pre>Router# configure terminal</pre>	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	<pre>policy-map type control <i>policy-map-name</i></pre> <p>例 :</p> <pre>Router(config)# policy-map type control TAL</pre>	制御ポリシー マップ コンフィギュレーション モードを開始して、制御ポリシーを定義します。
ステップ 4	<pre>class type control {<i>class-map-name</i> always} event session-start</pre> <p>例 :</p> <pre>Router(config-control-policymap)# class type control TAL-subscribers event session-start</pre>	制御ポリシー マップ クラス コンフィギュレーション モードを開始して、関連付けられた実行するアクションのセットと一致させる必要のある条件を定義します。 <ul style="list-style-type: none"> • 「Identifying Traffic for Automatic Logon in a Control Policy Class Map」の項で設定された制御クラス マップを指定します。

	コマンドまたはアクション	目的
ステップ 5	<pre>action-number authorize [aaa {list-name list {list-name default}} [password password]] [upon network-service-found {continue stop}] [use method authorization-type] identifier nas-port</pre> <p>例： Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier nas-port</p>	NAS ポート ID を認可要求のユーザ名フィールドに挿入します。
ステップ 6	<pre>end</pre> <p>例： Router(config-control-policymap-class-control)# end</p>	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

オプション 60 およびオプション 82 を含む NAS-Port-ID の設定

オプション 60 およびオプション 82 を含めた NAS-Port-ID 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. **radius-server attribute nas-port-id include {identifier1 [plus identifier2] [plus identifier3]} [separator separator]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<pre>enable</pre> <p>例： Router> enable</p>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • 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	<pre>configure terminal</pre> <p>例： Router# configure terminal</p>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<pre>radius-server attribute nas-port-id include {identifier1 [plus identifier2] [plus identifier3]} [separator separator]</pre> <p>例： Router(config)# radius-server attribute nas-port-id include circuit-id plus vendor-class-id</p>	NAS-Port-ID のオプション 60 およびオプション 82 に DHCP リレー エージェントを含めます。

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の設定例

- 「例 : NAS-Port-ID のオプション 60 およびオプション 82」 (P.195)

例 : NAS-Port-ID のオプション 60 およびオプション 82

次の例では、**radius-server attribute nas-port-id include** コマンドを使用して、回線 ID、リモート ID、およびベンダー クラス ID を使用したオプション 60 およびオプション 82 の認可を設定します。

```
interface Ethernet0/0
  service-policy type control RULEA
  !
interface Ethernet1/0
  service-policy type control RULEB
  !
class-map type control match-all CONDA
  match source-ip-address 10.1.1.0 255.255.255.0
  !
class-map type control match-all CONDB
  match vendor-class-id vendor1
  !
policy-map type control RULEA
  class type control CONDA event session-start
    1 authorize aaa list TAL_LIST password cisco identifier vendor-class-id
  !
policy-map type control RULEB
  class type control CONDB event session-start
    1 authorize aaa list TAL_LIST password cisco identifier nas-port
  !
radius-server attribute nas-port-id include circuit-id plus remote-id plus vendor-class-id
separator #
```

その他の参考資料

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 』
自動加入者ログインのための ISG ポリシーの設定	『 Cisco IOS Intelligent Services Gateway Configuration Guide 』の「 Configuring ISG Policies for Automatic Subscriber Logon 」の項
DHCP リレー エージェントの設定	『 Configuring the Cisco IOS DHCP Relay Agent 』の「 Configuring the Cisco IOS DHCP Relay Agent 」の項

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
<ul style="list-style-type: none"> • 	選択したプラットフォーム、Cisco ソフトウェア 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
<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> - 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 <p>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。</p>	http://www.cisco.com/cisco/web/support/index.html

DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon の機能情報

表 17 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。

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 17 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 17 DHCP オプション 60 およびオプション 82 のサポートおよび VPN-ID のサポートの機能情報

機能名	リリース	機能情報
ISG : 認証 : DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	12.2(33)SRD	<p>サービス プロバイダーは、DHCP オプション 60 およびオプション 82 によって TAL をサポートでき、オプション 82 への VPN-ID 拡張によってホールセール型の IP セッションをサポートできます。</p> <p>この機能はプラットフォームに依存せず、Cisco 7600 ルータ、Cisco 7200 ルータ、および Cisco 7301 ルータでサポートされます。</p> <p>次のコマンドが導入または変更されました。</p> <p>radius-server attribute nas-port-id include</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2008–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2011, シスコシステムズ合同会社.
All rights reserved.

