RADIUS 論理回線 ID

論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。管理者は、顧客が物理回線を移動しても変化しない仮想ポートを使用します。この仮想ポートは、管理者の顧客プロファイルデータベースのメンテナンスを容易にし、管理者が顧客に対して追加のセキュリティ チェックを実施できるようにします。

RADIUS 論理回線 ID の前提条件

この機能は任意の RADIUS サーバーと一緒に使用できますが、RADIUS サーバーによっては、Access-Accept メッセージで Calling-Station-ID 属性を返せるようにディレクトリ ファイルを変更する必要があります。たとえば、「ATTRIBUTE Calling-Station-Id 31 string (*, *)」のようにディクショナリを変更しなければ、Merit RADIUS サーバーで LLID ダウンロードはサポートされません。

RADIUS 論理回線 ID の制約事項

RADIUS 論理回線 ID 機能は RADIUS のみをサポートしています。TACACS+ はサポートしていません。

この機能は、PPP over Ethernet over ATM（PPPoEoATM）コールと PPP over Ethernet over VLAN（PPPoEoVLAN）（Dot1Q）コールにしか適用できません。ISDN などのその他のコールは使用できません。

RADIUS 論理回線 ID に関する情報

事前認可

LLID は、加入者線の論理識別を表す英数字文字列です（1 ～ 253 文字にする必要があります）。また、LLID は、RADIUS サーバー上の顧客プロファイル データベース上に保存されます。顧客プロファイルデータベースがアクセスルータから事前認可要求を受け取ると、RADIUS サーバーが LLID を Calling-Station-ID 属性（属性 31）としてルータに送信します。

レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）が、事前認可用に設定されている場合に、事前認可要求を顧客プロファイル データベースに送信します。**subscriber access** コマンドを使用して、LAC を事前認可用に設定します。

（注） LLID のダウンロードは「事前認可」と呼ばれています。これは、サービス（ドメイン）認可またはユーザー認証および認可の前に実施されるためです。

RADIUS サーバー上の顧客プロファイルデータベースは、ルータに接続された物理ネットワーク アクセス サーバー（NAS）ごとのユーザー プロファイルで構成されています。各ユーザー プロファイルには、ルータ上の物理ポートを表すユーザー名（属性 1）と一致したプロファイルが格納されています。ルータは、事前認可用に設定されている場合に、接続先の物理 NAS ポートの代表ユーザー名を使用して顧客プロファイルデータベースに問い合わせます。顧客プロファイルデータベース内で一致するものが見つかると、顧客プロファイルデータベースが、ユーザー プロファイル内の LLID を含む Access-Accept メッセージを返します。LLID は、Calling-Station-ID 属性として Access-Accept レコード内に定義されています。

事前認可プロセスは、認証に使用される実際のユーザー名を RADIUS サーバーに提供することもできます。物理 NAS ポート情報がユーザー名（属性 1）として使用されるため、RADIUS 属性 77（Connect-Info）を認証ユーザー名を含めるように設定できます。この設定によって、RADIUS サーバーは、LLID をルータに返す前に、選択した認可要求に対して追加の検証（プライバシー ルールに対するユーザー名の分析など）を実施できます。

RADIUS 論理回線 ID の設定方法

事前認可の設定

LLID をダウンロードして、LAC を事前認可用に設定するには、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** *interface-name*
4. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**]

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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** *interface-name* 例： 例： `Router (config)# ip radius source-interface Loopback1`	事前認可要求用のユーザー名の IP アドレス部分を指定します。
ステップ 4	**subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id** [**default** | *list-name*] [**send username**] 例： 例： `Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username`	LLID のダウンロードを可能にして、ルータを事前認可用に設定できるようにします。 **send username** オプションは、Access-Request メッセージ内の Connect-Info（属性 77）にセッションの認証ユーザー名を含めるように指定します。

RADIUS ユーザー プロファイル内の LLID の設定

ユーザー プロファイルを事前認可用に設定するには、顧客プロファイル データベースに NAS ポート ユーザーを追加して、ユーザー プロファイルに RADIUS インターネット技術特別調査委員会（IETF）属性 31（Calling-Station-ID）を追加します。

手順の概要

1. UserName=nas_port: ip-address:slot/module/port/vpi.vci
2. User-Name=nas-port: ip-address:slot/module/port/vlan-id
3. Calling-Station-Id = “string (*,*)”

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UserName=nas_port: ip-address:slot/module/port/vpi.vci	（任意）PPPoE over ATM NAS ポート ユーザーを追加します。
ステップ 2	User-Name=nas-port: ip-address:slot/module/port/vlan-id	（任意）PPPoE over VLAN NAS ポート ユーザーを追加します。
ステップ 3	Calling-Station-Id = “string (*,*)”	ユーザー プロファイルに属性 31 を追加します。 • String：ユーザーがかけてきた電話番号を含む 1 つ以上のオクテット。

論理回線 ID の確認

機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **debug radius**

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug radius** 例： `Router# debug radius`	RADIUS 属性 31 が、LAC 上の Accounting-Request と、LNS 上の Access-Request および Accounting-Request 内の LLID であることを確認します。

RADIUS 論理回線 ID の設定例

事前認可用の LAC 設定例

次の例は、LLID をダウンロードすることによって、LAC を事前認可用に設定する方法を示しています。

```
aaa new-model
aaa group server radius sg_llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example.com
 domain example.com#184
 initiate-to ip 10.1.1.1
 local name s7200_2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
!
Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet1/0/0
 ip address 10.1.1.8 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 1/100
```

```
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

LLID 用の RADIUS ユーザー プロファイルの例

次の例は、ユーザー プロファイルを PPPoEoVLAN および PPPoEoATM に対する LLID 問い合わせ用に設定する方法と属性 31 の追加方法を示しています。

```
pppoeovlan
----------
nas-port:10.1.0.3:6/0/0/0    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
pppoeoa
--------
nas-port:10.1.0.3:6/0/0/1.100    Password = "password1",
    Service-Type = Outbound,
    Calling-Station-ID = "cat-example"
```

その他の参考資料

次の項で、RADIUS EAP サポート機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
AAA を使用した ppp 認証の設定	「Configuring Authentication」モジュール。
RADIUS の設定	「Configuring RADIUS」モジュール。
PPP の設定	「Configuring Asynchronous SLIP and PPP」モジュール。
ダイヤル テクノロジー コマンド	『*Cisco IOS Dial Technologies Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 1938	『*A One-Time Password System*』
RFC 2869	『*RADIUS Extensions*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RADIUS 論理回線 ID の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : RADIUS* 論理回線 *ID* の機能情報

機能名	リリース	機能情報
RADIUS 論理回線 ID	Cisco IOS XE Release 2.1	論理回線 ID（LLID）ブロッキング機能としても知られる RADIUS 論理回線 ID 機能を使用すれば、管理者は、顧客コールが発信された物理回線に基づいて顧客を追跡できます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 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。**subscriber access**
発信側ステーション ID 属性 31	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。
LLID ブロッキング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

用語集

attribute ：RADIUS Internet Engineering Task Force（IETF）属性は、クライアントとサーバーの間で認証、認可、およびアカウンティング（AAA）情報を通信するために使用される 255 個の標準属性からなるオリジナル セットの 1 つです。IETF 属性は標準であるため、属性データは事前定義されてその内容も認識されています。このため、IETF 属性を介して AAA 情報を交換するすべてのクライアントとサーバーは、属性の厳密な意味や各属性値の一般的な限界などの属性データを一致させる必要があります。

CHAP ：チャレンジ ハンドシェイク認証プロトコル。PPP カプセル化を使用した回線上でサポートされ、不正アクセスを防止するセキュリティ機能。CHAPそれ自体が不正アクセスを防止するわけではなく、単に、リモートエンドを識別するだけです。その後で、ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。

EAP ：拡張認証プロトコル。認証フェーズ（Link Control Protocol（LCP）フェーズではなく）でネゴシエートされる複数の認証メカニズムをサポートする PPP 認証プロトコル。EAP を使用すれば、汎用のインターフェイスを介して、サードパーティ製の認証サーバーと PPP 実装の間でデータのやり取りができます。

LCP ：リンク制御プロトコル。PPP で使用するためのデータ リンク接続を確立して、設定し、テストするプロトコル。

MD5 (HMAC variant) ：Message Digest 5。パケット データの認証に使用するハッシュ アルゴリズム。HMAC は、メッセージ認証用の重要なハッシングです。

NAS ：ネットワーク アクセス サーバー。公衆電話交換網（PSTN）などのリモート アクセス ネットワーク上でユーザーにローカル ネットワーク アクセスを提供するデバイス。

PAP ：パスワード認証プロトコル。PPP ピアの相互認証を可能にする認証プロトコル。ローカル ルータに接続を試みているリモート ルータは、認証要求を送信するように要求されます。CHAP と違って、PAP はパスワードとホスト名またはユーザー名をクリア テキスト（暗号化なし）で渡します。PAP それ自体が不正アクセスを防止するわけではなく、単に、リモート エンドを識別するだけです。ルータまたはアクセス サーバーがそのユーザーのアクセスを許可するかどうかを決定します。PAP は、PPP 回線上でのみサポートされます。

PPP ：ポイントツーポイント プロトコル。ポイントツーポイント リンク上でネットワーク層プロトコル情報をカプセル化するプロトコル。PPP は RFC 1661 で規定されています。

RADIUS ：リモート認証ダイヤルイン ユーザー サービス。モデムおよび ISDN 接続の認証、および接続のトラッキングのためのデータベースです。

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。