



RADIUS 論理回線 ID

Logical Line Identification (LLID, 論理回線 ID) 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。

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、「[RADIUS 論理回線 ID の機能情報](#)」(P.9) 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://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。

この章の構成

- ・「[RADIUS 論理回線 ID の前提条件](#)」(P.2)
- ・「[RADIUS 論理回線 ID の制約事項](#)」(P.2)
- ・「[RADIUS 論理回線 ID に関する情報](#)」(P.2)
- ・「[RADIUS 論理回線 ID の設定方法](#)」(P.3)
- ・「[RADIUS 論理回線 ID の設定例](#)」(P.5)
- ・「[その他の参考資料](#)」(P.7)
- ・「[RADIUS 論理回線 ID の機能情報](#)」(P.9)
- ・「[用語集](#)」(P.10)

RADIUS 論理回線 ID の前提条件

この機能は任意の RADIUS サーバと一緒に使用できますが、RADIUS サーバによっては、Access-Accept メッセージで Calling-Station-ID アトリビュート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 (*, *)」のようにディレクトリを変更しなければ、Merit RADIUS サーバで LLID ダウンロードをサポートできません。

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

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 サーバが LLID を Calling-Station-ID アトリビュート (アトリビュート 31) としてルータに送信します。

Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) Access Concentrator (LAC; L2TP アクセス コンセントレータ) 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) 認可またはユーザ認証および認可の前に実施されるためです。

RADIUS サーバ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 Network Access Server (NAS; ネットワーク アクセス サーバ) ごとのユーザ プロファイルで構成されています。各ユーザ プロファイルには、ルータ上の物理ポートを表すユーザ名 (アトリビュート 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 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 アトリビュートとして 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名を RADIUS サーバに提供することもできます。物理 NAS ポート情報がユーザ名 (アトリビュート 1) として使用されるため、RADIUS アトリビュート 77 (Connect-Info) を認証ユーザ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名の分析など) を実施できます。

RADIUS 論理回線 ID の設定方法

RADIUS 論理回線 ID 機能の設定タスクについては、次の各項を参照してください。一覧内の各作業は、必須と任意に分けています。

- ・「事前認可の設定」(P.3) (必須)
- ・「RADIUS ユーザ プロファイル内の LLID の設定」(P.4) (必須)
- ・「論理回線 ID の確認」(P.4) (任意)

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 <i>interface-name</i> 例： Router (config)# ip radius source-interface Loopback1	事前認可要求用のユーザ名の 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 <i>list-name</i>][send <i>username</i>] 例： Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send <i>username</i>	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 <i>username</i> オプションは、Access-Request メッセージ内の Connect-Info (アトリビュート 77) にセッションの認証ユーザ名を含めるように指定します。

■ RADIUS 論理回線 ID の設定方法

RADIUS ユーザ プロファイル内の LLID の設定

ユーザ 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 ユーザを追加して、ユーザ プロファイルに RADIUS Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) アトリビュート 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. `UserName=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	<code>UserName=nas_port: ip-address:slot/module/port/vpi.vci</code>	(任意) PPPoE over ATM NAS ポート ユーザを追加します。
ステップ 2	<code>User-Name=nas-port: ip-address:slot/module/port/vlan-id</code>	(任意) PPPoE over VLAN NAS ポート ユーザを追加します。
ステップ 3	<code>Calling-Station-Id = "string (*,*)"</code>	<p>ユーザ プロファイルにアトリビュート 31 を追加します。</p> <ul style="list-style-type: none"> String : ユーザ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	<code>enable</code>	特権 EXEC モードをイネーブルにします。
	例： <code>Router> enable</code>	<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	<code>debug radius</code>	RADIUS アトリビュート 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。
	例： <code>Router# debug radius</code>	

RADIUS 論理回線 ID の設定例

ここでは、次の設定例について説明します。

- ・「事前認可用の LAC 設定：例」(P.5)
- ・「LLID 用の RADIUS ユーザ プロファイル：例」(P.6)

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 config-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 water.com
  domain water.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 Ethernet1/0
  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
  no ip address
  no atm ilmi-keepalive
!
```

■ RADIUS 論理回線 ID の設定例

```

interface ATM4/0.1 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 プロファイル：例

次の例は、ユーザ 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アトリビュート 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 = "cisco",
  Service-Type = Outbound,
  Calling-Station-ID = "cat-example"

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

```

その他の参考資料

次の項で、RADIUS 論理回線 ID に関する参考資料を紹介します。

関連資料

内容	参照先
AAA 認証	『Configuring RADIUS』モジュールの「Configuring AAA Preauthentication」の項
アクセス要求のアトリビュートスクリーニング	『Configuring RADIUS』モジュールの「RADIUS Attribute Screening」の項
ブロードバンド アクセス : PPP とルーテッド ブリッジ エンカプセレーション	『Cisco IOS Broadband Access Aggregation and DSL Configuration Guide, Release 12.4T』
ダイヤル テクノロジー	『Cisco IOS Dial Technologies Configuration Guide, Release 12.4T』

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
<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>	<p>http://www.cisco.com/techsupport</p>

RADIUS 論理回線 ID の機能情報

表 1 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 1 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 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	12.2(13)T 12.2(15)B 12.3(14)YM1 12.4(2)T 12.3(14)YM2 12.2(28)SB 12.2(31)SB2 12.2(33)SRC	Logical Line Identification (LLID; 論理回線 ID) プ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 Release 12.2(13)T で導入されました。 この機能は、Cisco IOS Release 12.2(15)B に統合されました。 この機能は、Cisco IOS Release 12.3(14)YM1 に統合され、 subscriber access コマンドに send username キーワードが追加されました。 この機能は、Cisco IOS Release 12.4(2)T に統合されました。 この機能は、Cisco IOS Release 12.3(14)YM2 に統合されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(31)SB2 に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能により、 subscriber access コマンドが導入されました。

用語集

LLID ブロッキング：管理者が、顧客の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るようにする機能。RADIUS 論理回線 ID としても知られています。

RADIUS 論理回線 ID：管理者が、顧客の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るようにする機能。LLID ブロッキング としても知られています。

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。

© 2002, 2003, 2005–2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2002–2011, シスコシステムズ合同会社.
All rights reserved.