RADIUS EAP サポート

RADIUS EAP サポート機能は、ユーザーに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバー（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークンカードや公開キーなどの認証スキームでネットワークに対するエンド ユーザーとデバイスの認証対象アクセスを補強できます。

RADIUS EAP サポートの前提条件

クライアント上で EAP RADIUS を有効化する前に、次のタスクを実行する必要があります。

- **interface** コマンドを使用してインターフェイス 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。
- **encapsulation** コマンドを使用して、PPP をカプセル化するためのインターフェイスを設定します。

これらのタスクの実行方法については、「Configuring Asynchronous SLIP and PPP」モジュールを参照してください。

RADIUS EAP サポートの制約事項

EAP がプロキシ モードで動作中に、認証時間が大幅に増加する可能性があります。これは、ピアからのすべてのパケットを RADIUS サーバーに送信する必要があり、RADIUS サーバーからのすべての EAP パケットをクライアントに送り返す必要があるためです。この追加処理は遅延の原因になりますが、**ppp timeout authentication** コマンドを使用して、デフォルトの認証タイムアウト値を増やすことができます。

RADIUS EAP サポートに関する情報

EAP は、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 用の認証プロトコルです。EAP を使用すると、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。

EAP のしくみ

デフォルトでは、EAP はプロキシモードで実行されます。このため、EAP では、RADIUS サーバーに存在するバックエンドサーバー、または RADIUS サーバーを介してアクセスできるバックエンド サーバーに対する認証プロセス全体を、NAS によってネゴシエートすることができます。LCP の交換中にクライアントと NAS の間で EAP がネゴシエートされると、その後のすべての認証メッセージは、クライアントとバックエンド サーバーの間で透過的に送信されます。NAS は認証プロセスに直接関与しなくなります。つまり、NAS はプロキシとして機能し、リモート ピア間で EAP メッセージを送信します。

（注） EAP は、ローカル モードでも実行できます。その場合、セッションは Message Digest 5（MD5）アルゴリズムを使用して認証され、Challenge Handshake Authentication Protocol（CHAP）と同じ認証ルールに従います。プロキシ モードを無効にしてローカルで認証するには、**ppp eap local** コマンドを使用する必要があります。

新しくサポートされた属性

RADIUS EAP サポート機能では、次の RADIUS 属性のサポートが追加されています。

番号	IETF 属性	説明
79	EAP-Message	PPP type、request-id、length、および EAP-type の各フィールドを含む EAP メッセージの 1 つのフラグメントをカプセル化します。

番号	IETF 属性	説明
80	Message Authenticator	メッセージの発信元整合性を保証します。無効なチェックサムを伴って受信されたすべてのメッセージは、通知されることなく両端で破棄されます。この属性には、RADIUS要求または応答メッセージ全体の HMAC-MD5 チェックサムが含まれており、キーとして RADIUS サーバー シークレットが使用されます。

RADIUS EAP サポートの設定方法

EAP の設定

このタスクを実行して、PPP カプセル化用に設定されたインターフェイス上で EAP を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ppp authentication eap**
4. **ppp eap identity** *string*
5. **ppp eap password** [*number*] *string*
6. **ppp eap local**
7. **ppp eap wait**
8. **ppp eap refuse** [**callin**]

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	**ppp authentication eap** 例：	認証プロトコルとして EAP を有効にします。

	コマンドまたはアクション	目的
	`Router(config-if)# ppp authentication eap`	
ステップ 4	**ppp eap identity** *string* 例： `Router(config-if)# ppp eap identity user`	（任意）ピアから要求されたときの EAP ID を指定します。
ステップ 5	**ppp eap password** [*number*] *string* 例： `Router(config-if)# ppp eap password 7 141B1309`	（任意）ピア認証用の EAP パスワードを設定します。 このコマンドは、クライアント上でのみ設定する必要があります。
ステップ 6	**ppp eap local** 例： `Router(config-if)# ppp eap local`	（任意）RADIUS バックエンドサーバーを使用する代わりにローカルで認証します。これはデフォルトの設定です。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 7	**ppp eap wait** 例： `Router(config-if)# ppp eap wait`	（任意）発信者が自分自身を最初に認証するのを待機します。デフォルトでは、クライアントの方が発信者よりも先に自分自身を認証します。 （注） このコマンドは、NAS 上でのみ設定する必要があります。
ステップ 8	**ppp eap refuse** [**callin**] 例： `Router(config-if)# ppp eap refuse`	（任意）EAP を使用した認証を拒否します。**callin** キーワードが有効になっている場合は、着信コールのみが認証されません。 （注） このコマンドは、NAS 上でのみ設定する必要があります。

EAP の確認

クライアントまたは NAS 上の EAP 設定を確認するには、特権 EXEC コンフィギュレーションモードで次のコマンドの少なくとも 1 つを使用します。

コマンド	目的
`Router# show users`	ルータのアクティブ回線に関する情報を表示します。
`Router# show interfaces`	ルータまたはアクセス サーバーで設定されているすべてのインターフェイスの統計情報を表示します。

コマンド	目的
Router# **show running-config**	使用している設定が実行コンフィギュレーションの一部として表示されていることを確認します。

設定例

クライアント上の EAP ローカル設定例

次の例は、EAP 用に設定されたクライアントのサンプル設定です。

```
interface Ethernet0/0
 ip address 10.1.1.202 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface BRI0/0
 ip address 192.168.101.100 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 192.168.101.101 56167
 dialer-group 1
 isdn switch-type basic-5ess
 ppp eap identity user
 ppp eap password 7 141B1309
!
!
ip default-gateway 10.1.1.1
ip classless
ip route 192.168.101.101 255.255.255.255 BRI0/0
no ip http server
!
dialer-list 1 protocol ip permit
```

NAS 用の EAP プロキシ設定例

次の例は、EAP プロキシを使用するように設定された NAS のサンプル設定です。

```
aaa authentication login default group radius
aaa authentication login NOAUTH none
aaa authentication ppp default if-needed group radius
aaa session-id common
enable secret 5 $1$x5D0$cfTL/D8Be.34PgTbdGdgl/
!
username dtw5 password 0 lab
username user password 0 lab
ip subnet-zero
no ip domain-lookup
ip host lab24-boot 172.19.192.254
ip host lb 172.19.192.254
!
isdn switch-type primary-5ess
!
```

```
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 10.1.1.108 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial3:23
 ip address 192.168.101.101 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.101.100 60213
 dialer-group 1
 isdn switch-type primary-5ess
 isdn T321 0
 ppp authentication eap
 ppp eap password 7 011F0706
!
!
ip default-gateway 10.0.190.1
ip classless
ip route 192.168.101.0 255.255.255.0 Serial3:23
no ip http server
!
dialer-list 1 protocol ip permit
!
radius-server host 10.1.1.201 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
call rsvp-sync
!
mgcp profile default
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication NOAUTH
line 1 48
line aux 0
ine vty 0 4
lpassword lab
```

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。

関連項目	マニュアル タイトル
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 EAP サポートの機能情報

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 EAP* サポートの機能情報

機能名	リリース	機能情報
RADIUS EAP サポート	Cisco IOS XE Release 3.9S	RADIUS EAP サポート機能は、ユーザーに PPP 内でのクライアント認証方式（独自の認証を含む）の適用を可能にします。この認証方式は、ネットワーク アクセス サーバー（NAS）ではサポートされない可能性があり、拡張可能認証プロトコル（EAP）を通して実現されます。この機能が導入される前は、PPP 接続用のさまざまな認証方式をサポートするために、特別なベンダー固有設定と、クライアントと NAS に対する変更が必要でした。RADIUS EAP サポートを使用すれば、トークン カードや公開キーなどの認証スキームでネットワークに対するエンドユーザーとデバイスの認証対象アクセスを補強できます。 次のコマンドが導入または変更されました。**ppp authentication**、**ppp eap identity, ppp eap local**、**ppp eap password**、**ppp eap refuse**、**ppp eap wait**

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。© 2001-2009 Cisco Systems, Inc. All rights reserved.

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。