# RADIUS EAP Support

The RADIUS EAP Support feature makes it possible for users to apply the client authentication methods within PPP (including proprietary authentication), which may not be supported by the network access server (NAS); to be accomplished through the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific configuration and changes to the client and NAS. RADIUS EAP support allows authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for RADIUS EAP Support

Before enabling EAP RADIUS on the client, you must perform the following tasks:

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.

For more information on completing these tasks, refer to the " Configuring Asynchronous SLIP and PPP " module.

# Restrictions for RADIUS EAP Support

When EAP is running in proxy mode, there may be a significant increase in the authentication time because every packet from the peer must be sent to the RADIUS server and every EAP packet from the RADIUS server must be sent back to the client. Although this extra processing causes delays, you can increase the default authentication timeout value by using the **ppp timeout authentication** command.

# Information About RADIUS EAP Support

EAP is an authentication protocol for PPP that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the link control protocol [LCP] phase). EAP allows a third-party authentication server to interact with a PPP implementation through a generic interface.

## How EAP Works

By default, EAP runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the NAS to a back-end server that may reside on or be accessed through a RADIUS server. After EAP is negotiated between the client and the NAS during LCP exchange, all further authentication messages are transparently transmitted between the client and the back-end server. The NAS is no longer directly involved in the authentication process; that is, the NAS works as a proxy, sending EAP messages between the remote peers.

**Note** EAP can also run in a local mode; the session is authenticated using the Message Digest 5 (MD5) algorithm and obeys the same authentication rules as Challenge Handshake Authentication Protocol (CHAP). To disable proxy mode and authenticate locally, you must use the **ppp eap local** command.

## Newly Supported Attributes

The RADIUS EAP Support feature introduces support for the following RADIUS attributes:

| Number | IETF Attribute | Description |
|---|---|---|
| 79 | EAP-Message | Encapsulates one fragment of an EAP message, which includes the PPP type, request-id, length, and EAP-type fields. |
| 80 | Message Authenticator | Ensures source integrity of the message; all messages that are received with invalid checksums are silently discarded by either end. This attribute contains an HMAC-MD5 checksum of the entire RADIUS request or response message and uses the RADIUS server secret as the key. |

# How to Configure RADIUS EAP Support

## Configuring EAP

Perform this task to configure EAP on an interface configured for PPP encapsulation.

### SUMMARY STEPS

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**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ppp authentication eap**<br>**Example:**<br>`Router(config-if)# ppp authentication eap` | Enables EAP as the authentication protocol. |
| **Step 4** | **ppp eap identity** *string*<br>**Example:**<br>`Router(config-if)# ppp eap identity user` | (Optional) Specifies the EAP identity when requested by the peer. |
| **Step 5** | **ppp eap password** [*number*] *string*<br>**Example:**<br>`Router(config-if)# ppp eap password 7 141B1309` | (Optional) Sets the EAP password for peer authentication.<br>This command should only be configured on the client. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **ppp eap local**<br>**Example:**<br>`Router(config-if)# ppp eap local` | (Optional) Authenticates locally instead of using a RADIUS back-end server, which is the default.<br>**Note** This command should only be configured on the NAS. |
| **Step 7** | **ppp eap wait**<br>**Example:**<br>`Router(config-if)# ppp eap wait` | (Optional) Waits for the caller to authenticate itself first. By default, the client always authenticates itself before the caller does.<br>**Note** This command should only be configured on the NAS. |
| **Step 8** | **ppp eap refuse** [**callin**]<br>**Example:**<br>`Router(config-if)# ppp eap refuse` | (Optional) Refuses to authenticate using EAP. If the **callin** keyword is enabled, only incoming calls are not authenticated.<br>**Note** This command should only be configured on the NAS. |

# Verifying EAP

To verify EAP configurations on your client or NAS, use at least one of the following commands in privileged EXEC configuration mode:

| Command | Purpose |
|---|---|
| `Router# show users` | Displays information about the active lines on the router. |
| `Router# show interfaces` | Displays statistics for all interfaces configured on the router or access server. |
| `Router# show running-config` | Ensures that your configurations appear as part of the running configuration. |

# Configuration Examples

## EAP Local Configuration on Client Example

The following example is a sample configuration for a client configured for EAP:

```
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
```

# EAP Proxy Configuration for NAS Example

The following example is a sample configuration for a NAS configured to use EAP proxy:

```
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
```

# Additional References

The following sections provide references related to RADIUS EAP Support feature.

### Related Documents

| Related Topic | Document Title |
|---|---|
| Configuring PPP Authentication Using AAA | " Configuring Authentication " module. |
| Configuring RADIUS | " Configuring RADIUS " module. |
| PPP Configuration | " Configuring Asynchronous SLIP and PPP " module. |
| Dial Technologies commands | *Cisco IOS Dial Technologies Command Reference* |
| Security Commands | *Cisco IOS Security Command Reference* |

### Standards

| Standard | Title |
|---|---|
| None | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 2284 | *PPP Extensible Authentication Protocol (EAP)* |
| RFC 1938 | *A One-Time Password System* |
| RFC 2869 | *RADIUS Extensions* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/techsupport |

# Feature Information for RADIUS EAP Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1: Feature Information for RADIUS EAP Support*

| Feature Name | Releases | Feature Information |
|---|---|---|
| RADIUS EAP Support | Cisco IOS XE Release 3.9S | The RADIUS EAP Support feature makes it possible for users to apply the client authentication methods within PPP (including proprietary authentication), which may not be supported by the network access server (NAS); to be accomplished through the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific configuration and changes to the client and NAS. RADIUS EAP support allows authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks.<br><br>The following commands were introduced or modified: **ppp authentication**, **ppp eap identity, ppp eap local**, **ppp eap password**, **ppp eap refuse**, **ppp eap wait**. |

# Glossary

**attribute** --A RADIUS Internet Engineering Task Force (IETF) attribute is one of the original set of 255 standard attributes that are used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers that exchange AAA information through IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

**CHAP** --Challenge Handshake Authentication Protocol. Security feature that is supported on lines using PPP encapsulation and prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

**EAP** --Extensible Authentication Protocol. A PPP authentication protocol that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the Link Control Protocol [LCP] phase). EAP allows a third-party authentication server to interact with the PPP implementation through a generic interface.

**LCP** --link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

**MD5 (HMAC variant)** --Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a key hashing for message authentication.

**NAS** --network access server. A device providing local network access to users across a remote access network such as the public switched telephone network (PSTN).

**PAP** --Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

**PPP** --Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

**RADIUS** --Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental. 