RADIUS EAP Support

Feature History

Release	Modification
12.2(2)XB5	This feature was introduced on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS400 platforms.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Contents

Feature Overview

The RADIUS EAP Support feature allows users to apply to the client authentication methods that may not be supported by the network access server; this is done via the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific work and changes to the client and NAS.

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.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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 via 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.

Benefits

The RADIUS EAP Support feature makes it possible to apply to the client various authentication methods within PPP (including proprietary authentication) that are not supported by the NAS. Thus, customers can use standard support mechanisms for authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks.

Restrictions

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 will cause delays, you can increase the default authentication timeout value by using the **ppp timeout authentication** command.

Related Documents

- The section "Configuring PPP Authentication Using AAA" in the chapter "Configuring Authentication" in *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter "Configuring RADIUS" in *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter "PPP Configuration" in *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

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

Prerequisites

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 chapter "Configuring Media-Independent PPP and Multilink PPP" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for the RADIUS EAP Support feature. Each task in the list is identified as either required or optional.

- Configuring EAP (required)
- Verifying EAP (optional)

Configuring EAP

To configure EAP on an interface configured for PPP encapsulation, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# ppp authentication eap`	Enables EAP as the authentication protocol.
`Router(config-if)# ppp eap identity string`	(Optional) Specifies the EAP identity when requested by the peer.
`Router(config-if)# ppp eap password [number] string`	(Optional) Sets the EAP password for peer authentication. **Note** This command should only be configured on the client.
`Router(config-if)# ppp eap local`	(Optional) Authenticates locally instead of using a RADIUS back-end server, which is the default. **Note** This command should only be configured on the NAS.
`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. **Note** This command should only be configured on the NAS.
`Router(config-if)# ppp eap refuse [callin]`	(Optional) Refuses to authenticate using EAP. If the **callin** keyword is enabled, only incoming calls will not be authenticated. **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

This section provides the following configuration examples:

- EAP Local Configuration on Client Example
- EAP Proxy Configuration for NAS Example

EAP Local Configuration on Client Example

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

```
interface Ethernet0/0
 ip address 1.1.1.202 255.255.255.0
 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 1.1.1.1
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 1.1.1.108 255.255.255.0
 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 1.1.1.201 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
line vty 0 4
 password lab
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Command

- **ppp authentication**

Modified Commands

- **ppp eap identity**
- **ppp eap local**
- **ppp eap password**
- **ppp eap refuse**
- **ppp eap wait**

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

ppp authentication {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in Table 1.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

When you enable PAP, CHAP, or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 1 lists the protocols used to negotiate PPP authentication.

Table 1 ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

ppp eap identity *string*

no ppp eap identity *string*

Syntax Description

string	EAP identity.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Use the **ppp eap identity** command to configure the client to use a different identity when requested by the peer.

Examples

The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenable proxy mode (which is the default), use the **no** form of this command.

ppp eap local

no ppp eap local

Syntax Description

This command has no arguments or keywords.

Defaults

Authentication is performed via proxy mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local** command.

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

Examples

The following example shows how to configure EAP to authenticate locally:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
 ppp eap local
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp eap password [*number*] *string*

no ppp eap password [*number*] *string*

Syntax Description

number	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
string	Character string that specifies the EAP password.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

Examples

The following example shows how to set the EAP password "7 141B1309" on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp eap refuse [**callin**]

no ppp eap refuse [**callin**]

Syntax Description

callin	(Optional) Authentication is refused for incoming calls only.

Defaults

The server will not refuse EAP authentication challenges received from the peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Use the **ppp eap refuse** command to disable EAP authentication for all calls. If the **callin** keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.

Examples

The following example shows how to refuse EAP authentication on incoming calls from the peer:

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ppp eap wait

no ppp eap wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

Use the **ppp eap wait** command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

Examples

The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

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 via 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.