EAP Authentication with RADIUS Server

Contents

Introduction

This document provides a sample configuration of a Cisco IOS® based access point for Extensible Authentication Protocol (EAP) authentication of wireless users against a database accessed by a RADIUS server.

Due to the passive role that the access point plays in EAP (bridges wireless packets from the client into wired packets destined to the authentication server, and vice versa), this configuration is used with virtually all EAP methods. These methods include (but are not limited to) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) version 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS), and EAP-Tunneled TLS (TTLS). You must appropriately configure the authentication server for each of these EAP methods.

This document covers how to configure the access point (AP) and the RADIUS server, which is Cisco Secure ACS in the configuration example in this document.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You are familiar with the Cisco IOS GUI or CLI.

- You are familiar with the concepts behind EAP authentication.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Aironet AP products that run Cisco IOS.
- Assumption of only one Virtual LAN (VLAN) in the network.
- A RADIUS authentication server product that successfully integrates into a user database.These are the supported authentication servers for Cisco LEAP and EAP-FAST:Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Belted RADIUSInterlink MeritThese are the supported authentication servers for the Microsoft PEAP-MS-CHAP version 2 and PEAP-GTC:Microsoft Internet Authentication Service (IAS)Cisco Secure ACSFunk Steel Belted RADIUSInterlink MeritAny additional authentication server Microsoft can authorize.**Note:** GTC or One-Time Passwords require additional services which require additional software on both the client and server side, as well as hardware or software token generators.Consult the manufacturer of the client supplicant for details on which authentication servers are supported with their products for EAP-TLS, EAP-TTLS and other EAP methods.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

This configuration describes how to configure EAP authentication on an IOS based AP. In the example in this document, LEAP is used as a method of EAP authentication with RADIUS server.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

As with most password-based authentication algorithms, Cisco LEAP is vulnerable to dictionary attacks. This is not a new attack or new vulnerability of Cisco LEAP. The creation of a strong password policy is the most effective way to mitigate dictionary attacks. This includes the use of strong passwords and the periodical expiration of passwords. Refer to Dictionary Attack on Cisco LEAP to get more information about dictionary attacks and how to prevent them.

This document uses this configuration for both GUI and CLI:

- IP address of the AP is 10.0.0.106.
- IP address of the RADIUS server (ACS) is 10.0.0.3.

Network EAP or Open Authentication with EAP

In any EAP/802.1x based authentication method, you can question what the differences are

between Network EAP and Open authentication with EAP. These items refer to the values in the Authentication Algorithm field in the headers of management and association packets. Most manufacturers of wireless clients set this field at the value 0 (Open authentication), then signal a desire to do EAP authentication later in the association process. Cisco sets the value differently, from the start of association with the Network EAP flag.

If your network has clients that are:

- Cisco clients—Use Network-EAP.
- Third party clients (include CCX compliant products)—Use Open with EAP.
- A combination of both Cisco and third party clients—Choose both Network-EAP and Open with EAP.

Define Authentication Server

The first step in the EAP configuration is to define the authentication server and establish a relationship with it.

1. On the access point Server Manager tab (under the **Security > Server Manager** menu item), complete these steps:Enter the IP address of the authentication server in the Server field.Specify the Shared Secret and the ports.Click **Apply** in order to create the definition and populate the dropdown lists.Set the EAP Authentication type Priority 1 field to the server IP address under Default Server Priorities.Click **Apply**.You can also issue these commands from the CLI:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#aaa group server radius rad_eap

AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646

AP(config-sg-radius)#exit

AP(config)#aaa new-model

AP(config)#aaa authentication login eap_methods group rad_eap

AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#end

AP#write memory
```

2. The access point must be configured in the authentication server as an AAA client.For example, in Cisco Secure ACS, this happens on the Network Configuration page where the name of the access point, IP address, shared secret and authentication method (RADIUS Cisco Aironet or RADIUS Cisco IOS/PIX) are defined. Refer to the documentation from the manufacturer for other non-ACS authentication servers.Ensure that the authentication server is configured to perform the desired EAP authentication method. For example, for a Cisco Secure ACS that does LEAP, configure LEAP authentication on the System Configuration - Global Authentication Setup page. Click **System Configuration**, then click **Global Authentication Setup**. Refer to the documentation from the manufacturer for other non-ACS

authentication servers or other EAP methods.This image shows Cisco Secure ACS configured for PEAP, EAP-FAST, EAP-TLS, LEAP and EAP-MD5.

Define Client Authentication Methods

Once the access point knows where to send client authentication requests, configure it to accept those methods.

Note: These instructions are for a WEP based installation. For WPA (which uses ciphers instead of WEP), refer to WPA Configuration Overview.

1. On the access point Encryption Manager tab (under the **Security > Encryption Manager** menu item), complete these steps:Specify that you want to use **WEP encryption**.Specify that WEP is **Mandatory**.Verify that the key size is set to **128-bits**.Click **Apply**.You can also issue these commands from the CLI:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#encryption mode wep mandatory

AP(config-if)#end

AP#write memory
```

2. Complete these steps on the access point SSID Manager tab (under the **Security > SSID Manager** menu item):Select the desired SSID.Under "Authentication Methods Accepted," check the box labelled **Open** and use the dropdown list to choose **With EAP**.Check the box labelled **Network-EAP** if you have Cisco client cards. See the discussion in the Network EAP or Open Authentication with EAP section.Click **Apply**.

You can also issue these commands from the CLI:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#ssid labap1200

AP(config-if-ssid)#authentication open eap eap_methods

AP(config-if-ssid)#authentication network-eap eap_methods

AP(config-if-ssid)#end

AP#write memory
```

Once you confirm basic functionality with a basic EAP configuration, you can add additional features and key management at a later time. Layer more complex functions on top of functional foundations in order to make troubleshooting easier.

Verify

This section provides information you can use to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show radius server-group all**—Displays a list of all configured RADIUS server-groups on the AP.

Troubleshoot

Troubleshoot Procedure

Complete these steps in order to troubleshoot your configuration.

1. In the client-side utility or software, create a new profile or connection with the same or similar parameters in order to ensure that nothing has become corrupted in the configuration of the client.
2. In order to eliminate the possibility of RF issues that prevent successful authentication, temporarily disable authentication as shown in these steps:From the CLI, use the commands **no authentication open eap eap_methods**, **no authentication network-eap eap_methods** and **authentication open**.From the GUI, on the SSID Manager page, un-check **Network-EAP**, check **Open**, and set the dropdown list back to **No Addition**.If the client successfully associates, then RF does not contribute to the association problem.
3. Verify that shared secret passwords are synchronized between the access point and the authentication server. Otherwise, you can receive this error message:
   `Invalid message authenticator in EAP request`
   From the CLI, check the line `radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>`.From the GUI, on the Server Manager page, re-enter the shared secret for the appropriate server in the box labelled "Shared Secret."The shared secret entry for the access point on the RADIUS server must contain the same shared secret password as those previously mentioned.
4. Remove any user groups from the RADIUS server. Sometimes conflicts can occur between user groups defined by the RADIUS server, and user groups in the underlying domain. Check the logs of the RADIUS server for failed attempts, and the reasons those attempts failed.

Troubleshoot Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Debugging Authentications provides a significant amount of detail about how to gather and interpret the output of debugs related to EAP.

Note: Before you issue **debug** commands, refer to the Important Information on Debug Commands.

- **debug dot11 aaa authenticator state-machine**—Displays major divisions (or states) of the negotiation between the client and the authentication server. Here is an output from a **successful** authentication:

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CL IENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
------------------Lines Omitted for simplicity------------------
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SE RVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
0040.96ac.dd05
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)
```

  Note: In Cisco IOS Software releases prior to 12.2(15)JA, the syntax of this **debug** command is **debug dot11 aaa dot1x state-machine**.
- **debug dot11 aaa authenticator process**—Displays the individual dialog entries of the negotiation between the client and the authentication server.**Note:** In Cisco IOS Software releases prior to 12.2(15)JA, the syntax of this debug command is **debug dot11 aaa dot1x process**.
- **debug radius authentication**—Displays the RADIUS negotiations between the server and client, both of which, are bridged by the AP. This is an output for **failed** authentication:

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
```

```
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
---------------------------Lines Omitted-----------------------------------
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
---------------------------------Lines Omitted-----------------------
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed
```

- **debug aaa authentication**—Displays the AAA negotiations for authentication between the client device and the authentication server.

Related Information

- Debug Authentications
- Configuring Authentication Types
- LEAP Authentication on a Local RADIUS Server
- Configuring RADIUS and TACACS+ Servers
- Configuring Cisco Secure ACS for Windows v3.2 With PEAP-MS-CHAPv2 Machine Authentication

- Cisco Secure ACS for Windows v3.2 With EAP-TLS Machine Authentication
- Configuring PEAP/EAP on Microsoft IAS
- Troubleshooting Microsoft IAS as a RADIUS server
- Microsoft 802.1X Authentication Client
- Technical Support & Documentation - Cisco Systems