Autonomous アクセス ポイントの内部 RADIUS サーバの EAP-FAST の設定例

目次

概要

このドキュメントでは、Autonomous アクセス ポイント（AP）を RADIUS サーバとして機能するように設定し、Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol（EAP-FAST）を実行して、GUI インターフェイスの操作性と外観を持つように更新された最新の Cisco IOS® リリース（15.2JB）によってクライアント認証を行う方法について説明します。

通常、外部 RADIUS サーバは、ユーザを認証するために使用されます。 場合によっては、これが適切なソリューションではないことがあります。 この場合、アクセス ポイント（AP）は RADIUS サーバとして機能します。 また、ユーザの認証は、アクセス ポイントで設定されたローカル データベースを照会することによって実行されます。 これをローカル RADIUS サーバ機能と呼びます。 アクセス ポイントのローカル RADIUS サーバ機能を、ネットワーク内の他のアクセス ポイントから利用することもできます。

前提条件

要件

この設定を開始する前に、次の項目に関する知識を得ておくことを推奨します。

- Cisco IOS GUI または CLI

- 拡張認証プロトコル（EAP）の背後にある概念
- サービス セット ID（SSID）の設定
- RADIUS

使用するコンポーネント

このドキュメントの情報は、Cisco IOS リリース 15.2JB を実行し、かつ内部 RADIUS サーバとして機能する 3600 AP に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

GUI による設定

1. AP を ローカル RADIUS サーバとして設定するには、[AP GUI] > [Security] > [Server Manager] に移動し、次の詳細を入力します。
   ホスト名または IP アドレス共有秘密Authentication Portアカウンティング ポート（Accounting Port）
   注: この例では、認証とアカウンティング ポート用に、それぞれ 1812 と 1813 を使用します。 ただし、1645 と 1646 も使用できます。

   [Apply] をクリックします。

2. AP の[Local RADIUS Server configuration] に移動し、[General Set-Up] タブをクリックして、次の詳細を入力します。
   ネットワーク アクセス サーバ（NAS）として、AP の IP アドレス（Bridge-Group Virtual Interface（BVI）int IP）**共有秘密**
   [Apply] をクリックします。

   [Individual User] で、[Username] と [Password] を入力します。 [Group Name] が必要な場合は、設定します（この例では、[Group Name] は使用しません）。

3. [LEAP] および [MAC] チェックボックスをオフにします。

4. [EAP-FAST Set-Up] タブをクリックし、[PAC Encryption Keys] と [PAC Content] に詳細を入力します。

注: 32 桁の 16 進数を使用するので、この例では、0 ~ 9 を 4 回ずつ使用します。

5. [Encryption Manager] に移動し、暗号化として [Cipher] を [AES CCMP] に設定して、[Apply All Radios] または [Required Radios] をクリックします。

SSID の設定

1. [Security] > [SSID manager] に移動し、[Create New] をクリックします。

2. 詳細を入力し、[Apply] をクリックします。

3. [Client Authentication Settings] 画面で、[Open Authentication] チェックボックスをオンにし、ドロップダウン メニューから [with EAP] を選択します。 [Network EAP] チェックボックスをオンにし、ドロップダウン メニューから [RADIUS Server] を選択します。 これは、[Server Manager and Local RADIUS Server] ページで AAA として設定した AP の IP アドレスです。

Wireless Protected Access Version 2 (WPAv2) が必須になるように設定する

1. [Client Authenticated Key Management] 画面で、[Key Management] ドロップダウン メニューから [Mandatory] を選択します。 [Enable WPA] チェックボックスをオンにし、ドロップダウン メニューから [WPAv2] を選択します。

2. ページの一番下にある [Apply] をクリックします。 SSID をブロードキャストするには、[Single SSID] オプション ボタンをクリックし、ドロップダウン メニューから [SSID] を選択して、[Apply] をクリックします。

3. [Networks] に移動し、無線の [2.4 GHz] と [5 GHz] を有効にします。 無線が稼働中であることを確認します。

設定用の CLI コマンド

show run
```
Building configuration...

Current configuration : 3204 bytes
!
! Last configuration change at 01:11:36 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$06l4$E2pi.VeGTKUxxiwPScUEp.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
dot11 syslog
!
dot11 ssid EAPFAST
  authentication open eap eap_methods1
  authentication network-eap eap_methods1
  authentication key-management wpa version 2
  guest-mode
```

```
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 01300F175804
!
!
!
class-map match-all _class_voice0
 match ip dscp ef
 class-map match-all _class_voice1
 match ip dscp default
!
!
policy-map voice
 class _class_voice0
 set cos 6
 class _class_voice1
 set cos 6
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 stbc
 power local 14
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

```
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.135.185 255.255.255.128
 no ip route-cache
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
 eapfast authority id 01234567890123456789012345678901
 eapfast authority info cisco
 eapfast server-key primary 7 E1F54D861DC7150A7B949E5B4E630D8E5B
 eapfast server-key secondary 7 E7281DB670D36C052F60D36337436ABA13
 nas 10.105.135.185 key 7 01100F175804
 user user nthash 7 075A76681B514A2436465D28517D7A7178611403375334215677 7C79030
D2D5448
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.105.135.185 auth-port 1812 acct-port 1813 key 7 045802150C2E
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
transport input all
!
end

ap#
```

確認

クライアントに接続し、認証が正常に行われると、次のログが AP に表示されます。

```
show run
Building configuration...

Current configuration : 3204 bytes
!
! Last configuration change at 01:11:36 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$06l4$E2pi.VeGTKUxxiwPScUEp.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
dot11 syslog
!
dot11 ssid EAPFAST
  authentication open eap eap_methods1
  authentication network-eap eap_methods1
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 01300F175804
!
!
!
class-map match-all _class_voice0
 match ip dscp ef
 class-map match-all _class_voice1
 match ip dscp default
!
```

```
!
policy-map voice
 class _class_voice0
 set cos 6
 class _class_voice1
 set cos 6
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 stbc
 power local 14
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.135.185 255.255.255.128
 no ip route-cache
!
ip forward-protocol nd
```

```
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
 eapfast authority id 01234567890123456789012345678901
 eapfast authority info cisco
 eapfast server-key primary 7 E1F54D861DC7150A7B949E5B4E630D8E5B
 eapfast server-key secondary 7 E7281DB670D36C052F60D36337436ABA13
 nas 10.105.135.185 key 7 01100F175804
 user user nthash 7 075A76681B514A2436465D28517D7A7178611403375334215677 7C79030
D2D5448
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.105.135.185 auth-port 1812 acct-port 1813 key 7 045802150C2E
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
transport input all
!
end

ap#
```

トラブルシューティング

この設定のトラブルシューティングを行うには、次の手順を実行します。

1. 正常な認証を妨げる無線周波数（RF）の問題が生じないようにするため、SSID の方式を [Open] に設定して認証を一時的にディセーブルにします。

2. [SSID Manager] ページの GUI から、[Network-EAP] チェック ボックスをオフにして [Open] をオンにします。

3. CLI から、**authentication open** コマンドと **no authentication network-eap eap_methods** コマンドを使用します。 クライアントが関連付けに成功する場合には、RF はアソシエーションの問題に関係しません。

4. すべての共有秘密パスワードが同期されていることを確認します。 次の行は、同じ共有秘密パスワードが含まれている必要があります。
   radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>nas x.x.x.x key <shared_secret>
5. ユーザ グループと関連する設定を削除します。 場合によっては、AP が定義したユーザ グループと、ドメインのユーザ グループ間で、競合が発生することがあります。

debug コマンド

注: [debug](#) コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください

。

役立つ debug コマンドの一覧を次に示します。

- **debug dot11 aaa authenticator all**：802.1x または EAP プロセスを使用して関連付けと認証を行う際にクライアントが実行したさまざまなネゴシエーションが、オーセンティケータ（AP）側からの視点で表示されます。 このデバッグは Cisco IOS ソフトウェア リリース 12.2(15)JA で導入されました。 上記以降のリリースでは、このコマンドが **debug dot11 aaa dot1x all** に代わるコマンドとして使用されています。

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
Create new client 0040.96af.3e93 for application 0x1
*Mar 1 00:26:03.097: dot11_auth_initialize_client:
0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
Lines Omitted for simplicity ------------------
*Mar 1 00:26:03.098: dot11_auth_dot1x_start:
in the dot11_auth_dot1x_start


*Mar 1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar 1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96af.3e93(client)

*Mar 1 00:26:03.133: *Mar 1 00:26:03.099:
dot11_auth_dot1x_send_id_req_to_client:
Client 0040.96af.3e93 timer started for 30 seconds
*Mar 1 00:26:03.132: dot11_auth_parse_client_pak:
Received EAPOL packet from 0040.96af.3e93
-----------------------------------------------
Lines Omitted-----------------------------------
*Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length:
0x000A type: 0x1
01805BF0: 0100000A 0201000A 01757365 7231
.........user1(User Name of the client)


*Mar1 00:26:03.146: dot11_auth_dot1x_run_rfsm:
Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96af.3e93 data toserver
*Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
-----------------------------------------------
Lines Omitted-----------------------------------
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
Received server response:GET_CHALLENGE_RESPONSE
*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp:
found session timeout 10 sec


*Mar 1 00:26:03.150: dot11_auth_dot1x_run_rfsm:
Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93
*Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client:
Forwarding server message to client 0040.96af.3e93
-----------------------------------------------
Lines Omitted-----------------------------------
*Mar 1 00:26:03.151: dot11_auth_send_msg:
```

```
Sending EAPOL to requestor
*Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 10 seconds
*Mar 1 00:26:03.166: dot11_auth_parse_client_pak:
Received EAPOL packet(User Credentials) from 0040.96af.3e93
*Mar 1 00:26:03.166: EAP code: 0x2 id: 0x11 length: 0x0025
type: 0x1101805F90: 01000025 02110025...%...%01805FA0:
11010018 7B75E719 C5F3575E EFF64B27 ....{ug.EsW^ovK'


Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93
*Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96af.3e93 data
(User Credentials) to server
*Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
-----------------------------------------------
Lines Omitted----------------------------------------
*Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp:
Received server response: PASS


*Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm:
Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93
*Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client:
 Forwarding server message(Pass Message) to client
-----------------------------------------------
Lines Omitted-----------------------------------
*Mar 1 00:26:03.198: dot11_auth_send_msg:
Sending EAPOL to requestor
*Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 second
*Mar 1 00:26:03.199: dot11_auth_send_msg:
client authenticated 0040.96af.3e93,
node_type 64 for application 0x1
*Mar 1 00:26:03.199: dot11_auth_delete_client_entry:
0040.96af.3e93 is deleted for application 0x1
*Mar 1 00:26:03.200: %DOT11-6-ASSOC:
 Interface Dot11Radio0, Station Station Name
0040.96af.3e93 Associated KEY_MGMT[NONE]
```

- **debug radius authentication**：この debug コマンドを実行すると、サーバとクライアント（この場合は両方とも AP）間の RADIUS ネゴシエーションが表示されます。
- **debug radius local-server client**：この debug コマンドを実行すると、クライアントの認証が RADIUS サーバ側からの視点で表示されます。

```
 *Mar 1 00:30:00.742: RADIUS(0000001A):
SendAccess-Request(Client's User Name)
to 10.77.244.194:1812(Local Radius Server)


id 1645/65, len 128
*Mar 1 00:30:00.742: RADIUS:
User-Name [1] 7 "user1"
*Mar 1 00:30:00.742: RADIUS:
Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 00:30:00.743: RADIUS:
Calling-Station-Id [31] 16 "0040.96af.3e93" (Client)
```

```
*Mar 1 00:30:00.743: RADIUS:
Service-Type [6] 6 Login [1]
*Mar 1 00:30:00.743: RADIUS:
Message-Authenticato[80]
*Mar 1 00:30:00.743: RADIUS:
23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{]
*Mar 1 00:30:00.743: RADIUS:
EAP-Message [79] 12
*Mar 1 00:30:00.743:
RADIUS:   02 02 00 0A 01 75 73 65 72 31
[?????user1]
*Mar 1 00:30:00.744: RADIUS:
NAS-Port-Type [61] 6 802.11 wireless
--------------------------------
Lines Omitted For Simplicity--------------------
*Mar 1 00:30:00.744: RADIUS:
NAS-IP-Address [4] 6 10.77.244.194(Access Point IP)

*Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap"

---------------------------------
Lines Omitted---------------------------------
*Mar 1 00:30:00.745: RADIUS:
Received from id 1645/65 10.77.244.194:1812, Access-Challenge, len 117
*Mar 1 00:30:00.746: RADIUS:
75 73 65 72 31 [user1]
*Mar 1 00:30:00.746: RADIUS:
Session-Timeout [27] 6 10
*Mar 1 00:30:00.747: RADIUS: State [24] 50
*Mar 1 00:30:00.747: RADIUS:
BF 2A A0 7C 82 65 76 AA 00 00 00 00 00 00 00 00
[?*?|?ev?????????]
-------------------------------------
Lines Omitted for simplicity -------------
*Mar 1 00:30:00.756:
RADIUS/ENCODE(0000001A):Orig. component type = DOT11
*Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 00:30:00.756: RADIUS: 63 69 73 [cis]
*Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 00:30:00.756: RADIUS: 32 [2]
*Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194
*Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26
*Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194


*Mar 1 00:30:00.779: RADIUS(0000001A):
Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189
*Mar 1 00:30:00.779: RADIUS:
authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F
*Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1"
*Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0"
*Mar 1 00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93"
*Mar 1 00:30:00.758: RADIUS:
92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF [??$I????????k???]
*Mar 1 00:30:00.759: RADIUS: EAP-Message [79] 39
*Mar 1 00:30:00.759: RADIUS:
02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2  [??????????????E?]
*Mar 1 00:30:00.759: RADIUS:
73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4 [s]3??/??P?8??;??]
*Mar 1 00:30:00.759: RADIUS:
75 73 65 72 31 [user1]
```

```
----------------------------------------
Lines Omitted--------------------------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS:
NAS-IP-Address [4] 6 10.77.244.194
*Mar 1 00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap"

*Mar 1 00:30:00.822: RADIUS:
Received from id 1645/67 10.77.244.194:1812, Access-Accept, len 214
*Mar 1 00:30:00.822:
RADIUS: authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A
----------------------------------------
Lines Omitted--------------------------
*Mar 1 00:30:00.823: RADIUS: 75 73 65 72 31 [user1]
*Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59
*Mar 1 00:30:00.823: RADIUS:
Cisco AVpair [1] 53 "EAP-FAST:session-key=?+*ve=];q,oi[d6|-z."
*Mar 1 00:30:00.823:
RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS:
Message-Authenticato[80] 18
*Mar 1 00:30:00.824: RADIUS:
06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36
[?-?????????????6]
*Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments,
37, total 37 bytes
*Mar 1 00:30:00.826: found leap session key
*Mar 1 00:30:00.830: %DOT11-6-ASSOC:
Interface Dot11Radio0, Station Station Name
Associated KEY_MGMT[NONE]
```

- **debug radius local-server packets**：この debug コマンドを実行すると、RADIUS サーバ側から見た、実行済みのすべてのプロセスが表示されます。