

EAP-FAST avec le serveur RADIUS interne sur l'exemple de configuration de point d'accès autonome

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Configuration avec le GUI](#)

[Configurez le SSID](#)

[Configurez la version 2 Sans fil \(WPAv2\) de Protected Access comme obligatoire](#)

[Commande CLI pour les configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Commandes de débogage](#)

Introduction

Ce document décrit comment configurer le point d'accès autonome pour agir en tant que serveur de RAYON qui exécute l'authentification Protocol-flexible d'authentification extensible de Cisco par l'intermédiaire du protocole sécurisé (EAP-FAST) pour l'authentification de client avec la dernière release de Cisco IOS® (15.2JB), qui a été mise à jour pour avoir l'aspect et l'impression d'une interface gui.

Habituellement un serveur RADIUS externe est utilisé afin d'authentifier des utilisateurs. Dans certains cas, ce n'est pas une solution faisable. Dans ces situations, un Point d'accès (AP) peut agir en tant que serveur de RAYON. Dans cette situation, des utilisateurs sont authentifiés contre la base de données locale configurée au Point d'accès. Ceci s'appelle une caractéristique locale de serveur de RAYON. Vous pouvez également faire d'autres Points d'accès dans l'utilisation de réseau que le serveur local de RAYON comportent sur AP.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- GUI ou CLI de Cisco IOS
- Concepts derrière le Protocole EAP (Extensible Authentication Protocol)
- Configuration d'Identifiant SSID (Service Set Identifier)
- RAYON

Composants utilisés

Les informations dans ce document sont basées sur des 3600 AP qui exécutent le Cisco IOS Release 15.2JB et agissent en tant que serveur RADIUS interne.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Configuration avec le GUI

1. Afin de configurer AP en tant que serveur local de RAYON, naviguez vers **AP GUI > Security > Server Manager**, et écrivez ces détails :

Adresse Internet ou adresse IP Secret partagé Port d'authentification Port de traçabilité

Remarque: Pour l'authentification et les ports de traçabilité, cet exemple utilise 1812 et 1813, respectivement. Cependant, 1645 et 1646 peuvent également être utilisés.

Cliquez sur **Apply**.

2. Naviguez vers la **configuration du serveur RADIUS locale** sur AP, cliquez sur l'onglet de **configuration générale**, et écrivez ces détails :

Serveur d'accès à distance (NAS) avec l'adresse IP d'AP IP (de Bridge Group Virtual Interface (BVI) international) **Secret partagé**

Cliquez sur **Apply**.

Créez un **utilisateur individuel** avec un **nom d'utilisateur et mot de passe**. Si un **nom de groupe** est exigé, alors configurez-le (cet exemple n'utilise pas un **nom de groupe**).

3. Décochez les cases de **LEAP** et de **MAC**.

4. Cliquez sur l'onglet **Setup d'EAP-FAST**, et écrivez les détails pour les **clés de chiffrement PAC** et le **contenu PAC**.

Remarque: Cet exemple utilise zéro neuf quatre fois puisqu'il a 32 caractères hexadécimaux.

5. Naviguez vers le **gestionnaire de cryptage**, configurez le **chiffrement** avec **AES CCMP** comme cryptage, et cliquez sur **Apply toutes les radios** ou **radios requises**.

Configurez le SSID

1. Naviguez vers la **Sécurité > le gestionnaire SSID**, et le clic **créent nouveau**.
2. Écrivez les détails, et cliquez sur **Apply**.
3. Sur l'**authentification client** les configurations examinent, cochent la **case à cocher Open Authentication**, et la sélectionnent **avec l'EAP** du menu déroulant. Cochez la case d'**EAP de réseau**, et sélectionnez le **serveur de RAYON** du menu déroulant. Ceci devrait être l'adresse IP AP que vous avez configurée comme AAA page de serveur sur de gestionnaire du serveur et de gens du pays RAYON.

Configurez la version 2 Sans fil (WPAv2) de Protected Access comme obligatoire

1. Sur l'écran d'**Authenticated Key Management de client**, **obligatoire** choisi du menu déroulant de **gestion des clés**. Cochez la case de l'**enable WPA**, et sélectionnez **WPAv2** du menu déroulant.
2. Cliquez sur **Apply** en bas de la page. Afin d'annoncer le SSID, cliquez sur les cases d'option **simples SSID**, sélectionnez le **SSID** du menu déroulant, et cliquez sur **Apply**.
3. Naviguez vers des **réseaux**, et activez les radios pour **2.4 gigahertz** et **5 gigahertz**. Assurez-vous que les radios sont en service.

Commande CLI pour les configurations

```
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 nhash 7 075A76681B514A2436465D28517D7A71786114033753342156777C79030
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#

```

Vérifiez

Si vous vous connectez au client, alors c'est le log qui affiche sur AP après une authentification réussie :

```
*Mar 1 00:45:02.035: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio1,
Associated To AP root XXXX.XXXX.XXXX [EAP-FAST WPAv2]
```

Dépannez

Terminez-vous ces étapes afin de dépanner cette configuration.

1. Afin d'éliminer la possibilité que les questions de Radiofréquence (RF) empêchent l'authentification réussie, placez la méthode sur le SSID **pour s'ouvrir** afin de désactiver temporairement l'authentification.
2. Du GUI à la page de **gestionnaire SSID**, décochez la case de **Network-EAP**, et cochez

ouvert.

3. Du CLI, n'utilisez l'**authentication open** de commandes et **aucun eap_methods d'authentication network-eap**. Si le client s'associe avec succès, le rf ne contribue pas au problème d'association.
4. Vérifiez que tous les mots de passe secret partagés sont synchronisés. Ces lignes doivent contenir la même chose mot de passe secret partagé :
<shared_secret> principal du l'acct-port X du l'authentique-port X de l'hôte x.x.x.x de rayon-serveur<shared_secret> de clé du nas x.x.x.x
5. Retirez tous les groupes d'utilisateurs et leurs configurations associées. Parfois les conflits se produisent entre les groupes d'utilisateurs définis par AP et les groupes d'utilisateurs sur le domaine.

Commandes de débogage

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Voici une liste de commandes de débogage utiles.

- **l'authentificateur de debug dot11 aaa entièrement** ceci mettent au point des expositions les diverses négociations qu'un client intervient pendant que le client s'associe et authentifie par le 802.1x ou le processus d'EAP de la perspective de l'authentificateur (AP). Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Ce **dot1x tout de debug dot11 aaa d'obsoletes** de commande en cela et des versions ultérieures.

```
*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 to server
*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]
```


- **authentification de debug radius** - Ceci mettront au point des expositions les négociations de RAYON entre le serveur et client, qui, dans ce cas, sont AP.
- **client de debug radius local-server** - Ceci mettront au point des expositions l'authentification du client de la perspective du serveur de RAYON.

```
*Mar 1 00:30:00.742: RADIUS(0000001A):
Send Access-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]

- **paquets de debug radius local-server** - Ceci mettent au point des expositions tous les processus par lesquels sont exécutés et de la perspective du serveur de RAYON.