Authentification EAP sur ACS 5.3 avec des Points d'accès

Contenu

Introduction

Ce document décrit une configuration d'échantillon d'un Point d'accès articulé autour d'un logiciel de Cisco IOS® (AP) pour l'authentification de Protocole EAP (Extensible Authentication Protocol) des utilisateurs de sans fil contre une base de données accédée à par un serveur de RAYON.

AP jette un pont sur les paquets Sans fil du client dans les paquets de câble destinés au serveur d'authentification et vice versa. Puisqu'AP joue ce rôle passif dans l'EAP, cette configuration est utilisée avec pratiquement toutes les méthodes d'EAP. Ces méthodes incluent, mais ne sont pas limitées à, EAP léger (LEAP), EAP protégé (PEAP) - version 2 de la Microsoft Challenge Handshake Authentication Protocol (MSCHAP), PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (JEÛNEZ), EAP-Transport Layer Security (TLS), et EAP-Tunneled TLS (TTL). Vous devez configurer convenablement le serveur d'authentification pour chacune de ces méthodes d'EAP.

Ce document décrit comment configurer AP et le serveur de RAYON, qui est un Cisco Secure Access Control Server (ACS) 5.3 dans cette configuration d'échantillon.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du GUI de logiciel de Cisco IOS ou de l'interface de ligne de commande (CLI)
- Connaissance des concepts de l'authentification EAP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Aironet 3602 Points d'accès qui exécute la version du logiciel Cisco IOS 15.2(2)JB
- Cisco Secure Access Control Server 5.3

Cet exemple de configuration suppose qu'il y a seulement un VLAN dans le réseau.

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

Ce document utilise cette configuration pour le GUI et le CLI :

- L'adresse IP d'AP est 10.105.136.11.
- L'adresse IP du serveur de RAYON (l'ACS) est 10.106.55.91.

Configuration avec le GUI

Définir le serveur d'authentification

Cette procédure décrit comment définir le serveur d'authentification et établir des relations avec elle.

1. Dans le GUI AP, naviguez vers le **Security > Server Manager**.
2. Dans les serveurs entreprise sectionnez, écrivez l'adresse IP du serveur d'authentification (**10.106.55.91**) dans le champ de serveur.
3. Spécifiez le secret partagé, le port d'authentification, et le port de traçabilité. Vous pouvez utiliser les ports 1813, 1814 ou 1645, 1646.
4. Cliquez sur Apply afin de créer la définition et remplir listes déroulantes.
5. Dans la section Default Server Priorities, placez le champ prioritaire 1 d'authentification EAP

à l'adresse IP du serveur (**10.106.55.91**).

6. Cliquez sur **Apply**.

Configurez ACS

Si vous envoyez des utilisateurs à un serveur RADIUS externe, AP doit être un client d'Authentification, autorisation et comptabilité (AAA) pour ce serveur RADIUS externe. Cette procédure décrit comment configurer l'ACS.

1. Dans le GUI de Cisco Secure ACS, **ressources de réseau en** clic. Dans ACS 5.3, des périphériques peuvent être groupés par des emplacements.

2. Créez un emplacement. Sous des groupes de périphériques réseau, **emplacement de** clic. Le clic **créent le nouveau emplacement**. Dans la zone d'identification, écrivez un nom d'emplacement (**IOS_lab**). Écrivez une description (**LABORATOIRE IOS**) pour cet emplacement. Sélectionnez le général **tous les emplacements** comme emplacement de parent. Cliquez sur Submit pour valider.

3. Créez un groupe pour l'IOS aps. **Type de périphérique de** clic. Le clic **créent** pour créer un nouveau groupe. Dans la zone d'identification, écrivez un nom de groupe (**IOS_APs**). Écrivez une description (**IOS aps dans le LABORATOIRE**) pour ce groupe. Sélectionnez **tous les types de périphérique** en tant que parent. Cliquez sur Submit pour valider.

4. Ajoutez AP. **Périphériques de réseau de** clic **et clients d'AAA**. Dans la zone d'identification, écrivez le nom de votre IOS AP (**AP**). Écrivez une description pour cet AP (**IOS AP**).

   Sous des groupes de périphériques réseau, à côté du champ Location, cliquez sur **choisi**, cochez la case à côté d'IOS_lab, et cliquez sur OK pour valider. Sous l'adresse IP, soyez sure adresse IP simple est activé, et écrit l'adresse IP de votre AP (**10.105.136.11**).

   Sous des options d'authentification, **RAYON de** contrôle. Dans le domaine **secret partagé**, écrivez un secret (**Cisco**). Gardez les autres valeurs à leurs par défaut. Cliquez sur Submit pour valider.

5. Ajoutez les qualifications d'utilisateur de sans fil. Naviguez vers des **utilisateurs et l'identité enregistre >** des **groupes d'identité**. Le clic **créent** pour créer un nouveau groupe. Dans la zone d'identification, écrivez un nom de groupe (**EAP_Users**). Écrivez une description (**utilisateurs pour la radio d'EAP**). Cliquez sur Submit pour valider.

6. Créez un utilisateur dans ce groupe. **Utilisateurs de** clic. Le clic **créent** pour créer un nouvel utilisateur. Dans la zone d'identification, écrivez un nom d'utilisateur (**rayon**). Assurez-vous que l'état d'utilisateur **est activé**. Écrivez une description pour l'utilisateur (**rayon de test**). À côté du champ de groupe d'identité, le clic **choisi**, cochent la case à côté d'EAP_Users, et cliquent sur OK pour valider.

   Sous les informations de mot de passe, écrivez le **<password>** dans les domaines de mot de passe et de confirmation du mot de passe. Puisque cet accès des besoins de l'utilisateur au réseau mais n'a pas besoin de l'accès à aucun périphérique de Cisco pour la Gestion, il n'y a aucun besoin de mot de passe d'enable.

7. Cliquez sur Submit pour valider. Le nouvel utilisateur apparaît dans la liste, et l'ACS est maintenant prêt.

8. Naviguez vers des **éléments de stratégie** > l'**autorisation et des autorisations** > des **profils d'accès au réseau** > d'**autorisation** afin de vérifier qu'on accorde l'utilisateur la permission d'accès. Il devrait y a un profil de PermitAccess. On accorde des utilisateurs qui reçoivent ce profil l'accès au réseau.

9. Naviguez **pour accéder à des stratégies** > des **services d'accès** > l'**admin de périphérique de par défaut** pour examiner l'autorisation. Assurez-vous que l'**identité**, le **mappage de groupe**, et l'**autorisation** sont vérifiés.

10. Cliquez sur l'onglet **permis de protocoles**, sélectionnez les cases pour des méthodes requises d'EAP, et cliquez sur Submit pour valider.

Configurez le SSID

Cette procédure décrit comment configurer l'Identifiant SSID (Service Set Identifier) sur AP.

1. Dans le GUI de Cisco Secure ACS, naviguez vers le **Security > SSID Manager**. Cliquez sur New, écrivez le nom SSID (**rayon**), activez les deux interfaces par radio, et cliquez sur Apply.

2. Naviguez vers le **Security > Encryption Manager**, **AES** choisi **CCMP** comme chiffrement, et cliquez sur Appliquer-**tout** pour appliquer ce cryptage sur les deux radios.

3. Naviguez vers le **Security > SSID Manager**, et sélectionnez le **rayon** SSID. Dans l'authentification client les configurations sectionnent, vérifient l'**authentification ouverte**, choisie **avec l'EAP de la** liste déroulante, et de l'**EAP de réseau de** contrôle.

   Dans la section d'Authenticated Key Management de client, **obligatoires** choisis de la liste déroulante de gestion des clés, vérifient l'**enable WPA**, et sélectionnent **WPAv2 de la** liste déroulante. Cliquez sur **Apply**.

4. Afin d'annoncer ce SSID sur les deux radios, trouvez la section de configurations de mode/infrastructure SSID d'invité à la même page. Pour les deux radios, placez le mode de balise **pour choisir le BSSID**, et pour sélectionner le nom SSID (**rayon**) de la liste déroulante simple du mode SSID d'invité de positionnement. Cliquez sur **Apply**.

5. Naviguez vers le **réseau** > l'**interface réseau** > le **Radio0-802.11n 2G.Hz** > **configurations** > **enable** afin d'activer les deux interfaces par radio.

6. Testez la Connectivité de client.

Configuration avec le CLI

Remarques :

Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

C'est la même configuration faite dans le CLI :

```
show run
Building configuration...

Current configuration : 2511 bytes
!
! Last configuration change at 01:17:48 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$1u04$jr7DG0DC5KZ6bVaSYUhck0
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.106.55.91
!
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 authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
ip cef
!
ip dhcp pool test
!
!
!
dot11 syslog
!
dot11 ssid radius
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption mode ciphers aes-ccm
 !
 ssid radius
 !
 antenna gain 0
 stbc
```

```
 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
 !
 encryption mode ciphers aes-ccm
 !
 ssid radius
 !
 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
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.136.11 255.255.255.128
!
ip default-gateway 10.105.136.1
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 route 0.0.0.0 0.0.0.0 10.105.136.1
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.106.55.91 key 7 00271A1507545A545C606C
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 transport input all
!
end
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Connectez le client ; après l'authentification réussie, c'est le résumé de configuration qui paraît dans le GUI AP :

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Dans le CLI, sélectionnez la commande de **show dot11 associations** afin de confirmer la configuration :

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [radius] :

MAC Address    IP address      Device        Name         Parent      State
f8db.7f75.7804 10.105.136.116  unknown       -            self        EAP-Assoc
```

Vous pouvez également présenter le **show radius server-group toute la** commande afin d'afficher une liste de tous les servers-group configurés de RAYON sur AP.

Dépannez

Cette procédure décrit comment dépanner votre configuration.

1. En utilitaire ou logiciel de côté client, créez un nouveau profil ou connexion avec la même chose ou les paramètres semblables afin de s'assurer que rien n'est devenu corrompu dans la configuration de client.

2. Les questions de Radiofréquence (RF) peuvent empêcher l'authentification réussie. Temporairement authentification de débronchement afin d'éliminer cette possibilité :

   Du CLI, sélectionnez ces commandes :

   aucun eap_methods d'eap d'authentication openaucun eap_methods d'authentication network-eapauthentication open

   Du GUI, à la page de gestionnaire SSID, décochez le **Network-EAP**, vérifiez **ouvert**, et placez la liste déroulante à **aucun ajout**.

   Si le client s'associe avec succès, le rf ne contribue pas au problème d'association.

3. Vérifiez que les mots de passe secret partagés sont synchronisés entre AP et le serveur d'authentification. Autrement, vous pourriez recevoir ce message d'erreur :

   `Invalid message authenticator in EAP request`Du CLI, vérifiez la ligne :

radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>Du GUI, à la page de gestionnaire du serveur, ressaisissez le secret partagé pour le serveur compétent dans le domaine secret partagé.

L'entrée secrète partagée pour AP sur le serveur de RAYON doit contenir la même chose mot de passe secret partagé.

4. Supprimez tout groupe d'utilisateurs du serveur RADIUS. Les conflits peuvent se produire entre les groupes d'utilisateurs définis par le serveur de RAYON et les groupes d'utilisateurs dans le domaine sous-jacent. Vérifiez les logs du serveur de RAYON pour des essais ratés et pour les raisons pour les pannes.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Employez ces commandes de débogage afin d'étudier et afficher les négociations parmi des périphériques :

- **state-machine d'authentificateur de debug dot11 aaa**
- **authentification de debug radius**
- **debug aaa authentication**

state-machine d'authentificateur de debug dot11 aaa

Cette commande affiche des divisions importantes (ou des états) de la négociation entre le client et le serveur d'authentification. C'est un exemple de sortie d'une authentification réussie :

```
ap#debug dot11 aaa authenticator state-machine
state machine debugging is on
ap#
*Mar  1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Sending identity
request to f8db.7f75.7804
*Mar  1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Client
f8db.7f75.7804 timer started for 30 seconds
*Mar  1 01:38:35.431: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar  1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar  1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar  1 01:38:35.435: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar  1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar  1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar  1 01:38:35.443: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar  1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar  1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar  1 01:38:35.447: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar  1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
```

```
*Mar  1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
------------------Lines Omitted for simplicity------------------
*Mar  1 01:38:36.663: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar  1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar  1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar  1 01:38:36.667: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar  1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar  1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar  1 01:38:36.671: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_PASS) for f8db.7f75.7804
*Mar  1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar  1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar  1 01:38:36.719: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```

authentification de debug radius

Cette commande affiche les négociations de RAYON entre le serveur et le client, qui pont par AP. C'est un exemple de sortie d'une authentification réussie :

```
ap#debug radius authentication

*Mar  1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: ssid [347] 6
*Mar  1 01:50:50.635: RADIUS:   72 61 64 69 [ radi]
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: service-type [345] 4 1
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: interface [222] 3
*Mar  1 01:50:50.635: RADIUS:   32 [ 2]
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6:
*Mar  1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.635: RADIUS(000001F6): sending
*Mar  1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/73, len 140
*Mar  1 01:50:50.635: RADIUS:  authenticator 0F 74 18 0E F3 08 ED 51 -
8B EA F7 31 AC C9 CA 6B
*Mar  1 01:50:50.635: RADIUS:  User-Name  [1]   8   "radius"
*Mar  1 01:50:50.635: RADIUS:  Framed-MTU  [12]  6   1400
*Mar  1 01:50:50.635: RADIUS:  Called-Station-Id   [30]  26  "1C-E6-C7-E1-D8-90:
radius"
*Mar  1 01:50:50.635: RADIUS:  Calling-Station-Id  [31]  16  "f8db.7f75.7804"
*Mar  1 01:50:50.635: RADIUS:  Service-Type [6]   6   Login  [1]
*Mar  1 01:50:50.635: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.635: RADIUS:   E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78
[ P+"&v(yp_x]
*Mar  1 01:50:50.635: RADIUS:  EAP-Message [79]  13
*Mar  1 01:50:50.635: RADIUS:   02 01 00 0B 01 72 61 64 69 75 73
[ radius]
*Mar  1 01:50:50.635: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:50.635: RADIUS:  NAS-Port   [5]   6   282
*Mar  1 01:50:50.635: RADIUS:  NAS-Port-Id  [87]  5   "282"
```

```
*Mar  1 01:50:50.635: RADIUS:  NAS-IP-Address [4]   6   10.105.136.11
*Mar  1 01:50:50.635: RADIUS:  Nas-Identifier  [32]  4   "ap"
*Mar  1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access
-Challenge, len 94
*Mar  1 01:50:50.639: RADIUS:  authenticator 5E A4 A7 B9 01 CC F4 20 -
2E D0 2A 1A A4 58 05 9E
*Mar  1 01:50:50.639: RADIUS:  State               [24]  32
*Mar  1 01:50:50.639: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.639: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.639: RADIUS:  EAP-Message         [79]  24
*Mar  1 01:50:50.639: RADIUS:   01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF
72 61 64 69 75 73         [ *twradius]
*Mar  1 01:50:50.639: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.643: RADIUS:   CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF
[ D-aiO4]
*Mar  1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73
*Mar  1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes
*Mar  1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: ssid             [347] 6
*Mar  1 01:50:50.647: RADIUS:   72 61 64 69              [ radi]
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: service-type     [345] 4
1
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: interface        [222] 3
*Mar  1 01:50:50.647: RADIUS:   32                 [ 2]
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6:
*Mar  1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.647: RADIUS(000001F6): sending
*Mar  1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
   id 1645/74, len 167
*Mar  1 01:50:50.647: RADIUS:  authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E
05 B0 87 3B 76
*Mar  1 01:50:50.647: RADIUS:  User-Name           [1]   8   "radius"
*Mar  1 01:50:50.647: RADIUS:  Framed-MTU          [12]  6   1400
*Mar  1 01:50:50.647: RADIUS:  Called-Station-Id   [30]  26  "1C-E6-C7-E1-D8-90:
radius"
*Mar  1 01:50:50.647: RADIUS:  Calling-Station-Id  [31]  16  "f8db.7f75.7804"
*Mar  1 01:50:50.647: RADIUS:  Service-Type        [6]   6   Login
[1]
*Mar  1 01:50:50.647: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.647: RADIUS:   FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F
[ {I'?]
*Mar  1 01:50:50.647: RADIUS:  EAP-Message         [79]  8
*Mar  1 01:50:50.647: RADIUS:   02 DC 00 06 03 19
*Mar  1 01:50:50.647: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:50.647: RADIUS:  NAS-Port            [5]   6   282
*Mar  1 01:50:50.647: RADIUS:  NAS-Port-Id         [87]  5   "282"
*Mar  1 01:50:50.647: RADIUS:  State               [24]  32
*Mar  1 01:50:50.647: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.647: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.647: RADIUS:  NAS-IP-Address      [4]   6   10.105.136.11
*Mar  1 01:50:50.647: RADIUS:  Nas-Identifier      [32]  4   "ap"
*Mar  1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access
-Challenge, len 78
```

```
*Mar  1 01:50:50.647: RADIUS:  authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93
8C 8E 29 94 EC
*Mar  1 01:50:50.647: RADIUS:  State               [24]  32
*Mar  1 01:50:50.651: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.651: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.651: RADIUS:  EAP-Message         [79]  8
*Mar  1 01:50:50.651: RADIUS:   01 DD 00 06 19 21                 [ !]
*Mar  1 01:50:50.651: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.651: RADIUS:   A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86
[ T*RX/]
*Mar  1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74
*Mar  1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
*Mar  1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: ssid              [347] 6
*Mar  1 01:50:50.655: RADIUS:   72 61 64 69              [ radi]
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: service-type      [345] 4
1
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: interface         [222] 3

------------------Lines Omitted for simplicity------------------

11        [ l2^w$qM{60]
*Mar  1 01:50:51.115: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:51.115: RADIUS:  NAS-Port            [5]   6   282
*Mar  1 01:50:51.115: RADIUS:  NAS-Port-Id         [87]  5   "282"
*Mar  1 01:50:51.115: RADIUS:  State               [24]  32
*Mar  1 01:50:51.115: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:51.115: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:51.115: RADIUS:  NAS-IP-Address      [4]   6   10.105.136.11
*Mar  1 01:50:51.115: RADIUS:  Nas-Identifier      [32]  4   "ap"
*Mar  1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access
-Challenge, len 115
*Mar  1 01:50:51.115: RADIUS:  authenticator 74 CF 0F 34 1F 1B C1 CF -
E9 27 79 D5 F8 9C 5C 50
*Mar  1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```

debug aaa authentication

Cette commande affiche les négociations d'AAA pour l'authentification entre le périphérique de client et le serveur d'authentification.

```
ap#debug radius authentication

*Mar  1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: ssid [347] 6
*Mar  1 01:50:50.635: RADIUS:   72 61 64 69 [ radi]
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: service-type [345] 4 1
*Mar  1 01:50:50.635: RADIUS:  AAA Unsupported Attr: interface [222] 3
*Mar  1 01:50:50.635: RADIUS:   32 [ 2]
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6:
*Mar  1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar  1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.635: RADIUS(000001F6): sending
```

```
*Mar  1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
id 1645/73, len 140
*Mar  1 01:50:50.635: RADIUS:  authenticator 0F 74 18 0E F3 08 ED 51 -
8B EA F7 31 AC C9 CA 6B
*Mar  1 01:50:50.635: RADIUS:  User-Name  [1]   8   "radius"
*Mar  1 01:50:50.635: RADIUS:  Framed-MTU  [12]  6   1400
*Mar  1 01:50:50.635: RADIUS:  Called-Station-Id   [30]  26  "1C-E6-C7-E1-D8-90:
radius"
*Mar  1 01:50:50.635: RADIUS:  Calling-Station-Id  [31]  16  "f8db.7f75.7804"
*Mar  1 01:50:50.635: RADIUS:  Service-Type [6]   6   Login  [1]
*Mar  1 01:50:50.635: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.635: RADIUS:   E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78
[ P+"&v(yp_x]
*Mar  1 01:50:50.635: RADIUS:  EAP-Message [79]  13
*Mar  1 01:50:50.635: RADIUS:   02 01 00 0B 01 72 61 64 69 75 73
[ radius]
*Mar  1 01:50:50.635: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:50.635: RADIUS:  NAS-Port   [5]   6   282
*Mar  1 01:50:50.635: RADIUS:  NAS-Port-Id  [87]  5   "282"
*Mar  1 01:50:50.635: RADIUS:  NAS-IP-Address [4]   6   10.105.136.11
*Mar  1 01:50:50.635: RADIUS:  Nas-Identifier  [32]  4   "ap"
*Mar  1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access
-Challenge, len 94
*Mar  1 01:50:50.639: RADIUS:  authenticator 5E A4 A7 B9 01 CC F4 20 -
2E D0 2A 1A A4 58 05 9E
*Mar  1 01:50:50.639: RADIUS:  State               [24]  32
*Mar  1 01:50:50.639: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.639: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.639: RADIUS:  EAP-Message         [79]  24
*Mar  1 01:50:50.639: RADIUS:   01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF
72 61 64 69 75 73         [ *twradius]
*Mar  1 01:50:50.639: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.643: RADIUS:   CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF
[ D-aiO4]
*Mar  1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73
*Mar  1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes
*Mar  1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: ssid              [347] 6
*Mar  1 01:50:50.647: RADIUS:   72 61 64 69              [ radi]
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: service-type      [345] 4
1
*Mar  1 01:50:50.647: RADIUS:  AAA Unsupported Attr: interface         [222] 3
*Mar  1 01:50:50.647: RADIUS:   32                 [ 2]
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6:
*Mar  1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491
*Mar  1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11
*Mar  1 01:50:50.647: RADIUS(000001F6): sending
*Mar  1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645
   id 1645/74, len 167
*Mar  1 01:50:50.647: RADIUS:  authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E
05 B0 87 3B 76
*Mar  1 01:50:50.647: RADIUS:  User-Name           [1]   8   "radius"
*Mar  1 01:50:50.647: RADIUS:  Framed-MTU          [12]  6   1400
*Mar  1 01:50:50.647: RADIUS:  Called-Station-Id   [30]  26  "1C-E6-C7-E1-D8-90:
radius"
*Mar  1 01:50:50.647: RADIUS:  Calling-Station-Id  [31]  16  "f8db.7f75.7804"
*Mar  1 01:50:50.647: RADIUS:  Service-Type        [6]   6   Login
[1]
```

```
*Mar  1 01:50:50.647: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.647: RADIUS:   FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F
[ {I'?]
*Mar  1 01:50:50.647: RADIUS:  EAP-Message         [79]  8
*Mar  1 01:50:50.647: RADIUS:   02 DC 00 06 03 19
*Mar  1 01:50:50.647: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:50.647: RADIUS:  NAS-Port            [5]   6   282
*Mar  1 01:50:50.647: RADIUS:  NAS-Port-Id         [87]  5   "282"
*Mar  1 01:50:50.647: RADIUS:  State               [24]  32
*Mar  1 01:50:50.647: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.647: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.647: RADIUS:  NAS-IP-Address      [4]   6   10.105.136.11
*Mar  1 01:50:50.647: RADIUS:  Nas-Identifier      [32]  4   "ap"
*Mar  1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access
-Challenge, len 78
*Mar  1 01:50:50.647: RADIUS:  authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93
8C 8E 29 94 EC
*Mar  1 01:50:50.647: RADIUS:  State               [24]  32
*Mar  1 01:50:50.651: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:50.651: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:50.651: RADIUS:  EAP-Message         [79]  8
*Mar  1 01:50:50.651: RADIUS:   01 DD 00 06 19 21                 [ !]
*Mar  1 01:50:50.651: RADIUS:  Message-Authenticato[80]  18
*Mar  1 01:50:50.651: RADIUS:   A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86
[ T*RX/]
*Mar  1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74
*Mar  1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
*Mar  1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: ssid             [347] 6
*Mar  1 01:50:50.655: RADIUS:   72 61 64 69              [ radi]
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: service-type     [345] 4
1
*Mar  1 01:50:50.655: RADIUS:  AAA Unsupported Attr: interface        [222] 3

------------------Lines Omitted for simplicity------------------

11        [ l2^w$qM{60]
*Mar  1 01:50:51.115: RADIUS:  NAS-Port-Type       [61]  6   802.11 wireless
[19]
*Mar  1 01:50:51.115: RADIUS:  NAS-Port            [5]   6   282
*Mar  1 01:50:51.115: RADIUS:  NAS-Port-Id         [87]  5   "282"
*Mar  1 01:50:51.115: RADIUS:  State               [24]  32
*Mar  1 01:50:51.115: RADIUS:   32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35
[27SessionID=acs5]
*Mar  1 01:50:51.115: RADIUS:   31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B    [ 1
/165489511/9;]
*Mar  1 01:50:51.115: RADIUS:  NAS-IP-Address      [4]   6   10.105.136.11
*Mar  1 01:50:51.115: RADIUS:  Nas-Identifier      [32]  4   "ap"
*Mar  1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet
*Mar  1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout
*Mar  1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access
-Challenge, len 115
*Mar  1 01:50:51.115: RADIUS:  authenticator 74 CF 0F 34 1F 1B C1 CF -
E9 27 79 D5 F8 9C 5C 50
*Mar  1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```