Déboguer les authentifications

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Conventions](#)
[Capturer les débogages](#)
[PAE](#)
[Authentification MAC](#)
[WPA](#)
[Authentification administrative/HTTP](#)
[Informations connexes](#)

Introduction

La communication sans fil a recours à l'authentification de plusieurs manières. Le type d'authentification le plus commun passe par le Extensible Authentication Protocol (EAP), sous divers types et formes. D'autres types d'authentification incluent l'authentification des adresses MAC et l'authentification administrative. Ce document décrit comment déboguer et interpréter les données de sortie des authentifications de débogage. Les informations issues de ces activités de débogage s'avèrent inestimables lors du dépannage d'installations sans fil.

Remarque : les parties de ce document qui font référence à des produits non Cisco sont basées sur l'expérience de l'auteur et non sur une formation formelle. Ils sont conçus pour votre commodité et non comme une assistance technique. Pour obtenir une assistance technique faisant autorité sur des produits non Cisco, contactez l'assistance technique de ce produit.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification relative aux réseaux sans fil
- Interface de ligne de commande logicielle Cisco IOS® (CLI)
- Configuration du serveur RADIUS

Composants utilisés

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

- Produits sans fil basés sur la plate-forme logicielle Cisco IOS, quel que soit leur modèle et leur version
- HyperTerminal de Hilgraeve

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Capturer les débogages

Si vous ne pouvez pas capturer et analyser les informations de débogage, elles sont inutiles. Le moyen le plus simple de capturer ces données consiste à utiliser une fonction de capture d'écran intégrée à l'application Telnet ou de communication.

Cet exemple décrit comment capturer la sortie avec l'application Hilgraeve HyperTerminal. La plupart des systèmes d'exploitation Microsoft Windows incluent HyperTerminal, mais vous pouvez appliquer les concepts à n'importe quelle application d'émulation de terminal. Pour plus d'informations sur la demande, référez-vous à Hilgraeve.

Complétez ces étapes afin de configurer HyperTerminal pour communiquer avec votre point d'accès (AP) ou pont :

1. Afin d'ouvrir HyperTerminal, choisissez Démarrer > Programmes > Outils système > Communications > HyperTerminal.

   Figure 1 : lancement d'HyperTerminal

2. Lorsque HyperTerminal s'ouvre, procédez comme suit :

   a. Entrez un nom pour la connexion.

   b. Sélectionnez une icône.

   c. Click OK.

3. Pour les connexions Telnet, procédez comme suit :

   a. Dans le menu déroulant Connect Using, sélectionnez TCP/IP.

   b. Saisissez l'adresse IP du périphérique sur lequel vous souhaitez exécuter les

débogages.

c. Click OK.

Figure 2 : connexion Telnet

4. Pour les connexions de console, procédez comme suit :

a. Dans le menu déroulant Connect Using, sélectionnez le port COM auquel le câble de console est connecté.

b. Click OK.

La feuille de propriétés de la connexion s'affiche.

c. Définissez la vitesse de connexion au port de console.

d. Afin de restaurer les paramètres de port par défaut, cliquez sur Restore Defaults.

Remarque : la plupart des produits Cisco respectent les paramètres de port par défaut.

Les paramètres de port par défaut sont les suivants :

- Bits par seconde : 9 600
- Bits de données : 8
- Parité : aucune
- Bits d'arrêt : 1
- Contrôle de flux - Aucun

Figure 3 : propriétés de COM1

À ce stade, la connexion Telnet ou console s’établit et vous êtes invité à saisir un nom d’utilisateur et un mot de passe.

Remarque : l'équipement Cisco Aironet attribue un nom d'utilisateur et un mot de passe par défaut Cisco (sensibles à la casse).

5. Afin d'exécuter des débogages, complétez ces étapes :

a. Émettez la commande enable afin de passer en mode privilégié.

b. Entrez le mot de passe enable.

Remarque : n'oubliez pas que le mot de passe par défaut pour les équipements Aironet est Cisco (sensible à la casse).

Remarque : afin de voir le résultat des débogages d'une session Telnet, utilisez la commande terminal monitor ou term mon afin d'activer le terminal monitor.

Figure 4 : session Telnet connectée

6. Après avoir établi une connexion, procédez comme suit afin de collecter une capture d'écran :

    a. Choisissez Capture Text dans le menu Transfert.

    Figure 5 : enregistrement d'une capture d'écran

    b. Lorsqu'une boîte de dialogue s'ouvre et vous invite à entrer un nom de fichier pour la sortie, entrez un nom de fichier.

7. Complétez ces étapes afin de désactiver le retour à la ligne :

    Remarque : vous pouvez lire les débogages plus facilement lorsque vous désactivez le retour à la ligne.

    a. Dans le menu HyperTerminal, choisissez File.

    b. Choisissez Properties.

    c. Dans la feuille de propriétés de connexion, cliquez sur l'onglet Paramètres.

    d. Cliquez sur Configuration ASCII.

    e. Décochez la case Renvoyer à la ligne qui dépasse la largeur du terminal.

    f. Pour fermer les paramètres ASCII, cliquez sur OK.

    g. Afin de fermer la feuille de propriétés de connexion, cliquez sur OK.

    Figure 6 : paramètres ASCII

Maintenant que vous pouvez capturer n'importe quelle sortie d'écran dans un fichier texte, les débogages que vous exécutez dépendent de ce qui est négocié. Les sections suivantes de ce document décrivent le type de connexion négociée fourni par les débogages.

PAE

Ces débogages sont les plus utiles pour les authentifications EAP :

- debug radius authentication : les résultats de ce débogage commencent par ce mot : `RADIUS`.
- debug dot11 aaa authenticator process : les résultats de ce débogage commencent par le texte suivant : `dot11_auth_dot1x_`.
- debug dot11 aaa authenticator state-machine : les résultats de ce débogage commencent par le texte suivant : `dot11_auth_dot1x_run_rfsm`.

Ces débogages montrent :

- Ce qui est rapporté pendant les parties RADIUS d'une boîte de dialogue d'authentification
- Les actions qui sont effectuées pendant cette boîte de dialogue d'authentification
- Les différents états par lesquels le dialogue d'authentification passe

Cet exemple montre une authentification LEAP (Light EAP) réussie :

Exemple d'authentification EAP réussie

```
<#root>

Apr  8 17:45:48.208: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr  8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client:
   sending identity request for 0002.8aa6.304f
Apr  8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client:
   Started timer client_timeout 30 seconds
Apr  8 17:45:48.210: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,EAP_START

) for 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
    id is not matching req-id:1resp-id:2, waiting for response
Apr  8 17:45:48.213: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.213: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
    tarted timer server_timeout 60 seconds
Apr  8 17:45:48.214: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.214: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:45:48.215: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.215: RADIUS(0000001C): Storing nasport 17 in rad_db
Apr  8 17:45:48.215: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.215: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.216: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.216: RADIUS(0000001C): sending
Apr  8 17:45:48.216: RADIUS(0000001C): Send Access-Request
    to 10.0.0.3:1645 id 21645/93, len 139
Apr  8 17:45:48.216: RADIUS:  authenticator 92 26 A8 31 ED 60 6A 88
    - 84 8C 80 B2 B8 26 4C 04
Apr  8 17:45:48.216: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.216: RADIUS:  Framed-MTU          [12]  6   1400
```

```
Apr  8 17:45:48.217: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.217: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.217: RADIUS:  Service-Type        [6]   6   Login  [1]
Apr  8 17:45:48.217: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.217: RADIUS:  EAP-Message         [79]  14
Apr  8 17:45:48.218: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
    [?????aironet]
Apr  8 17:45:48.218: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless     [19]
Apr  8 17:45:48.218: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.218: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.218: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.224: RADIUS: Received from id 21645/93 10.0.0.3:1645,
    Access-Challenge, len 69
Apr  8 17:45:48.224: RADIUS:  authenticator C8 6D 9B B3 67 60 44 29
    - CC AB 39 DE 00 A9 A8 CA
Apr  8 17:45:48.224: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.224: RADIUS:   01 43 00 17 11 01 00 08 63 BB E7 8C 0F AC EB 9A
    [?C??????c???????]
Apr  8 17:45:48.225: RADIUS:   61 69 72 6F 6E 65 74
    [aironet]
Apr  8 17:45:48.225: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.225: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.226: RADIUS(0000001C): Received from id 21645/93
Apr  8 17:45:48.226: RADIUS/DECODE: EAP-Message fragments, 23, total 23 bytes
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found eap pak in
    server response
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found session timeout
    20 sec
Apr  8 17:45:48.227: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_REPLY

) for
    0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.232: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_run_rfsm: Executing Action
    (

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:45:48.233: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.234: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:45:48.234: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.234: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS(0000001C): sending
```

```
Apr  8 17:45:48.234: RADIUS(0000001C): Send Access-Request to
    10.0.0.3:1645 id 21645/94, len 166
Apr  8 17:45:48.235: RADIUS:  authenticator 93 B5 CC B6 41 97 A0 85
    - 1B 4D 13 0F 6A EE D4 11
Apr  8 17:45:48.235: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.235: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.236: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.236: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.236: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.236: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.236: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.236: RADIUS:   02 43 00 27 11 01 00 18 30 9F 55 AF 05 03 71 7D
    [?C?'????0?U???q}]
Apr  8 17:45:48.236: RADIUS:   25 41 1B B0 F4 A9 7C EE F5 51 24 9A FC 6D 51 6D
    [?A????|??Q$??mQm]
Apr  8 17:45:48.237: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.237: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless   [19]
Apr  8 17:45:48.237: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.238: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.238: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.242: RADIUS: Received from id 21645/94 10.0.0.3:1645,
    Access-Challenge, len 50
Apr  8 17:45:48.243: RADIUS:  authenticator 59 2D EE 24 CF B2 87 AF
    - 86 D0 C9 00 79 BE 6E 1E
Apr  8 17:45:48.243: RADIUS:  EAP-Message         [79]  6
Apr  8 17:45:48.243: RADIUS:   03 43 00 04
    [?C??]
Apr  8 17:45:48.244: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.244: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.244: RADIUS(0000001C): Received from id 21645/94
Apr  8 17:45:48.244: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:45:48.244: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
    found session timeout 20 sec
Apr  8 17:45:48.245: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_REPLY

)
for 0002.8aa6.304f
Apr  8 17:45:48.245: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.246: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.249: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:45:48.250: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.251: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
```

```
    [labap1200ip1]
Apr  8 17:45:48.251: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.251: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS(0000001C): sending
Apr  8 17:45:48.252: RADIUS(0000001C): Send Access-Request to
    10.0.0.3:1645 id 21645/95, len 150
Apr  8 17:45:48.252: RADIUS:  authenticator 39 1C A5 EF 86 9E BA D1
    - 50 FD 58 80 A8 8A BC 2A
Apr  8 17:45:48.253: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.253: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.253: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.253: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.254: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.254: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.254: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.254: RADIUS:   01 43 00 17 11 01 00 08 50 9A 67 2E 7D 26 75 AA
    [?C??????P?g.}&u?]
Apr  8 17:45:48.254: RADIUS:   61 69 72 6F 6E 65 74
    [aironet]
Apr  8 17:45:48.254: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless  [19]
Apr  8 17:45:48.254: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.255: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.255: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.260: RADIUS: Received from id 21645/95 10.0.0.3:1645,
    Access-Accept, len 206
Apr  8 17:45:48.260: RADIUS:  authenticator 39 13 3C ED FC 02 68 63
    - 24 13 1B 46 CF 93 B8 E3
Apr  8 17:45:48.260: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr  8 17:45:48.261: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.261: RADIUS:   02 00 00 27 11 01 00 18 FA 53 D0 29 6C 9D 66 8E
    [???'?????S?)l?f?]
Apr  8 17:45:48.262: RADIUS:   C4 A3 CD 54 08 8C 35 7C 74 0C 6A EF D4 6D 30 A4
    [???T??5|t?j??m0?]
Apr  8 17:45:48.262: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  59
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   53
    "leap:session-key=G:3asil;mwerAEJNYH-JxI,"
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  31
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   25
    "auth-algo-type=eap-leap"
Apr  8 17:45:48.262: RADIUS:  Class               [25]  31
Apr  8 17:45:48.263: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 64 36
    [CISCOACS:00001d6]
Apr  8 17:45:48.263: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 31 37
    [3/0a000066/17]
Apr  8 17:45:48.263: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.264: RADIUS(0000001C): Received from id 21645/95
Apr  8 17:45:48.264: RADIUS/DECODE: EAP-Message fragments, 39, total 39 bytes
Apr  8 17:45:48.264: found leap session key
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: PASS
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    found leap session key in server response
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
    leap session key length 16
Apr  8 17:45:48.266: dot11_auth_dot1x_run_rfsm:
```

```
    Executing Action(
SERVER_WAIT,SERVER_PASS
) for 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:45:48.266: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station RKIBBE-W2K4 0002.8aa6.304f Associated KEY_MGMT[NONE]
```

Notez le flux dans les débogages de **machine d'état**. Il y a une progression à travers plusieurs états :

1. DÉBUT_EAP
2. CLIENT_ATTENTE
3. RÉPONSE_CLIENT
4. SERVEUR_ATTENTE
5. RÉPONSE_SERVEUR

   Remarque : lorsque les deux négocient, il peut y avoir plusieurs itérations de CLIENT_WAIT et CLIENT_REPLY, ainsi que de SERVER_WAIT et de SERVER_REPLY.

6. PASSE_SERVEUR

Le débogage du **processus** montre chaque étape individuelle à travers chaque état. Les débogages **radius** montrent la conversation réelle entre le serveur d'authentification et le client. La façon la plus simple de travailler avec les débogages EAP est de regarder la progression des messages de machine d'état à travers chaque état.

Quand quelque chose échoue dans la négociation, les débogages de la **machine d'état** montrent pourquoi le processus s'est arrêté. Recherchez des messages similaires à ceux-ci :

- **CLIENT TIMEOUT** - Cet état indique que le client n'a pas répondu dans un délai approprié. Cette absence de réponse peut être due à l'une des raisons suivantes :
  - Il y a un problème avec le logiciel client.
  - La valeur du délai d'attente du client EAP (du sous-onglet Authentification EAP sous Sécurité avancée) a expiré.

  Certains EAP, en particulier le PEAP (Protected EAP), mettent plus de 30 secondes pour terminer l'authentification. Réglez ce compteur sur une valeur supérieure (entre 90 et 120 secondes).

  Voici un exemple d'une tentative de DÉLAI D'ATTENTE DU CLIENT :

Exemple **CLIENT TIMEOUT**

<#root>

```
Apr 12 17:51:09.373: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr 12 17:51:09.373: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0040.96a0.3758
Apr 12 17:51:09.374: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr 12 17:51:39.358: dot11_auth_dot1x_run_rfsm:
    Executing Action(
CLIENT_WAIT,TIMEOUT
) for 0040.96a0.3758
Apr 12 17:51:39.358: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0040.96a0.3758
Apr 12 17:51:39.358: %DOT11-7-AUTH_FAILED:
    Station 0040.96a0.3758 Authentication failed
```

Remarque : recherchez les messages d'erreur système similaires à ce message :

```
%DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached
          max retries, removing the client
```

Remarque : de tels messages d'erreur peuvent indiquer un problème de radiofréquence (RF).

- Non-concordance du secret partagé entre le point d'accès et le serveur RADIUS : dans cet exemple de journal, le serveur RADIUS n'accepte pas la demande d'authentification du point d'accès. Le point d'accès continue d'envoyer la demande au serveur RADIUS, mais le serveur RADIUS rejette la demande car le secret partagé ne correspond pas.

  Afin de résoudre ce problème, assurez-vous de vérifier que le secret partagé sur l'AP est le même que celui qui est utilisé dans le serveur RADIUS.

Non-concordance du secret partagé entre AP et le serveur RADIUS

```
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_DEAD:
    RADIUS server 10.10.1.172:1645, 1646 is not responding.
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server
    10.10.1.172:1645,1646 has returned.
Jun  2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758
    Authentication failed
```

- **server_timeout** : cet état indique que le serveur d'authentification n'a pas répondu dans un

délai approprié. Cette absence de réponse se produit en raison d'un problème sur le serveur. Vérifiez que ces situations sont vraies :

- Le point d'accès dispose d'une connectivité IP au serveur d'authentification.

  Remarque : vous pouvez utiliser la commande ping afin de vérifier la connectivité.

- Les numéros de port d'authentification et de comptabilité sont corrects pour le serveur.

  Remarque : vous pouvez vérifier les numéros de port dans l'onglet Gestionnaire de serveur.

- Le service d'authentification est en cours d'exécution et fonctionnel.

Voici un exemple de tentative de `server_timeout` :

Exemple `server_timeout`

<#root>

```
Apr  8 20:02:55.469: dot11_auth_dot1x_start:
    in the dot11_auth_dot1x_start
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 20:02:55.470: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,EAP_START

) for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 20:02:55.471: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.472: dot11_auth_parse_client_pak:
    id is not matching req-id:1resp-id:2, waiting for response
Apr  8 20:02:55.474: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 20:02:55.475: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [248] 14
Apr  8 20:02:55.476: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
```

```
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [150] 2
Apr  8 20:02:55.476: RADIUS(00000031): Storing nasport 32 in rad_db
Apr  8 20:02:55.476: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.476: RADIUS/ENCODE(00000031): acct_session_id: 49
Apr  8 20:02:55.477: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.477: RADIUS(00000031): sending
Apr  8 20:02:55.477: RADIUS(00000031): Send Access-Request
    to 10.0.0.3:1234 id 21645/145, len 139
Apr  8 20:02:55.478: RADIUS:  authenticator B6 F7 BB 41 0E 9F 44 D1
    - 9A F8 E2 D7 5D 70 F2 76
Apr  8 20:02:55.478: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 20:02:55.478: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 20:02:55.478: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 20:02:55.478: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 20:02:55.478: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 20:02:55.478: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 20:02:55.478: RADIUS:  EAP-Message         [79]  14
Apr  8 20:02:55.479: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
    [?????aironet]
Apr  8 20:02:55.479: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless [19]
Apr  8 20:02:55.479: RADIUS:  NAS-Port            [5]   6   32
Apr  8 20:02:55.479: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 20:02:55.480: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 20:03:00.478: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:05.475: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:10.473: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS:
    No response from (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response no app start; FAIL
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response; FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    detailed aaa_status 1
Apr  8 20:03:15.471: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 20:03:15.471: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 20:03:15.471: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- **SERVER_FAIL** - Cet état indique que le serveur a fourni une réponse d'authentification qui a échoué en fonction des informations d'identification de l'utilisateur. Le débogage RADIUS qui précède cet échec indique le nom d'utilisateur qui a été présenté au serveur d'authentification. Assurez-vous de vérifier le journal des tentatives ayant échoué dans le

serveur d'authentification pour plus de détails sur la raison pour laquelle le serveur a refusé l'accès client.

Voici un exemple de tentative de SERVER_FAIL :

Exemple SERVER_FAIL

<#root>

```
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:46:13.605: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:46:13.605: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:46:13.606: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:46:13.606: RADIUS(0000001D): Using existing nas_port 18
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS/ENCODE(0000001D): acct_session_id: 29
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS(0000001D): sending
Apr  8 17:46:13.607: RADIUS(0000001D): Send Access-Request
    to 10.0.0.3:1645 id 21645/97, len 176
Apr  8 17:46:13.607: RADIUS:  authenticator 88 82 8C BB DC 78 67 76
    - 36 88 1D 89 2B DC C9 99
Apr  8 17:46:13.607: RADIUS:  User-Name           [1]   14  "unknown_user"
Apr  8 17:46:13.607: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:46:13.608: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:46:13.608: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:46:13.608: RADIUS:  Service-Type        [6]   6   Login   [1]
Apr  8 17:46:13.608: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.608: RADIUS:  EAP-Message         [79]  46
Apr  8 17:46:13.608: RADIUS:  02 44 00 2C 11 01 00 18 02
    69 C3 F1 B5 90 52 F7    [?D?,?????i????R?]
Apr  8 17:46:13.609: RADIUS:
    B2 57 FF F0 74 8A 80 59 31 6D C7 30 D3 D0 AF 65
    [?W??t??Y1m?0???e]
Apr  8 17:46:13.609: RADIUS:   75 6E 6B 6E 6F 77 6E 5F 75 73 65 72
    [unknown_user]
Apr  8 17:46:13.609: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless           [19]
Apr  8 17:46:13.609: RADIUS:  NAS-Port            [5]   6   18
Apr  8 17:46:13.610: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:46:13.610: RADIUS:  Nas-Identifier      [32]  16
    "labap1200ip102"
Apr  8 17:46:13.622: RADIUS: Received from id 21645/97
    10.0.0.3:1645,

Access-Reject

, len 56
Apr  8 17:46:13.622: RADIUS:  authenticator 55 E0 51 EF DA CE F7 78
    - 92 72 3D 97 8F C7 97 C3
Apr  8 17:46:13.622: RADIUS:  EAP-Message         [79]  6
Apr  8 17:46:13.623: RADIUS:   04 44 00 04                          [?D??]
Apr  8 17:46:13.623: RADIUS:  Reply-Message       [18]  12
Apr  8 17:46:13.623: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D  [Rejected??]
```

```
Apr  8 17:46:13.623: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.624: RADIUS(0000001D): Received from id 21645/97
Apr  8 17:46:13.624: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:46:13.624: RADIUS/DECODE: Reply-Message fragments,
    10, total 10 bytes
Apr  8 17:46:13.624: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 17:46:13.625: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:46:13.625: dot11_auth_dot1x_run_rfsm:
    xecuting Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 17:46:13.625: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:46:13.626: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:46:13.626: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- No Response from Client : dans cet exemple, le serveur RADIUS envoie un message de passe au point d'accès, que le point d'accès transfère, puis il associe le client. Finalement, le client ne répond pas au point d'accès. Par conséquent, le point d'accès le désauthentifie après avoir atteint le nombre maximal de nouvelles tentatives.

Aucune réponse du client

```
<#root>

Sep 22 08:42:04: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 08:42:04: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Associated KEY_MGMT[NONE]
Sep 22 10:35:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:35:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,


Deauthenticating Station

 0040.96a0.3758
    Reason: Previous authentication no longer valid
```

Le point d’accès transmet une réponse de demande de confirmation du radius au client. Le client ne répond pas et atteint le nombre maximal de tentatives, ce qui entraîne l’échec d’EAP et la désauthentification du client par l’AP.

Aucune réponse du client

<#root>

```
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Sep 22 10:43:02: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:43:05: %DOT11-4-MAXRETRIES: Packet to client 0040.96a0.3758
    reached
```

max retries

```
, removing the client
Sep 22 10:43:05: Client 0040.96a0.3758 failed: reached maximum retries
```

Radius envoie un message de passe au point d'accès, le point d'accès transfère le message de passe au client et ce dernier ne répond pas. Le point d'accès le désauthentifie après avoir atteint le nombre maximal de nouvelles tentatives. Le client tente ensuite une nouvelle demande d'identité au point d'accès, mais le point d'accès rejette cette demande car le client a déjà atteint le nombre maximal de nouvelles tentatives.

Aucune réponse du client

<#root>

```
Sep 22 10:57:08: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:57:08: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Reassociated KEY_MGMT[NONE]
Sep 22 10:57:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached max retries, removing the client
Sep 22 10:57:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station0040.96a0.3758 Reason:
    Previous authentication no longer valid
Sep 22 10:57:15: AAA/BIND(00001954): Bind i/f
```

```
Sep 22 10:57:15: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Sending identity request to 0040.96a0.3758
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Client 0040.96a0.3758 timer started for 30 seconds
Sep 22 10:57:15: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:57:15: Client 0040.96a0.3758 failed: reached maximum retries
```

Les débogages de **processus** et/ou de **radius** qui précèdent immédiatement le message de machine d'état montrent les détails de l'échec.

Pour plus d'informations sur la façon de configurer EAP, référez-vous à Authentification EAP avec le serveur RADIUS.

Authentification MAC

Ces débogages sont les plus utiles pour l'authentification MAC :

- debug radius authentication : lorsqu'un serveur d'authentification externe est utilisé, les résultats de ce débogage commencent par ce mot : `RADIUS`.
- debug dot11 aaa authenticator mac-authen : les résultats de ce débogage commencent par ce texte : `dot11_auth_dot1x_`.

Ces débogages montrent :

- Ce qui est rapporté pendant les parties RADIUS d'une boîte de dialogue d'authentification
- Comparaison entre l'adresse MAC fournie et celle qui est authentifiée par rapport à

Lorsqu'un serveur RADIUS externe est utilisé avec l'authentification d'adresse MAC, les débogages RADIUS s'appliquent. Le résultat de cette conjonction est un affichage de la conversation réelle entre le serveur d'authentification et le client.

Lorsqu'une liste d'adresses MAC est créée localement sur le périphérique en tant que base de données de nom d'utilisateur et de mot de passe, seuls les débogages **mac-authen** affichent les résultats. Lorsque la correspondance ou la non-correspondance d'adresses est déterminée, ces sorties s'affichent.

Remarque : saisissez toujours des caractères alphabétiques en minuscules dans une adresse MAC.

Cet exemple illustre une authentification MAC réussie par rapport à une base de données locale :

Exemple d'authentification MAC réussie

```
Apr  8 19:02:00.109: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:02:00.109: dot11_auth_mac_start: method_index: 0x4500000B, req: 0xA7626C
Apr  8 19:02:00.109: dot11_auth_mac_start: client->unique_id: 0x28
Apr  8 19:02:00.110: dot11_mac_process_reply: AAA reply for 0002.8aa6.304f PASSED
Apr  8 19:02:00.145: %DOT11-6-ASSOC: Interface Dot11Radio0, Station RKIBBE-W2K4
    0002.8aa6.304f Associated KEY_MGMT[NONE]
```

Cet exemple montre l'échec de l'authentification MAC sur une base de données locale :

Exemple d'authentification MAC défaillante

```
Apr  8 19:01:22.336: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:01:22.336: dot11_auth_mac_start: method_index: 0x4500000B,
    req: 0xA7626C
Apr  8 19:01:22.336: dot11_auth_mac_start: client->unique_id: 0x27
Apr  8 19:01:22.337: dot11_mac_process_reply:
    AAA reply for 0002.8aa6.304f FAILED
Apr  8 19:01:22.337: %DOT11-7-AUTH_FAILED:
    Station 0002.8aa6.304f Authentication failed
```

Lorsqu'une authentification d'adresse MAC échoue, vérifiez l'exactitude des caractères entrés dans l'adresse MAC. Assurez-vous que vous avez saisi des caractères alphabétiques en minuscules dans une adresse MAC.

Pour plus d'informations sur la façon de configurer l'authentification MAC, référez-vous à Configuration des types d'authentification (Guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet, 12.2(13)JA).

WPA

Bien que le protocole WPA (Wi-Fi Protected Access) ne soit pas un type d'authentification, il s'agit d'un protocole négocié.

- WPA négocie entre le point d'accès et la carte client.
- La gestion des clés WPA négocie après l'authentification réussie d'un client par un serveur d'authentification.
- WPA négocie à la fois une PTK (Pairwise Transient Key) et une GTK (Groupwise Transient Key) dans une connexion en quatre étapes.

Remarque : comme WPA nécessite que l'EAP sous-jacent réussisse, vérifiez que les clients peuvent s'authentifier avec cet EAP avant d'activer WPA.

Ces débogages sont les plus utiles pour les négociations WPA :

- debug dot11 aaa authenticator process : les résultats de ce débogage commencent par le texte suivant : `dot11_auth_dot1x_`.
- debug dot11 aaa authenticator state-machine : les résultats de ce débogage commencent par le texte suivant : `dot11_auth_dot1x_run_rfsm`.

Par rapport aux autres authentifications de ce document, les débogages WPA sont simples à lire et à analyser. Un message PTK doit être envoyé et une réponse appropriée doit être reçue. Ensuite, un message GTK doit être envoyé et une autre réponse appropriée reçue.

Si les messages PTK ou GTK ne sont pas envoyés, la configuration ou le niveau logiciel sur l'AP peut être en défaut. Si les réponses PTK ou GTK du client ne sont pas reçues, vérifiez la configuration ou le niveau de logiciel sur le demandeur WPA de la carte client.

Exemple de négociation WPA réussie

```
<#root>

labap1200ip102#

Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake:
    building PTK msg 1 for 0030.6527.f74a

Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake:
    verifying PTK msg 2 from 0030.6527.f74a

Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)

Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake:
    building PTK msg 3 for 0030.6527.f74a

Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake:
    verifying PTK msg 4 from 0030.6527.f74a

Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)

Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
    building GTK msg 1 for 0030.6527.f74a

Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
    dot11_dot1x_get_multicast_key len 32 index 1
Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK:
    27 CA 88 7D 03 D9 C4 61 FD 4B BE 71 EC F7 43 B5 82 93 57 83

Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake:
    verifying GTK msg 2 from 0030.6527.f74a

Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header:
    Warning: Invalid key info (exp=0x391, act=0x301
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning:
    Invalid key len (exp=0x20, act=0x0)

Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station   0030.6527.f74a Associated KEY_MGMT[WPA]
```

```
labap1200ip102#
```

Pour plus d'informations sur la façon de configurer WPA, référez-vous à Vue d'ensemble de la configuration WPA.

Authentification administrative/HTTP

Vous pouvez limiter l'accès administratif au périphérique aux utilisateurs répertoriés dans une base de données locale de noms d'utilisateurs et de mots de passe ou à un serveur d'authentification externe. L'accès administratif est pris en charge avec RADIUS et TACACS+.

Ces débogages sont les plus utiles pour l'authentification administrative :

- debug radius authentication ou debug tacacs authentication : les résultats de ce débogage commencent par l'un des mots suivants : `RADIUS` ou `TACACS`.
- debug aaa authentication : les résultats de ces débogages commencent par ce texte : `AAA/AUTHEN`.
- debug aaa authorization : les résultats de ces débogages commencent par ce texte : `AAA/AUTEUR`.

Ces débogages montrent :

- Ce qui est rapporté pendant les parties RADIUS ou TACACS d'une boîte de dialogue d'authentification
- Négociations réelles pour l'authentification et l'autorisation entre le périphérique et le serveur d'authentification

Cet exemple montre une authentification administrative réussie lorsque l'attribut `Service-Type RADIUS` est défini sur `Administrative` :

Exemple d'authentification administrative réussie avec un attribut de type de service

```
<#root>

Apr 13 19:43:08.030: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 19:43:08.030: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0
    adapter=0 port=2 channel=0
Apr 13 19:43:08.031: AAA/MEMORY: create_user (0xA1BB6C) user='NULL' ruser='NULL'
    ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGINN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): port='tty2'
    list='' action=LOGIN service=LOGIN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): using "default" list
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540):
    Method=tac_admin (tacacs+)
Apr 13 19:43:08.032: TAC+: send AUTHEN/START packet ver=192 id=3200017540
```

```
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=ERROR
Apr 13 19:43:08.032: AAA/AUTHEN/START (3200017540):
    Method=rad_admin (radius)
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN/CONT (3200017540):
    continue_login (user='(undef)')
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN/CONT (3200017540):
    continue_login (user='aironet')
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
Apr 13 19:43:08.033: RADIUS: Pick NAS IP for u=0xA1BB6C tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:43:08.033: RADIUS: ustruct sharecount=1
Apr 13 19:43:08.034: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:43:08.034: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
    id 21646/48, len 76
Apr 13 19:43:08.034: RADIUS:  authenticator 91 A0 98 87 C1 FC F2 E7
    - E7 E4 57 DF 20 D0 82 27
Apr 13 19:43:08.034: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:43:08.034: RADIUS:  NAS-Port            [5]   6   2
Apr 13 19:43:08.035: RADIUS:  NAS-Port-Type       [61]  6   Virtual         [5]
Apr 13 19:43:08.035: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:43:08.035: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:43:08.035: RADIUS:  User-Password       [2]   18  *
Apr 13 19:43:08.042: RADIUS: Received from id 21646/48 10.0.0.3:1645,
    Access-Accept, len 62
Apr 13 19:43:08.042: RADIUS:  authenticator C9 32 E7 8F 97 5F E6 4C
    - 6B 90 71 EE ED 2C 2B 2B
Apr 13 19:43:08.042:

RADIUS:  Service-Type        [6]   6
    Administrative            [6]

Apr 13 19:43:08.042: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:43:08.042: RADIUS:  Class               [25]  30
Apr 13 19:43:08.043: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 36
    [CISCOACS:00000366]
Apr 13 19:43:08.043: RADIUS:   39 2F 30 61 30 30 30 30 36 36 2F 32
    [9/0a000066/2]
Apr 13 19:43:08.044: RADIUS: saved authorization data for user A1BB6C at B0C260
Apr 13 19:43:08.044: AAA/AUTHEN(3200017540): Status=PASS
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147):
    Port='tty2' list='' service=EXEC
Apr 13 19:43:08.044: AAA/AUTHOR/HTTP: tty2(1763745147) user='aironet'
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV service=shell
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV cmd*
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): found list "default"
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): Method=tac_admin (tacacs+)
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): user=aironet
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV service=shell
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV cmd*
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147): Post authorization status = ERROR
Apr 13 19:43:08.046: tty2 AAA/AUTHOR/HTTP(1763745147):
    Method=rad_admin (radius)
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147):
    Post authorization status = PASS_ADD
Apr 13 19:43:08.443: AAA/MEMORY: free_user (0xA1BB6C) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGIN
```

Cet exemple montre une authentification administrative réussie lorsque vous utilisez des attributs spécifiques au fournisseur afin d'envoyer une instruction de niveau privé :

Exemple d'authentification administrative réussie avec un attribut spécifique au fournisseur

<#root>

```
Apr 13 19:38:04.699: RADIUS: cisco AVPair ""shell:priv-lvl=15""
    not applied for shell
Apr 13 19:38:04.699: AAA/AUTHOR (380584213): Post authorization status
    = PASS_ADD
Apr 13 19:38:04.802: AAA/MEMORY: free_user (0xAA0E38) user='aironet'
    ruser='NULL' port='tty3' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN
Apr 13 19:38:04.901: AAA: parse name=tty3 idb type=-1 tty=-1
Apr 13 19:38:04.901: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0
    adapter=0  port=3 channel=0
Apr 13 19:38:04.902: AAA/MEMORY: create_user (0xAA23BC) user='NULL'
    ruser='NULL' ds0=0 port='tty3' rem_addr='10.0.0.25'
    authen_type=ASCII service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): port='tty3' list=''
    action=LOGIN service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): using "default" list
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=tac_admin (tacacs+)
Apr 13 19:38:04.902: TAC+: send AUTHEN/START packet ver=192 id=1346300140
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=ERROR
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN/CONT (1346300140): continue_login
    (user='(undef)')
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN/CONT (1346300140): continue_login
    (user='aironet')
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: RADIUS: Pick NAS IP for u=0xAA23BC tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:38:04.904: RADIUS: ustruct sharecount=1
Apr 13 19:38:04.904: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:38:04.925: RADIUS(00000000): Send Access-Request to
    10.0.0.3:1645 id 21646/3, len 76
Apr 13 19:38:04.926: RADIUS:  authenticator 0C DD 2B B7 CA 5E 7C B9
    - 46 90 FD 7A FD 56 3F 07
Apr 13 19:38:04.926: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:38:04.926: RADIUS:  NAS-Port            [5]   6   3
Apr 13 19:38:04.926: RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
Apr 13 19:38:04.926: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:38:04.926: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:38:04.926: RADIUS:  User-Password       [2]   18  *
Apr 13 19:38:04.932: RADIUS: Received from id 21646/3 10.0.0.3:1645,
    Access-Accept, len 89
Apr 13 19:38:04.933: RADIUS:  authenticator FA A4 31 49 51 87 9D CA
    - 9D F7 B3 9B EF C2 8B 7E
Apr 13 19:38:04.933: RADIUS:  Vendor, Cisco       [26]  27
Apr 13 19:38:04.933: RADIUS:
```

```
   Cisco AVpair     [1]   21  ""shell:priv-lvl=15""

Apr 13 19:38:04.934: RADIUS:  Service-Type        [6]   6   Login       [1]
Apr 13 19:38:04.934: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:38:04.934: RADIUS:  Class               [25]  30
Apr 13 19:38:04.934: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 33
    [CISCOACS:0000363]
Apr 13 19:38:04.934: RADIUS:   61 2F 30 61 30 30 30 30 36 36 2F 33
    [a/0a000066/3]
Apr 13 19:38:05.634: AAA/AUTHOR (3854191802): Post authorization
    status = PASS_ADD
Apr 13 19:38:05.917: AAA/MEMORY: free_user (0xA9D054) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0
```

Le problème le plus courant avec l'authentification administrative est l'échec de la configuration du serveur d'authentification pour envoyer les attributs de niveau de privilège ou de type de service administratif appropriés. Cet exemple a échoué lors de l'authentification administrative car aucun attribut de niveau privilège ou de type de service administratif n'a été envoyé :

Sans attributs spécifiques au fournisseur ou au type de service

<#root>

```
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Port='tty3'
    list=''

service=EXEC

Apr 13 20:02:59.516: AAA/AUTHOR/HTTP: tty3(2007927065) user='aironet'
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV service=shell
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV cmd*
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): found list "default"
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Method=tac_admin (tacacs+)
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): user=aironet
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV service=shell
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV cmd*
Apr 13 20:02:59.516: AAA/AUTHOR (2007927065): Post authorization status = ERROR
Apr 13 20:02:59.517: tty3 AAA/AUTHOR/HTTP(2007927065): Method=rad_admin (radius)
Apr 13 20:02:59.517: AAA/AUTHOR (2007927065): Post authorization status = PASS_ADD
Apr 13 20:02:59.561: AAA/MEMORY: free_user (0xA756E8) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0  vrf= (id=0)
Apr 13 20:02:59.620: AAA/MEMORY: free_user (0x9E5B04) user='aironet'
    ruser='NULL'  port='tty3' rem_addr='10.0.0.25' authen_type=ASCII


service=LOGIN

 priv=0 vrf= (id=0)
Apr 13 20:03:04.501: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 20:03:04.501: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0
    port=2 channel=0
Apr 13 20:03:04.502: AAA/MEMORY: create_user (0xA9C7A4) user='NULL'
    ruser='NULL' ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): port='tty2' list=''
```

```
    action=LOGIN service=LOGIN
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): using "default" list
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=tac_admin (tacacs+)
Apr 13 20:03:04.503: TAC+: send AUTHEN/START packet ver=192 id=377202642
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=ERROR
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN/CONT (377202642): continue_login (user='(undef)')
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETPASS
Apr 13 20:03:04.504: AAA/AUTHEN/CONT (377202642): continue_login (user='aironet')
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Status=GETPASS
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.504: RADIUS: Pick NAS IP for u=0xA9C7A4 tableid=0
    cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 20:03:04.505: RADIUS: ustruct sharecount=1
Apr 13 20:03:04.505: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 20:03:04.505: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
    id 21646/59, len 76
Apr 13 20:03:04.505: RADIUS:  authenticator 0F BD 81 17 8F C5 1C B4
    - 84 1C 66 4D CF D4 96 03
Apr 13 20:03:04.505: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 20:03:04.506: RADIUS:  NAS-Port            [5]   6   2
Apr 13 20:03:04.506: RADIUS:  NAS-Port-Type       [61]  6   Virtual           [5]
Apr 13 20:03:04.506: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 20:03:04.506: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 20:03:04.507: RADIUS:  User-Password       [2]   18  *
Apr 13 20:03:04.513: RADIUS: Received from id 21646/59 10.0.0.3:1645,


Access-Accept

, len 56
Apr 13 20:03:04.513: RADIUS:  authenticator BB F0 18 78 33 D0 DE D3
    - 8B E9 E0 EE 2A 33 92 B5
Apr 13 20:03:04.513: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 20:03:04.513: RADIUS:  Class               [25]  30
Apr 13 20:03:04.514: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 38
    [CISCOACS:0000368]
Apr 13 20:03:04.514: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 32
    [3/0a000066/2]
Apr 13 20:03:04.515: RADIUS: saved authorization data for user A9C7A4 at A9C99C
Apr 13 20:03:04.515: AAA/AUTHEN(377202642): Status=PASS
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): Port='tty2' list=''
    service=EXEC
Apr 13 20:03:04.515: AAA/AUTHOR/HTTP: tty2(2202245138) user='aironet'
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV service=shell
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV cmd*
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): found list "default"
Apr 13 20:03:04.516: tty2 AAA/AUTHOR/HTTP(2202245138): Method=tac_admin (tacacs+)
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): user=aironet
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV service=shell
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV cmd*
Apr 13 20:03:04.517:

AAA/AUTHOR

(2202245138):

Post authorization status = ERROR

Apr 13 20:03:04.517: tty2 AAA/AUTHOR/HTTP(2202245138): Method=rad_admin (radius)
```

```
Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post authorization status
    = PASS_ADD
Apr 13 20:03:04.619: AAA/MEMORY: free_user (0xA9C7A4) user='aironet'
    ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
    service=LOGIN priv=0 vrf=
```

Pour plus d'informations sur la façon de configurer l'authentification administrative, référez-vous à Administration du point d'accès (Guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet, 12.2(13)JA).

Pour plus d'informations sur la façon de configurer le privilège d'administration pour les utilisateurs sur le serveur d'authentification, référez-vous à Exemple de configuration : Authentification locale pour les utilisateurs du serveur HTTP. Vérifiez la section qui correspond au protocole d'authentification que vous utilisez.

Informations connexes

- Guide de configuration du logiciel Cisco IOS pour points d'accès Cisco Aironet, 12.2(13)JA
- Authentification EAP avec le serveur RADIUS
- Authentification LEAP avec serveur RADIUS local
- Sécurité sans fil Cisco Aironet - Forum Aux Questions
- Exemple de configuration d'un point d'accès des services de domaine sans fil en tant que serveur AAA
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.