Déboguer les authentifications

Contenu

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 se rapportent à des Produits de non-Cisco sont basées sur l'expérience de l'auteur, pas sur la formation formelle. Ils sont destinés pour votre commodité et pas comme Soutien technique. Pour le Soutien technique bien fondé sur des Produits de non-Cisco, entrez en contact avec le Soutien technique pour ce produit.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification comme elle associe aux réseaux Sans fil
- Interface de ligne de commande de logiciel de 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 articulés autour d'un logiciel de Cisco IOS de tous modèle et version
- HyperTerminal de Hilgraeve

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.

Conventions

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

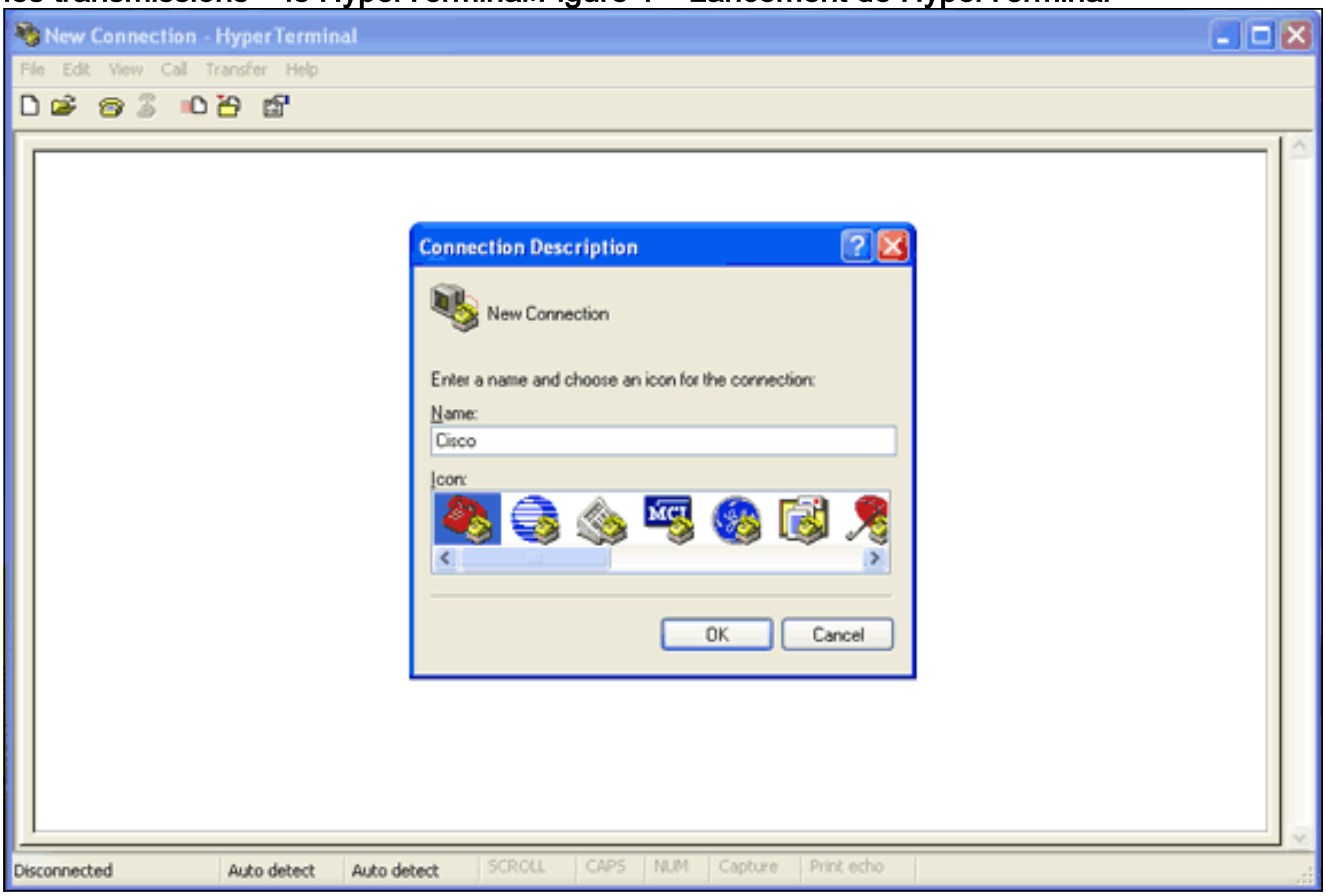
Debugs de capture

Si vous ne pouvez pas capturer et analyser mettez au point les informations, les informations sont inutiles. Le moyen le plus simple de capturer ces données est avec une fonction de capture d'écran qui est établie dans le telnet ou l'application des communications.

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

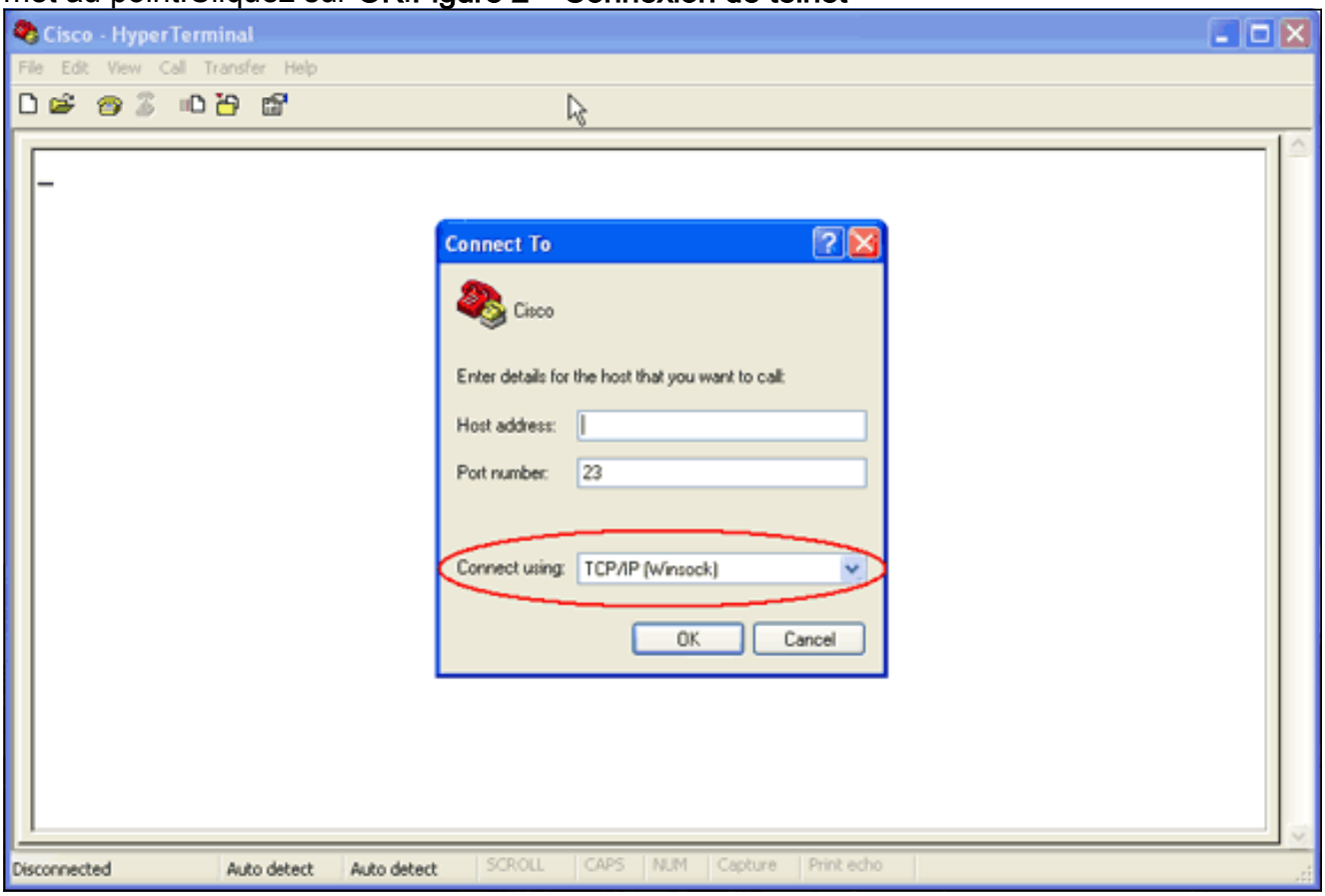
Terminez-vous ces étapes afin de configurer le HyperTerminal pour communiquer avec votre Point d'accès (AP) ou passerelle :

1. Afin d'ouvrir le HyperTerminal, choisissez le **début > les programmes > les outils système > les transmissions > le HyperTerminal**.**Figure 1 – Lancement de HyperTerminal**

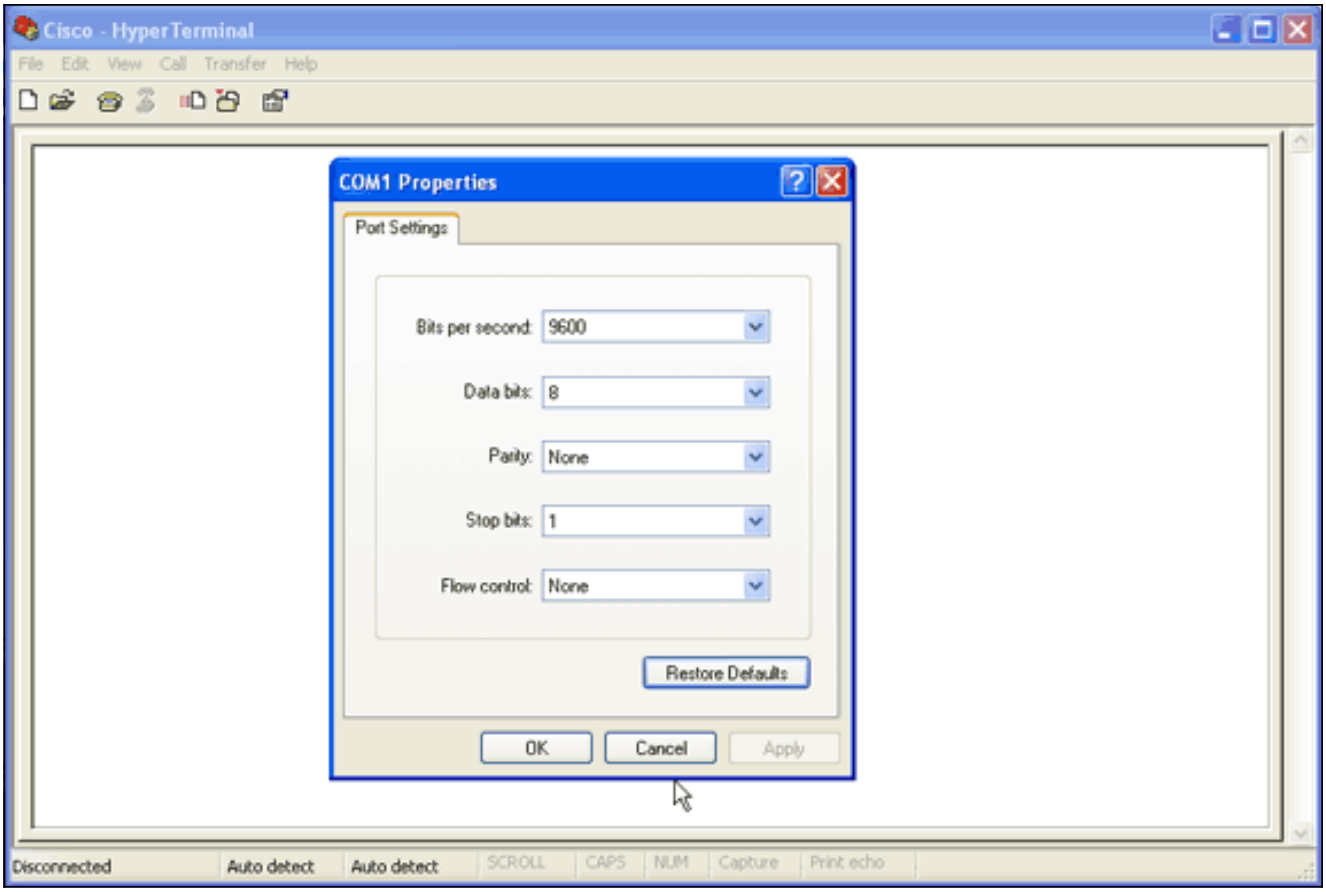


2. Quand le HyperTerminal s'ouvre, terminez-vous ces étapes :Écrivez un nom pour la connexion.Choisissez une icône.Cliquez sur **OK**.

3. Pour des connexions de telnet, terminez-vous ces étapes :Du connecter utilisant le menu déroulant, choisissez le **TCP/IP**.Écrivez l'adresse IP du périphérique où vous voulez exécuter met au point.Cliquez sur **OK**.**Figure 2 – Connexion de telnet**

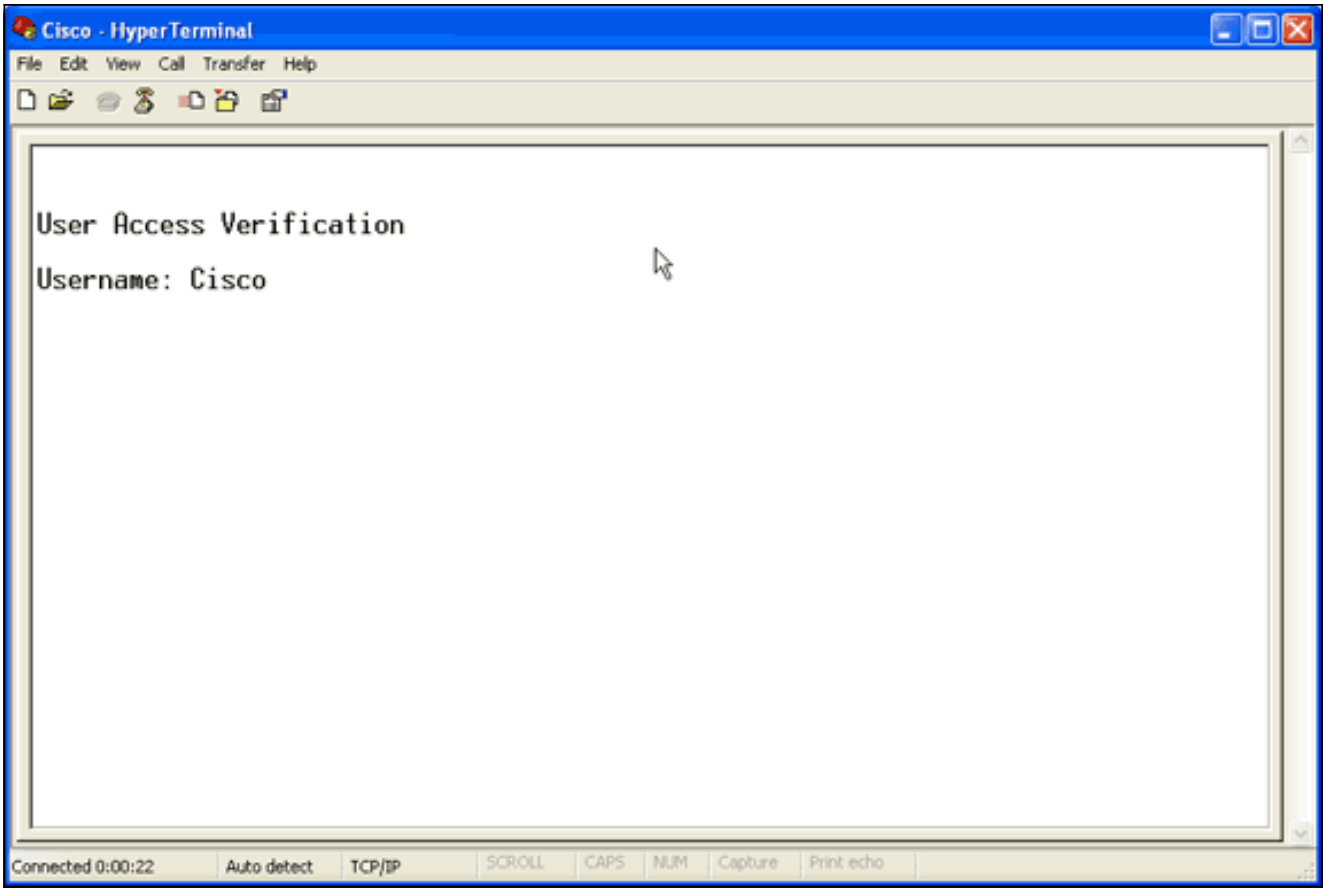


4. Pour des connexions de console, terminez-vous ces étapes :Du connecter utilisant le menu déroulant, choisissez le port COM où le câble de console est connecté.Cliquez sur **OK**.La fiche de propriété pour la connexion apparaît.Placez la vitesse pour la connexion au port de console.Afin de restaurer les configurations par défaut de port, la **restauration de** clic **se transfère**.**Remarque:** La plupart des Produits Cisco suivent les configurations par défaut de port.Les configurations par défaut de port sont :Bits par seconde — 9600Bits de données — 8Parité — AucunBits d'arrêt — 1Contrôle de flux — Aucun**Figure 3 – COM1 Properties**

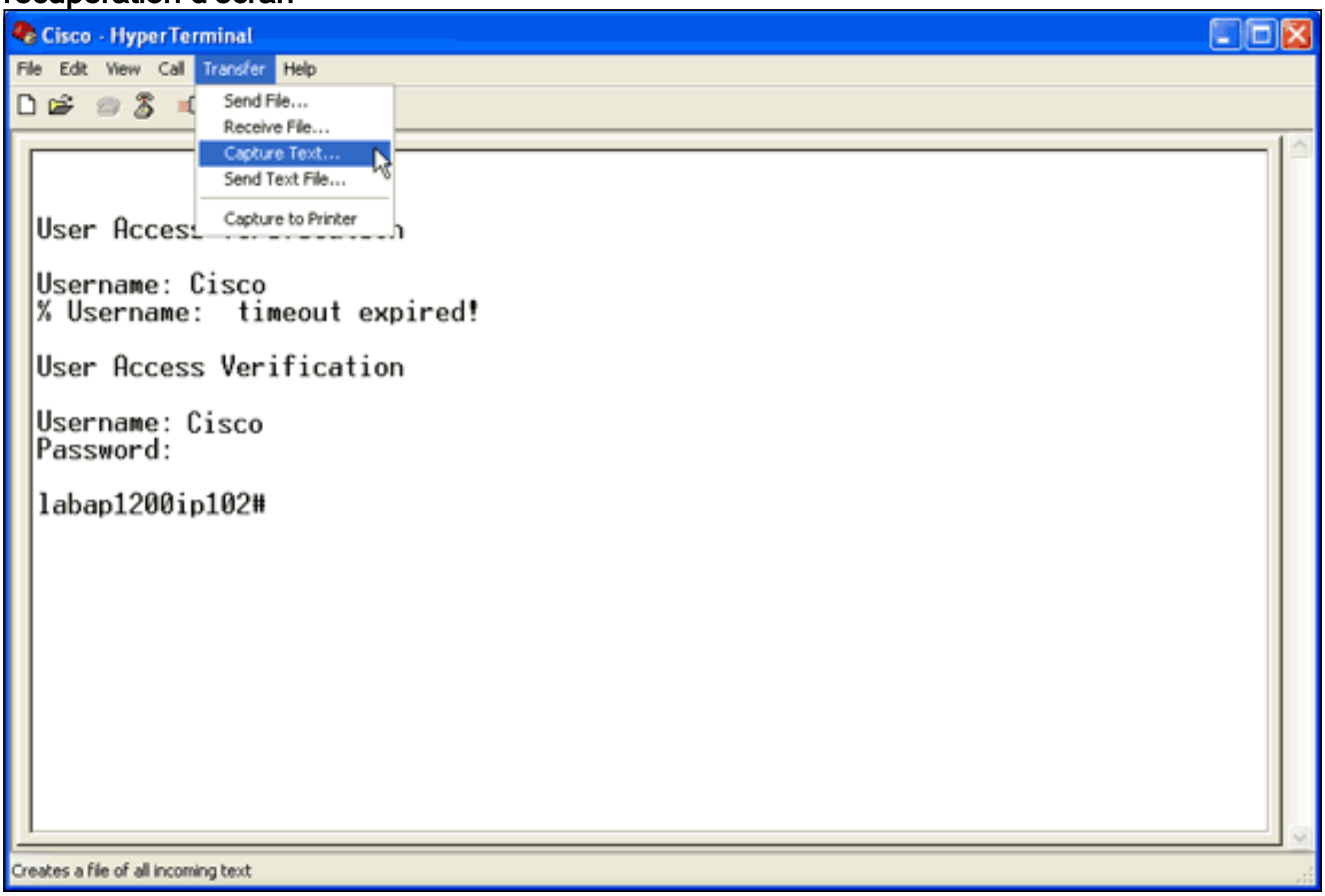


En ce moment, le telnet ou la connexion de console établit, et vous êtes incité pour un nom d'utilisateur et un mot de passe.**Remarque:** L'équipement Cisco Aironet génère un nom d'utilisateur par défaut et le mot de passe de *Cisco* (distinguant majuscules et minuscules).

5. Afin de s'exécuter met au point, se termine ces étapes :Émettez la commande d'**enable** afin d'entrer le mode privilégié.Entrez le mot de passe d'enable.**Remarque:** Souvenez-vous que le mot de passe par défaut pour le matériel d'Aironet est *Cisco* (distinguant majuscules et minuscules).**Remarque:** Afin de voir la sortie de met au point d'une session de telnet, emploie le **terminal monitor** ou la commande de **lundi de terme** afin d'activer le terminal monitor.**Figure 4 – Session de telnet connectée**



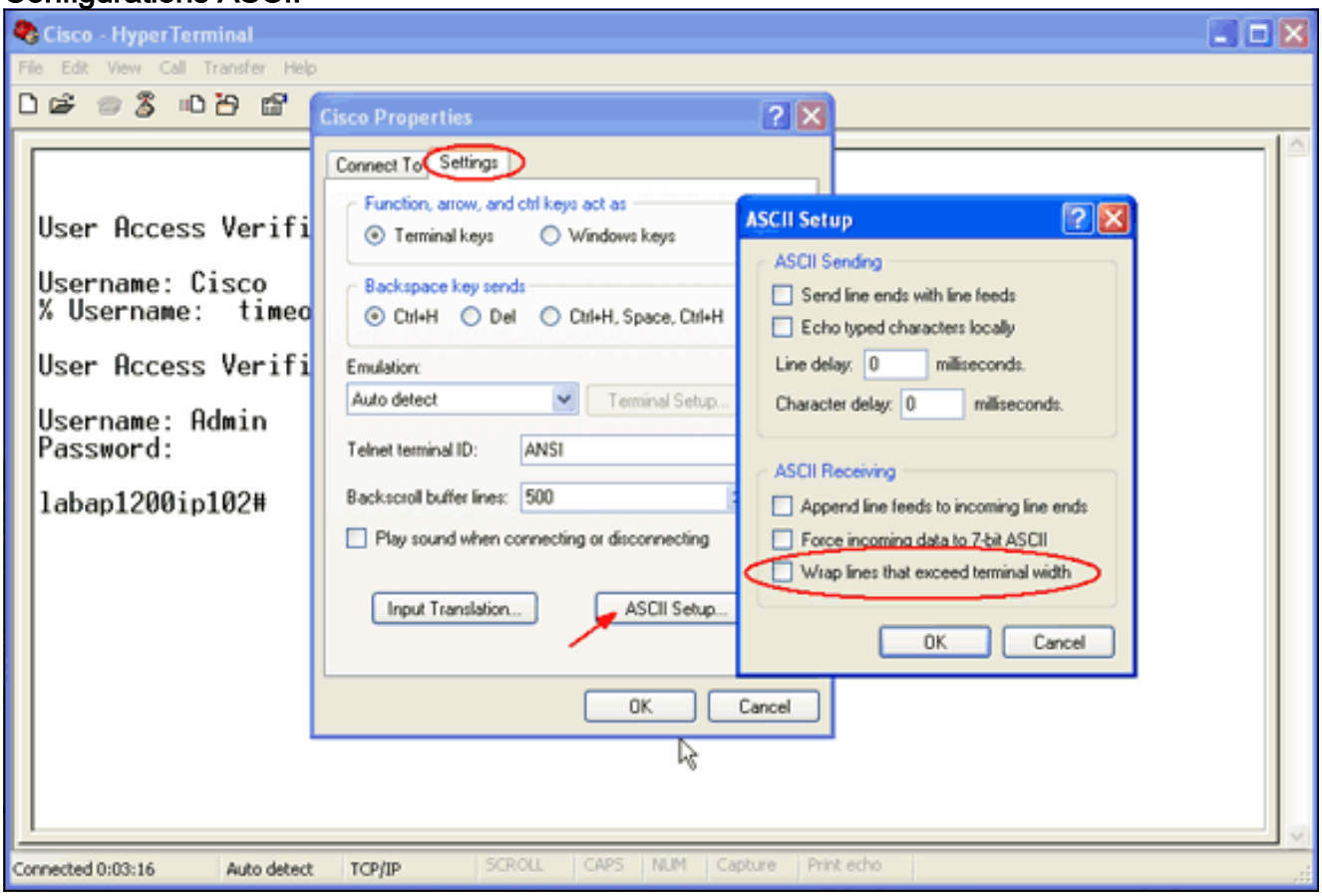
6. Après que vous établissiez une connexion, terminez-vous ces étapes afin de collecter une capture d'écran :Choisissez la **capture text du** menu de transfert.**Figure 5 – Sauvegardez une récupération d'écran**



Quand une boîte de dialogue s'ouvre que vous incite pour un nom du fichier pour la sortie, écrivez un nom du fichier.

7. Terminez-vous ces étapes afin de désactiver le bouclage d'écran :**Remarque:** Vous pouvez

lire met au point plus facilement quand vous désactivez le bouclage d'écran.Du menu de HyperTerminal, choisissez le **fichier**.Choisissez **Properties**.Sur la fiche de propriété de la connexion, cliquez sur l'**onglet Settings**.**Installation du** clic **ASCII**.Décochez les **lignes de bouclage qui dépassent le terminal width**.Afin de fermer les configurations ASCII, cliquez sur OK.Afin de fermer la fiche de propriété de la connexion, cliquez sur OK.**Figure 6 – Configurations ASCII**



Maintenant que vous pouvez saisir n'importe quelle sortie d'écran à un fichier texte, met au point que vous vous exécutez dépendez de ce qui est négocié. Les sections suivantes de ce document décrivent le type de connexion négociée fournie par met au point.

EAP

Ceux-ci met au point sont les plus utiles pour des authentifications EAP :

- **authentification de debug radius** — Les sorties de ceci mettent au point le début avec ce mot : `RAYON`.
- **processus d'authentificateur de debug dot11 aaa** — Les sorties de ceci mettent au point le début avec ce texte : `dot11_auth_dot1x_`.
- **state-machine d'authentificateur de debug dot11 aaa** — Les sorties de ceci mettent au point le début avec ce texte : `dot11_auth_dot1x_run_rfsm`.

Ceux-ci met au point l'exposition :

- Ce qui est signalé pendant les parties de RAYON d'un dialogue d'authentification
- Les mesures qui sont prises pendant ce dialogue d'authentification
- Les divers états par lesquels les transitions de dialogue d'authentification

Cet exemple affiche une authentification légère réussie d'EAP (LEAP) :

Exemple réussi d'authentification EAP

```
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 que l'écoulement dans le **state-machine** met au point. Il y a une progression par plusieurs états :

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY**Remarque:** En tant que deux négociez, il peut y avoir plusieurs itérations de CLIENT_WAIT et CLIENT_REPLY, aussi bien que SERVER_WAIT et de SERVER_REPLY.
6. SERVER_PASS

Le processus mettent au point des expositions chaque étape individuelle par chaque état. **Le rayon** met au point l'exposition la conversation réelle entre le serveur d'authentification et le client. Le moyen le plus simple de fonctionner avec l'EAP met au point est d'observer la progression des messages d'ordinateur d'état par chaque état.

Quand quelque chose échoue dans la négociation, le **state-machine** met au point l'exposition pourquoi le processus a arrêté. Observez pour des messages semblables à ces exemples :

- **DÉLAI D'ATTENTE de CLIENT** — Cet état indique que le client n'a pas répondu dans une durée appropriée. Ce manque de répondre peut se produire en raison d'une de ces raisons :Il y a un problème avec le logiciel client.La valeur du dépassement de durée de client d'EAP (du subtab d'authentification EAP sous la sécurité avancée) a expiré.Quelques eap, en particulier l'EAP protégé (PEAP), prennent plus long que 30 secondes pour se terminer l'authentification. Placez ce temporisateur à une valeur supérieure (entre 90 et 120 secondes).C'est un exemple d'une tentative de DÉLAI D'ATTENTE de CLIENT :**Remarque:** Observez pour tous les messages d'erreur de système qui sont semblables 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 secrète partagée entre AP et le serveur de RAYON** — dans ce log d'exemple, le serveur de RAYON ne reçoit pas la demande d'authentification d'AP. AP continue à envoyer la demande au serveur de RAYON, mais le serveur de RAYON rejette la demande parce que le secret partagé est mal adapté.Afin de résoudre ce problème, soyez sûr de vérifier que le secret partagé sur AP est le même qui est utilisé dans le serveur de RAYON.
- **server_timeout** — Cet état indique que le serveur d'authentification n'a pas répondu dans une durée appropriée. Ce manque de répondre se produit en raison d'un problème sur le serveur. Vérifiez que ces situations sont vraies :AP a la connectivité IP au serveur d'authentification.**Remarque:** Vous pouvez employer la **commande ping** afin de vérifier la Connectivité.L'authentification et les nombres de port de traçabilité sont corrects pour le serveur.**Remarque:** Vous pouvez vérifier les numéros de port de l'onglet de gestionnaire du serveur.Le service d'authentification est courant et fonctionnel.C'est un exemple d'une tentative de server_timeout :
- **SERVER_FAIL** — Cet état indique que le serveur a donné une réponse d'authentification infructueuse basée sur les identifiants utilisateurs. Le RAYON mettent au point qui précède

cette panne affiche le nom d'utilisateur qui a été présenté au serveur d'authentification. Soyez sûr de vérifier la procédure de connexion d'essais ratés le serveur d'authentification pour des détails supplémentaires sur pourquoi le serveur a refusé l'accès client.C'est un exemple d'une tentative `SERVER_FAIL` :

- **Aucune réponse de client** — Dans cet exemple, le serveur de rayon envoie un message de passage à AP qu'AP en avant en fonction et alors il associe le client. Par la suite le client ne répond pas à AP. Par conséquent, AP le désauthentifie après qu'il atteigne les relances maximum.AP en avant une réponse de défi d'obtenir du rayon au client. Le client ne répond pas et atteint des relances maximum qui fait échouer l'EAP et AP pour désauthentifier le client.Le rayon envoie un message de passage à AP, AP en avant le message de passage au client, et le client ne répond pas. AP le désauthentifie après qu'il atteigne les relances maximum. Le client tente alors une nouvelle demande d'identité à AP, mais AP rejette cette demande parce que le client a déjà atteint les relances maximum.

`Le processus` et/ou le **`rayon`** met au point qui *précèdent* immédiatement l'exposition de message d'ordinateur d'état les détails de la panne.

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

Authentification MAC

Ceux-ci met au point sont les plus utiles pour l'authentification MAC :

- **authentification de debug radius** — Quand un serveur d'authentification externe est utilisé, les sorties de ceci mettent au point le début avec ce mot : `RAYON`.
- **MAC-authen d'authentificateur de debug dot11 aaa** — Les sorties de ceci mettent au point le début avec ce texte : `dot11_auth_dot1x_`.

Ceux-ci met au point l'exposition :

- Ce qui est signalé pendant les parties de RAYON d'un dialogue d'authentification
- La comparaison entre l'adresse MAC qui est donnée et celle contre lesquelles est authentifié

Quand un serveur RADIUS externe est utilisé avec l'authentification d'adresse MAC, le RAYON met au point s'appliquent. Le résultat de cette conjonction est un affichage de la conversation réelle entre le serveur d'authentification et le client.

Quand une liste d'adresses MAC est établie localement au périphérique comme nom d'utilisateur et base de données de mots de passe, seulement le **`MAC-authen`** met au point des sorties d'exposition. Comme la correspondance ou la non-concordance d'adresse est déterminée, affichage de ces sorties.

Remarque: Écrivez toujours toutes les lettres dans une adresse MAC en minuscules.

Ce les exemples affiche une authentification MAC réussie contre une base de données locale :

Exemple réussi d'authentification MAC

`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]
```

Ce les exemples affiche une authentification MAC défectueuse contre une base de données locale :

Exemple défectueux d'authentification MAC

```
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
```

Quand une authentification d'adresse MAC échoue, vérifiez la précision des caractères qui sont écrits dans l'adresse MAC. Soyez sûr que vous avez écrit toutes les lettres dans une adresse MAC en minuscules.

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

WPA

Bien que le Protocole WPA (Wi-Fi Protected Access) ne soit pas un type d'authentification, c'est un protocole négocié.

- Le WPA négocie entre AP et la carte client.
- La Gestion de clé WPA négocie après qu'un client soit avec succès authentifié par un serveur d'authentification.
- Le WPA négocie un Pairwise Transient Key (PTK) et une clé passagère de Groupwise (GTK) dans une prise de contact à quatre voies.

Remarque: Puisque le WPA exige que l'EAP sous-jacent soit réussi, vérifiez que les clients peuvent avec succès authentifier avec cet EAP avant que vous engagiez le WPA.

Ceux-ci met au point sont les plus utiles pour des négociations WPA :

- **processus d'authentificateur de debug dot11 aaa** — Les sorties de ceci mettent au point le début avec ce texte : `dot11_auth_dot1x_`.
- **state-machine d'authentificateur de debug dot11 aaa** — Les sorties de ceci mettent au point le début avec ce texte : `dot11_auth_dot1x_run_rfsm`.

Relativement aux autres authentifications dans ce document, le WPA met au point sont simple pour lire et analyser. Un message PTK devrait être envoyé et une réponse appropriée être reçu. Ensuite, un message GTK devrait être envoyé et une autre réponse appropriée être reçu.

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

Exemple réussi de négociation WPA

```
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 configurer le WPA, référez-vous à l'aperçu de configuration WPA.

Authentification Administrative/HTTP

Vous pouvez limiter l'accès administratif au périphérique aux utilisateurs qui sont répertoriés dans le l'un ou l'autre un nom et une base de données de mots de passe d'utilisateur local ou à un serveur d'authentification externe. L'accès administratif est pris en charge avec le RAYON et le TACACS+.

Ceux-ci met au point sont les plus utiles pour l'authentification administrative :

- **authentification de debug radius** ou **authentification de debug tacacs** — Les sorties de ceci mettent au point le début avec un de ces mots : RAYON ou TACACS.
- **debug aaa authentication** — Les sorties de ceci met au point le début avec ce texte : AAA/AUTHEN.
- **autorisation de debug aaa** — Les sorties de ceci met au point le début avec ce texte : AAA/AUTHOR.

Ceux-ci met au point l'exposition :

- Ce qui est signalé pendant les parties de RAYON ou TACACS d'une authentification dialoguez
- Les négociations réelles pour l'authentification et l'autorisation entre le périphérique et le serveur d'authentification

Cet exemple affiche une authentification administrative réussie quand l'`attribut RADIUS de type de service` est placé à `administratif` :

Exemple administratif réussi d'authentification avec l'attribut de type de service

```
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:0000366] 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 affiche une authentification administrative réussie quand vous employez des attributs de constructeur-particularité afin d'envoyer une déclaration « niveau priv » :

Exemple administratif réussi d'authentification avec l'attribut de Constructeur-particularité

```
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
```

La plupart de problème courant avec l'authentification administrative est le manque de configurer le serveur d'authentification pour envoyer les attributs de type de service niveau du privilège ou administratifs appropriés. Cette tentative d'exemple a manqué authentification administrative parce qu'aucun attribut niveau du privilège ou attributs de type de service administratifs n'a été envoyé :

Sans attributs de Constructeur-particularité ou de type de service

```
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 configurer l'authentification administrative, référez-vous à gérer le Point d'accès (guide de configuration du logiciel de Cisco IOS pour des Points d'accès de Cisco Aironet, 12.2(13)JA).

Pour plus d'informations sur la façon configurer le privilège d'administrateur aux utilisateurs sur le serveur d'authentification, référez-vous à la configuration d'échantillon : Authentification locale pour des utilisateurs de serveur HTTP. Vérifiez la section qui apparie le 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 de LEAP avec le serveur local de RAYON
- 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
- Support et documentation techniques - Cisco Systems