調試身份驗證

目錄

簡介

無線通訊在許多方面使用身份驗證。最常見的身份驗證型別是不同型別和形式的可擴展身份驗證協定(EAP)。其他身份驗證型別包括MAC地址身份驗證和管理身份驗證。本文說明如何調試和解釋調試身份驗證的輸出。排除無線安裝故障時，這些調試資訊非常重要。

註：本文檔中涉及非思科產品的部分基於作者的經驗，而非正式培訓。它們旨在為您提供方便而非技術支援。如需非思科產品的權威技術支援，請聯絡該產品的技術支援。

必要條件

需求

思科建議您瞭解以下主題：

- 與無線網路相關的身份驗證
- Cisco IOS®軟體指令行介面(CLI)
- RADIUS伺服器配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 任何型號和版本的Cisco IOS軟體型無線產品
- Hilgraeve超級終端

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

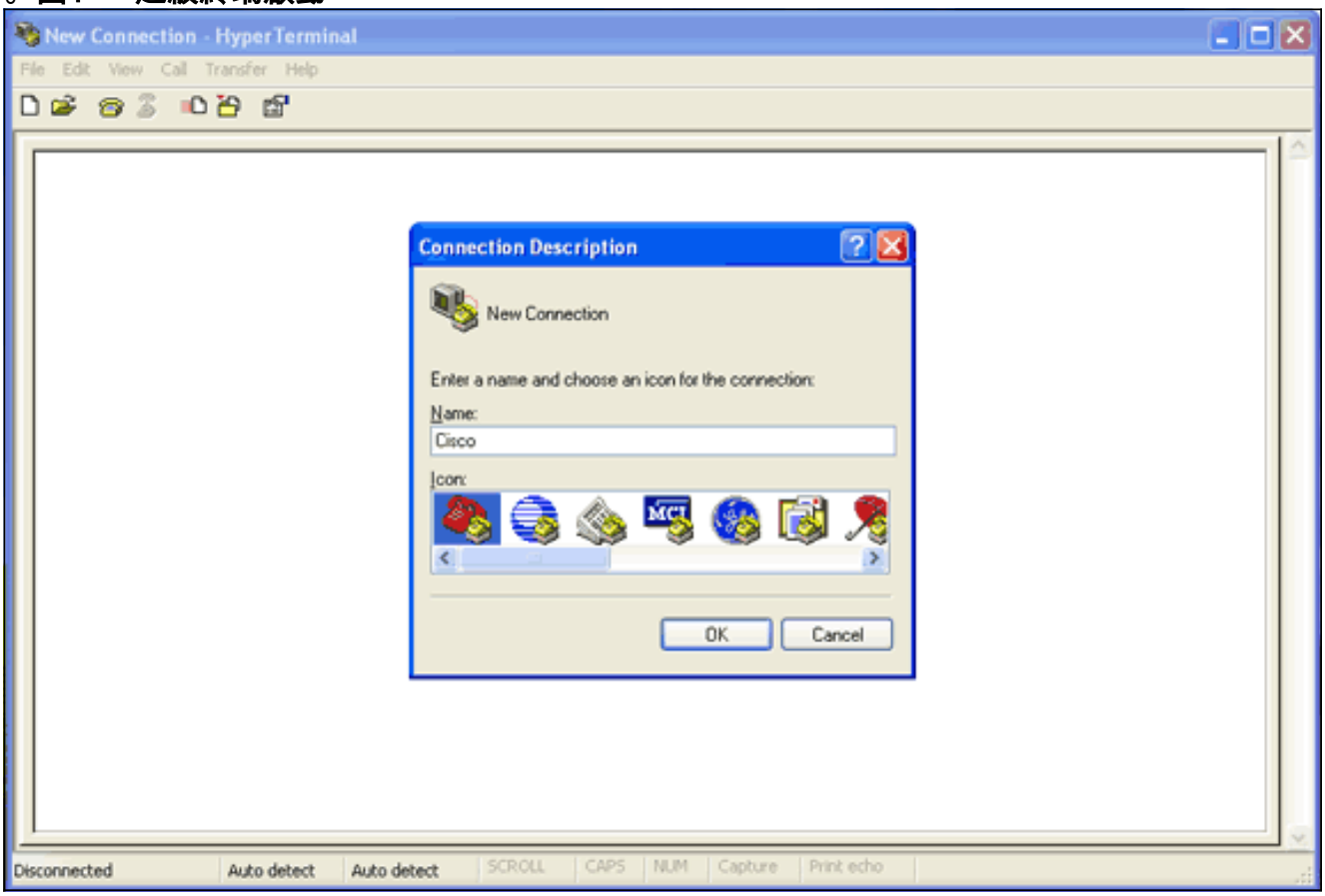
捕獲調試

如果無法擷取和分析偵錯資訊，該資訊將毫無用處。捕獲此資料的最簡單方法是使用內建於Telnet或通訊應用程式中的螢幕捕獲功能。

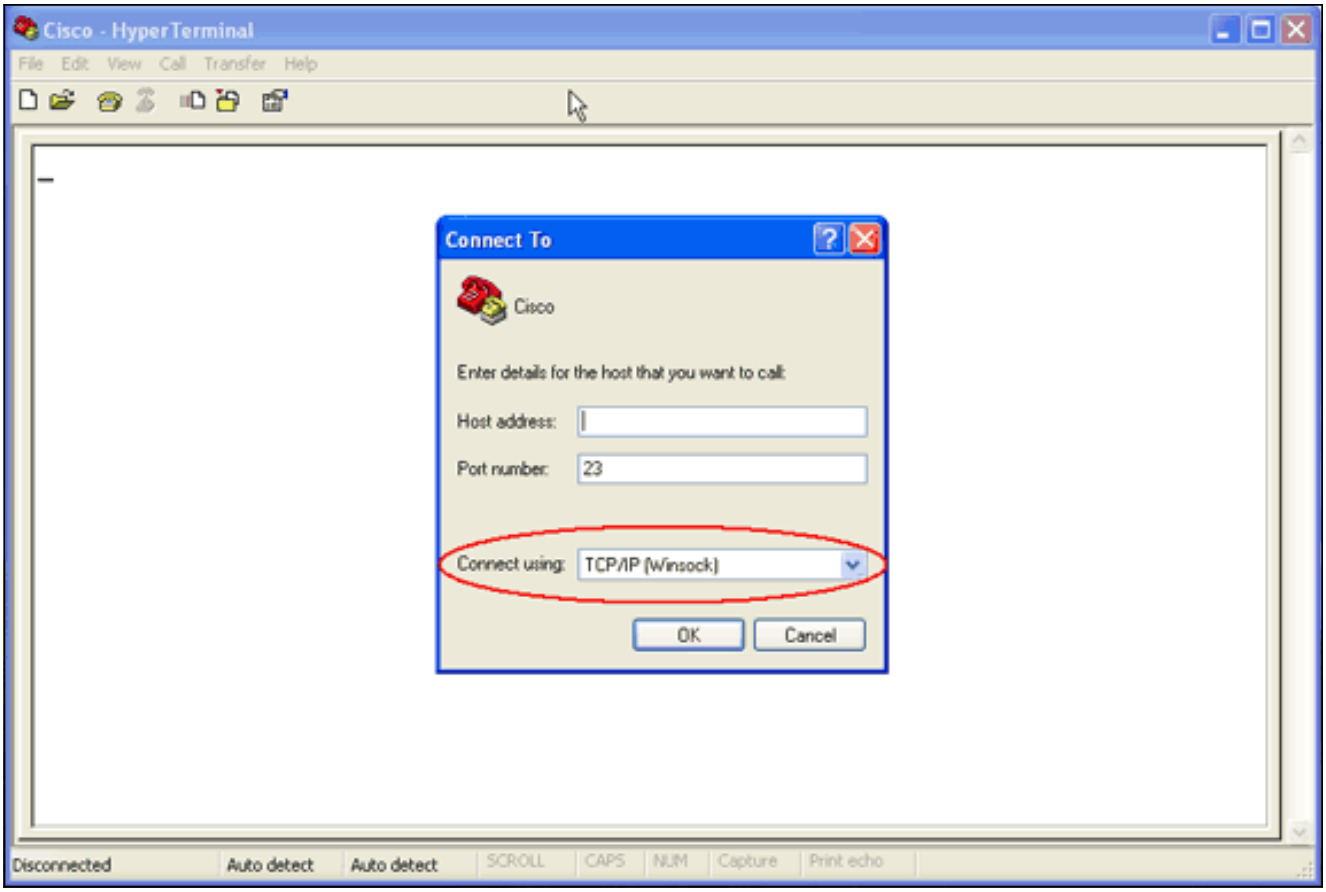
此範例說明如何使用Hilgraeve HyperTerminal應用程序擷取 輸出。大多數Microsoft Windows作業系統都包括超級終端機，但是您可以將這些概念應用到任何終端模擬應用程式。有關應用程式的更完整資訊，請參閱Hilgraeve 。

完成以下步驟，將超級終端配置為與接入點(AP)或網橋通訊：

1. 若要開啟超級終端機，請選擇**「開始」>「程式」>「系統工具」>「通訊」>「超級終端機」。圖1 — 超級終端啟動**

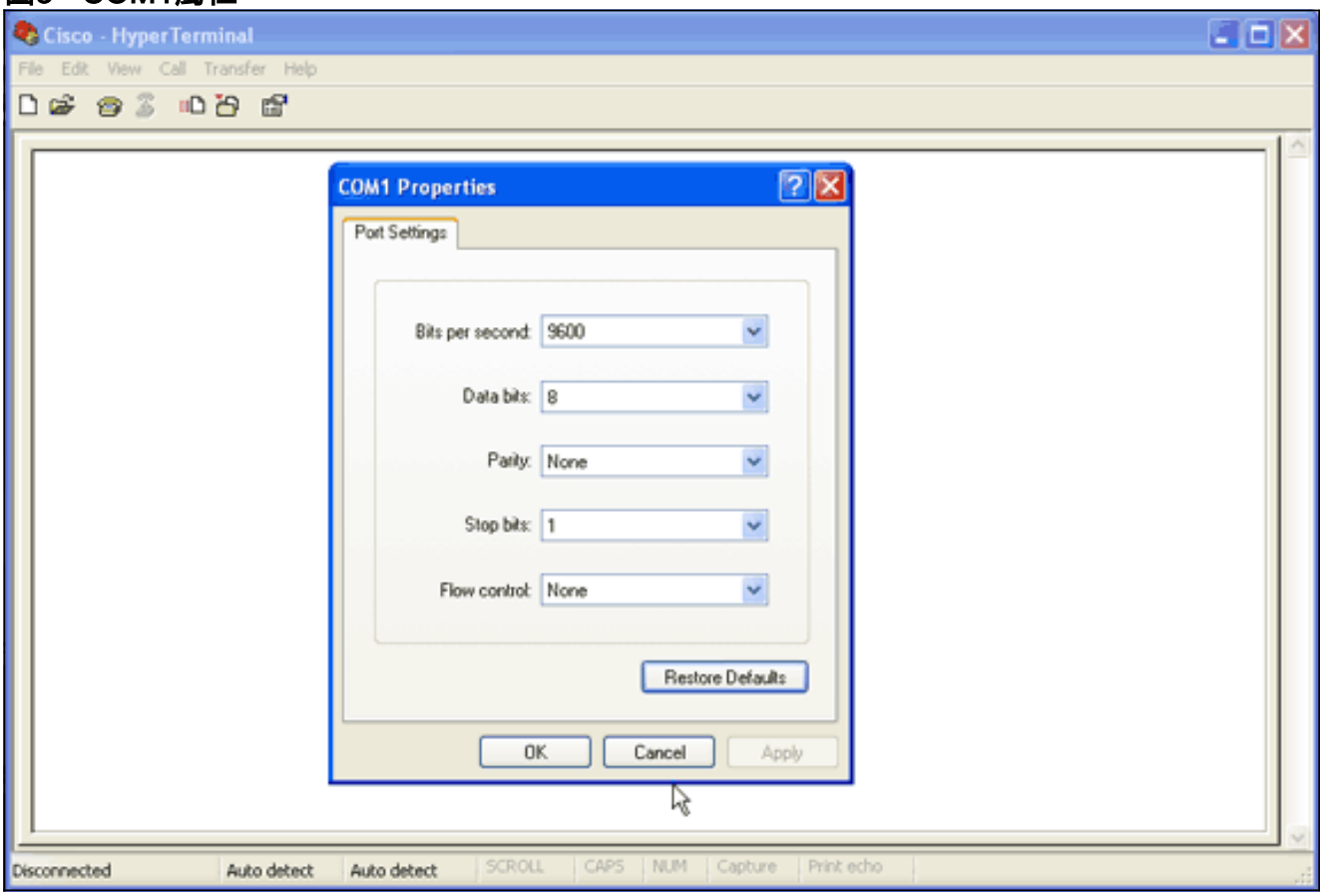


2. 超級終端開啟時，請完成以下步驟：輸入連線的名稱。選擇一個圖示。按一下「OK」（確定）。
3. 若是Telnet連線，請完成以下步驟：從Connect Using下拉選單中，選擇TCP/IP。輸入要運行調試的裝置的IP地址。按一下「OK」（確定）。**圖2 - Telnet連線**



4. 對於控制檯連線，請完成以下步驟：從使用連線下拉選單中，選擇控制檯電纜所連線的COM埠。按一下「OK」（確定）。將出現連線的屬性表。設定連線到控制檯埠的速度。若要還原預設連線埠設定，請按一下「Restore Defaults」。**註：大多**數思科產品都採用預設埠設定。預設埠設定如下：每秒位元數 — 9600資料位 — 8同位 — 無停止位元 — 1流量控制 — 無

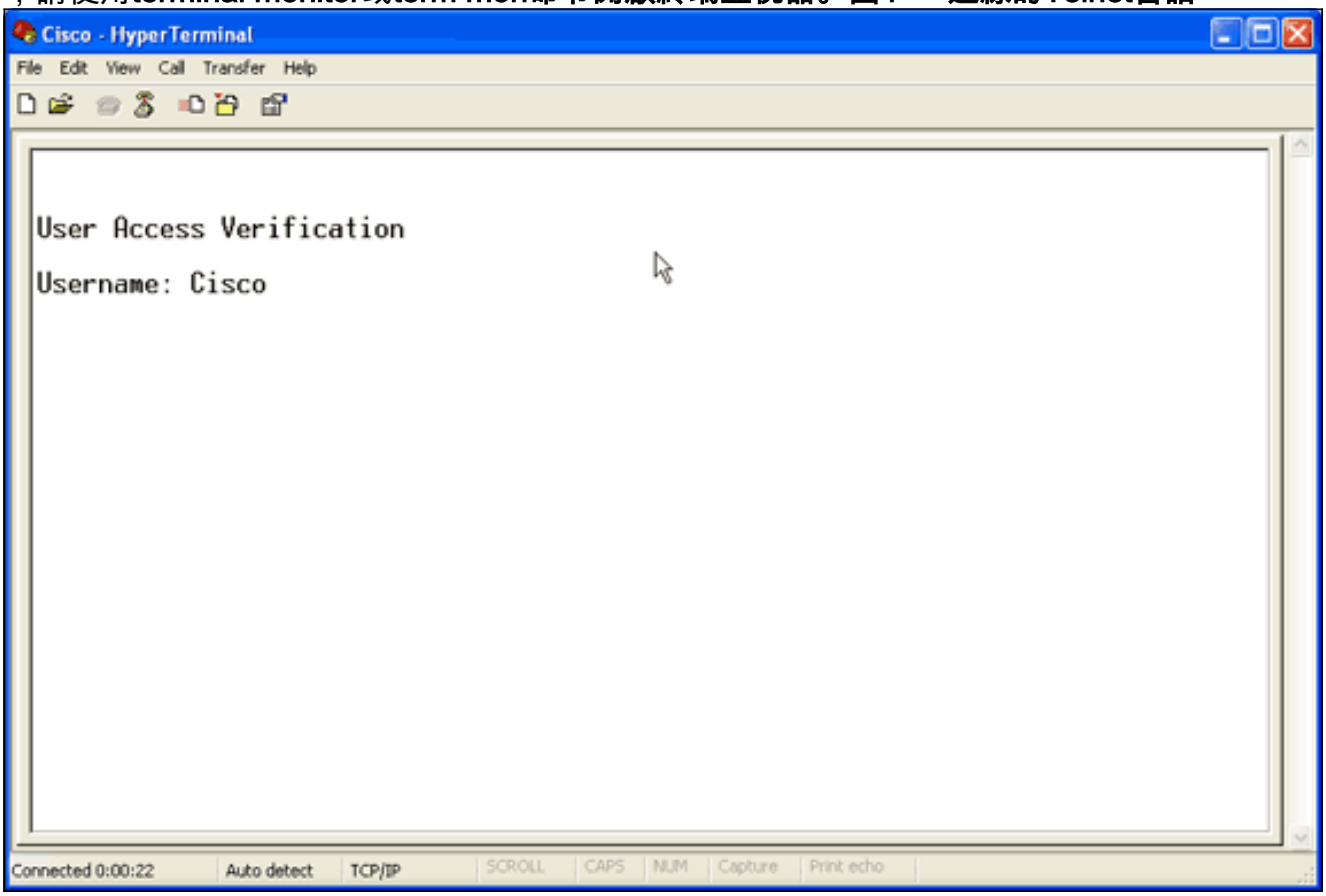
圖3 - COM1屬性



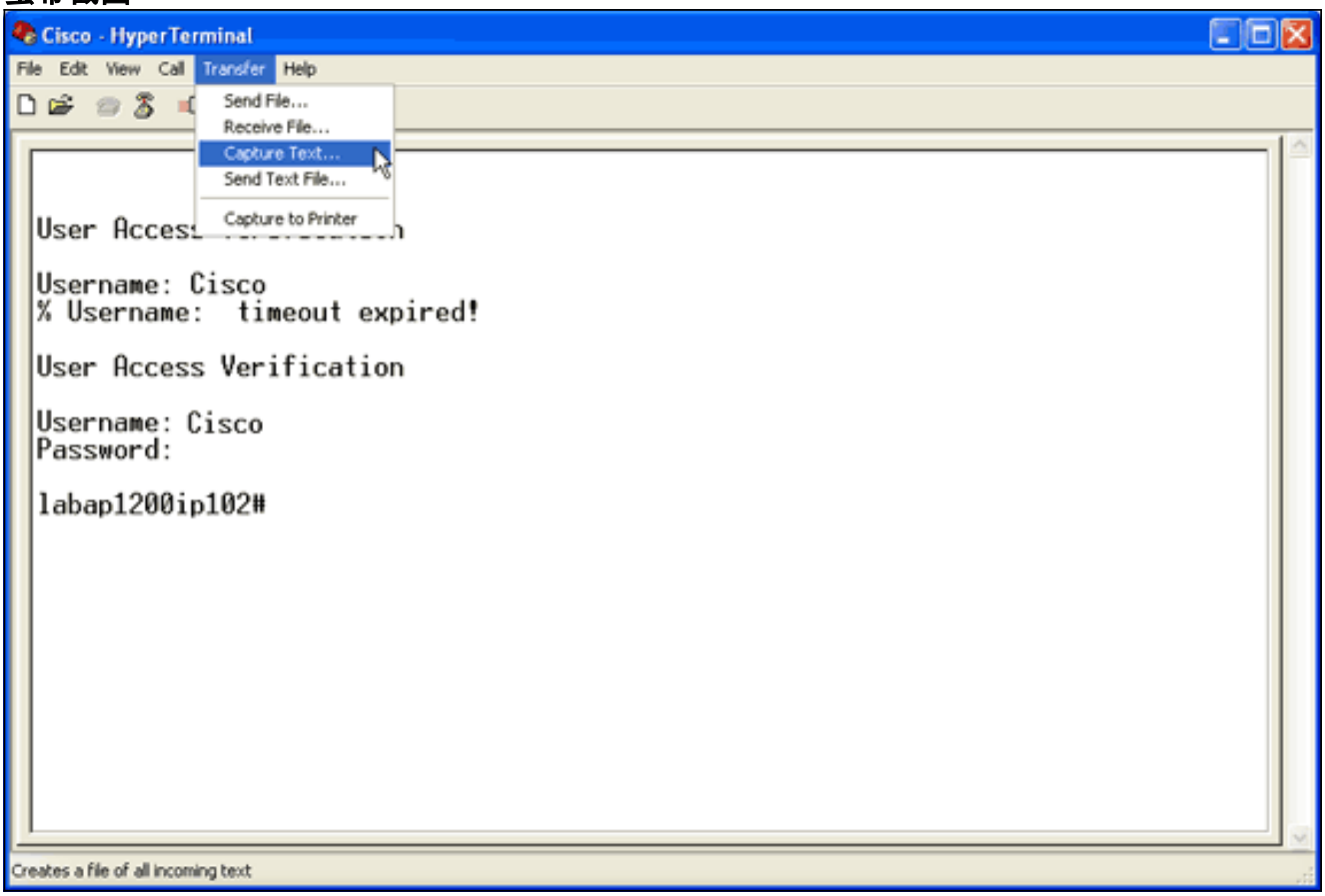
此時，會建立Telnet或控制檯連線，並提示您輸入使用者名稱和密碼。**注意：**Cisco Aironet裝

置分配預設使用者名稱和密碼*Cisco*（區分大小寫）。

5. 要運行調試，請完成以下步驟：發出**enable**命令以進入特權模式。輸入啟用密碼。**注意**：請記住，Aironet裝置的預設密碼是*Cisco*（區分大小寫）。**注意**：若要檢視Telnet會話的調試輸出，請使用**terminal monitor**或**term mon命令開啟終端監視器。圖4 — 連線的Telnet會話**

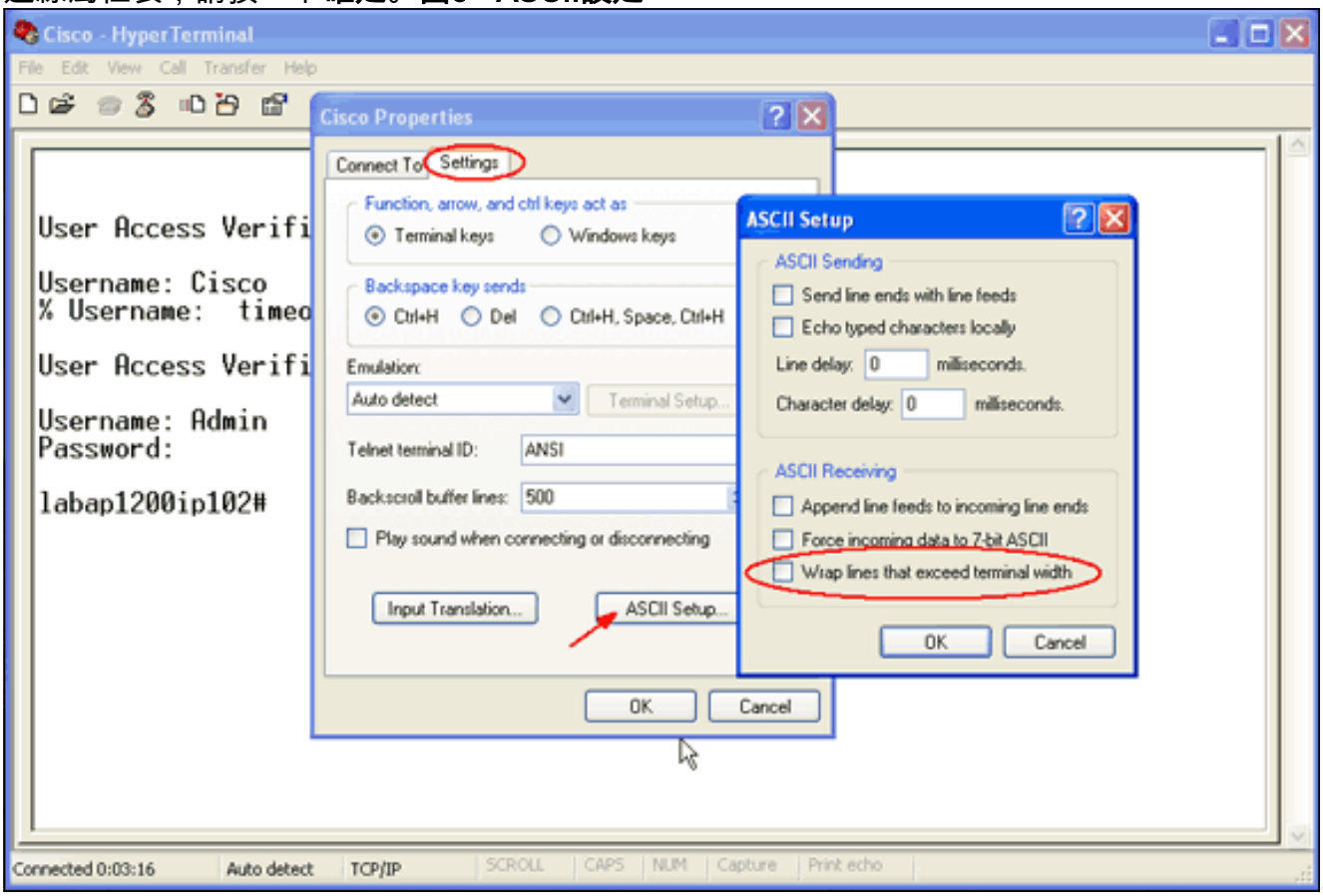


6. 建立連線後，請完成以下步驟以收集螢幕捕獲：從「傳輸」選單中選擇**捕獲文本。圖5 — 儲存螢幕截圖**



開啟一個提示您輸入輸出檔名的對話方塊時，請輸入檔名。

7. 完成以下步驟以禁用螢幕繞排：**注意：**禁用螢幕繞排時，可以更輕鬆地讀取調試。在「超級終端機」功能表中選擇**「檔案」**。選擇**Properties**。在連線屬性工作表上，按一下**設定**頁籤。按一下**ASCII Setup**。取消選中**超出終端寬度的換行**。要關閉ASCII設定，請按一下**確定**。要關閉連線屬性表，請按一下**確定**。**圖6 - ASCII設定**



現在，您可以將任何螢幕輸出捕獲到文本檔案中，運行的調試取決於協商的內容。本文檔的下一部分將介紹調試提供的協商連線的型別。

EAP

以下調試對EAP身份驗證最有幫助：

- **debug radius authentication** — 此調試的輸出以以下詞開頭：`RADIUS`。
- **debug dot11 aaa authenticator process** — 此調試的輸出以以下文本開頭：`dot11_auth_dot1x_`。
- **debug dot11 aaa authenticator state-machine** — 此調試的輸出以以下文本開頭：`dot11_auth_dot1x_run_rfsm`。

這些調試顯示：

- 身份驗證對話方塊的RADIUS部分期間報告的內容
- 身份驗證對話方塊期間執行的操作
- 身份驗證對話方塊轉換到的各種狀態

此示例顯示成功的輕量EAP(LEAP)身份驗證：

成功的EAP身份驗證示例
`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]
```

請注意狀態機流。此過程分為幾個狀態：

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY**注意：當二者進行協商時，可以有多次**CLIENT_WAIT**和**CLIENT_REPLY**的迭代，以及**SERVER_WAIT**和**SERVER_REPLY**。**
6. SERVER_PASS

process調試顯示每個狀態的每個單獨步驟。**radius** 偵錯顯示驗證伺服器和使用者端之間的實際對話。使用EAP調試最簡單的方法是觀察狀態機消息在每個狀態的進展。

當協商中發生故障時，**state-machine**調試會顯示進程停止的原因。注意類似以下示例的郵件：

- **CLIENT TIMEOUT** — 此狀態表示客戶端沒有在適當的時間內響應。出現此響應失敗的原因可能是以下其中之一：客戶端軟體有問題。EAP客戶端超時值（來自「高級安全」下的「EAP身份驗證」子頁籤）已過期。某些EAP，尤其是受保護的EAP(PEAP)，完成身份驗證需要超過30秒。將此計時器設定為更高的值（90秒和120秒之間）。以下是CLIENT TIMEOUT嘗試例：**注意：**注意任何類似於以下消息的系統錯誤消息：

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

  注意：此類錯誤消息可能表示射頻(RF)問題。
- **AP和RADIUS伺服器之間的共用金鑰不匹配** — 在此示例日誌中，RADIUS伺服器不接受來自AP的身份驗證請求。AP繼續向RADIUS伺服器傳送請求，但RADIUS伺服器拒絕該請求，因為

共用金鑰不匹配。為了解決此問題，請務必檢查AP上的共用金鑰是否與RADIUS伺服器中使用的共用金鑰相同。

- **server_timeout** — 此狀態表示身份驗證伺服器沒有在適當的時間內響應。由於伺服器上的問題，出現響應失敗。驗證以下情況是否正確：AP與身份驗證伺服器具有IP連線。**注意：**您可以使用ping命令驗證連線。伺服器的身份驗證和記帳埠號正確。**注意：您**可以從伺服器管理器頁籤檢查埠號。身份驗證服務正在運行且工作正常。以下是server_timeout嘗試的示例：
- **SERVER_FAIL** — 此狀態表示伺服器根據使用者憑據提供了不成功的身份驗證響應。在此失敗之前的RADIUS調試顯示提供給身份驗證伺服器的使用者名稱。請務必檢查身份驗證伺服器中的Failed Attempts（嘗試失敗次數）日誌，以瞭解有關伺服器拒絕客戶端訪問的原因的其他詳細資訊。以下是SERVER_FAIL嘗試的範例：
- No Response from Client — 在本示例中，radius伺服器向AP轉發的AP傳送傳遞消息，然後與客戶端關聯。最終，客戶端不會響應AP。因此，AP在達到最大重試次數後取消其身份驗證。AP將獲取質詢響應從radius轉發到客戶端。客戶端不響應並達到最大重試次數，這將導致EAP失敗，並且AP取消對客戶端的身份驗證。Radius向AP傳送傳遞消息，AP將傳遞消息轉發給客戶端，而客戶端不響應。AP在達到最大重試次數後取消身份驗證。然後客戶端嘗試向AP發出新的身份請求，但AP拒絕此請求，因為客戶端已達到最大重試次數。

緊接在狀態機器消息前面的**process** 和/或**radius**調試顯示故障的詳細資訊。

有關如何配置EAP的詳細資訊，請參閱使用RADIUS伺服器的EAP身份驗證。

MAC身份驗證

以下調試對MAC身份驗證最有幫助：

- debug radius authentication — 使用外部身份驗證伺服器時，此調試的輸出以以下詞開頭：RADIUS。
- debug dot11 aaa authenticator mac-authen — 此調試的輸出以以下文本開頭：dot11_auth_dot1x_。

這些調試顯示：

- 身份驗證對話方塊的RADIUS部分期間報告的內容
- 給定的MAC地址與進行身份驗證的MAC地址之間的比較

將外部RADIUS伺服器用於MAC位址驗證時，RADIUS偵錯會套用。此關聯的結果是顯示身份驗證伺服器和客戶端之間的實際會話。

當裝置的MAC地址清單作為使用者名稱和密碼資料庫本地構建時，只有**mac-auth debugs**顯示輸出。當確定地址匹配或不匹配時，將顯示這些輸出。

注意：始終以小寫形式在MAC地址中輸入任何字母字元。

以下範例顯示針對本機資料庫的MAC驗證成功：

成功的MAC身份驗證示例

```
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]
```

以下範例顯示針對本機資料庫的MAC驗證失敗：

失敗的MAC身份驗證示例

```
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
```

當MAC地址身份驗證失敗時，檢查在MAC地址中輸入的字元的準確性。確保在MAC地址中輸入了小寫字母字元。

有關如何配置MAC身份驗證的詳細資訊，請參閱配置身份驗證型別(適用於Cisco Aironet接入點的Cisco IOS軟體配置指南，12.2(13)JA)。

WPA

雖然Wi-Fi保護訪問(WPA)不是身份驗證型別，但它是協商協定。

- WPA在AP和客戶端卡之間進行協商。
- 在客戶端成功通過身份驗證伺服器進行身份驗證後，WPA金鑰管理將進行協商。
- WPA通過四向握手協商成對臨時金鑰(PTK)和成組臨時金鑰(GTK)。

注意：由於WPA要求基礎EAP成功，請在使用WPA之前驗證客戶端是否可以成功使用該EAP進行身份驗證。

這些調試對於WPA協商最有幫助：

- **debug dot11 aaa authenticator process** — 此調試的輸出以以下文本開頭：`dot11_auth_dot1x_`。
- **debug dot11 aaa authenticator state-machine** — 此調試的輸出以以下文本開頭：`dot11_auth_dot1x_run_rfsm`。

相對於本文檔中的其他身份驗證，WPA調試易於讀取和分析。應傳送PTK消息並收到適當的回覆。接下來，應傳送GTK消息並接收另一個適當的響應。

如果未傳送PTK或GTK消息，則AP上的配置或軟體級別可能存在故障。如果未收到來自客戶端的PTK或GTK響應，請檢查客戶端卡的WPA請求方上的配置或軟體級別。

成功的WPA協商示例

```
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#
```

有關如何配置WPA的詳細資訊，請參閱WPA配置概述。

管理/HTTP身份驗證

您可以限制本地使用者名稱和密碼資料庫中列出的使用者或外部身份驗證伺服器對裝置的管理訪問。RADIUS和TACACS+都支援管理存取。

以下調試對於管理身份驗證最有幫助：

- **debug radius authentication**或**debug tacacs authentication** — 此調試的輸出以以下詞之一開頭：RADIUS或TACACS。
- **debug aaa authentication** — 此調試的輸出以以下文本開頭：AAA/AUTHEN。
- **debug aaa authorization** — 此調試的輸出以以下文本開頭：AAA/。

這些調試顯示：

- 在驗證對話的RADIUS或TACACS部分期間報告的內容
- 裝置與身份驗證伺服器之間的身份驗證和授權的實際協商

此範例顯示當Service-Type RADIUS屬性設定為Administrative時成功的管理驗證：

具有服務型別屬性的成功管理身份驗證示例

```
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
```

此示例顯示當您使用供應商特定的屬性傳送「priv-level」語句時成功的管理身份驗證：

具有供應商特定屬性的成功管理身份驗證示例

```
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
```

管理身份驗證最常見的問題是未能將身份驗證伺服器配置為傳送適當的許可權級別或管理服務型別屬性。此示例嘗試管理身份驗證失敗，因為未傳送許可權級別屬性或管理服務型別屬性：

沒有特定於供應商或服務型別的屬性

```
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=
```

有關如何配置管理身份驗證的詳細資訊，請參閱管理接入點(適用於Cisco Aironet接入點的Cisco IOS軟體配置指南，12.2(13)JA)。

有關如何為身份驗證伺服器上的使用者配置管理許可權的詳細資訊，請參閱示例配置：HTTP伺服器使用者的本地身份驗證。檢查與您使用的身份驗證協定匹配的部分。

相關資訊

- 適用於Cisco Aironet存取點的Cisco IOS軟體組態設定指南12.2(13)JA
- 使用RADIUS伺服器的EAP身份驗證
- 使用本地RADIUS伺服器的LEAP身份驗證
- Cisco Aironet無線安全常見問題
- 作為AAA伺服器的無線域服務AP配置示例
- 技術支援與文件 - Cisco Systems