認証のデバッグ

目次

[はじめに](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[デバッグのキャプチャ](#)
[EAP](#)
[MAC 認証](#)
[WPA](#)
[管理認証および HTTP 認証](#)
[関連情報](#)

はじめに

無線通信では、さまざまな認証方法が使用されます。 最も一般的な認証タイプは、さまざまなタイプや形式の Extensible Authentication Protocol (EAP) です。 その他の認証タイプには、MAC アドレス認証や管理認証があります。 このドキュメントでは、デバッグの方法、および認証のデバッグでの出力の解釈方法を説明しています。 これらのデバッグからの情報は、無線製品設置時のトラブルシューティングに非常に役立ちます。

注: このドキュメントのシスコ以外の製品に関する説明は、著者の経験に基づくものであり、正式なトレーニングに基づくものではありません。 これらの説明は、利便性のために掲載しているものであり、テクニカルサポートではありません。 Cisco 以外の製品に関する正式なテクニカルサポートについては、対象製品のテクニカルサポートにお問い合せください。

前提条件

要件

次の項目に関する知識が推奨されます。

- 無線ネットワークに関連する認証
- Cisco IOS® ソフトウェア コマンドライン インターフェイス (CLI)
- RADIUS サーバの設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア ベースの無線製品のすべてのモデルとバージョン
- Hilgraeve ハイパーターミナル

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

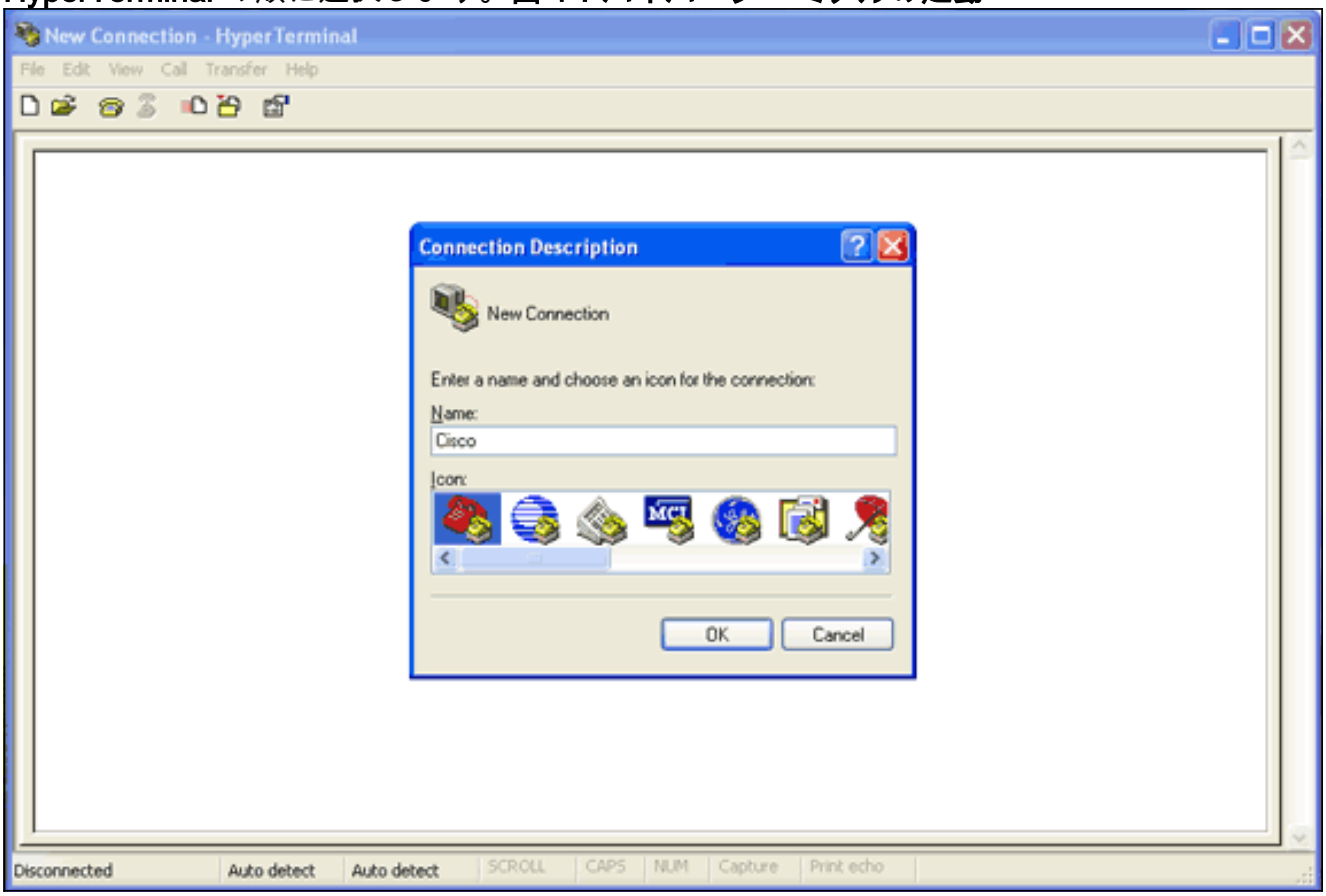
デバッグのキャプチャ

デバッグ情報については、キャプチャして分析できない場合、その情報は役に立ちません。 このデータをキャプチャする一番簡単な方法は、Telnet や通信アプリケーションに組み込まれているスクリーン キャプチャ機能を使用する方法です。

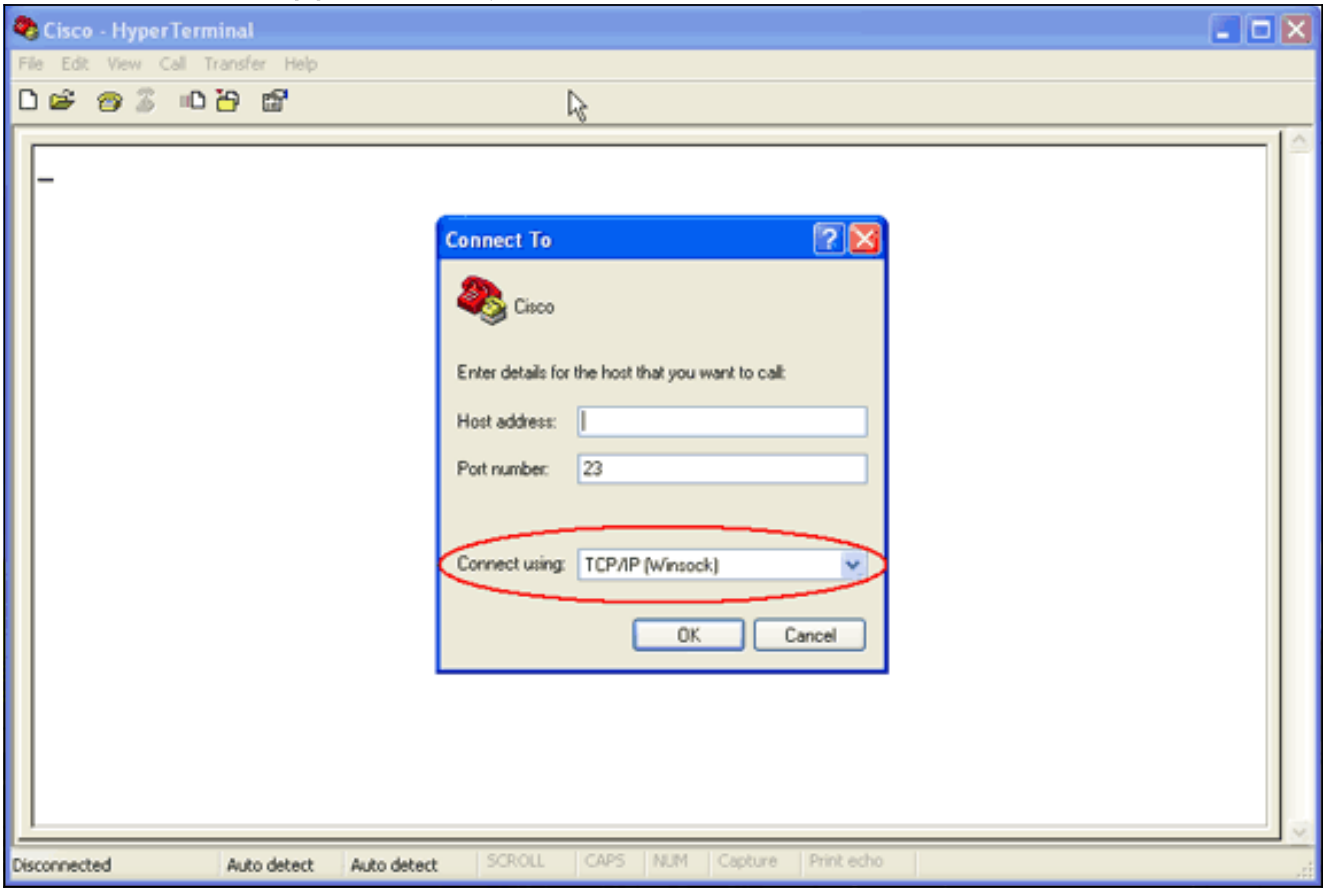
次の例では、Hilgraeve ハイパーターミナル アプリケーションを使用して出力をキャプチャする方法を説明しています。 ほとんどの Microsoft Windows オペレーティング システムにはハイパーターミナルがインストールされていますが、この概念は他のターミナル エミュレーション アプリケーションにも適用できます。 このアプリケーションに関するすべての情報は、Hilgraevesを参照してください。

これらの手順を実行して、ハイパーターミナルを設定し、Access Point（AP; アクセス ポイント）やブリッジとの通信を行います。

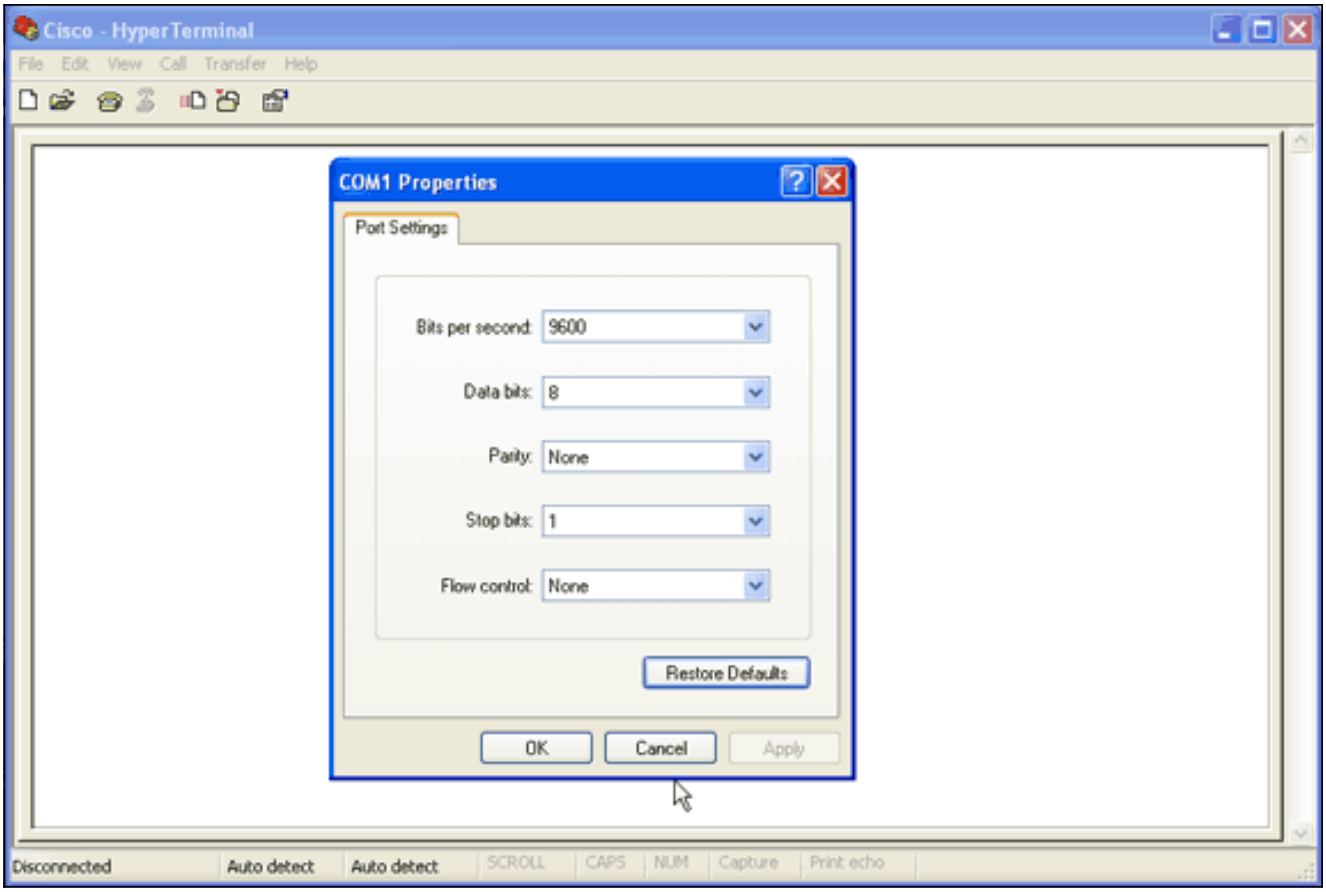
1. ハイパーターミナルを開くには、**Start > Programs > System Tools > Communications > HyperTerminal** の順に選択します。**図 1：ハイパーターミナルの起動**



2. ハイパーターミナルの画面が開いたら、次の手順を実行します。接続名を入力する。アイコンを選択する。[OK] をクリックします。
3. Telnet 接続を行う場合は、次の手順を実行します。Connect Using ドロップダウン メニューから、**TCP/IP** を選択する。デバッグを実行するデバイスの IP アドレスを入力する。[OK] をクリックします。**図 2：Telnet 接続**

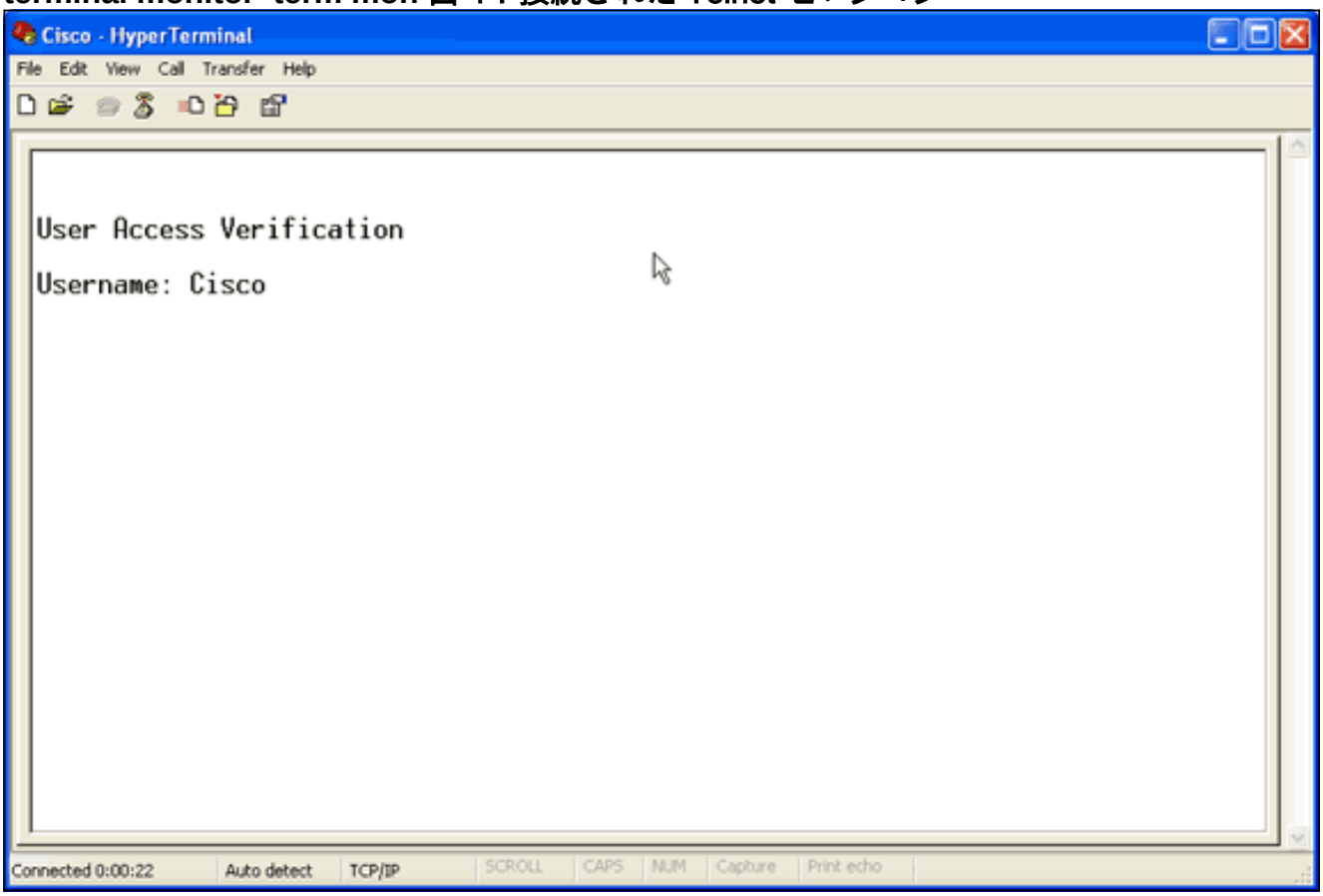


4. コンソール接続を行う場合は、次の手順を実行します。Connect Using ドロップダウン メニューから、コンソール ケーブルが接続されている COM ポートを選択する。[OK] をクリックします。接続のプロパティ シートが表示されます。コンソール ポートへの接続速度を設定します。デフォルトのポート設定を復元するには、**Restore Defaults** をクリックする。**注**：ほとんどのシスコ製品では、デフォルトのポート設定に従います。デフォルトのポート設定は次のとおりです。二番目の 9600 ごとのビットデータ ビット：8パリティ：なしストップ ビット：1フロー制御：なし**図 3：COM1 のプロパティ**



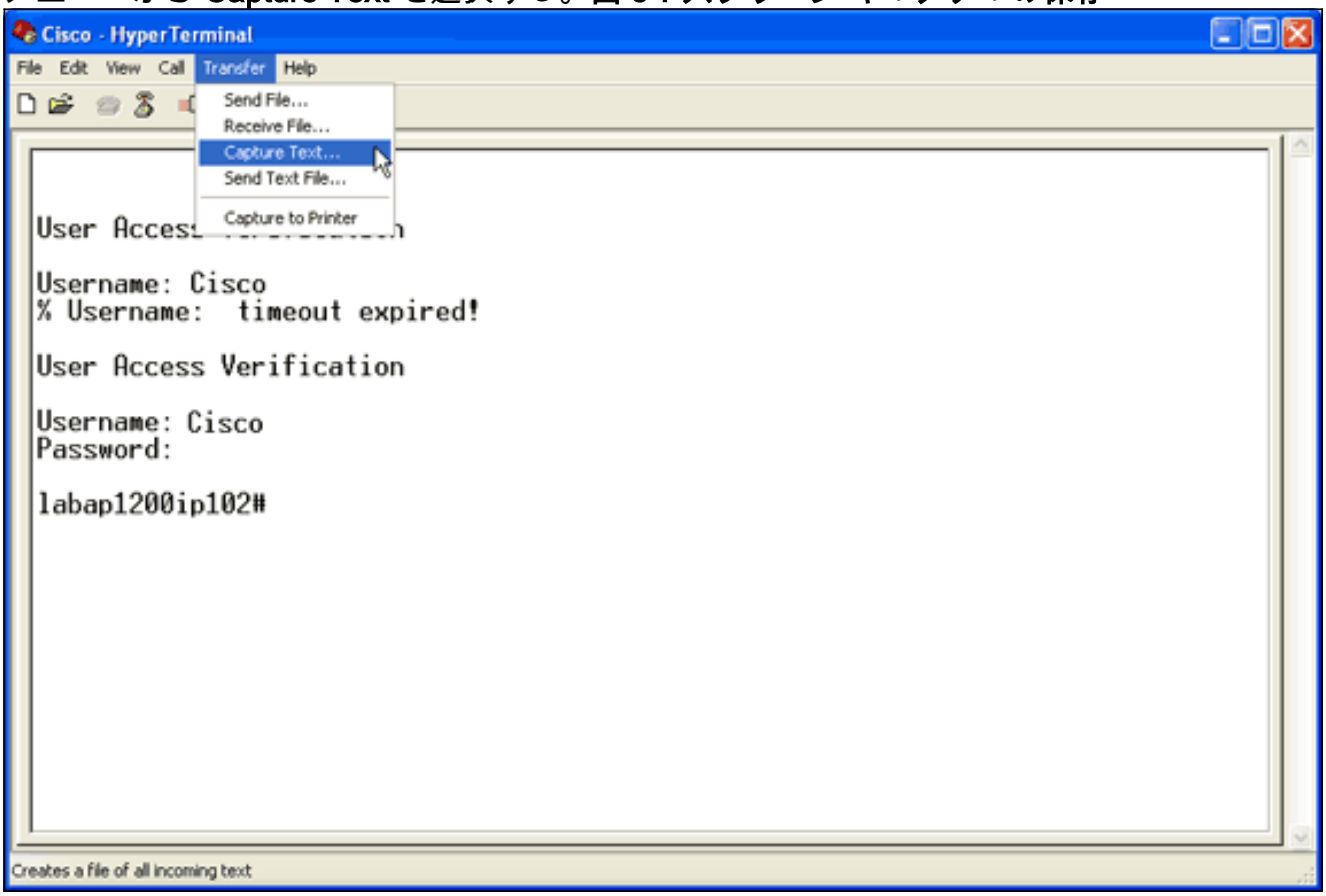
この時点で、Telnet 接続またはコンソール接続が確立されると、ユーザ名とパスワードを入力するように求められます。**注:** Cisco Aironet *Cisco*

5. デバッグを実行するには、次の手順を実行します。**enable** コマンドを発行して、特権モードに入る。イネーブル パスワードを入力します。**注:** Cisco Aironet *Cisco***注:** Telnet **terminal monitor term mon 図 4：接続された Telnet セッション**



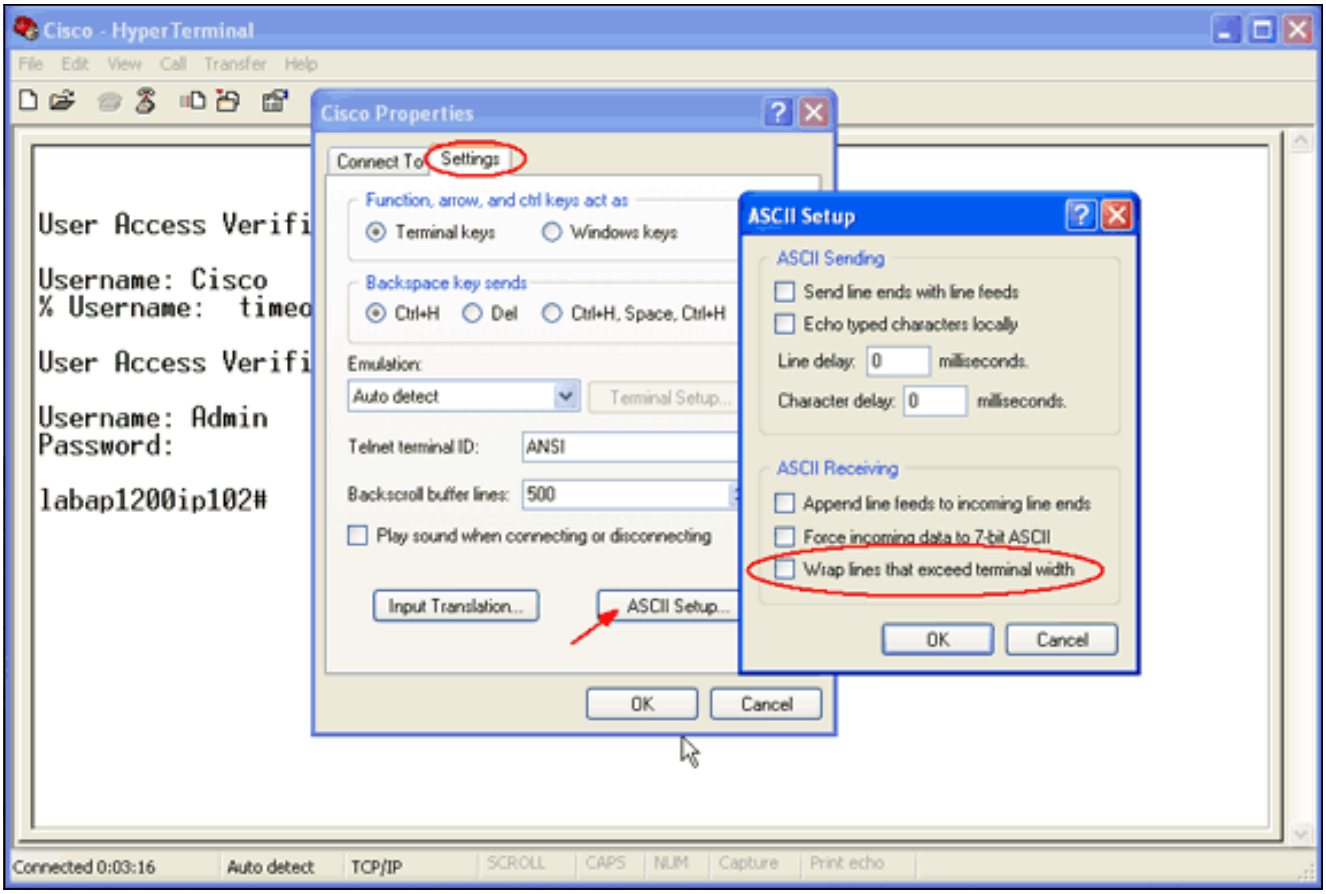
6. 接続が確立されたら、次の手順を実行してスクリーン キャプチャを収集します。Transfer

メニューから Capture Text を選択する。**図 5：スクリーン キャプチャの保存**



ダイアログボックスが開いて、出力用のファイル名を入力するように求められたら、ファイル名を入力する。

7. 画面上での右端の折り返しオプションをディセーブルにするには、次の手順を実行します。**注:** ハイパーターミナルのメニューから、**File** を選択する。**Properties** を選択します。接続のプロパティ シートで、**Settings** タブをクリックする。**ASCII Setup** をクリックする。**Wrap lines that exceed terminal width** のチェックマークを外す。**OK** をクリックして、ASCII Settings を閉じる。**OK** をクリックして、接続のプロパティ シートを閉じる。**図 6：ASCII 設定**



これで画面出力をキャプチャしてテキスト ファイルに出力できるようになりましたが、実行するデバッグは、ネゴシエートされる内容によって異なります。 このドキュメントの次のセクションでは、デバッグで判明するネゴシエート中の接続のタイプについて説明しています。

EAP

EAP 認証の場合、次のデバッグが最も役立ちます。

- **debug radius authentication** —このデバッグの出力はこのワードから開始します: `RADIUS`.
- **debug dot11 aaa authenticator process** —このデバッグの出力はこのテキストから開始します: `dot11_auth_dot1x_`.
- **debug dot11 aaa authenticator state-machine** —このデバッグの出力はこのテキストから開始します: `dot11_auth_dot1x_run_rfsm`.

これらのデバッグでは、次の情報が表示されます。

- 認証ダイアログで、RADIUS に関わる部分の内容
- その認証ダイアログ中に行われる処理
- 認証ダイアログの移行中に経過するさまざまな状態

この例では、Light EAP (LEAP) 認証の成功例を示します。

EAP 認証の成功例

```
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]
```

state-machine デバッグの推移に注目してください。 ステートは、次のように変化します。

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY**注:** 2 CLIENT_WAIT CLIENT_REPLY SERVER_WAIT SERVER_REPLY
6. SERVER_PASS

process デバッグではそれぞれのステート中における個々のステップが表示されます。 **radius** デバッグでは認証サーバとクライアント間の実際の通信内容が表示されます。 EAP デバッグの一番簡単な使用方法は、それぞれのステートでの state machine メッセージの推移を確認することです。

ネゴシエーション中に何らかの失敗が発生すると、処理が中止された理由が **state-machine** デバッグで表示されます。 次の例のようなメッセージを確認してください。

- **CLIENT TIMEOUT**：この状態は、クライアントが適切な時間内に応答しなかったことを示します。 次のいずれかの理由によって、この応答ができない状態が発生する可能性があります。クライアント ソフトウェアに問題がある。EAP クライアントのタイムアウト値（Advanced Security の EAP Authentication のサブタブ）が終了している。一部の EAP（特に Protected EAP（PEAP））では認証が完了するまでに 30 秒よりも長くかかります。 このタイマーに大きい値（90 ~ 120 秒）を設定します。CLIENT TIMEOUT の試行例を次に示します。**注:**

```
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
```

注: Radio FrequencyRF;

- **AP と RADIUS サーバ間での共有秘密鍵の不一致**：このログ例では、RADIUS サーバで AP からの認証要求が受け入れられていません。 AP からは引き続き RADIUS サーバへ要求が送信されますが、共有秘密鍵が一致しないため、RADIUS サーバでは要求が拒否されます。この問題を解決するには、AP 上の共有秘密鍵が RADIUS サーバで使用される共通秘密鍵と同じであることを必ず確認してください。
- **server_timeout**：この状態は、認証サーバが適切な時間内に応答しなかったことを示します。サーバ側の問題が原因で、この応答ができない状態が発生する可能性があります。 これらの状態に該当していることを確認します。AP では認証サーバへの IP 接続が確立されている。**注: ping** サーバの認証およびアカウンティングのポート番号が正しい。**注:** Server Manager 認証サービスが実行中で機能している。server_timeout の試行例を次に示します。
- **SERVER_FAIL** — この状態はサーバがユーザーの資格情報に基づいて不成功な認証応答を与えたことを示します。 この失敗が発生する前の RADIUS デバッグで、認証サーバに送信されたユーザ名が表示されます。 サーバがクライアントのアクセスを拒否した理由の詳細については、認証サーバの Failed Attempts ログをチェックしてください。次に、SERVER_FAIL が発生したときの例を示します。
- **クライアントからの応答なし**：この例では、RADIUS サーバによってパス メッセージが AP に送信されますが、このパス メッセージは AP によって転送され、クライアントが関連付けられます。 最終的に、クライアントによる AP への応答は行われません。 したがって、AP では最大リトライ回数に到達した後に認証解除が行われます。AP では RADIUS からの get challenge 応答がクライアントに転送されます。 クライアントでは応答が行われず、最大リトライ回数に到達しますが、これは EAP が失敗し、AP ではクライアントが認証解除されることになります。RADIUS からパス メッセージが AP に送信され、AP ではこのパス メッセージがクライアントに転送されますが、クライアントでは応答が行われません。 AP では最大リトライ回数に到達した後に認証解除が行われます。 次に、クライアントによって AP への新規の ID 要求が試行されますが、クライアントがすでに最大リトライ数に達しているため、AP ではこの要求が拒否されます。

ステート マシン メッセージ**直前**の **process** デバッグまたは **radius** デバッグには、失敗の詳細が示されます。

EAP の設定方法についての詳細は、『RADIUS サーバとの EAP 認証』を参照してください。

MAC 認証

MAC 認証の場合、次のデバッグが最も役立ちます。

- **debug radius authentication** —外部認証サーバが使用されるとき、このデバッグの出力はこのワードから開始します: `RADIUS`.
- **debug dot11 aaa authenticator mac-authen** —このデバッグの出力はこのテキストから開始します: `dot11_auth_dot1x_`.

これらのデバッグでは、次の情報が表示されます。

- 認証ダイアログで、RADIUS に関わる部分の内容
- 割り当てられている MAC アドレスと、認証された MAC アドレスの比較

MAC アドレス認証に外部 RADIUS サーバを使用している場合、RADIUS デバッグが適用されます。 この組み合せの場合、認証サーバとクライアント間の実際の通信内容が表示されます。

MAC アドレスのリストが、ユーザ名とパスワードのデータベースとしてデバイスにローカルで作成されている場合、**mac-authen** デバッグの出力だけが表示されます。 アドレスの一致または不一致が確認されると、その出力が表示されます。

注: MAC アドレスのアルファベット文字は常に小文字で入力します。

次に、ローカル データベースによる MAC 認証が成功したときの例を示します。

MAC 認証の成功例

```
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
```

次に、ローカル データベースによる MAC 認証が失敗したときの例を示します。

MAC 認証の失敗例

```
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
```

MAC アドレスの認証が失敗した場合は、MAC アドレスに入力されている文字が正しいことをチェックしてください。 MAC アドレスのアルファベット文字を小文字で入力していることを確認します。

MAC 認証の設定方法の詳細は、『Cisco Aironet アクセス ポイントのための Cisco IOS ソフトウェア設定ガイド、12.2(13)JA』の「認証タイプの設定」を参照してください。

WPA

Wi-Fi Protected Access（WPA）は認証タイプではありませんが、ネゴシエーションのプロトコルです。

- WPA では、AP とクライアント カード間のネゴシエートが行われます。
- WPA のキー管理では、クライアントが認証サーバで正常に認証された後に、ネゴシエートを行います。
- WPA では、Pairwise Transient Key（PTK）と Groupwise Transient Key（GTK）の両方を、4 ウェイ ハンドシェイクでネゴシエートします。

注: WPA は、基となる EAP 認証が成功していることが前提なので、WPA を使用する前に、クライアントが EAP を使用して正常に認証されることを確認してください。

WPA ネゴシエーションの場合、次のデバッグが最も役立ちます。

- **debug dot11 aaa authenticator process** —このデバッグの出力はこのテキストから開始します：`dot11_auth_dot1x_`.
- **debug dot11 aaa authenticator state-machine** —このデバッグの出力はこのテキストから開始します: `dot11_auth_dot1x_run_rfsm`.

このドキュメントの他の認証に比べると、WPA のデバッグの解釈と分析は簡単です。 PTK メッセージが送信され、対応する応答が受信されます。 次に、GTK メッセージが送信され、対応する別の応答が受信されます。

PTK メッセージまたは GTK メッセージが送信されない場合は、AP の設定またはソフトウェア レベルに問題がある可能性があります。 PTK または GTK の応答がクライアントから受信されな

い場合は、クライアント カードの WPA サプリカントの設定またはソフトウェア レベルをチェックしてください。

WPA ネゴシエーションの成功例

```
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#
```

WPA の設定方法についての詳細は、『WPA 設定の概要』を参照してください。

管理認証および HTTP 認証

デバイスに対する管理アクセスを、ローカルのユーザ名とパスワードのデータベースまたは外部認証サーバに設定されているユーザに制限することができます。 管理アクセスは、RADIUS と TACACS+ の両方でサポートされています。

管理認証の場合、次のデバッグが最も役立ちます。

- **debug radius authentication** か **debug tacacs authentication** —このデバッグの出力はこれらのワードの 1 つから開始します: RADIUS　TACACS。
- **debug aaa authentication** —このの出力はこのテキストからデバッグ開始します: AAA/AUTHEN.

• **debug aaa authorization** —このの出力はこのテキストからデバッグ開始します: AAA/AUTHOR.
これらのデバッグでは、次の情報が表示されます。

- 認証ダイアログで、RADIUS または TACACS に関わる部分の内容
- 認証および許可のための、デバイスと認証サーバ間の実際のネゴシエーション

次に、Service-Type RADIUS アトリビュートが Administrative 用に設定されている場合に、管理認証が成功したときの例を示します。

Service-Type アトリビュートを使用した管理認証の成功例

```
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
```

次に、ベンダー固有のアトリビュートを使用して「priv-level」設定を送信している場合に、管理認証が成功したときの例を示します。

ベンダー固有のアトリビュートを使用した管理認証の成功例

```
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
```

管理認証でよくある問題は、適切な特権レベルや管理サービス タイプのアトリビュートを送信す

るための認証サーバの設定の不具合です。 次に、特権レベルのアトリビュートや管理サービス タイプのアトリビュートが送信されなかったために、管理認証が失敗したときの例を示します。

ベンダー固有のアトリビュートや Service-Type アトリビュートが存在しない場合

```
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=
```

管理認証の設定方法の詳細は、『Cisco Aironet アクセス ポイントのための Cisco IOS ソフトウェア設定ガイド、12.2(13)JA』の「アクセス ポイントの管理」を参照してください。

認証サーバのユーザに管理権限を設定する方法に関する詳細については設定 例を参照して下さい: HTTPサーバ ユーザ向けのローカル認証。 使用する認証プロトコルに対応したセクションを確認してください。

関連情報

- Cisco Aironet アクセス ポイント用 Cisco IOS ソフトウェア設定ガイド、12.2(13)JA
- RADIUS サーバとの EAP 認証
- ローカル RADIUS サーバを使った LEAP 認証
- Cisco Aironet ワイヤレス セキュリティに関する FAQ [英語]
- AAA サーバとしての無線ドメイン サービス AP の設定例
- テクニカル サポートとドキュメント – Cisco Systems