디버그 인증

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[디버그 캡처](#)
[EAP](#)
[MAC 인증](#)
[WPA](#)
[관리/HTTP 인증](#)
[관련 정보](#)

소개

무선 통신에서는 다양한 방법으로 인증을 사용합니다.가장 일반적인 인증 유형은 다양한 유형 및 형식의 EAP(Extensible Authentication Protocol)입니다.기타 인증 유형에는 MAC 주소 인증 및 관리 인증이 포함됩니다.이 문서에서는 디버그 인증에서 출력을 디버깅하고 해석하는 방법에 대해 설명합니다.이러한 디버그의 정보는 무선 설치 문제를 해결할 때 매우 유용합니다.

참고: 이 문서의 일부 중 Cisco 제품이 아닌 제품을 참조하는 부분은 정식 교육이 아닌 작성자의 경험에 기초합니다.이 서비스는 기술 지원이 아닌 고객의 편의를 위해 제공됩니다.Cisco 제품이 아닌 제품에 대한 신뢰할 수 있는 기술 지원은 해당 제품의 기술 지원에 문의하십시오.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 무선 네트워크와 관련된 인증
- Cisco IOS® 소프트웨어 CLI(Command Line Interface)
- RADIUS 서버 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 모든 모델 및 버전의 Cisco IOS 소프트웨어 기반 무선 제품
- 힐그레이브 하이퍼터미널

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

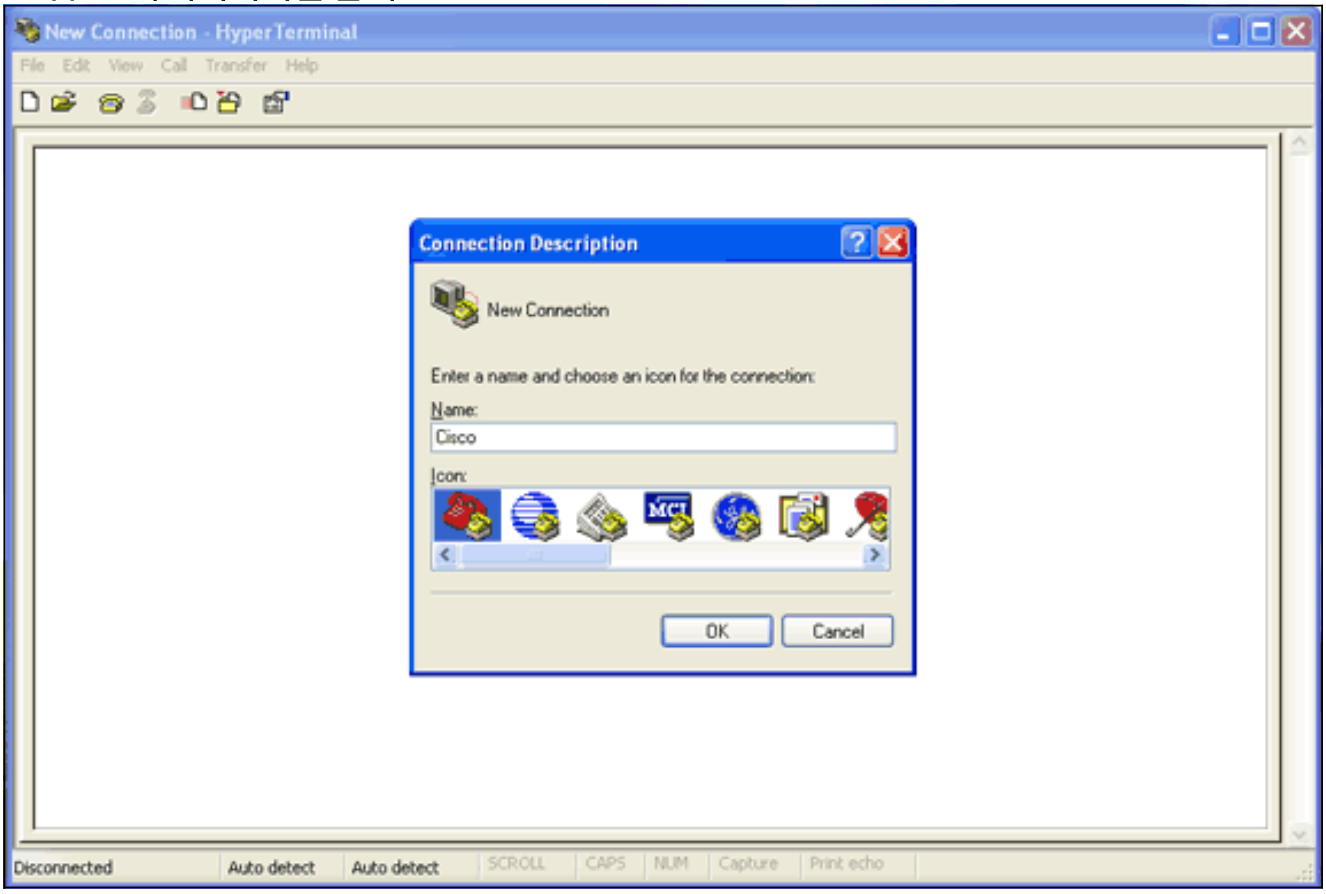
디버그 캡처

디버그 정보를 캡처하고 분석할 수 없으면 해당 정보는 사용할 수 없습니다.이 데이터를 캡처하는 가장 쉬운 방법은 텔넷 또는 통신 애플리케이션에 내장된 화면 캡처 기능을 사용하는 것입니다.

이 예에서는 Hilgraeve HyperTerminal 응용 프로그램을 사용하여 출력을 캡처하는 방법을 설명합니다.대부분의 Microsoft Windows 운영 체제에는 HyperTerminal이 포함되어 있지만, 모든 터미널 에뮬레이션 애플리케이션에 이 개념을 적용할 수 있습니다.애플리케이션에 대한 자세한 내용은 Hilgreve를 참조하십시오 .

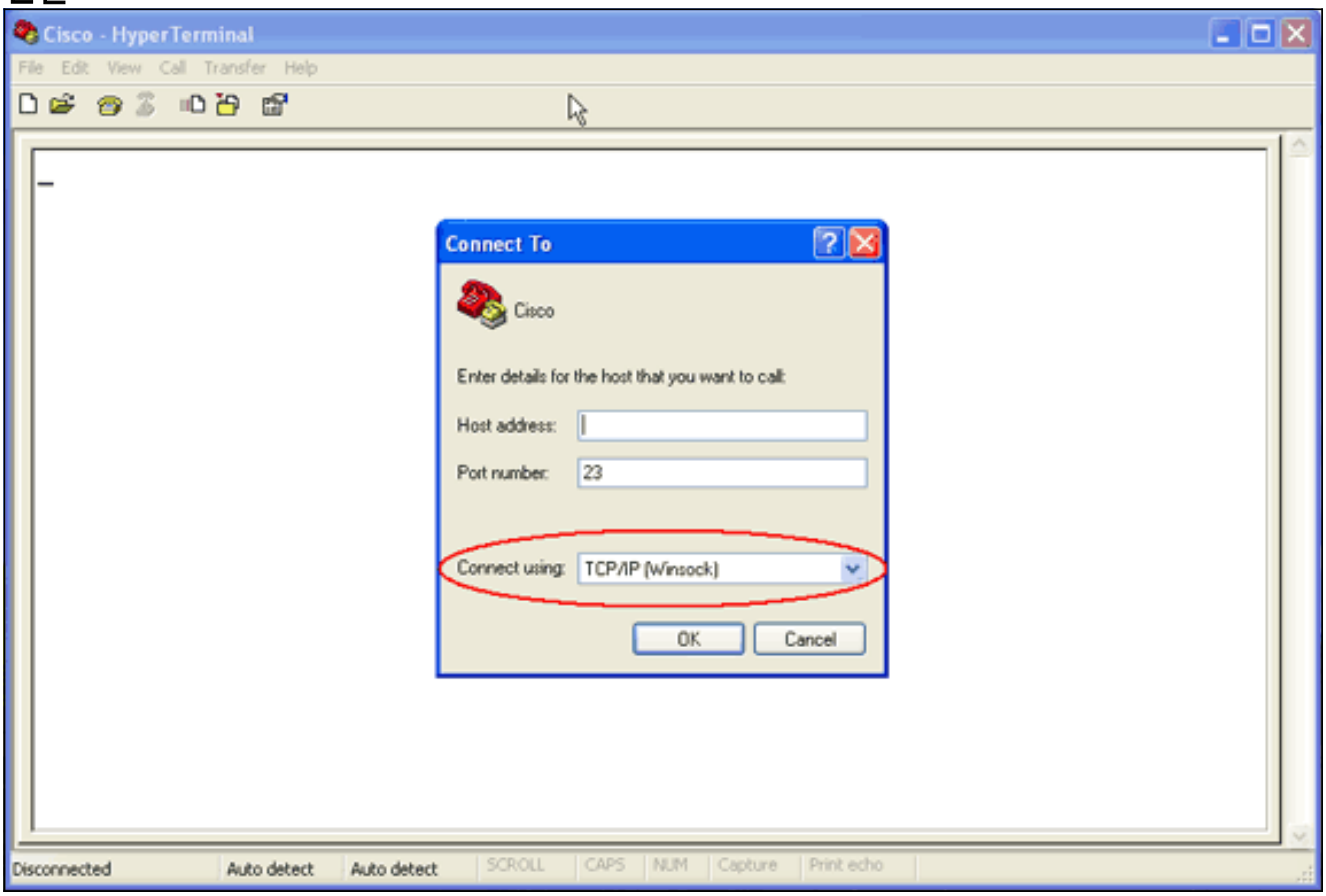
하이퍼터미널이 액세스 포인트(AP) 또는 브리지와 통신하도록 구성하려면 다음 단계를 완료하십시오.

1. 하이퍼터미널을 열려면 **시작 > 프로그램 > 시스템 도구 > 통신 > 하이퍼터미널을** 선택합니다 .**그림 1 - 하이퍼터미널 출시**

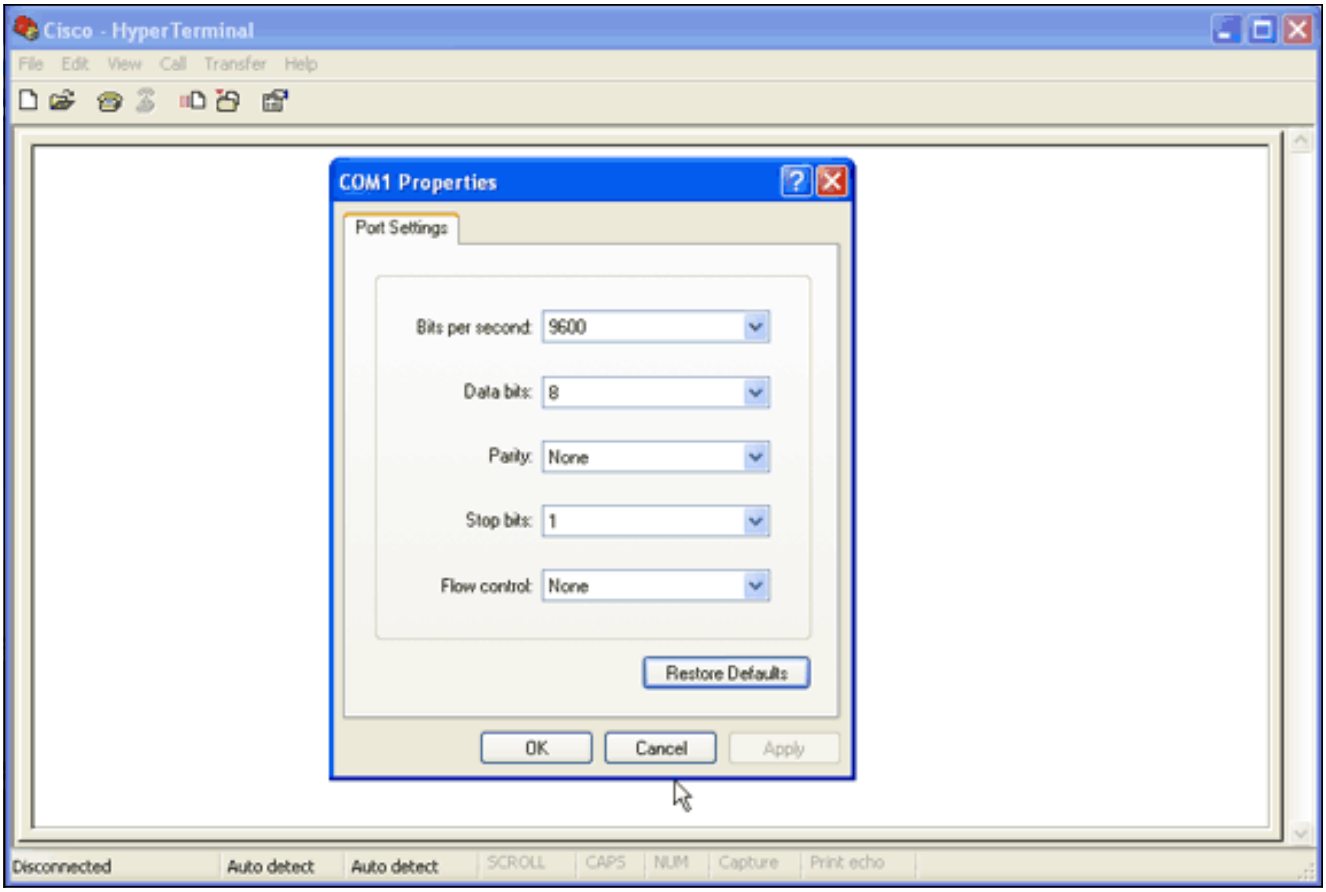


2. 하이퍼터미널이 열리면 다음 단계를 완료하십시오.연결 이름을 입력합니다.아이콘을 선택합니다.**확인을 클릭합니다**.
3. 텔넷 연결의 경우 다음 단계를 완료합니다.Connect Using 드롭다운 메뉴에서 **TCP/IP**를 선택합니다.디버그를 실행할 디바이스의 IP 주소를 입력합니다.**확인을 클릭합니다.그림 2 - 텔넷**

연결

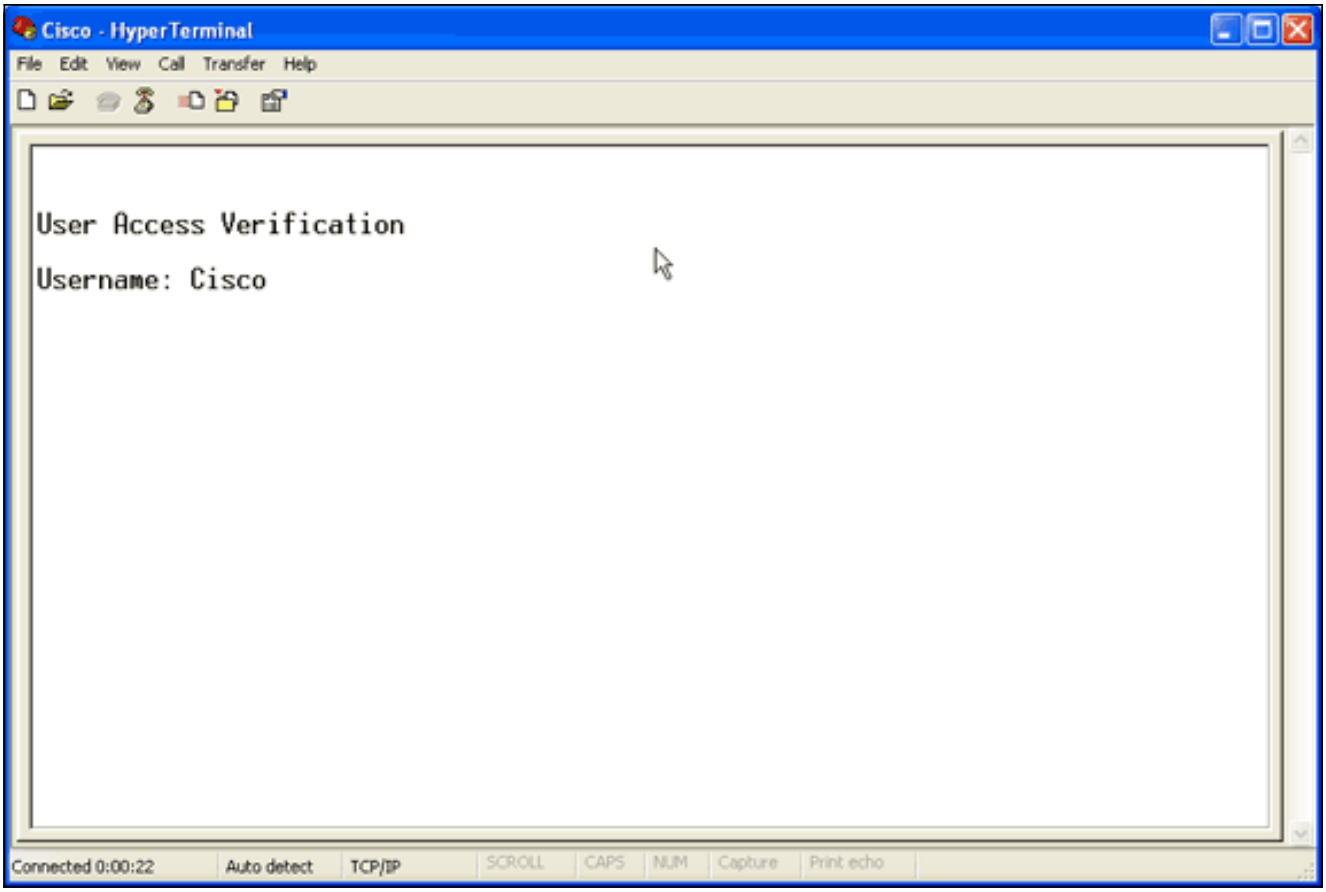


4. 콘솔 연결의 경우 다음 단계를 완료합니다.연결 사용 드롭다운 메뉴에서 콘솔 케이블이 연결된 COM 포트를 선택합니다.**확인**을 **클릭합니다**.연결의 속성 시트가 나타납니다.콘솔 포트에 대한 연결 속도를 설정합니다.기본 포트 설정을 복원하려면 Restore Defaults(기본값 복원)를 **클릭합니다**.**참고:** 대부분의 Cisco 제품은 기본 포트 설정을 따릅니다.기본 포트 설정은 다음과 같습니다.초당 비트 수 - 9600데이터 비트 - 8패리티 - 없음정지 비트 - 1흐름 제어 - 없음**그림 3 - COM1 속성**

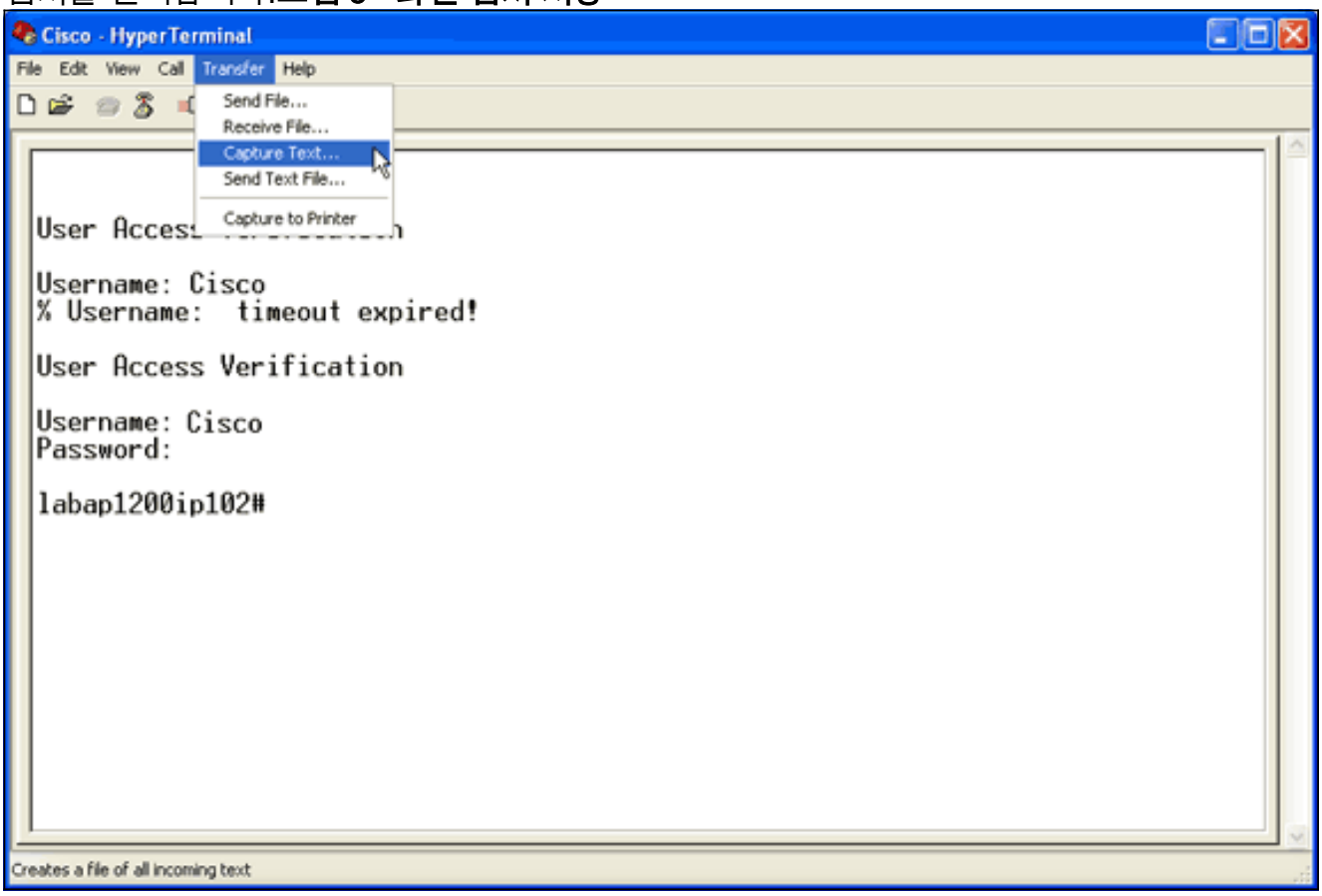


이때 텔넷 또는 콘솔 연결이 설정되고 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다 .**참고:** Cisco Aironet 장비는 *Cisco*의 기본 사용자 이름과 비밀번호(대/소문자 구분)를 모두 할당합니다.

5. 디버깅을 실행하려면 다음 단계를 완료하십시오.특별 권한 모드를 시작하려면 enable 명령을 실행합니다.enable 비밀번호를 입력합니다.**참고:** Aironet 장비의 기본 비밀번호는 *Cisco*(대/소문자 구분)입니다.**참고:** 텔넷 세션의 디버그 출력을 보려면 터미널 모니터를 켜려면 **terminal monitor** 또는 **term mon** 명령을 사용합니다.**그림 4 - 연결된 텔넷 세션**



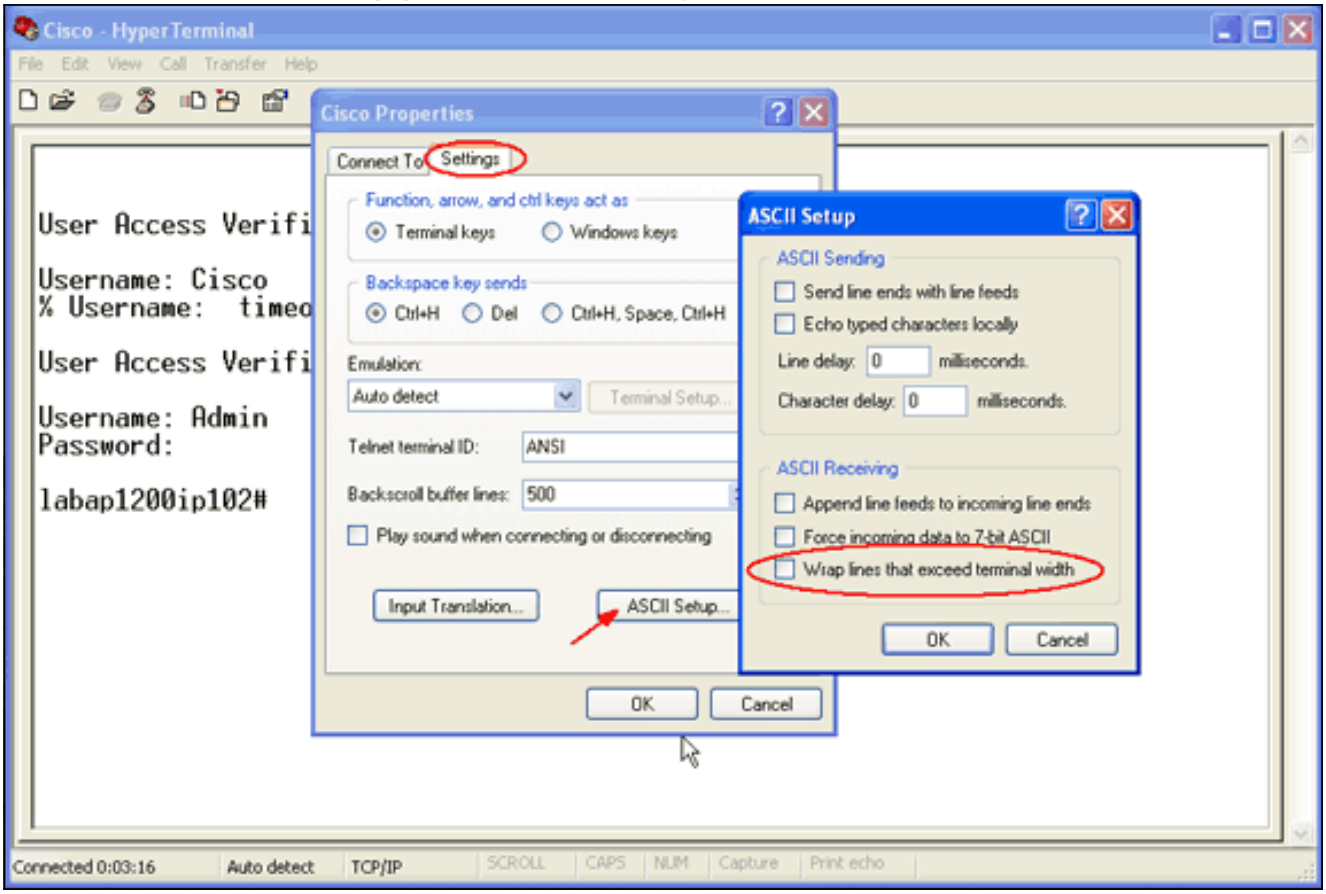
6. 연결을 설정한 후 화면 캡처를 수집하려면 다음 단계를 완료하십시오.전송 메뉴에서 텍스트 캡처를 선택합니다.**그림 5 - 화면 캡처 저장**



출력의 파일 이름을 묻는 대화 상자가 열리면 파일 이름을 입력합니다.

7. 화면 래핑을 비활성화하려면 다음 단계를 완료합니다.**참고:** 화면 래핑을 비활성화하면 디버그를 더 쉽게 읽을 수 있습니다.하이퍼터미널 메뉴에서 **파일**을 선택합니다.등록 정보**를 선택합니다**.연결 속성 시트에서 **설정** 탭을 클릭합니다.ASCII **Setup을 클릭합니다.터미널 너비를 초**

과하는 줄 바꿈을 선택 취소합니다.ASCII 설정을 닫으려면 **확인**을 클릭합니다.연결 속성 시트를 닫으려면 확인을 **누릅니다**.**그림 6 - ASCII 설정**



화면 출력을 텍스트 파일로 캡처할 수 있으므로 실행하는 디버그는 협상된 내용에 따라 달라집니다.이 문서의 다음 섹션에서는 디버그가 제공하는 협상된 연결 유형에 대해 설명합니다.

EAP

이러한 디버그는 EAP 인증에 가장 유용합니다.

- **debug radius authentication**—이 디버그 출력은 다음 단어로 시작합니다.`RADIUS`.
- **debug dot11 aaa authenticator process** - 이 디버그 출력은 다음 텍스트로 시작합니다 `.dot11_auth_dot1x_`입니다.
- **debug dot11 aaa authenticator state-machine** - 이 디버그 출력은 다음 텍스트로 시작합니다 `.dot11_auth_dot1x_run_rfsm`.

다음 디버그가 표시됩니다.

- 인증 대화 상자의 RADIUS 부분에서 보고된 내용
- 인증 대화 상자 중에 수행되는 작업
- 인증 대화 상자가 전환되는 다양한 상태

다음 예에서는 성공적인 LEAP(Light EAP) 인증을 보여줍니다.

성공한 EAP 인증 예

```
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 의 흐름 **확인합니다**.다음과 같은 여러 상태를 통해 진행이 이루어집니다.

1. EAP_START
2. _
3. _
4.
5. **참고:** 두 협상 시 CLIENT_WAIT 및 CLIENT_REPLY와 SERVER_WAIT 및 SERVER_REPLY의 여러 이터레이션이 있을 수 있습니다.
6. _

프로세스 **디버그는** 각 상태를 통과하는 개별 단계를 표시합니다.RADIUS 디버그에서는 인증 서버와 클라이언트 간의 실제 대화를 표시합니다.EAP 디버그를 사용하는 가장 쉬운 방법은 각 상태를 통해 상태 시스템 메시지의 진행 상황을 확인하는 것입니다.

협상에서 오류가 발생하면 **state-machine** 이 프로세스가 중지된 이유를 표시합니다.다음 예와 유사한 메시지를 확인합니다.

- **CLIENT TIMEOUT(클라이언트 시간 초과)** - 이 상태는 클라이언트가 적절한 시간 내에 응답하지 않았음을 나타냅니다.이러한 응답 실패는 다음 이유 중 하나로 인해 발생할 수 있습니다.클라이언트 소프트웨어에 문제가 있습니다.EAP 클라이언트 시간 초과 값(Advanced Security(고급 보안) 아래의 EAP 인증 하위 탭에서)이 만료되었습니다.일부 EAP, 특히 PEAP(Protected EAP)는 인증을 완료하는 데 30초 이상 걸립니다.이 타이머를 더 높은 값(90~120초)으로 설정합니다.다음은 CLIENT TIMEOUT 시도의 예입니다.**참고:** 이 메시지와 유사한 시스템 오류 메시지가 있는지 확인합니다.
  ```
  %DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached
    max retries, removing the client
  ```
  참고: 이러한 오류 메시지는 RF(무선 주파수) 문제를 나타낼 수 있습니다.
- **AP와 RADIUS 서버 간의 공유 암호 불일치** - 이 예제 로그에서 RADIUS 서버는 AP의 인증 요

청을 수락하지 않습니다.AP는 RADIUS 서버에 요청을 계속 전송하지만 공유 암호가 일치하지 않으므로 RADIUS 서버는 요청을 거부합니다.이 문제를 해결하려면 AP의 공유 암호가 RADIUS 서버에서 사용되는 것과 같은지 확인하십시오.

- **server_timeout**—이 상태는 인증 서버가 적절한 시간 내에 응답하지 않았음을 나타냅니다.이 응답 실패는 서버의 문제로 인해 발생합니다.다음 상황이 사실인지 확인합니다.AP는 인증 서버에 IP 연결을 제공합니다.**참고: ping** 명령을 사용하여 연결을 확인할 수 있습니다.인증 및 어카운팅 포트 번호가 서버에 대해 정확합니다.**참고:** Server Manager 탭에서 포트 번호를 확인할 수 있습니다.인증 서비스가 실행 중이며 작동합니다.다음은 server_timeout 시도의 예입니다.
- **SERVER_FAIL -** 이 상태는 서버가 사용자 자격 증명을 기반으로 인증 응답을 실패했음을 나타냅니다.이 오류 앞에 오는 RADIUS 디버그는 인증 서버에 제공된 사용자 이름을 표시합니다.서버가 클라이언트 액세스를 거부한 이유에 대한 자세한 내용은 인증 서버의 Failed Attempts(실패 시도) 로그를 확인하십시오.다음은 SERVER_FAIL 시도의 예입니다.
- **No Response from Client(클라이언트에서 응답** 없음) - 이 예에서는 radius 서버가 AP가 전달하는 전달 메시지를 AP로 전송한 다음 클라이언트를 연결합니다.결국 클라이언트는 AP에 응답하지 않습니다.따라서 AP는 최대 재시도 횟수에 도달한 후 인증을 취소합니다.AP는 radius에서 클라이언트로 get challenge 응답을 전달합니다.클라이언트는 응답하지 않으며 최대 재시도 횟수에 도달하여 EAP에 실패하고 AP에서 클라이언트 인증을 취소합니다.Radius는 AP에 전달 메시지를 전송하고, AP는 클라이언트에 전달 메시지를 전달하며, 클라이언트는 응답하지 않습니다.AP는 최대 재시도 횟수에 도달한 후 인증을 취소합니다.그러면 클라이언트는 AP에 새 ID 요청을 시도하지만 클라이언트가 이미 최대 재시도 횟수에 도달했으므로 AP는 이 요청을 거부합니다.

상태 *메시지 바로 앞에 있는* **프로세스** 및/또는 **radius** *디버그에는 실패의 세부 정보가 표시됩니다.*

EAP를 구성하는 방법에 대한 자세한 내용은 RADIUS 서버를 사용하는 EAP 인증을 참조하십시오.

MAC 인증

이러한 디버그는 MAC 인증에 가장 유용합니다.

- **debug radius authentication**—외부 인증 서버를 사용할 경우 이 디버그 출력은 다음 단어로 시작합니다.RADIUS.
- **debug dot11 aaa authenticator mac-authen** - 이 디버그 출력은 다음 텍스트로 시작합니다 .dot11_auth_dot1x_입니다.

다음 디버그가 표시됩니다.

- 인증 대화 상자의 RADIUS 부분에서 보고된 내용
- 지정된 MAC 주소와 인증된 MAC 주소의 비교

외부 RADIUS 서버를 MAC 주소 인증과 함께 사용하면 RADIUS 디버그가 적용됩니다.이 연결의 결과는 인증 서버와 클라이언트 간의 실제 대화를 보여줍니다.

MAC 주소 목록이 디바이스에 사용자 이름 및 비밀번호 데이터베이스로 로컬로 빌드되면 **mac-authen 출력을** 표시합니다.주소 일치 또는 불일치가 확인되면 이러한 출력이 표시됩니다.

참고: 항상 MAC 주소의 알파벳 문자를 소문자로 입력합니다.

다음 예에서는 로컬 데이터베이스에 대한 성공적인 MAC 인증을 보여줍니다.

성공한 MAC 인증 예

```
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]
```

다음 예에서는 로컬 데이터베이스에 대한 실패한 MAC 인증을 보여 줍니다.

실패한 MAC 인증 예

```
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
```

MAC 주소 인증이 실패하면 MAC 주소에 입력된 문자의 정확성을 확인합니다.MAC 주소의 알파벳 문자를 소문자로 입력했는지 확인하십시오.

MAC 인증을 구성하는 방법에 대한 자세한 내용은 인증 유형 구성(Cisco Aironet 액세스 포인트의 Cisco IOS Software Configuration Guide, 12.2(13)JA)을 참조하십시오.

WPA

WPA(Wi-Fi Protected Access)는 인증 유형이 아니지만 협상된 프로토콜입니다.

- WPA는 AP와 클라이언트 카드 간에 협상합니다.
- WPA 키 관리는 클라이언트가 인증 서버에서 성공적으로 인증되면 협상합니다.
- WPA는 4방향 핸드셰이크에서 PTK(Pairwise Transient Key) 및 GTK(Groupwise Transient Key)를 모두 협상합니다.

참고: WPA에서는 기본 EAP가 성공해야 하므로 WPA에 참여하기 전에 클라이언트가 해당 EAP로 성공적으로 인증할 수 있는지 확인하십시오.

이러한 디버그는 WPA 협상에 가장 유용합니다.

- **debug dot11 aaa authenticator process** - 이 디버그 출력은 다음 텍스트로 시작합니다 `.dot11_auth_dot1x_`입니다.
- **debug dot11 aaa authenticator state-machine** - 이 디버그 출력은 다음 텍스트로 시작합니다 `.dot11_auth_dot1x_run_rfsm.`

이 문서의 다른 인증과 관련하여 WPA 디버그는 읽기 및 분석하기 쉽습니다.PTK 메시지를 보내고 적절한 응답을 받아야 합니다.그런 다음 GTK 메시지를 보내고 다른 적절한 응답을 받아야 합니다.

PTK 또는 GTK 메시지가 전송되지 않으면 AP의 컨피그레이션 또는 소프트웨어 수준이 잘못될 수 있습니다.클라이언트에서 PTK 또는 GTK 응답을 받지 못한 경우 클라이언트 카드의 WPA 신청자에서 컨피그레이션 또는 소프트웨어 수준을 확인하십시오.

성공한 WPA 협상 예

```
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 구성 방법에 대한 자세한 내용은 WPA 구성 개요를 참조하십시오.

관리/HTTP 인증

로컬 사용자 이름 및 비밀번호 데이터베이스에 나열되거나 외부 인증 서버에 나열된 사용자에게 디바이스에 대한 관리 액세스를 제한할 수 있습니다.관리 액세스는 RADIUS 및 TACACS+에서 모두 지원됩니다.

이러한 디버그는 관리 인증에 가장 유용합니다.

- **debug radius authentication** 또는 **debug tacacs authentication**—이 디버그 출력은 다음 단어 중 하나로 시작합니다.RADIUS 또는 TACACS.

• **debug aaa authentication**—이 디버그의 출력은 다음 텍스트로 시작합니다.`AAA/AUTHEN`.
• **debug aaa authorization** - 이 디버그의 출력은 다음 텍스트로 시작합니다.`AAA/`.

다음 디버그가 표시됩니다.

• 인증 대화 상자의 RADIUS 또는 TACACS 부분에서 보고하는 내용
• 디바이스와 인증 서버 간의 인증 및 권한 부여에 대한 실제 협상

다음 예에서는 Service-`Type RADIUS` 특성이 Administrative로 설정된 경우 성공적인 관리 인증을 .

서비스 유형 특성을 사용한 성공적인 관리 인증 예

```
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
```

다음 예에서는 "priv-level" 문을 보내기 위해 공급업체별 특성을 사용할 때 성공적인 관리 인증을 보여줍니다.

공급업체별 특성을 사용한 성공적인 관리 인증 예

```
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
```

관리 인증에서 가장 일반적인 문제는 적절한 권한 수준 또는 관리 서비스 유형 특성을 전송하도록 인증 서버를 구성하지 못한 것입니다.다음 예에서는 권한 수준 특성 또는 관리 서비스 유형 특성이 전송되지 않았으므로 관리 인증에 실패했습니다.

공급업체별 특성 또는 서비스 유형 특성 없음

```
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=
```

관리 인증을 구성하는 방법에 대한 자세한 내용은 액세스 포인트 관리(Cisco Aironet 액세스 포인트 12.2(13)JA)를 참조하십시오.

인증 서버의 사용자에게 관리 권한을 구성하는 방법에 대한 자세한 내용은 샘플 구성을 참조하십시오.HTTP 서버 사용자를 위한 로컬 인증.사용하는 인증 프로토콜과 일치하는 섹션을 확인합니다.

관련 정보

- Cisco Aironet Access Point용 Cisco IOS 소프트웨어 구성 가이드, 12.2(13)JA
- RADIUS 서버를 사용한 EAP 인증
- 로컬 RADIUS 서버를 사용한 LEAP 인증
- Cisco Aironet Wireless Security FAQ
- Wireless Domain Services AP as an AAA Server 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems