Debug-verificatie

Inhoud

Inleiding

Draadloze communicatie maakt op vele manieren gebruik van authenticatie. Het meest voorkomende authenticatietype is Extensible Verification Protocol (EAP) in verschillende typen en vormen. Andere authenticatietypen omvatten MAC-adresverificatie en administratieve authenticatie. Dit document beschrijft hoe u de uitvoer van debug-authenticaties kunt reinigen en interpreteren. De informatie uit deze bronnen is van onschatbare waarde wanneer u draadloze installaties bedient.

Opmerking: de gedeelten van dit document die verwijzen naar producten die niet afkomstig zijn van Cisco, zijn gebaseerd op de ervaring van de auteur en niet op formele training. Deze zijn bedoeld voor uw gemak en niet als technische ondersteuning. Neem voor gezaghebbende technische ondersteuning voor producten die niet afkomstig zijn van Cisco, contact op met de technische ondersteuning voor dat product.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Verificatie in verband met draadloze netwerken
- Cisco IOS® software commanline interface (CLI)
- Configuratie van RADIUS-servers

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS op software gebaseerde draadloze producten van elk model en elke versie
- Hilgraeve HyperTerminal

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

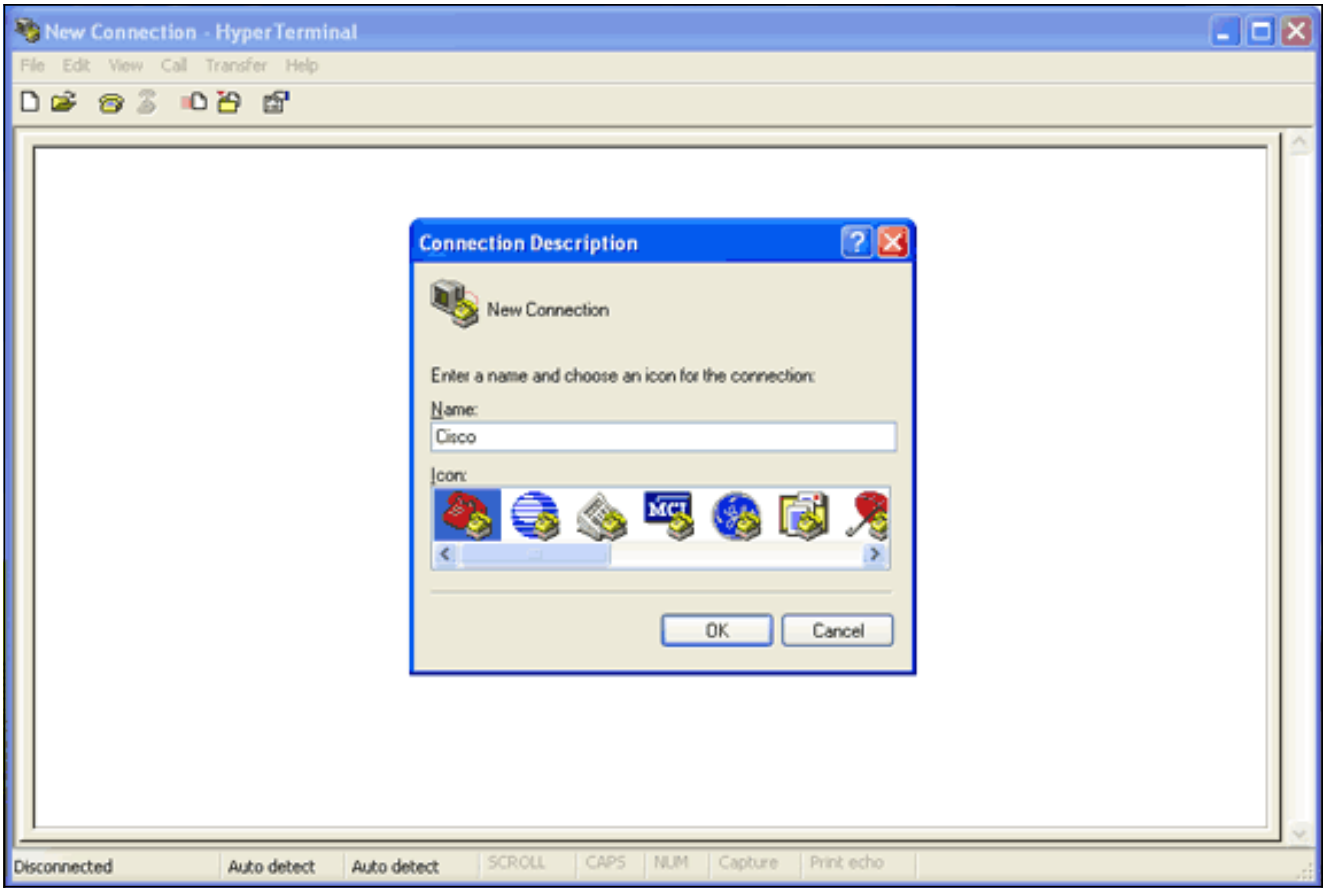
Capture Debugs

Als u geen debug-informatie kunt opnemen en analyseren, heeft deze informatie geen zin. De makkelijkste manier om deze gegevens op te nemen is met een scherm-opname functie die in de telnet of de communicatie toepassing ingebouwd is.

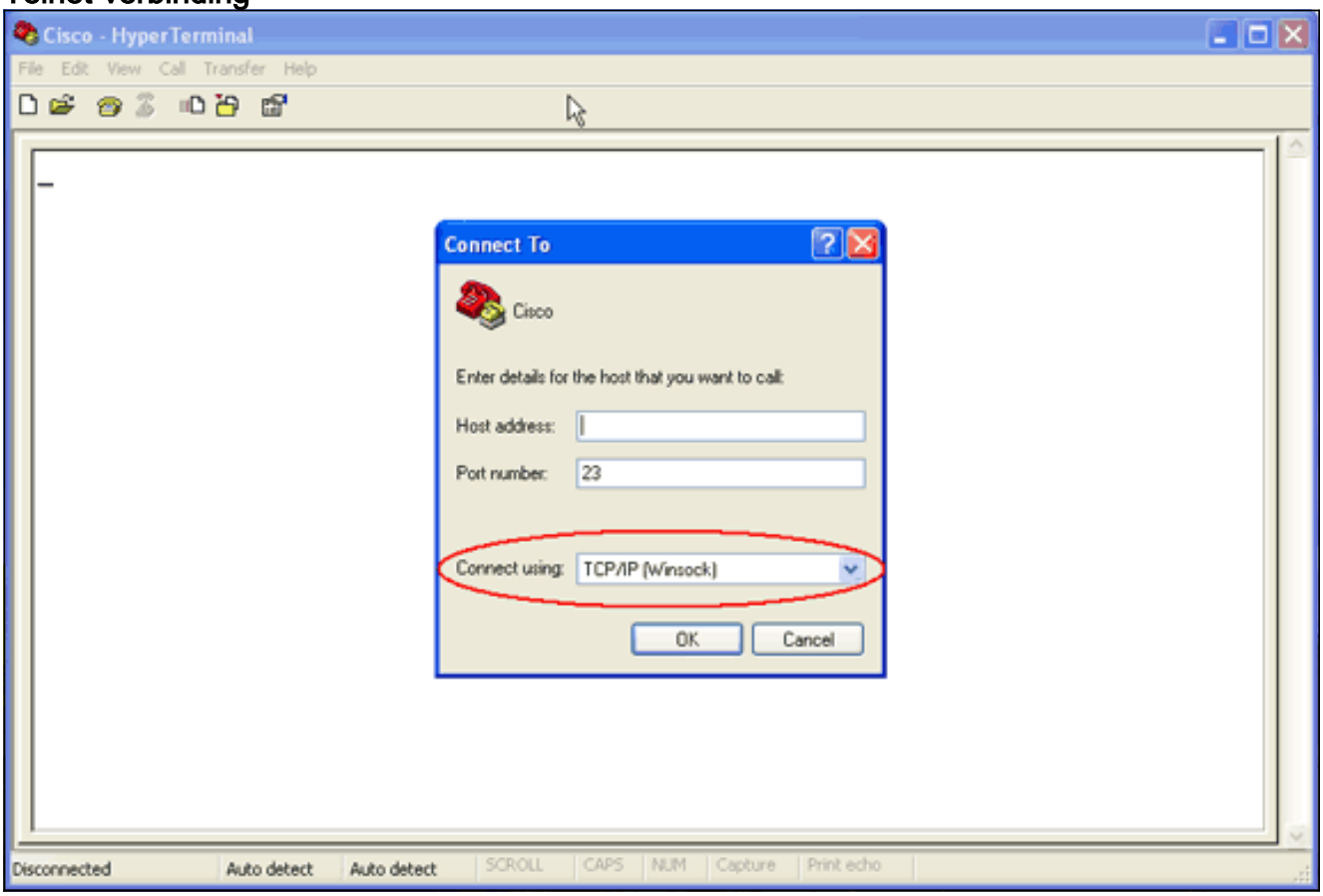
In dit voorbeeld wordt beschreven hoe u uitvoer kunt opnemen met de Hilgraeve HyperTerminal-applicatie. De meeste Microsoft Windows besturingssystemen omvatten HyperTerminal, maar u kunt de concepten op elke eindemulatietoepassing toepassen. Zie voor meer informatie over de applicatie Hilgraeve .

Voltooi deze stappen om HyperTerminal te configureren om met uw access point (AP) of brug te communiceren:

1. Om HyperTerminal te openen, kies **Start > Programma's > Gereedschappen > Communicatie > HyperTerminal**.**Afbeelding 1 - Start HyperTerminal**

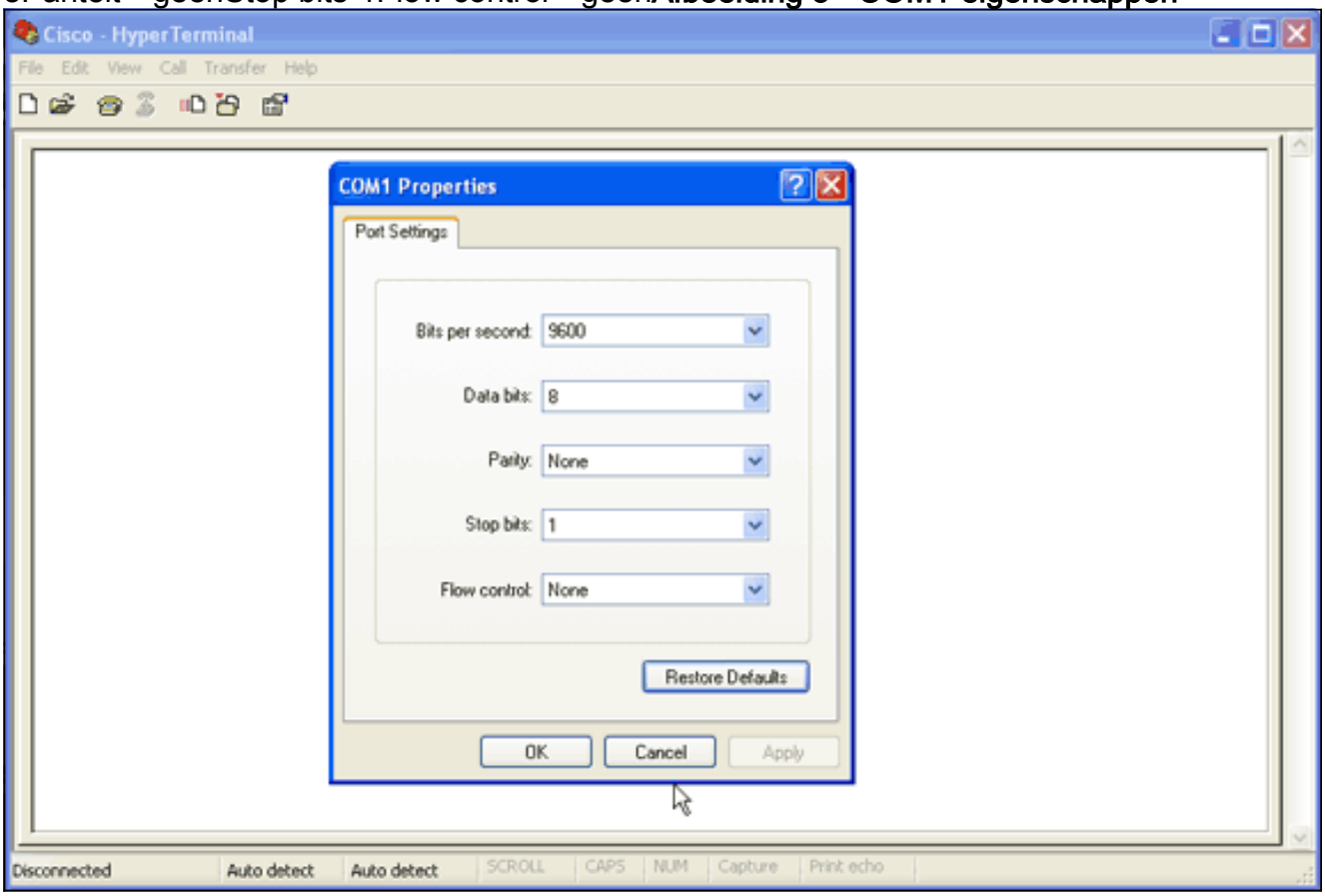


2. Wanneer HyperTerminal opent, voltooi deze stappen:Voer een naam in voor de verbinding.Kies een pictogram.Klik op **OK**.
3. Voor Telnet-verbindingen:Kies in het vervolgkeuzemenu Connect Gebruik **TCP/IP**.Voer het IP-adres in van het apparaat waar u de apparaten wilt uitvoeren.Klik op **OK**.**Afbeelding 2 - Telnet-verbinding**



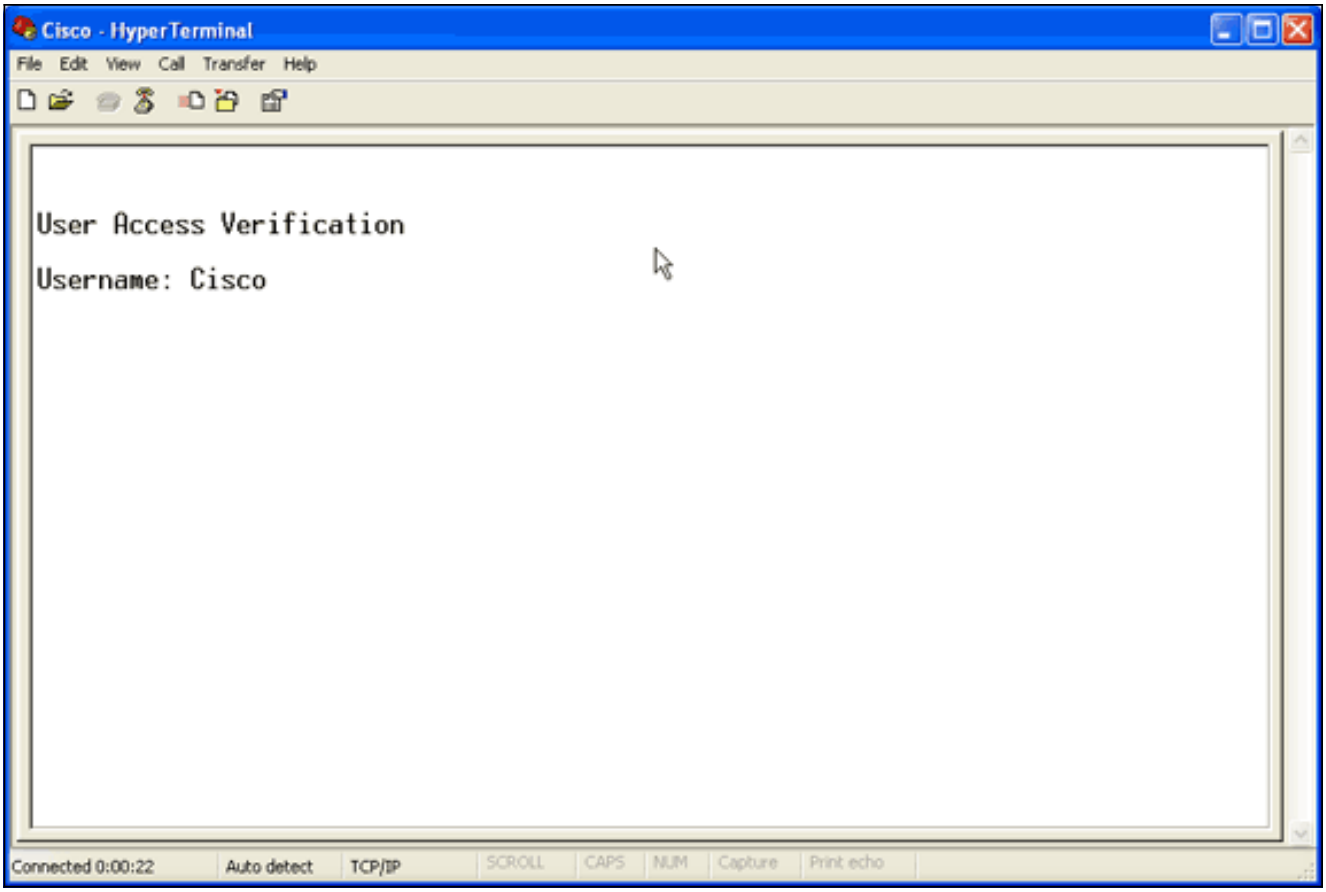
4. Voor consoleverbindingen:Kies in het vervolgkeuzemenu Connect Gebruik de COM-poort

waar de consolekabel is aangesloten.Klik op **OK**.Het kenblad voor de verbinding verschijnt.Stel de snelheid voor de aansluiting in op de troostpoort.Klik om de standaardinstellingen van de poort te herstellen op **Standaardinstellingen herstellen**.**Opmerking:** de meeste Cisco-producten volgen de standaardinstellingen van de poort.De standaardinstellingen van de poort zijn:its per seconde-9600Gegevensbits-8Pariteit—geenStop bits-1Flow control—geen**Afbeelding 3 - COM1-eigenschappen**

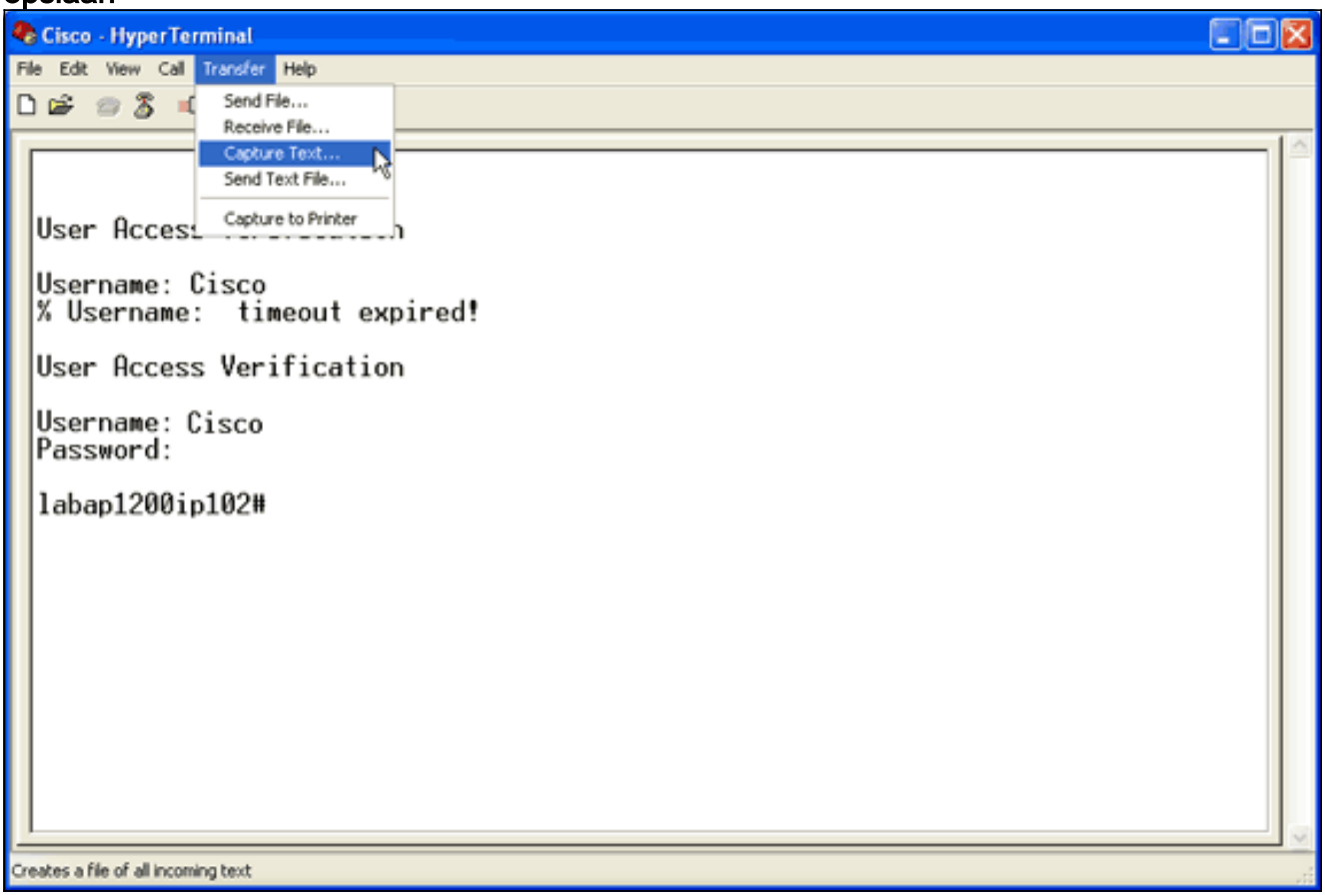


Op dit punt, de verbinding van het telnet of van de console, en u wordt gevraagd voor een gebruikersnaam en een wachtwoord.**Opmerking:** Cisco Aironet-apparatuur heeft zowel een standaard- als een defaultwachtwoord van *Cisco* (hoofdlettergevoelig) toegewezen.

5. Voltooi de volgende stappen om een debugs uit te voeren:Geef de opdracht **aan** om geprivilegieerde modus in te voeren.Typ het wachtwoord voor het activeren.**Opmerking:** Vergeet niet dat het defaultwachtwoord voor Aironet-apparatuur *Cisco* (hoofdlettergevoelig) is.**Opmerking:** Om de uitvoer van beelden van een Telnet-sessie te zien, gebruik de **terminal monitor** of **term mon** opdracht om de terminal monitor aan te zetten.**Afbeelding 4 - Connected Telnet-sessie**



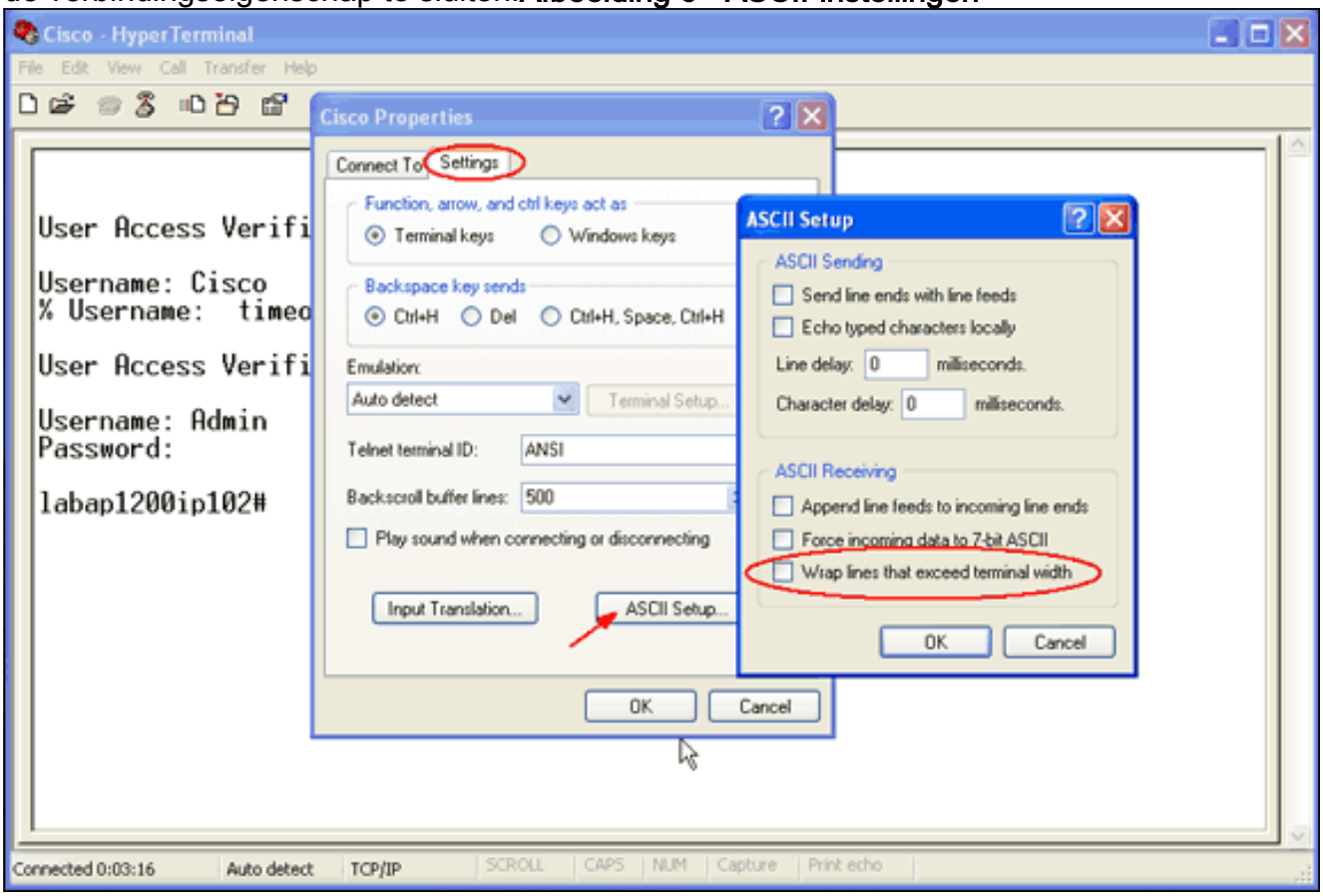
6. Nadat u een verbinding hebt gemaakt, voert u deze stappen uit om een screenshot te verzamelen:Kies **Opname tekst** in het menu Overdracht.**Afbeelding 5 - Een schermopname opslaan**



Wanneer een dialoogvenster wordt geopend dat u vraagt om een bestandsnaam voor de uitvoer, voert u een bestandsnaam in.

7. Voltooi deze stappen om de schermmap uit te schakelen:**Opmerking:** U kunt de knoppen

eenvoudiger lezen wanneer u de schermmap uitschakelt.Kies in het menu HyperTerminal **Bestand**.Kies **Eigenschappen**.Klik in het vel van de verbindingseigenschap op het tabblad **Instellingen**.Klik op **ASCII instellen**.Schakel **de omlooplijnen uit die de eindbreedte overschrijden**.Klik op **OK** om de ASCII-instellingen te sluiten.Klik op **OK** om het formulier voor de verbindingseigenschap te sluiten.**Afbeelding 6 - ASCII-instellingen**



Nu u een schermuitvoer naar een tekstbestand kunt opnemen, zijn de uitgangen die u gebruikt afhankelijk van wat wordt overeengekomen. In de volgende delen van dit document wordt het type van de door de distributeurs geleverde onderhandeling beschreven.

MAART

Deze cijfers zijn het meest behulpzaam voor MAP-authenticaties:

- **debugstraal verificatie**—de output van dit debug start met dit woord: `RADIUS`.
- **debug dot11 a authenticator proces**—de uitgangen van dit debug starten met deze tekst: `dot11_auth_dot1x_`.
- **debug dot11 a oor-oor**-de uitgangen van dit debug starten met deze tekst: `dot11_auth_dot1x_run_rfsm`.

Deze uitvindingen tonen:

- Wat tijdens de RADIUS-delen van een verificatiedialoog wordt gemeld
- De acties die tijdens die verificatiedialoog zijn ondernomen
- De verschillende staten via welke de echtheidscontrole - dialoog verloopt

Dit voorbeeld toont een succesvolle MAP-verificatie (Light EAP):

Succesvol EAP-verificatievoorbeeld

```
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]
```

Let op de stroom in de **uitwerpselen van de machine**. Er is een progressie door verschillende staten:

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY**Opmerking:** Tijdens de onderhandelingen kunnen er verschillende iteraties van CLIENT_WAIT en CLIENT_REPLY zijn, SERVER_WAIT en SERVER_REPLY.
6. SERVER_PASS

Het **proces** debug toont elke individuele stap door elke staat. De dieptepunten tonen het eigenlijke gesprek tussen de authenticatieserver en de client. De makkelijkste manier om met MAP-deposito's te werken is om de progressie van staatsmachineperichten door elke staat te zien.

Als er iets mis is in de onderhandelingen, **laten** de **debugs van de staatsmachine** zien waarom het proces is gestopt. Bekijk de berichten die vergelijkbaar zijn met deze voorbeelden:

- **CLIENT TIMEOUT**-Deze status geeft aan dat de client niet binnen de juiste tijd heeft gereageerd. Dit falen om te reageren kan om een van deze redenen optreden:Er is een probleem met de clientsoftware.De MAP client timeout waarde (van het MAP EMATIG Verificatiesubtabblad onder Geavanceerd security) is verlopen.Voor sommige MAP's, met name Protected EAP

(PEAP), duurt het langer dan 30 seconden om de echtheidscontrole te voltooien. Stel deze timer in op een hogere waarde (tussen 90 en 120 seconden).Dit is een voorbeeld van een poging `van CLIENT TIMEOUT`:**Opmerking:** Kijk naar alle foutmeldingen die vergelijkbaar zijn met dit bericht:

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

Opmerking: Dergelijke foutmeldingen kunnen duiden op een RF-probleem (radiofrequentie).

- **Gedeelde geheime mismatch tussen AP en de RADIUS server** - In dit voorbeeldlogbestand accepteert de RADIUS-server niet de authenticatieaanvraag van AP. AP blijft het verzoek naar de server van de RADIUS verzenden, maar de server van de RADIUS wijst het verzoek af omdat het gedeelde geheim verkeerd is afgestemd.Om dit probleem op te lossen, controleer of het gedeelde geheim op AP hetzelfde is dat in de RADIUS-server wordt gebruikt.
- **`server_timeout`** —Deze staat geeft aan dat de authenticatieserver niet in de juiste tijd reageerde. Deze mislukking om te reageren komt voor vanwege een probleem op de server. Controleer of deze situaties waar zijn:AP heeft IP connectiviteit op de authenticatieserver.**Opmerking:** U kunt de opdracht **ping** gebruiken om de connectiviteit te controleren.De authenticatie en accounting poortnummers zijn correct voor de server.**N.B.:** U kunt de poortnummers controleren op het tabblad Server Manager.De verificatiedienst werkt en functioneert.Dit is een voorbeeld van een `server_timeout` poging:
- **`SERVER_FAIL`** - Deze staat geeft aan dat de server een onsuccesvolle authenticatie respons gaf gebaseerd op de gebruikersreferenties. RADIUS debug die vóór deze fout gaat, toont de naam van de gebruiker die aan de authenticatieserver is voorgesteld. Controleer het logbestand van mislukte pogingen in de verificatieserver voor meer informatie over waarom de server de toegang tot de client ontzegd heeft.Dit is een voorbeeld van een poging `SERVER_FAIL`:
- **Geen respons van client**-In dit voorbeeld verstuurt de Straalserver een signaal naar AP dat de AP doorstuurt en dan associeert het de client. Uiteindelijk reageert de klant niet op de AP. Daarom deauthenticeert AP het nadat het de maximum herhalingen bereikt.AP stuurt een uitdaging-respons van de straal naar de cliënt door. De cliënt reageert niet en bereikt max. terugboekingen die ervoor zorgen dat EAP faalt en AP de cliënt onecht maakt.Radius stuurt een doorvoerbericht naar AP, AP stuurt het doorgeven bericht naar de client en de client reageert niet. AP deauthentificeert het nadat het de maximum herhalingen bereikt. De cliënt probeert dan een nieuw verzoek van de Identiteit aan AP, maar AP verwerpt dit verzoek omdat de cliënt de maximum herprobeert.

Het **`proces`** en/of de **`Straal`** **uiteinden die onmiddellijk** *aan het bericht van de staatsmachine voorafgaan, geven de details van de storing weer.*

Raadpleeg voor meer informatie over de manier waarop u EAP kunt configureren de EAP-verificatie met RADIUS-server.

MAC-verificatie

Deze debugs zijn het meest behulpzaam voor MAC-verificatie:

- **debug Straalverificatie**—Wanneer een externe authenticatieserver wordt gebruikt, beginnen de uitgangen van dit debug met dit woord: `RADIUS`.
- **debug dot11 a.mac-authen**: de uitgangen van dit debug beginnen met deze tekst: `dot11_auth_dot1x_`.

Deze uitvindingen tonen:

- Wat tijdens de RADIUS-delen van een verificatiedialoog wordt gemeld
- De vergelijking tussen het opgegeven MAC-adres en het adres dat is geauthentiseerd tegen

Wanneer een externe RADIUS-server wordt gebruikt met MAC-adresverificatie, gelden de RADIUS-debugs. Het resultaat van deze combinatie is een weergave van het werkelijke gesprek tussen de authenticatieserver en de client.

Wanneer een lijst van de adressen van MAC lokaal aan het apparaat als een gebruikersnaam en wachtwoordgegevensbestand wordt gebouwd, **tonen** slechts de **door mac-auen** **debugs** output. Aangezien de adresmatch of de onduidelijke weergave wordt bepaald, worden deze uitgangen weergegeven.

Opmerking: Voer altijd alle alfabetische tekens in in een MAC-adres in kleine letters in.

Deze voorbeelden tonen een succesvolle MAC-verificatie tegen een lokale gegevensbank:

Succesvol MAC-verificatievoorbeeld

```
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]
```

Deze voorbeelden tonen een mislukte MAC-verificatie tegen een lokale database:

Opgegeven MAC-verificatie

```
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
```

Wanneer een MAC-adresverificatie faalt, controleert u op de nauwkeurigheid van de tekens die in het MAC-adres zijn ingevoerd. Verzeker u dat u alle alfabetische tekens in een MAC-adres in kleine letters hebt ingevoerd.

Raadpleeg voor meer informatie over het configureren van MAC-verificatie de configuratietypen voor verificatie (Cisco IOS-softwarerelease Guide voor Cisco Aironet access points, 12.2(13)JA).

medearbeidster

Hoewel Wi-Fi Protected Access (WAP) geen authenticatietype is, is het een onderhandeld protocol.

- WAP onderhandelt tussen de AP en de clientkaart.
- WAP-sleutelbeheer onderhandelt nadat een client is geauthentiseerd door een verificatieserver.
- WAP onderhandelt zowel over een parwisise Transient Key (PTK) als over een Groepswijs Transient Key (GTK) in een viervoudige handdruk.

Opmerking: Omdat WAP vereist dat het onderliggende MAP succesvol is, controleer of klanten succesvol met dat MAP kunnen authenticeren voordat u WAP gebruikt.

Deze debugs zijn het meest behulpzaam voor de onderhandelingen van WAP:

- **debug dot11 a authenticator proces**—de uitgangen van dit debug starten met deze tekst: `dot11_auth_dot1x_`.
- **debug dot11 a oor-oor**-de uitgangen van dit debug starten met deze tekst: `dot11_auth_dot1x_run_rfsm`.

Vergeleken met de andere authenticaties in dit document, zijn wachtwoorden eenvoudig te lezen en te analyseren. Er moet een PTK-bericht worden verstuurd en een passend antwoord worden ontvangen. Vervolgens moet er een GTK-bericht worden verstuurd en moet er een ander passend antwoord worden ontvangen.

Als de PTK- of GTK-berichten niet worden verstuurd, kan de configuratie of het softwareciveau op de AP een fout maken. Als de PTK- of GTK-reacties van de client niet zijn ontvangen, controleert u het configuratie- of softwarerelease op de WAP-smeekbede van de client.

Succesvol WAP-onderhandelingsvoorbeeld

```
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#
```

Raadpleeg voor meer informatie over de configuratie van WAP het Overzicht van de WAP-configuratie.

Administratieve/HTTP-verificatie

U kunt de administratieve toegang tot het apparaat beperken tot gebruikers die in of een lokale gebruikersnaam en een wachtwoorddatabase zijn vermeld of naar een externe verificatieserver. Administratieve toegang wordt ondersteund met zowel RADIUS als TACACS+.

Deze debugs zijn het meest behulpzaam bij administratieve authenticatie:

- **debugstraal verificatie** of **debug tacacs verificatie**—de output van dit debug start met een van deze woorden: `RADIUS` of `TACACS`.
- **debug a authenticatie**: de uitgangen van deze debugs beginnen met deze tekst: `AAA/AUTOMATISCH`.
- **debug a autorisatie**—de uitgangen van deze sites beginnen met deze tekst: `AAA/AUTEUR`.

Deze uitvindingen tonen:

- Wat tijdens de RADIUS- of TACACS-delen van een verificatiedialoog is gemeld
- De eigenlijke onderhandelingen voor authenticatie en autorisatie tussen het apparaat en de authenticatieserver

Dit voorbeeld laat een succesvolle administratieve authenticatie zien wanneer de `Service-Type RADIUS` eigenschap wordt ingesteld op `Administratief`:

Succesvol voorbeeld voor administratieve verificatie met kenmerken van het servicetype

```
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
```

Dit voorbeeld laat een succesvolle administratieve authenticatie zien wanneer je verkoper-specifieke eigenschappen gebruikt om een verklaring op "priv level" te sturen:

Succesvol voorbeeld van administratieve verificatie met leverancierspecifieke kenmerken

```
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
```

Het meest voorkomende probleem met administratieve authenticatie is het falen om de authenticatieserver te configureren om de juiste voorrecht-niveau of administratieve service-type eigenschappen te verzenden. Dit voorbeeld heeft gefaald op administratieve authenticatie omdat er geen eigenschappen van het privilege-niveau of administratieve dienstverlenende eigenschappen werden verzonden:

Zonder leverancierspecifieke of servicetype-kenmerken

```
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=
```

Raadpleeg voor meer informatie over het configureren van beheerste verificatie het beheer van

het access point (Cisco IOS-softwareconfiguratie Guide voor Cisco Aironet access points, 12.2(13)JA).

Raadpleeg voor meer informatie over het configureren van beheerrechten voor gebruikers op de verificatieserver de configuratie van een monster: Lokale verificatie voor HTTP-servergebruikers. Controleer de sectie die overeenkomt met het verificatieprotocol dat u gebruikt.

Gerelateerde informatie

- Cisco IOS-softwarerelease voor Cisco Aironet access points, 12.2(13)JA
- EAP-verificatie met RADIUS-server
- LEAP-verificatie met lokale RADIUS-server
- FAQ op Cisco Aironet draadloze beveiliging
- Configuratievoorbeeld voor draadloze domeinservices als AAA-server
- Technische ondersteuning en documentatie – Cisco Systems