Autenticazioni debug

Sommario

Introduzione

La comunicazione wireless utilizza l'autenticazione in molti modi. Il tipo di autenticazione più comune è il protocollo EAP (Extensible Authentication Protocol), disponibile in diversi tipi e moduli. Altri tipi di autenticazione includono l'autenticazione dell'indirizzo MAC e l'autenticazione amministrativa. In questo documento viene descritto come eseguire il debug e interpretare l'output delle autenticazioni di debug. Le informazioni di questi debug sono preziose per la risoluzione dei problemi relativi alle installazioni wireless.

Nota: le parti di questo documento che fanno riferimento a prodotti non Cisco si basano sull'esperienza dell'autore, non sulla formazione formale. Sono concepiti per offrire la massima comodità e non come supporto tecnico. Per il supporto tecnico autorevole su prodotti non Cisco, contattare il supporto tecnico per tale prodotto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione correlata alle reti wireless
- Interfaccia della riga di comando (CLI) del software Cisco IOS®
- Configurazione server RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Prodotti wireless basati su software Cisco IOS di qualsiasi modello e versione
- Hilgraeve HyperTerminal

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

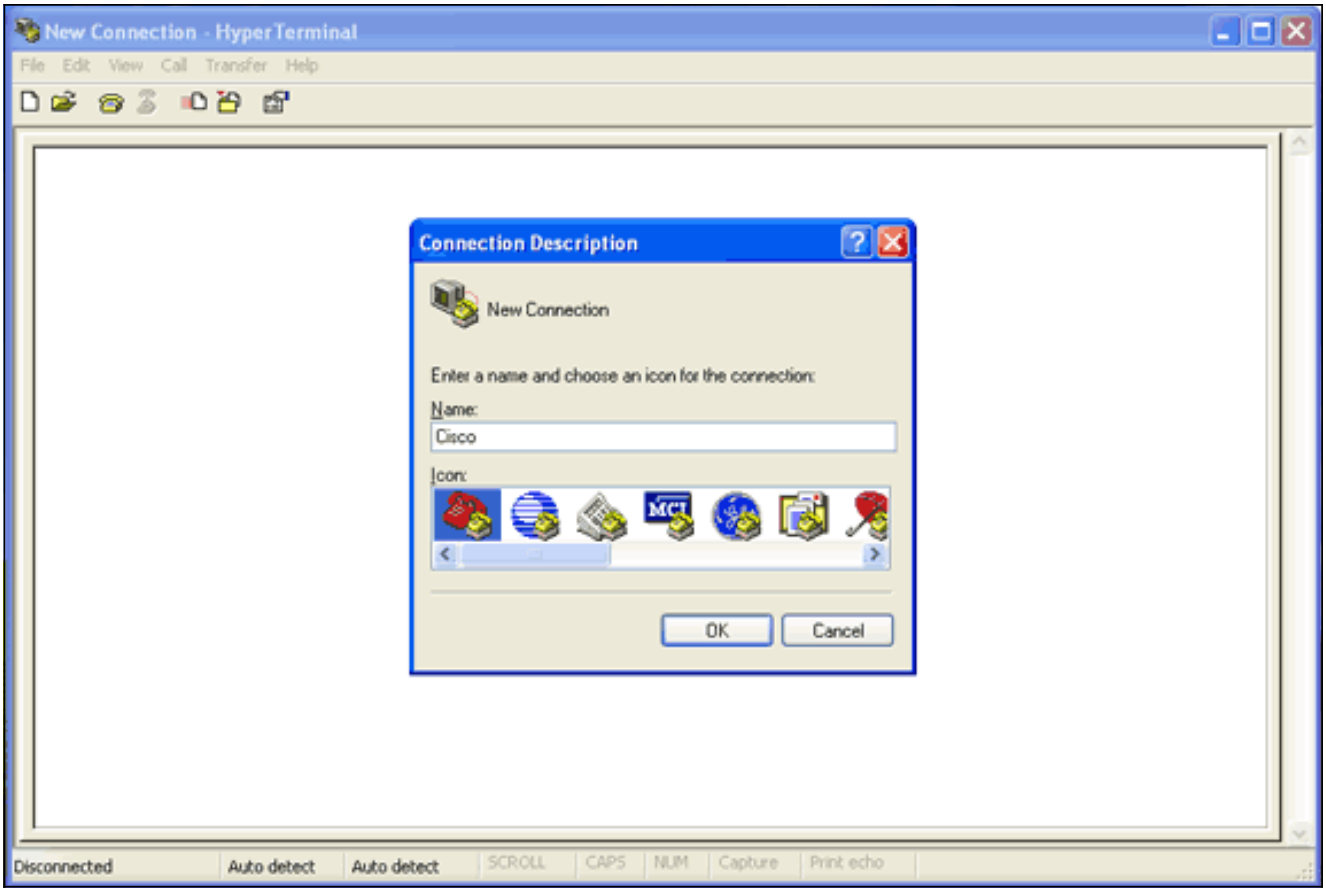
Acquisisci debug

Se non è possibile acquisire e analizzare le informazioni di debug, queste sono inutili. Il modo più semplice per acquisire questi dati è tramite una funzione di acquisizione schermo integrata nell'applicazione Telnet o di comunicazione.

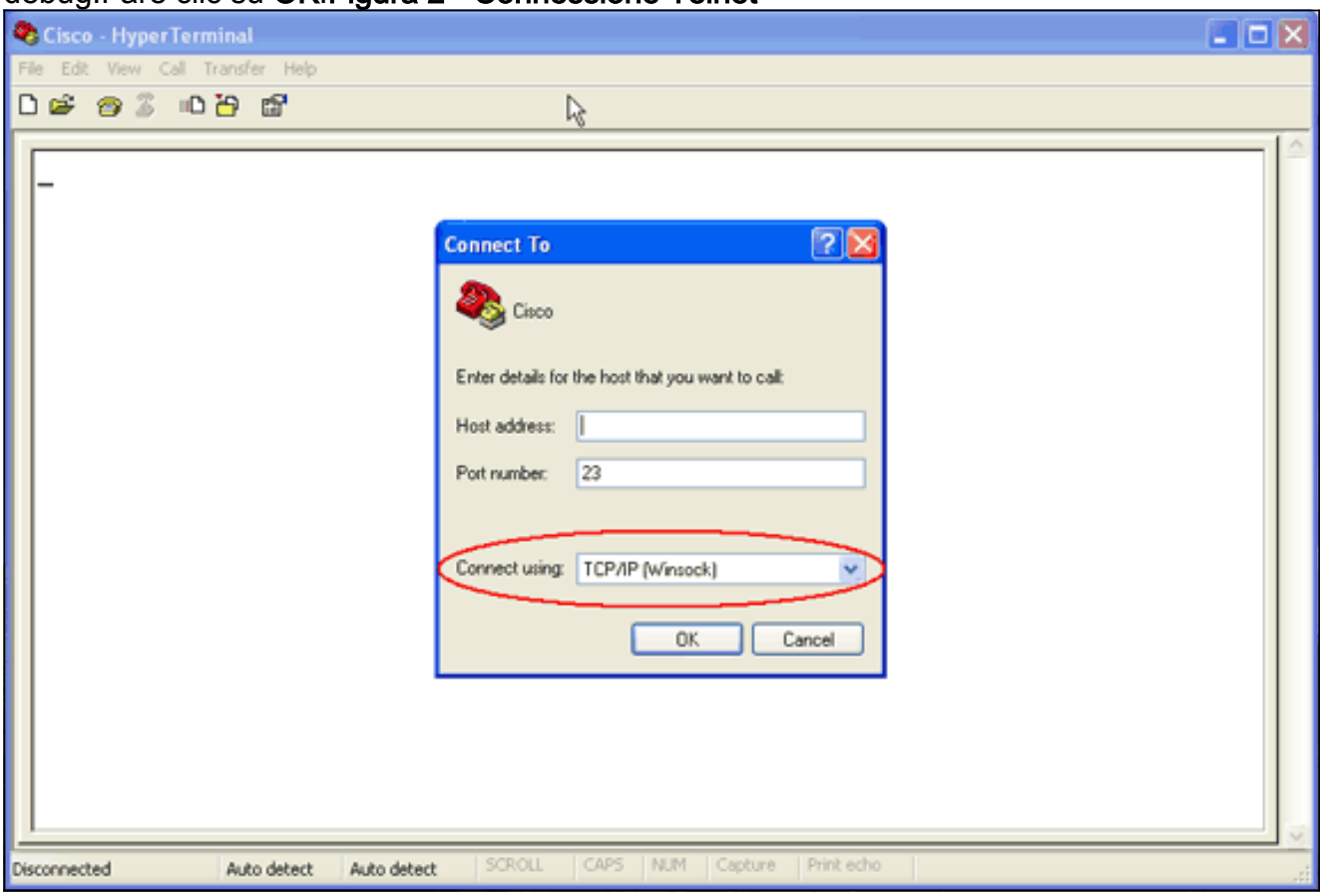
In questo esempio viene descritto come acquisire l'output con l'applicazione HyperTerminal Hilgraeve. La maggior parte dei sistemi operativi Microsoft Windows include HyperTerminal, ma è possibile applicare i concetti a qualsiasi applicazione di emulazione terminale. Per informazioni più complete sull'applicazione, fare riferimento a Hilgraeve .

Completare questa procedura per configurare HyperTerminal in modo che comunichi con il punto di accesso (AP) o il bridge:

1. Per aprire HyperTerminal, scegliere **Start > Programmi > Utilità di sistema > Comunicazioni > HyperTerminal**.**Figura 1 - Lancio di HyperTerminal**

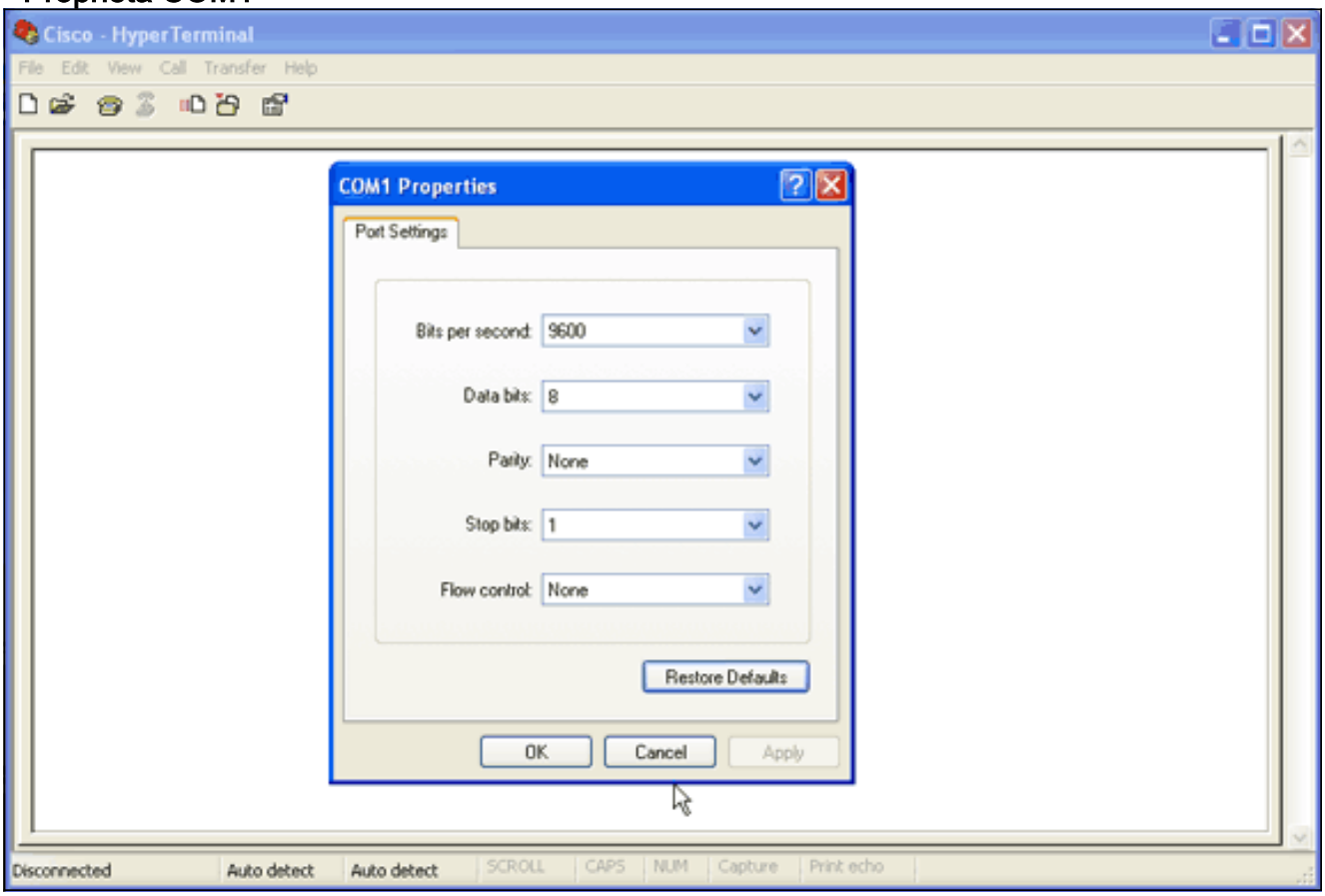


2. All'apertura di HyperTerminal, attenersi alla seguente procedura:Immettere un nome per la connessione.Scegliere un'icona.Fare clic su **OK**.
3. Per le connessioni Telnet, eseguire la procedura seguente:Dal menu a discesa Connetti tramite, scegliere **TCP/IP**.Immettere l'indirizzo IP del dispositivo in cui si desidera eseguire i debug.Fare clic su **OK**.**Figura 2 - Connessione Telnet**



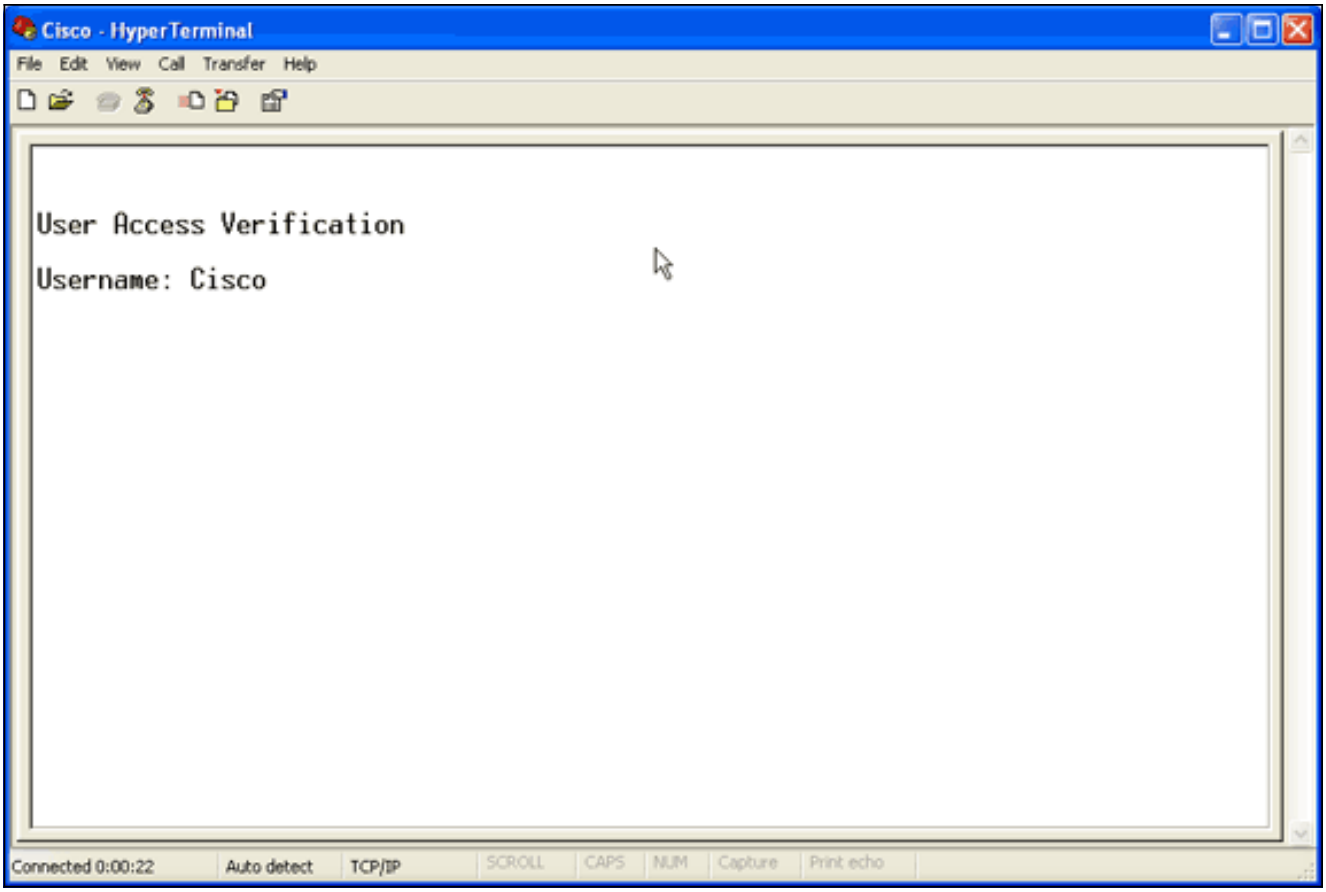
4. Per le connessioni da console, attenersi alla seguente procedura:Dal menu a discesa

Connetti tramite, scegliere la porta COM a cui è collegato il cavo console.Fare clic su **OK**.Verrà visualizzata la finestra delle proprietà della connessione.Impostare la velocità di connessione alla porta della console.Per ripristinare le impostazioni predefinite della porta, fare clic su **Ripristina impostazioni predefinite**.**Nota:** la maggior parte dei prodotti Cisco segue le impostazioni predefinite delle porte.Le impostazioni predefinite della porta sono:Bit per secondo—9600Bit di dati—8Parità: nessunaBit di stop—1Controllo flusso - Nessuno**Figura 3 - Proprietà COM1**

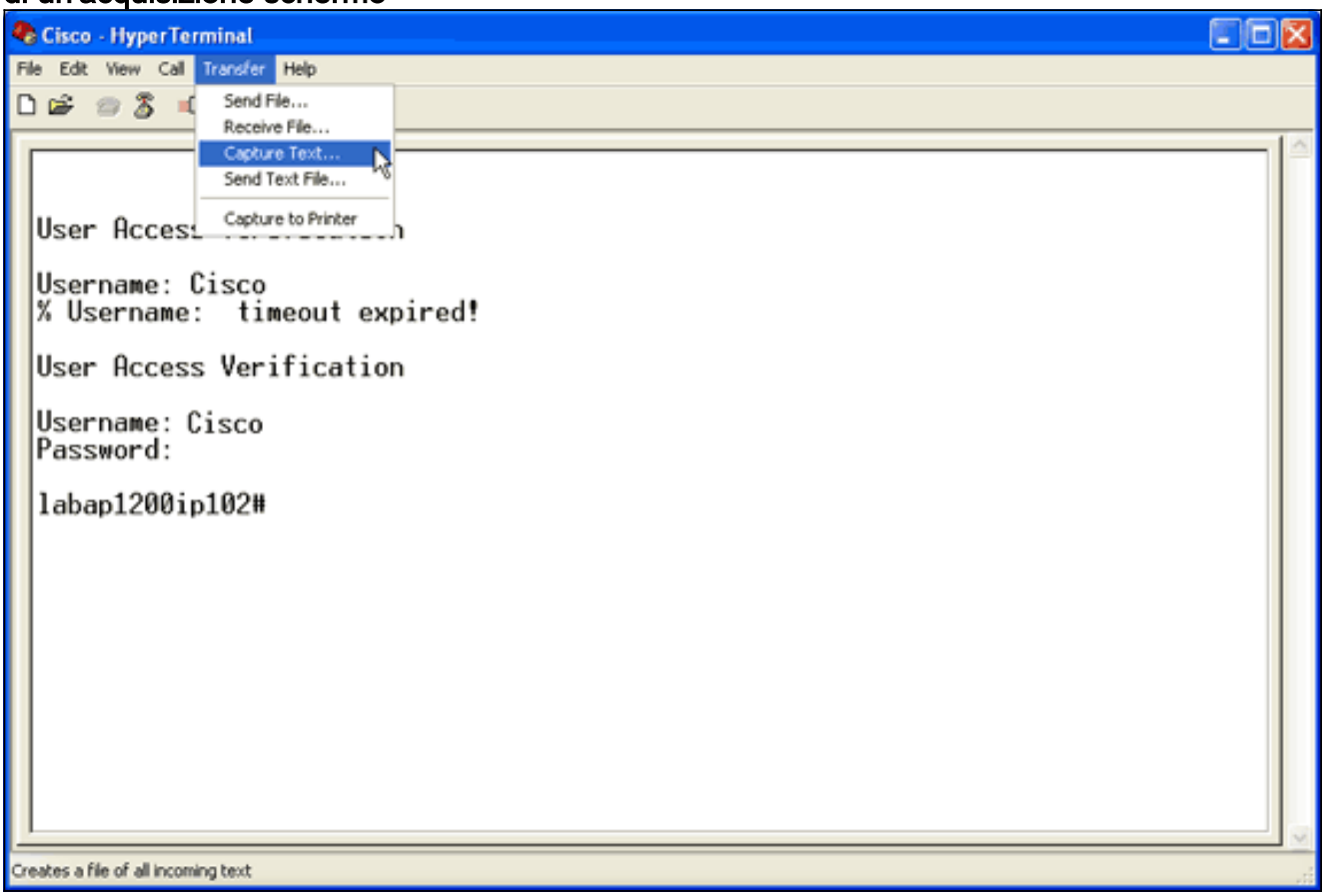


A questo punto, la connessione Telnet o console viene stabilita e viene richiesto di immettere un nome utente e una password.**Nota:** ai dispositivi Cisco Aironet vengono assegnati sia un nome utente che una password predefiniti di *Cisco* (con distinzione tra maiuscole e minuscole).

5. Per eseguire il debug, procedere come segue:Per accedere alla modalità privilegiata, usare il comando **enable**.Immettere la password di abilitazione.**Nota:** la password predefinita per le apparecchiature Aironet è *Cisco* (con distinzione tra maiuscole e minuscole).**Nota:** per visualizzare l'output dei debug di una sessione Telnet, usare il comando **terminal monitor** o **term mon** per accendere il monitor del terminale.**Figura 4 - Sessione Telnet connessa**



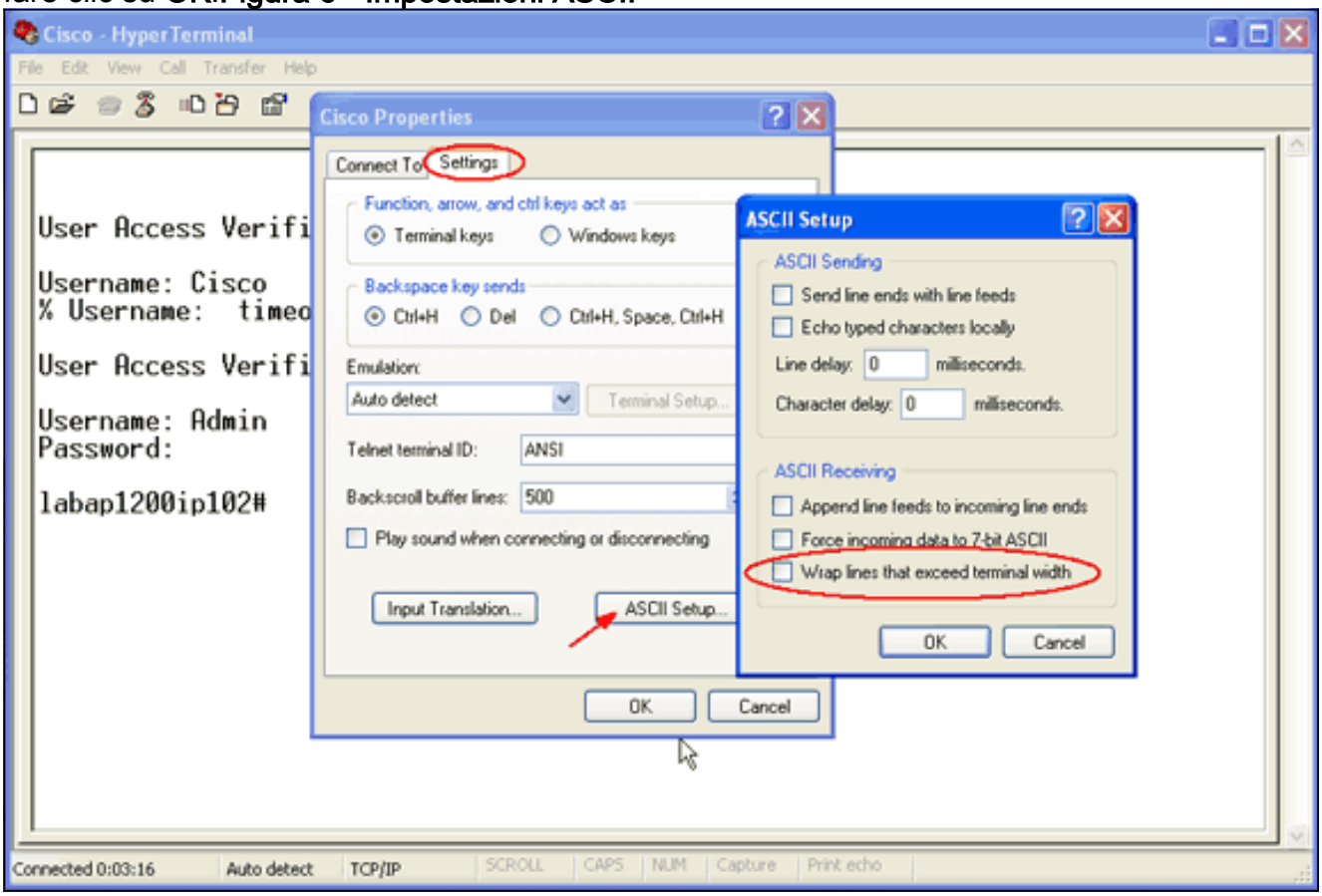
6. Dopo aver stabilito una connessione, completare i seguenti passaggi per raccogliere un'acquisizione schermo:Scegliere **Cattura testo** dal menu Trasferisci.**Figura 5 - Salvataggio di un'acquisizione schermo**



Quando viene visualizzata una finestra di dialogo in cui viene richiesto di specificare un nome file per l'output, immettere un nome file.

7. Per disabilitare il ritorno a capo automatico, completare la procedura seguente:**Nota:**

disabilitando il ritorno a capo automatico, è possibile leggere più facilmente i debug.Dal menu HyperTerminal scegliere **File**.Scegliere **Proprietà**.Nella finestra delle proprietà della connessione fare clic sulla scheda **Impostazioni**.Fare clic su **ASCII Setup**.Deselezionare **L'opzione Dispone le righe che superano la larghezza del terminale**.Per chiudere le impostazioni ASCII, fare clic su **OK**.Per chiudere la finestra delle proprietà della connessione, fare clic su **OK**.**Figura 6 - Impostazioni ASCII**



Ora che è possibile acquisire qualsiasi output dello schermo in un file di testo, i debug eseguiti dipendono da ciò che viene negoziato. Nelle sezioni seguenti di questo documento viene descritto il tipo di connessione negoziata fornita dai debug.

EAP

Questi debug sono i più utili per le autenticazioni EAP:

- **debug radius authentication**: gli output di questo comando di debug iniziano con questa parola: `RAGGIO`.
- **debug dot11 aaa authenticator process**: gli output di questo comando di debug iniziano con questo testo: `dot11_auth_dot1x_`.
- **debug dot11 aaa authentication state-machine**: gli output di questo comando di debug iniziano con questo testo: `dot11_auth_dot1x_run_rfsm`.

I seguenti debug mostrano:

- Elementi restituiti durante le parti RADIUS di una finestra di dialogo di autenticazione
- Azioni eseguite durante la finestra di dialogo di autenticazione
- I vari stati attraverso i quali la finestra di dialogo di autenticazione passa

Nell'esempio viene mostrata una riuscita autenticazione Light EAP (LEAP):

Esempio di autenticazione EAP riuscita

```
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]
```

Notate il flusso nei debug **della macchina a stati**. Vi è una progressione attraverso diversi stati:

1. AVVIO_EAP
2. ATTESA_CLIENT
3. RISPOSTA_CLIENT
4. ATTESA_SERVER
5. RISPOSTA_SERVER**Nota:** durante la negoziazione, possono esistere diverse iterazioni di CLIENT_WAIT e CLIENT_REPLY, nonché SERVER_WAIT e SERVER_REPLY.
6. PASSAGGIO_SERVER

Il debug del **processo** mostra ogni singolo passaggio attraverso ciascuno stato. I debug **radius** mostrano l'effettiva conversazione tra il server di autenticazione e il client. Il modo più semplice per utilizzare i debug EAP consiste nel controllare l'avanzamento dei messaggi della macchina a stati in ogni stato.

Quando si verifica un errore nella negoziazione, i debug **della macchina a stati** mostrano il motivo per cui il processo è stato interrotto. Guarda messaggi simili a questi esempi:

- **TIMEOUT CLIENT**: questo stato indica che il client non ha risposto entro un periodo di tempo appropriato. La mancata risposta può essere dovuta a uno dei motivi seguenti:Si è verificato un problema con il software client.Il valore di timeout del client EAP (dalla scheda secondaria

Autenticazione EAP in Protezione avanzata) è scaduto.Alcuni EAP, in particolare PEAP (Protected EAP), impiegano più di 30 secondi per completare l'autenticazione. Impostare il timer su un valore superiore (tra 90 e 120 secondi).Questo è un esempio di un tentativo di `TIMEOUT del CLIENT`:**Nota:** controllare se vengono visualizzati messaggi di errore di sistema simili al seguente:

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

Nota: tali messaggi di errore possono indicare un problema di radiofrequenza (RF).

- **Mancata corrispondenza del segreto condiviso tra il punto di accesso e il server RADIUS**: in questo log di esempio, il server RADIUS non accetta la richiesta di autenticazione del punto di accesso. L'access point continua a inviare la richiesta al server RADIUS, ma il server RADIUS la rifiuta perché il segreto condiviso non corrisponde.Per risolvere il problema, verificare che il segreto condiviso nell'access point sia lo stesso utilizzato nel server RADIUS.
- **`server_timeout`**: questo stato indica che il server di autenticazione non ha risposto entro il tempo appropriato. Questo errore di risposta si verifica a causa di un problema sul server. Verificare che si verifichino le seguenti situazioni:Il punto di accesso dispone di connettività IP al server di autenticazione.**Nota:** è possibile usare il comando **ping** per verificare la connettività.I numeri delle porte di autenticazione e accounting sono corretti per il server.**Nota:** è possibile controllare i numeri di porta dalla scheda Server Manager.Il servizio di autenticazione è in esecuzione e funzionante.Questo è un esempio di un tentativo di `server_timeout`:
- **`SERVER_FAIL`**: questo stato indica che il server ha inviato una risposta di autenticazione non riuscita in base alle credenziali dell'utente. Il debug RADIUS che precede questo errore mostra il nome utente presentato al server di autenticazione. Accertarsi di controllare il log dei tentativi non riusciti nel server di autenticazione per ulteriori dettagli sul motivo per cui il server ha negato l'accesso client.Questo è un esempio di tentativo di eseguire un'operazione `SERVER_FAIL`:
- **Nessuna risposta dal client**: in questo esempio, il server radius invia un messaggio di passaggio all'access point che l'access point inoltra e quindi associa il client. Alla fine il client non risponde all'access point. Pertanto, l'access point la disautentica dopo aver raggiunto il numero massimo di tentativi.L'access point inoltra al client una risposta di richiesta di verifica dal raggio. Il client non risponde e raggiunge il numero massimo di tentativi, il che provoca un errore di EAP e la deautenticazione del client da parte dell'AP.Radius invia un messaggio di passaggio all'access point, l'access point inoltra il messaggio di passaggio al client e il client non risponde. L'access point disautentica l'access point dopo aver raggiunto il numero massimo di tentativi. Il client tenta quindi di inviare una nuova richiesta di identità all'access point, ma l'access point la rifiuta perché il client ha già raggiunto il numero massimo di tentativi.

I debug del **`processo`** e/o **`del raggio`** immediatamente *precedenti* il messaggio della macchina a stati mostrano i dettagli dell'errore.

Per ulteriori informazioni su come configurare EAP, vedere Autenticazione EAP con server RADIUS.

Autenticazione MAC

Questi debug sono i più utili per l'autenticazione MAC:

- **debug radius authentication**: quando si usa un server di autenticazione esterno, gli output di questo comando di debug iniziano con questa parola: `RAGGIO`.
- **debug dot11 aaa authenticator mac-auto**: gli output di questo comando di debug iniziano con questo testo: `dot11_auth_dot1x_`.

I seguenti debug mostrano:

- Elementi restituiti durante le parti RADIUS di una finestra di dialogo di autenticazione
- Confronto tra l'indirizzo MAC specificato e quello autenticato in base a

Quando si utilizza un server RADIUS esterno con l'autenticazione dell'indirizzo MAC, vengono applicati i debug RADIUS. Il risultato di questa connessione è la visualizzazione della conversazione effettiva tra il server di autenticazione e il client.

Quando un elenco di indirizzi MAC viene compilato localmente sul dispositivo come database di nomi utente e password, solo i debug **`mac-auto`** mostrano gli output. Una volta determinata la corrispondenza o la mancata corrispondenza dell'indirizzo, vengono visualizzati questi output.

Nota: immettere sempre i caratteri alfabetici in un indirizzo MAC in minuscolo.

In questo esempio viene mostrata una corretta autenticazione MAC rispetto a un database locale:

Esempio di autenticazione MAC riuscita

```
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]
```

In questo esempio viene mostrata un'autenticazione MAC non riuscita su un database locale:

Esempio di autenticazione MAC non riuscita

```
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
```

Quando l'autenticazione di un indirizzo MAC ha esito negativo, verificare la correttezza dei caratteri immessi nell'indirizzo MAC. Assicurati di aver immesso qualsiasi carattere alfabetico in un indirizzo MAC in minuscolo.

Per ulteriori informazioni su come configurare l'autenticazione MAC, consultare il documento sulla

configurazione dei tipi di autenticazione (Guida alla configurazione del software Cisco IOS per i Cisco Aironet Access Point, 12.2(13)JA).

WPA

Sebbene Wi-Fi Protected Access (WPA) non sia un tipo di autenticazione, è un protocollo negoziato.

- WPA negozia tra l'access point e la scheda client.
- Gestione chiavi WPA esegue la negoziazione dopo che un client è stato autenticato da un server di autenticazione.
- WPA negozia sia una chiave temporanea Pairwise (PTK) che una chiave temporanea Groupwise (GTK) in un handshake a quattro vie.

Nota: poiché WPA richiede la riuscita dell'EAP sottostante, verificare che i client possano eseguire l'autenticazione con tale EAP prima di avviare WPA.

Questi debug sono i più utili per le negoziazioni WPA:

- **debug dot11 aaa authenticator process**: gli output di questo comando di debug iniziano con questo testo: `dot11_auth_dot1x_`.
- **debug dot11 aaa authentication state-machine**: gli output di questo comando di debug iniziano con questo testo: `dot11_auth_dot1x_run_rfsm`.

Rispetto alle altre autenticazioni in questo documento, i debug WPA sono semplici da leggere e analizzare. È necessario inviare un messaggio PTK e ricevere una risposta appropriata. Successivamente, è necessario inviare un messaggio GTK e ricevere un'altra risposta appropriata.

Se i messaggi PTK o GTK non vengono inviati, il livello di configurazione o software sull'access point può essere guasto. Se le risposte PTK o GTK dal client non vengono ricevute, controllare la configurazione o il livello software sul supplicant WPA della scheda client.

Esempio di negoziazione WPA riuscita

```
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#
```

Per ulteriori informazioni su come configurare WPA, vedere Cenni preliminari sulla configurazione WPA.

Autenticazione HTTP/amministrativa

Èpossibile limitare l'accesso amministrativo al dispositivo agli utenti elencati in un database di nome utente e password locale o in un server di autenticazione esterno. L'accesso amministrativo è supportato sia da RADIUS che da TACACS+.

Questi debug sono i più utili per l'autenticazione amministrativa:

- **debug radius authentication** o **debug tacacs authentication**: gli output di questo debug iniziano con una delle seguenti parole: `RADIUS` o `TACACS`.
- **debug aaa authentication**: gli output di questo debug iniziano con questo testo: `AAA/AUTORE`.
- **debug aaa authorization**: gli output di questo debug iniziano con questo testo: `AAA/AUTORE`.

I seguenti debug mostrano:

- Elementi riportati durante le parti RADIUS o TACACS di una finestra di dialogo di autenticazione
- Le negoziazioni effettive per l'autenticazione e l'autorizzazione tra il dispositivo e il server di autenticazione

Nell'esempio viene mostrata una corretta autenticazione amministrativa quando l'attributo `Service-Type RADIUS` è impostato su `Administrative`:

Esempio di autenticazione amministrativa con attributo Service-Type riuscita

```
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
```

Nell'esempio viene mostrata la riuscita dell'autenticazione amministrativa quando si usano attributi specifici del fornitore per inviare un'istruzione "priv-level":

Esempio di autenticazione amministrativa con attributo specifico del fornitore

```
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
```

Il problema più comune dell'autenticazione amministrativa è la mancata configurazione del server di autenticazione per l'invio degli attributi appropriati del livello di privilegio o del tipo di servizio amministrativo. In questo esempio l'autenticazione amministrativa non è riuscita perché non è stato inviato alcun attributo a livello di privilegio o di servizio amministrativo:

Senza attributi specifici del fornitore o del tipo di servizio

```
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=
```

Per ulteriori informazioni su come configurare l'autenticazione amministrativa, fare riferimento alla guida alla configurazione del software Cisco IOS per i Cisco Aironet Access Point, 12.2(13)JA.

Per ulteriori informazioni su come configurare i privilegi di amministrazione per gli utenti sul server di autenticazione, vedere Configurazione di esempio: Autenticazione locale per gli utenti del server HTTP. Selezionare la sezione corrispondente al protocollo di autenticazione utilizzato.

Informazioni correlate

- Guida alla configurazione del software Cisco IOS per Cisco Aironet Access Point, 12.2(13)JA
- Autenticazione EAP con server RADIUS
- Autenticazione LEAP con server RADIUS locale
- Domande frequenti su Cisco Aironet Wireless Security
- Esempio di configurazione di Wireless Domain Services AP come server AAA
- Documentazione e supporto tecnico – Cisco Systems