Debugauthentifizierungen

Inhalt

Einführung

Bei der Wireless-Kommunikation wird Authentifizierung in vielerlei Hinsicht verwendet. Der gebräuchlichste Authentifizierungstyp ist Extensible Authentication Protocol (EAP) in verschiedenen Typen und Formen. Andere Authentifizierungstypen sind MAC-Adressauthentifizierung und administrative Authentifizierung. In diesem Dokument wird beschrieben, wie die Ausgabe von Debugauthentifizierungen gedebuggt und interpretiert wird. Die Informationen aus diesen Debuggen sind bei der Fehlerbehebung bei Wireless-Installationen von unschätzbarem Wert.

Hinweis: Die Teile dieses Dokuments, die sich auf Produkte beziehen, die nicht von Cisco stammen, basieren auf der Erfahrung des Autors und nicht auf offiziellen Schulungen. Sie sind zu Ihrem Komfort und nicht als technische Unterstützung gedacht. Wenn Sie technischen Support für Produkte von Drittanbietern benötigen, wenden Sie sich an den technischen Support für dieses Produkt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Authentifizierung in Bezug auf Wireless-Netzwerke
- Cisco IOS® Software Command-Line Interface (CLI)
- RADIUS-Serverkonfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Softwarebasierte Cisco IOS Wireless-Produkte aller Modelle und Versionen
- Hilgraeve HyperTerminal

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

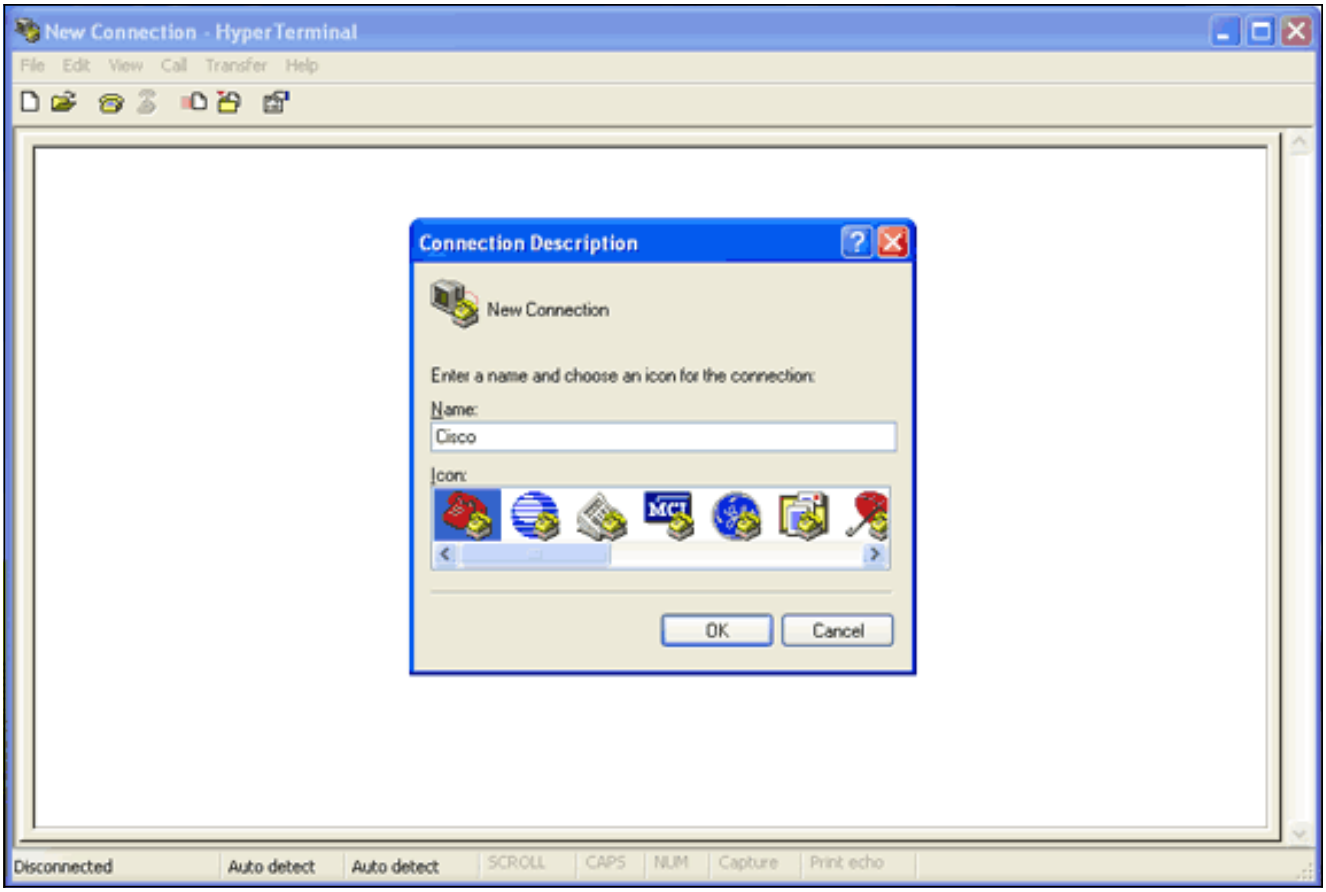
Erfassen von Debuggern

Wenn Sie Debuginformationen nicht erfassen und analysieren können, sind diese Informationen nutzlos. Die einfachste Methode zur Erfassung dieser Daten ist eine Screenshot-Funktion, die in die Telnet- oder Kommunikationsanwendung integriert ist.

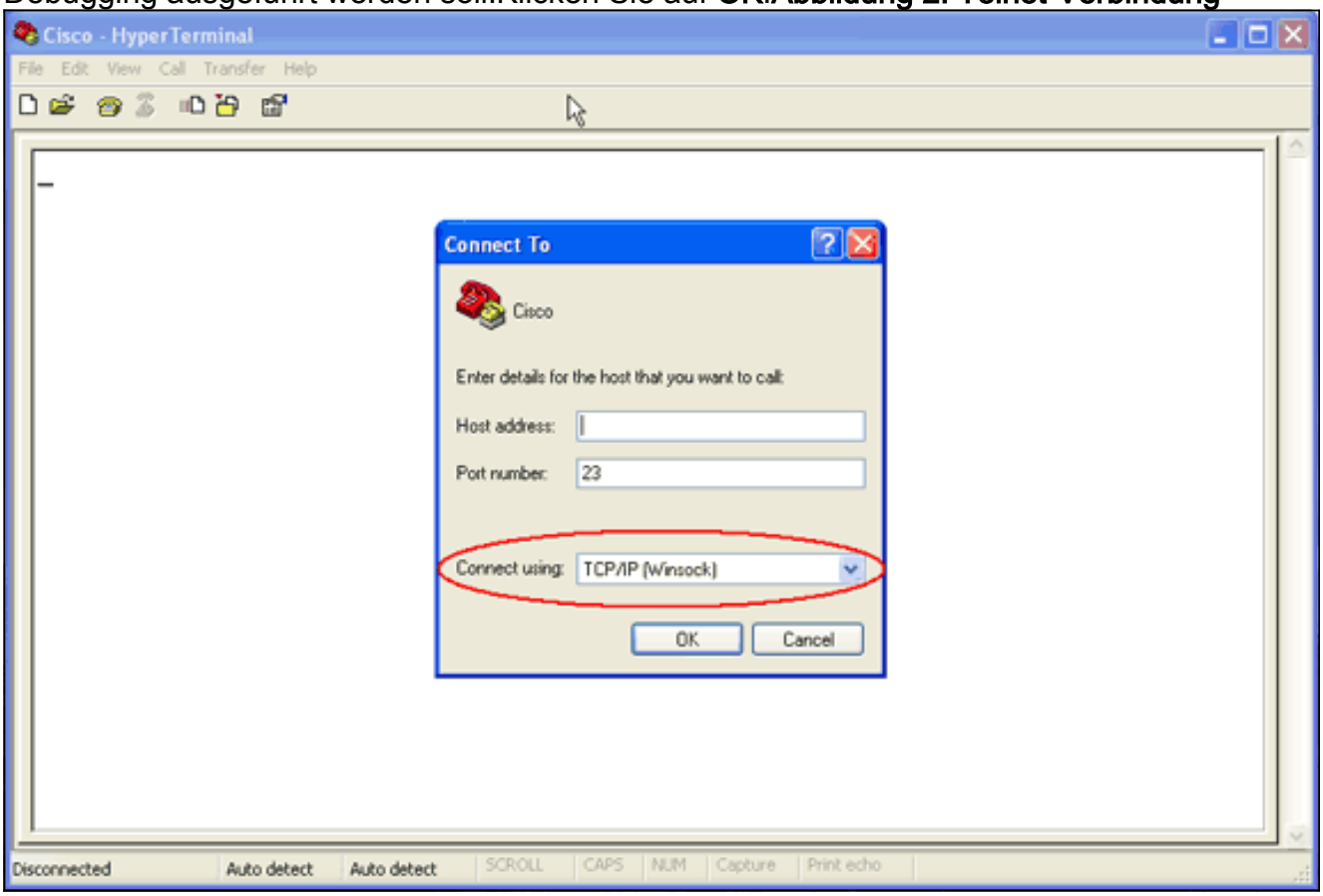
In diesem Beispiel wird beschrieben, wie Sie die Ausgabe mit der Hilgraeve HyperTerminal - Anwendung erfassen. Die meisten Microsoft Windows-Betriebssysteme beinhalten HyperTerminal, aber Sie können die Konzepte auf jede Terminal-Emulationsanwendung anwenden. Weitere vollständige Informationen zur Anwendung finden Sie in Hilgraeve .

Gehen Sie wie folgt vor, um HyperTerminal für die Kommunikation mit Ihrem Access Point (AP) oder Ihrer Bridge zu konfigurieren:

1. Um HyperTerminal zu öffnen, wählen Sie **Start > Programme > Systemprogramme > Kommunikation > HyperTerminal**.**Abbildung 1: Starten von HyperTerminal**

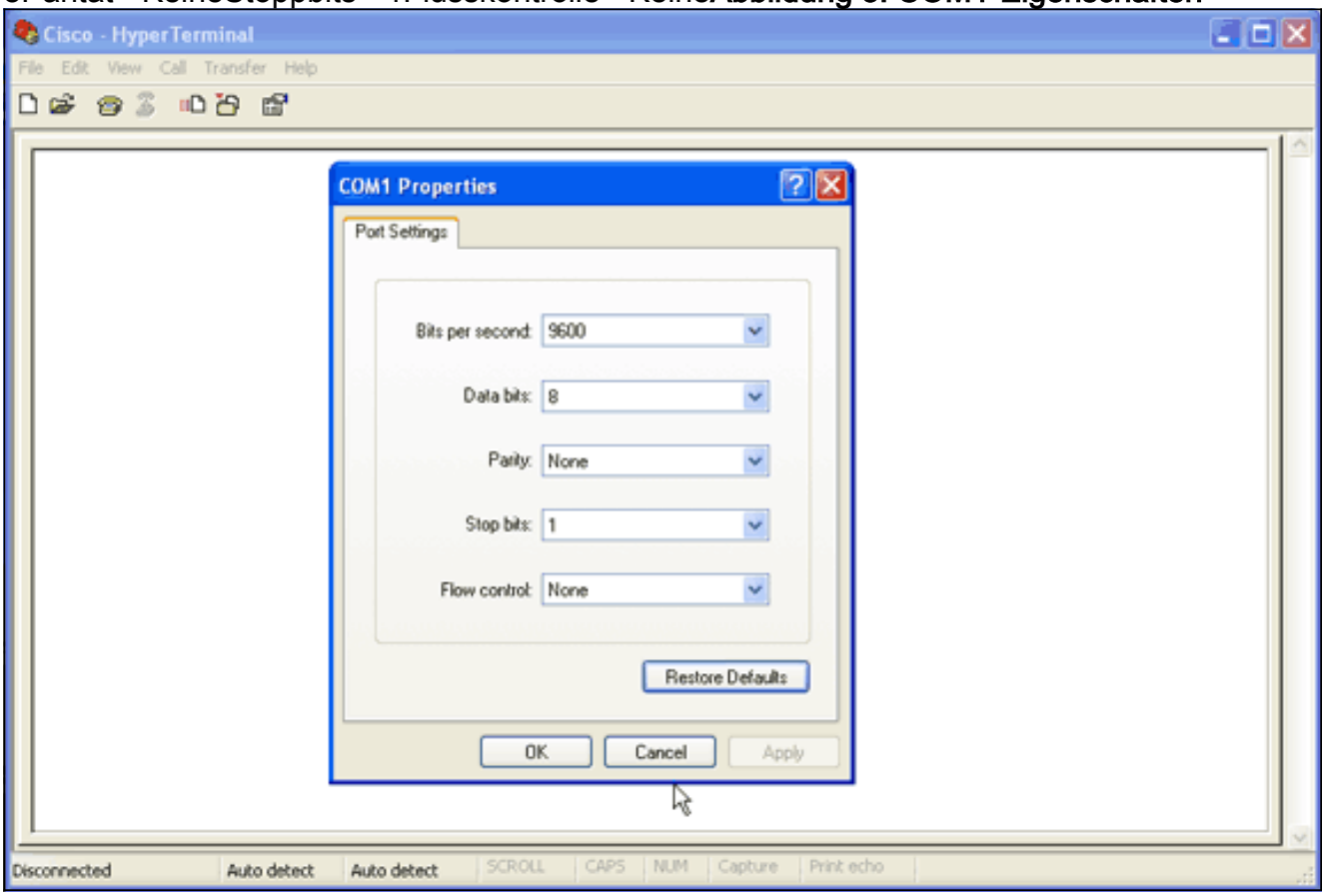


2. Gehen Sie wie folgt vor, wenn HyperTerminal geöffnet wird:Geben Sie einen Namen für die Verbindung ein.Wählen Sie ein Symbol aus.Klicken Sie auf **OK**.
3. Führen Sie für Telnet-Verbindungen die folgenden Schritte aus:Wählen Sie im Dropdown-Menü Verbindung über **TCP/IP** aus.Geben Sie die IP-Adresse des Geräts ein, auf dem die Debugging ausgeführt werden soll.Klicken Sie auf **OK**.**Abbildung 2: Telnet-Verbindung**



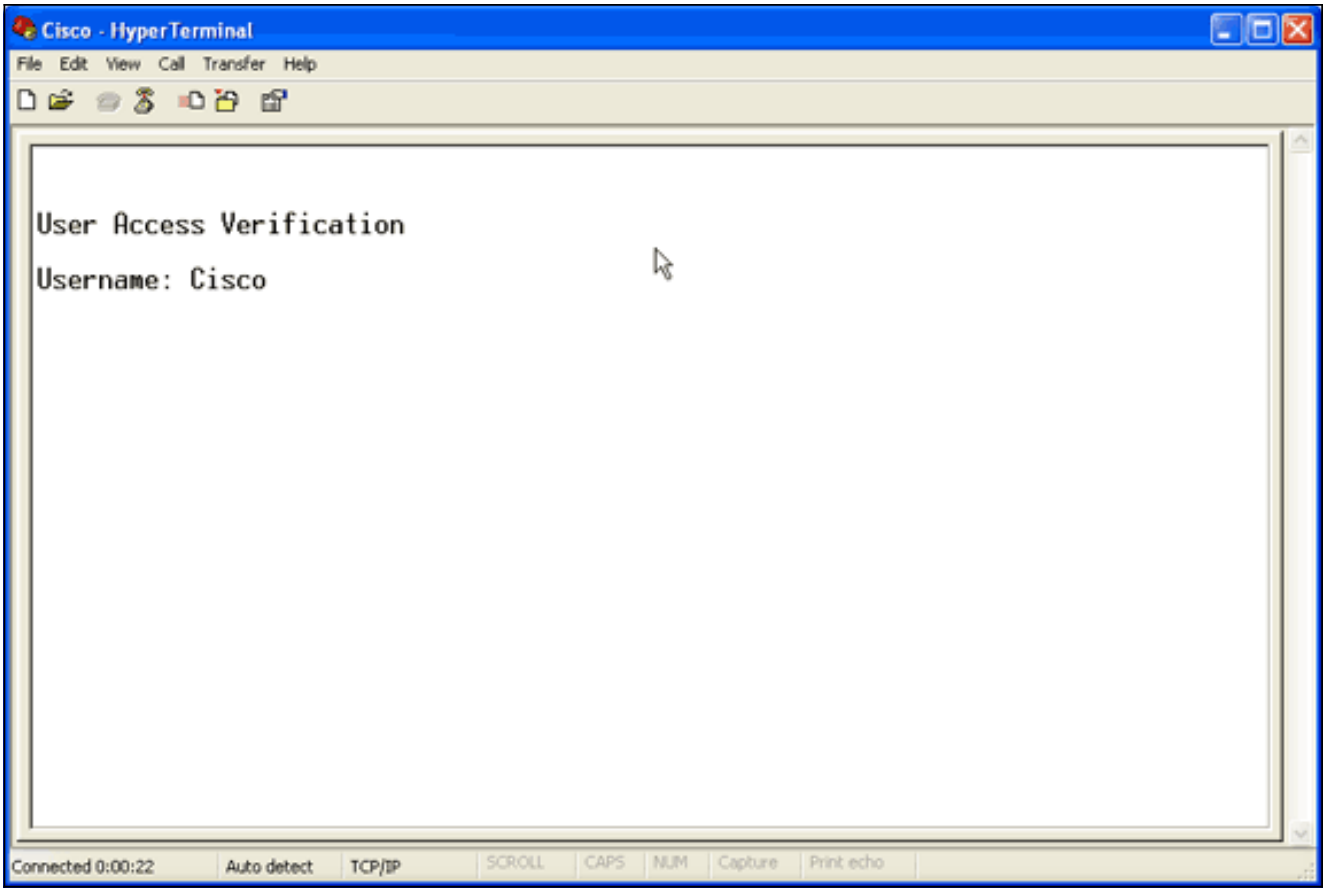
4. Führen Sie für Konsolenverbindungen die folgenden Schritte aus:Wählen Sie im Dropdown-

Menü Connect Using (Über verbinden) den COM-Port aus, an den das Konsolenkabel angeschlossen ist.Klicken Sie auf **OK**.Das Eigenschaftenblatt für die Verbindung wird angezeigt.Stellen Sie die Geschwindigkeit für die Verbindung zum Konsolenport ein.Um die Standardeinstellungen des Ports wiederherzustellen, klicken Sie auf **Standardeinstellungen wiederherstellen**.**Hinweis:** Die meisten Cisco Produkte befolgen die Standard-Porteinstellungen.Die Standard-Porteinstellungen sind:Bit pro Sekunde - 9600Datenbits: 8Parität - KeineStoppbits - 1Flusskontrolle - Keine**Abbildung 3: COM1-Eigenschaften**

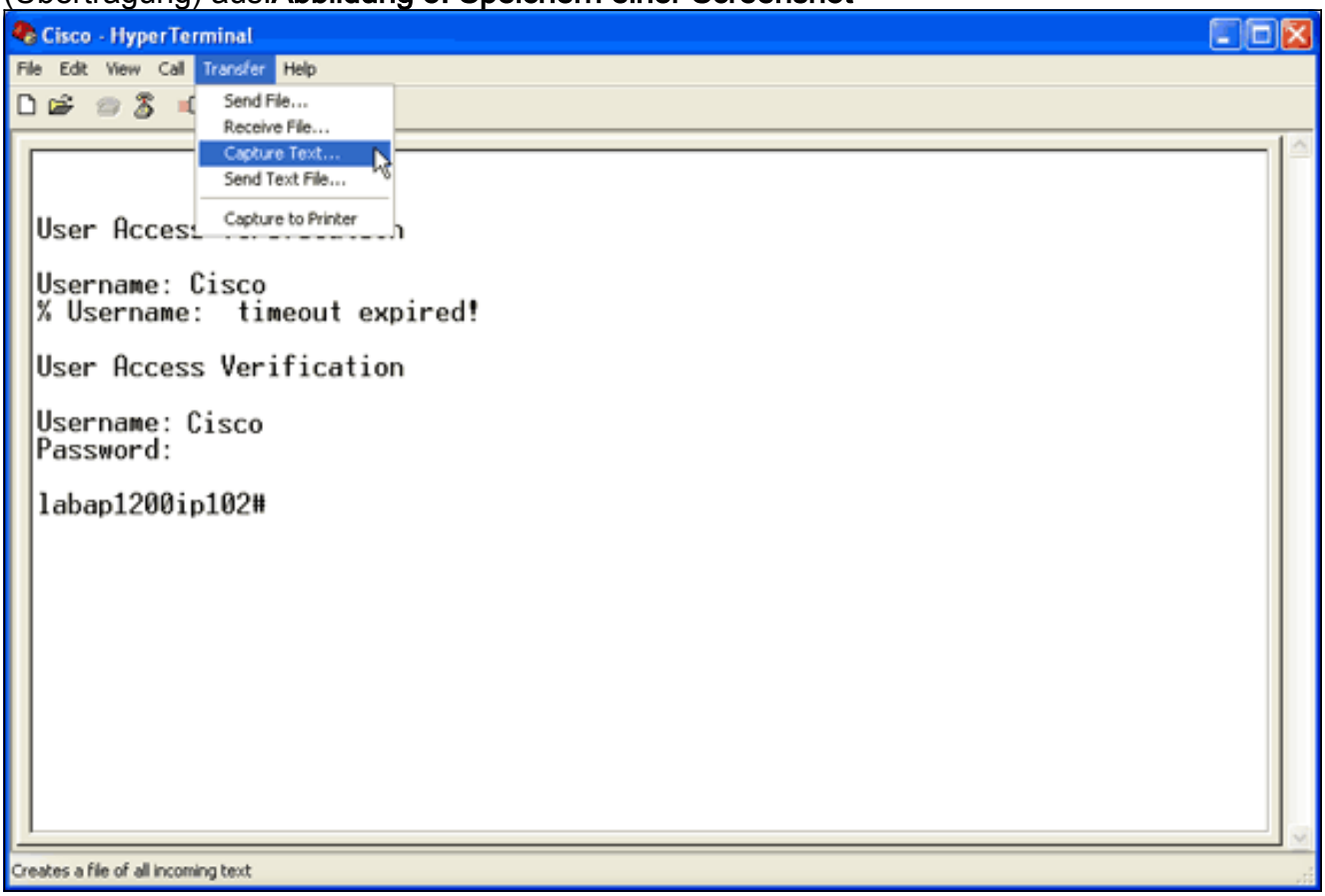


An diesem Punkt wird die Telnet- oder Konsolenverbindung hergestellt, und Sie werden aufgefordert, einen Benutzernamen und ein Kennwort einzugeben.**Hinweis:** Cisco Aironet-Geräte weisen sowohl einen Standardbenutzernamen als auch ein Standardkennwort von *Cisco zu* (Groß- und Kleinschreibung beachten).

5. Gehen Sie wie folgt vor, um das Debuggen auszuführen:Geben Sie den Befehl **enable** ein, um in den privilegierten Modus zu wechseln.Geben Sie das enable-Kennwort ein.**Hinweis:** Beachten Sie, dass das Standardkennwort für Aironet-Geräte *Cisco* ist (Groß- und Kleinschreibung beachten).**Hinweis:** Um die Ausgabe von Debuggen aus einer Telnet-Sitzung anzuzeigen, verwenden Sie den **Terminalmonitor** oder den Befehl **term mon**, um den Terminalmonitor einzuschalten.**Abbildung 4: Angeschlossene Telnet-Sitzung**



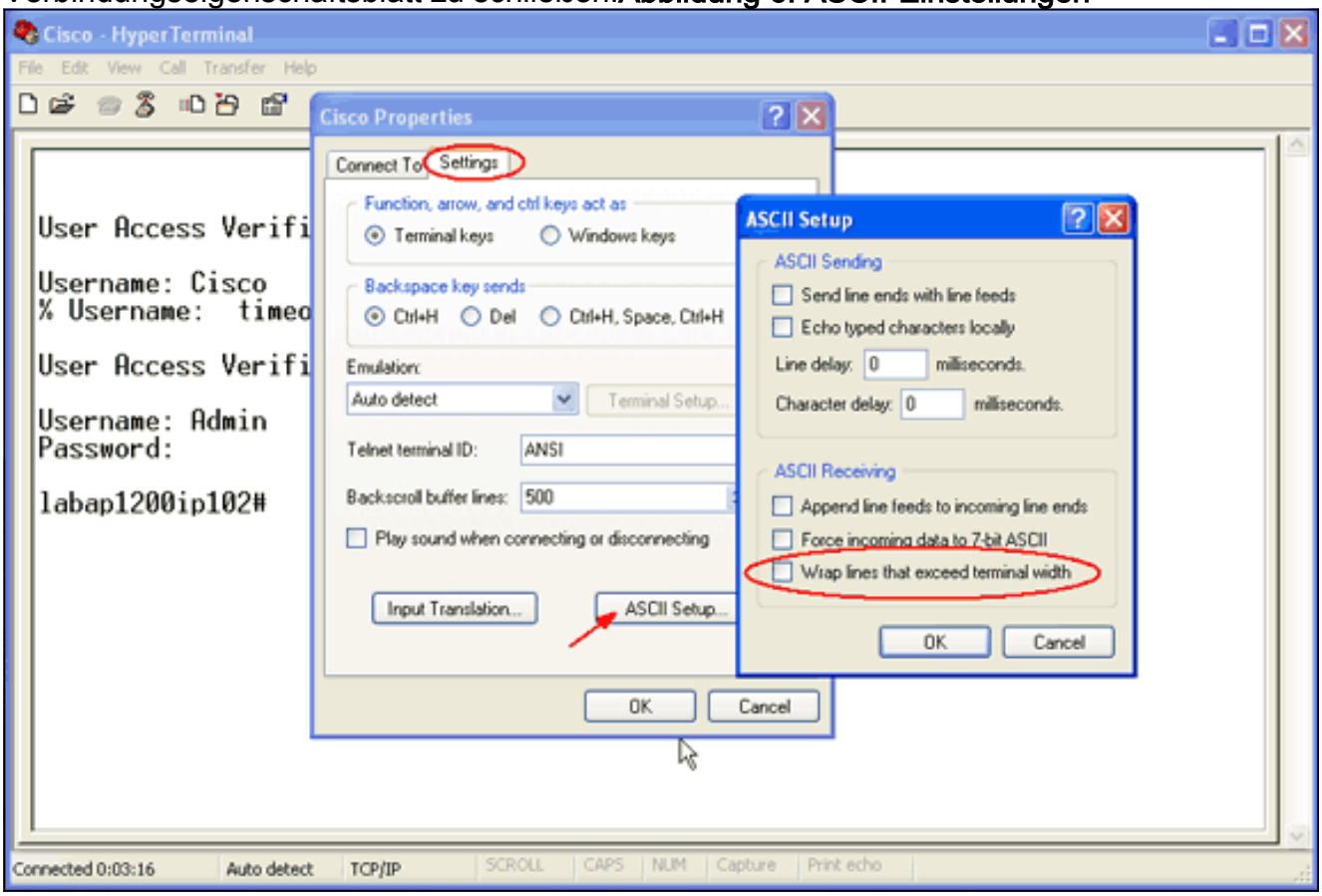
6. Führen Sie nach dem Herstellen einer Verbindung die folgenden Schritte aus, um eine Screenshot-Erfassung zu erfassen:Wählen Sie **Text erfassen** im Menü Transfer (Übertragung) aus.**Abbildung 5: Speichern einer Screenshot**



Wenn ein Dialogfeld geöffnet wird, in dem Sie zur Eingabe eines Dateinamens für die Ausgabe aufgefordert werden, geben Sie einen Dateinamen ein.

7. Gehen Sie wie folgt vor, um den Bildschirmwrap zu deaktivieren:**Hinweis:** Wenn Sie den

Bildschirmwrap deaktivieren, können Sie die Debugger einfacher lesen.Wählen Sie im Menü HyperTerminal die Option **File (Datei)**.Wählen Sie **Eigenschaften aus**.Klicken Sie im Verbindungseigenschaftsblatt auf die Registerkarte **Einstellungen**.Klicken Sie auf **ASCII-Einrichtung**.Deaktivieren Sie **Wrap-Zeilen, die die Klemmenbreite überschreiten**.Klicken Sie auf **OK**, um die ASCII-Einstellungen zu schließen.Klicken Sie auf **OK**, um das Verbindungseigenschaftsblatt zu schließen.**Abbildung 6: ASCII-Einstellungen**



Da Sie jetzt eine Bildschirmausgabe in eine Textdatei erfassen können, hängt das ausgeführte Debuggen von dem ab, was ausgehandelt wird. In den nächsten Abschnitten dieses Dokuments wird die Art der ausgehandelten Verbindung beschrieben, die von den Debuggern bereitgestellt wird.

EAP

Diese DebuggingInnen sind für EAP-Authentifizierungen am hilfreichsten:

- **Debug-Radius-Authentifizierung** - Die Ausgaben dieses Debuggens beginnen mit dem folgenden Wort: `RADIUS`.
- **debug dot11 aaa authentifizierer prozess** - Die Ausgaben dieses debug beginnen mit diesem text: `dot11_auth_dot1x_`.
- **debug dot11 aaa authentifizierer state-machine** - Die Ausgaben dieses Debug beginnen mit diesem Text: `dot11_auth_dot1x_run_rfsm`.

Diese Debuggen zeigen Folgendes an:

- Was wird in den RADIUS-Bereichen eines Authentifizierungsdialogs gemeldet?
- Die Aktionen, die während dieses Authentifizierungsdialogs durchgeführt werden
- Die verschiedenen Zustände, durch die der Authentifizierungsdialog wechselt

Dieses Beispiel zeigt eine erfolgreiche LEAP-Authentifizierung (Light EAP):

Beispiel für erfolgreiche EAP-Authentifizierung

```
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]
```

Beachten Sie den Fluss im **Debuggen für Zustandscomputer**. Es gibt mehrere Zustände:

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_ANTWORT**Hinweis:** Während der beiden Verhandlungen können mehrere Iterationen von CLIENT_WAIT und CLIENT_REPLY sowie SERVER_WAIT und SERVER_REPLY vorhanden sein.
6. SERVER_PASS

Das **Prozess-Debuggen** zeigt jeden einzelnen Schritt durch die einzelnen Zustände. Die **Radius-Debuggen** zeigen die tatsächliche Konversation zwischen dem Authentifizierungsserver und dem Client. Die einfachste Möglichkeit, mit EAP-Debuggen zu arbeiten, besteht darin, die Progression von Statuscomputernachrichten durch jeden Zustand zu überwachen.

Wenn in der Verhandlung etwas fehlschlägt, werden die **Debugging-Elemente des Zustands-Computers** angezeigt, warum der Prozess beendet wurde. Achten Sie auf ähnliche Meldungen wie die folgenden Beispiele:

- **CLIENT TIMEOUT (CLIENT-ZEITÜBERSCHREITUNG)**: Dieser Status gibt an, dass der Client nicht innerhalb einer angemessenen Frist geantwortet hat. Diese Nichtreaktion kann aus

einem der folgenden Gründe auftreten:Es besteht ein Problem mit der Client-Software.Der Zeitüberschreitungswert für den EAP-Client (über die Unterregisterkarte "EAP Authentication" unter "Advanced Security") ist abgelaufen.Einige EAPs, insbesondere PEAPs (Protected EAP), benötigen mehr als 30 Sekunden, um die Authentifizierung abzuschließen. Legen Sie für diesen Timer einen höheren Wert fest (zwischen 90 und 120 Sekunden).Dies ist ein Beispiel für einen `CLIENT TIMEOUT`-Versuch:**Hinweis:** Achten Sie auf Systemfehlermeldungen, die dieser Meldung ähneln:

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

Hinweis: Solche Fehlermeldungen können auf ein Funkfrequenzproblem hinweisen.

- **Gemeinsames geheimes Missverhältnis zwischen dem Access Point und dem RADIUS-Server** - In diesem Beispielprotokoll akzeptiert der RADIUS-Server die Authentifizierungsanfrage des Access Points nicht. Der Access Point sendet die Anforderung weiterhin an den RADIUS-Server, der RADIUS-Server lehnt die Anforderung jedoch ab, da der gemeinsame geheime Schlüssel nicht zugeordnet ist.Um dieses Problem zu beheben, stellen Sie sicher, dass der auf dem Access Point gemeinsam verwendete geheime Schlüssel derselbe ist, der auf dem RADIUS-Server verwendet wird.
- **`server_timeout`**: Dieser Status gibt an, dass der Authentifizierungsserver nicht in angemessener Zeit reagiert hat. Dieser Fehler tritt aufgrund eines Serverproblems auf. Überprüfen Sie, ob diese Situationen zutreffen:Der AP verfügt über IP-Verbindungen zum Authentifizierungsserver.**Hinweis:** Sie können den **Ping-**Befehl verwenden, um die Verbindung zu überprüfen.Die Authentifizierungs- und Accounting-Portnummern sind für den Server korrekt.**Hinweis:** Sie können die Portnummern auf der Registerkarte Server Manager überprüfen.Der Authentifizierungsdienst wird ausgeführt und funktioniert.Dies ist ein Beispiel für einen `Server_timeout`-Versuch:
- **`SERVER_FAIL`**: Dieser Status gibt an, dass der Server eine nicht erfolgreiche Authentifizierungsantwort basierend auf den Benutzeranmeldeinformationen gegeben hat. Das RADIUS-Debugging, das diesem Fehler vorangeht, zeigt den Benutzernamen an, der dem Authentifizierungsserver angezeigt wurde. Überprüfen Sie unbedingt die Anmeldung fehlgeschlagener Versuche im Authentifizierungsserver, um weitere Informationen darüber zu erhalten, warum der Server den Client-Zugriff verweigerte.Dies ist ein Beispiel für einen `SERVER_FAIL`-Versuch:
- **No Response from Client** (**Keine Antwort vom Client**): In diesem Beispiel sendet der Radius-Server eine Übermittlungsmeldung an den AP, den der Access Point weiterleitet, und ordnet dann den Client zu. Schließlich reagiert der Client nicht auf den Access Point. Daher deauthentifiziert der Access Point nach Erreichen der maximalen Wiederholungsversuche.Der Access Point leitet eine Get-Challenge-Antwort vom Radius an den Client weiter. Der Client reagiert nicht und erreicht die maximale Anzahl von Wiederholungen, wodurch EAP ausfällt und der Access Point den Client deauthentifiziert.Radius sendet eine Passnachricht an den AP, der AP leitet die Passnachricht an den Client weiter, und der Client reagiert nicht. Der Access Point deauthentifiziert sie, nachdem er die maximalen erneuten Versuche erreicht hat. Der Client versucht dann eine neue Identitätsanforderung an den AP, aber der Access Point lehnt diese Anforderung ab, da der Client bereits die maximalen Wiederholungen erreicht hat.

Das **`Prozess-`** **und/oder** **`Radius-`**Debuggen, das unmittelbar *vor der Meldung des Statuscomputers erfolgt, zeigt Details zum Fehler an.*

Weitere Informationen zur Konfiguration von EAP finden Sie unter EAP-Authentifizierung mit RADIUS-Server.

MAC-Authentifizierung

Diese DebuggingInnen sind für die MAC-Authentifizierung am hilfreichsten:

- **Debug-Radius-Authentifizierung** - Wenn ein externer Authentifizierungsserver verwendet wird, beginnen die Ausgaben dieses Debuggens mit dem folgenden Wort: `RADIUS`.
- **debug dot11 aaa authentifizierer mac-authen** - Die Ausgaben dieses Debuggens beginnen mit diesem Text: `dot11_auth_dot1x_`.

Diese Debuggen zeigen Folgendes an:

- Was wird in den RADIUS-Bereichen eines Authentifizierungsdialogs gemeldet?
- Der Vergleich zwischen der angegebenen MAC-Adresse und der authentifizierten Adresse

Wenn ein externer RADIUS-Server mit MAC-Adressauthentifizierung verwendet wird, gelten die RADIUS-Debug. Das Ergebnis dieser Verbindung ist die Anzeige der tatsächlichen Kommunikation zwischen dem Authentifizierungsserver und dem Client.

Wenn eine Liste von MAC-Adressen lokal auf dem Gerät als Benutzername- und Kennwortdatenbank erstellt wird, werden nur die **Ausgaben für `MAC-Authen-`**Debug angezeigt. Wenn die Adresse übereinstimmt oder nicht übereinstimmt, werden diese Ausgaben angezeigt.

Hinweis: Geben Sie in einer MAC-Adresse immer Buchstaben in Kleinbuchstaben ein.

Dieses Beispiel zeigt eine erfolgreiche MAC-Authentifizierung mit einer lokalen Datenbank:

Beispiel für erfolgreiche MAC-Authentifizierung

```
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]
```

Dieses Beispiel zeigt eine fehlgeschlagene MAC-Authentifizierung für eine lokale Datenbank:

Beispiel für fehlgeschlagene MAC-Authentifizierung

```
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
```

Wenn eine MAC-Adressauthentifizierung fehlschlägt, überprüfen Sie, ob die Zeichen, die in der MAC-Adresse eingegeben werden, korrekt sind. Stellen Sie sicher, dass Sie in einer MAC-Adresse alphabetische Zeichen in Kleinbuchstaben eingegeben haben.

Weitere Informationen zum Konfigurieren der MAC-Authentifizierung finden Sie unter Konfigurieren von Authentifizierungstypen (Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.2(13)JA).

WPA

Obwohl Wi-Fi Protected Access (WPA) kein Authentifizierungstyp ist, handelt es sich um ein ausgehandeltes Protokoll.

- WPA handelt zwischen dem AP und der Client-Karte aus.
- Die Aushandlung der WPA-Schlüsselverwaltung erfolgt, nachdem ein Client erfolgreich von einem Authentifizierungsserver authentifiziert wurde.
- WPA handelt sowohl eine paarweise Übergangstaste (PTK) als auch eine Groupwise Transient Key (GTK) in einem Vier-Wege-Handshake aus.

Hinweis: Da für WPA der Erfolg des zugrunde liegenden EAP erforderlich ist, müssen Sie sicherstellen, dass die Clients sich erfolgreich mit diesem EAP authentifizieren können, bevor Sie WPA aktivieren.

Diese DebuggingInnen sind für WPA-Verhandlungen am hilfreichsten:

- **debug dot11 aaa authentifizierer prozess** - Die Ausgaben dieses debug beginnen mit diesem text: `dot11_auth_dot1x_`.
- **debug dot11 aaa authentifizierer state-machine** - Die Ausgaben dieses Debug beginnen mit diesem Text: `dot11_auth_dot1x_run_rfsm`.

Im Vergleich zu anderen Authentifizierungen in diesem Dokument sind WPA-Debugger einfach zu lesen und zu analysieren. Es sollte eine PTK-Nachricht gesendet und eine angemessene Antwort empfangen werden. Als Nächstes sollte eine GTK-Nachricht gesendet und eine andere entsprechende Antwort empfangen werden.

Wenn keine PTK- oder GTK-Meldungen gesendet werden, kann die Konfigurations- oder Softwareebene des Access Points fehlerhaft sein. Wenn die PTK- oder GTK-Antworten vom Client nicht empfangen werden, überprüfen Sie die Konfigurations- oder Softwareebene auf der WPA-Komponente der Client-Karte.

Beispiel für erfolgreiche WPA-Verhandlungen

```
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#
```

Weitere Informationen zum Konfigurieren von WPA finden Sie unter Übersicht über die WPA-Konfiguration.

Administrator-/HTTP-Authentifizierung

Sie können den Administratorzugriff auf das Gerät auf Benutzer beschränken, die entweder in einer lokalen Benutzer- und Kennwortdatenbank oder auf einem externen Authentifizierungsserver aufgeführt sind. Der administrative Zugriff wird sowohl mit RADIUS als auch mit TACACS+ unterstützt.

Diese Debugger sind für die administrative Authentifizierung am hilfreichsten:

- **Debug Radius-Authentifizierung** oder **Debug-**Authentifizierung - Die Ausgaben dieses Debuggens beginnen mit einem der folgenden Wörter: `RADIUS` oder `TACACS`.
- **debug aaa authentication** - Die Ausgaben dieses Debuggers beginnen mit dem folgenden Text: `AAA/AUTHEN`.
- **debug aaa authorization** - Die Ausgaben dieses Debuggers beginnen mit dem folgenden Text: `AAA/AUTOR`.

Diese Debuggen zeigen Folgendes an:

- Was wird während der RADIUS- oder TACACS-Teile eines Authentifizierungsdialogs gemeldet?
- Die eigentlichen Verhandlungen für Authentifizierung und Autorisierung zwischen dem Gerät und dem Authentifizierungsserver

Dieses Beispiel zeigt eine erfolgreiche administrative Authentifizierung, wenn das `Service-Type` `RADIUS`-Attribut auf `Administrative` festgelegt ist:

Beispiel für eine erfolgreiche administrative Authentifizierung mit Diensttypattribut

```
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
```

Dieses Beispiel zeigt eine erfolgreiche administrative Authentifizierung, wenn Sie anbieterspezifische Attribute verwenden, um eine Anweisung der "Priv-Level" zu senden:

Beispiel für erfolgreiche administrative Authentifizierung mit anbieterspezifischem Attribut

```
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
```

Das häufigste Problem bei der administrativen Authentifizierung ist das Versagen, den Authentifizierungsserver so zu konfigurieren, dass er die entsprechenden Attribute auf Privilegien- oder Verwaltungsebene sendet. In diesem Beispiel wurde die administrative Authentifizierung fehlgeschlagen, da keine Attribute auf Privilegienebene oder administrativen Diensttypattribute gesendet wurden:

Ohne anbieterspezifische oder servicetypspezifische Attribute

```
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=
```

Weitere Informationen zum Konfigurieren der administrativen Authentifizierung finden Sie unter Verwaltung des Access Points (Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.2(13)JA).

Weitere Informationen zum Konfigurieren von Administratorberechtigungen für Benutzer auf dem Authentifizierungsserver finden Sie unter Beispielkonfiguration: Lokale Authentifizierung für HTTP-Serverbenutzer. Überprüfen Sie den Abschnitt, der dem verwendeten Authentifizierungsprotokoll entspricht.

Zugehörige Informationen

- Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.2(13)JA
- EAP-Authentifizierung mit RADIUS-Server
- LEAP-Authentifizierung mit lokalem RADIUS-Server
- Häufig gestellte Fragen zu Cisco Aironet Wireless Security
- Beispiel für eine Konfiguration eines AAA-Servers: Access Point für Wireless-Domänendienste
- Technischer Support und Dokumentation für Cisco Systeme