Autenticaciones de depuración

Contenido

Introducción

La comunicación inalámbrica utiliza la autenticación de muchos modos. El tipo de autenticación más común es EAP (Extensible Authentication Protocol) en diversos tipos y formas. Otros tipos de autenticación incluyen la autenticación de dirección MAC y la autenticación administrativa. Este documento describe cómo interpretar y hacer el debug de la salida de las autenticaciones de debug. La información de estos debugs es inestimable para resolver problemas de las instalaciones de red inalámbrica.

Nota: Las partes de este documento que hacen referencia a productos que no son de Cisco se basan en la experiencia del autor, no en la formación formal. Están pensados para su comodidad y no como soporte técnico. Para obtener asistencia técnica autorizada para productos que no sean de Cisco, póngase en contacto con la asistencia técnica de ese producto.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación relacionada con las redes inalámbricas
- Interfaz de línea de comandos (CLI) del software Cisco IOS®
- Configuración del servidor de RADIUS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Productos inalámbricos basados en software Cisco IOS de cualquier modelo y versión
- Hilgraeve HyperTerminal

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Capturar depuraciones

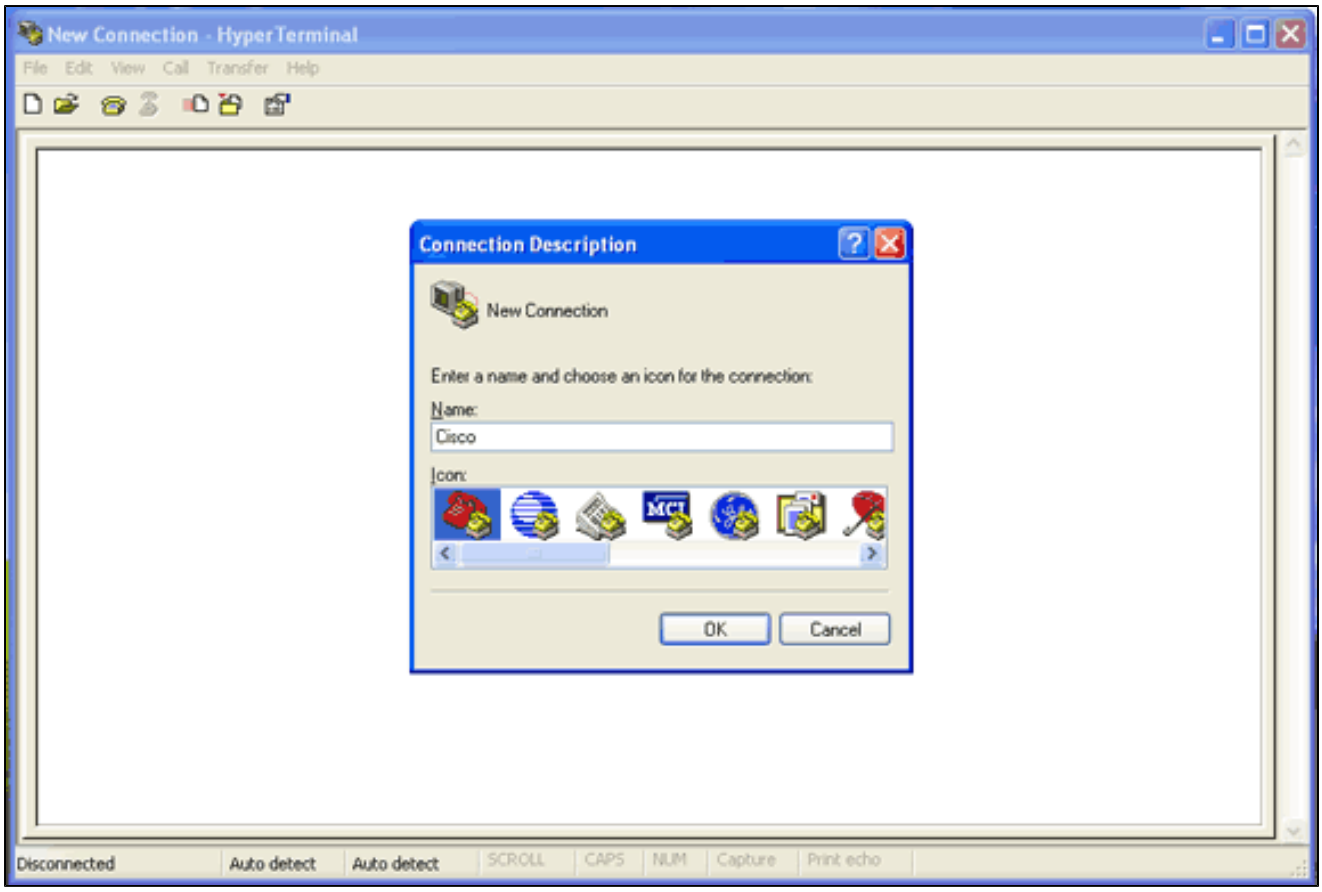
Si no puede capturar y analizar la información de depuración, la información es inútil. La forma más sencilla de capturar estos datos es con una función de captura de pantalla integrada en la aplicación Telnet o de comunicaciones.

Este ejemplo describe cómo capturar la salida con la aplicación Hilgraeve HyperTerminal. La mayoría de los sistemas operativos Microsoft Windows incluyen HyperTerminal, pero puede aplicar los conceptos a cualquier aplicación de emulación de terminal. Para obtener información más completa sobre la solicitud, consulte Hilgraeve.

Complete estos pasos para configurar HyperTerminal para comunicarse con su punto de acceso (AP) o puente:

1. Para abrir HyperTerminal, elija Inicio > Programas > Herramientas del sistema > Comunicaciones > HyperTerminal.

   Figura 1: Inicio de HyperTerminal



2. Cuando se abra HyperTerminal, complete estos pasos:

    a. Introduzca un nombre para la conexión.

    b. Seleccione un icono.

    c. Click OK.

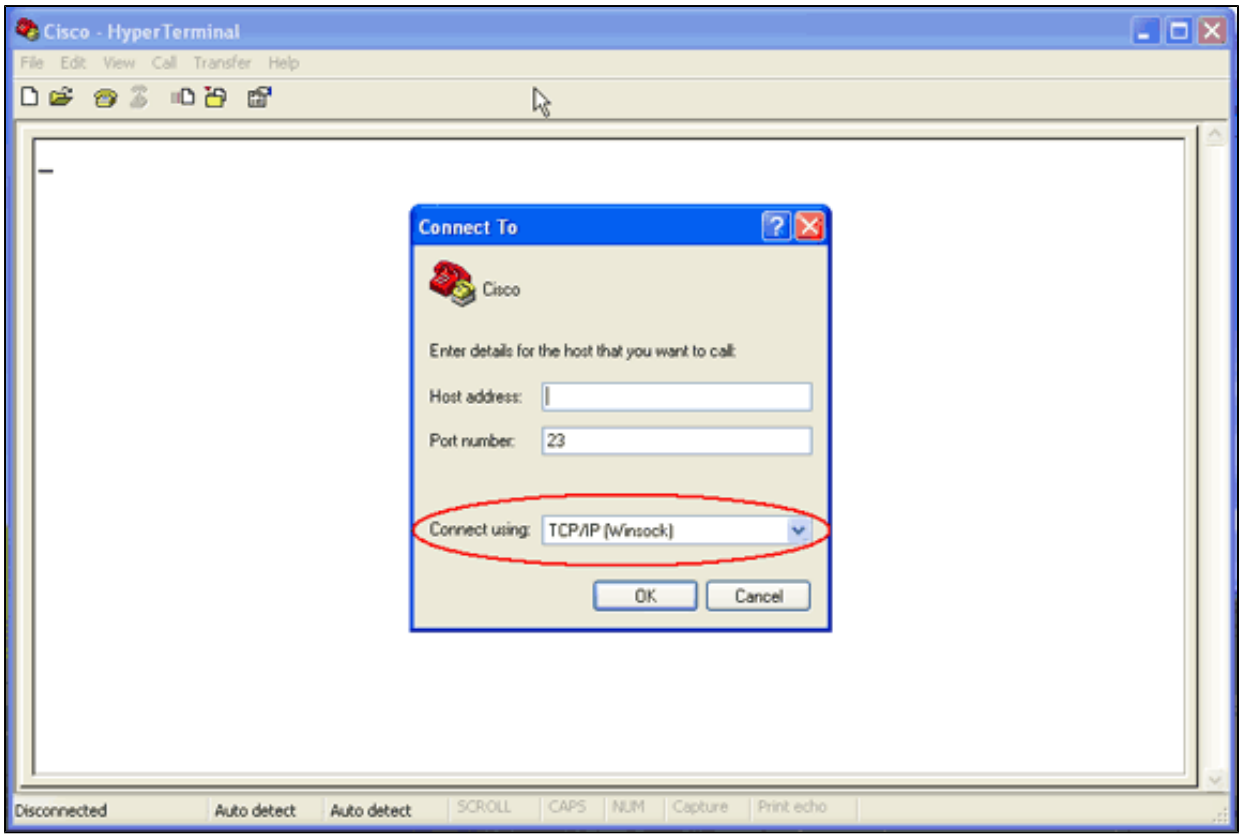
3. Para conexiones Telnet, complete estos pasos:

    a. En el menú desplegable Connect Using, elija TCP/IP.

    b. Introduzca la dirección IP del dispositivo en el que desea ejecutar las depuraciones.

    c. Click OK.

    Figura 2: Conexión Telnet



4. Para conexiones de consola, siga estos pasos:

   a. En el menú desplegable Connect Using (Conectar usando), seleccione el puerto COM al que está conectado el cable de la consola.

   b. Click OK.

      Aparecerá la hoja de propiedades de la conexión.

   c. Establezca la velocidad de la conexión al puerto de la consola.

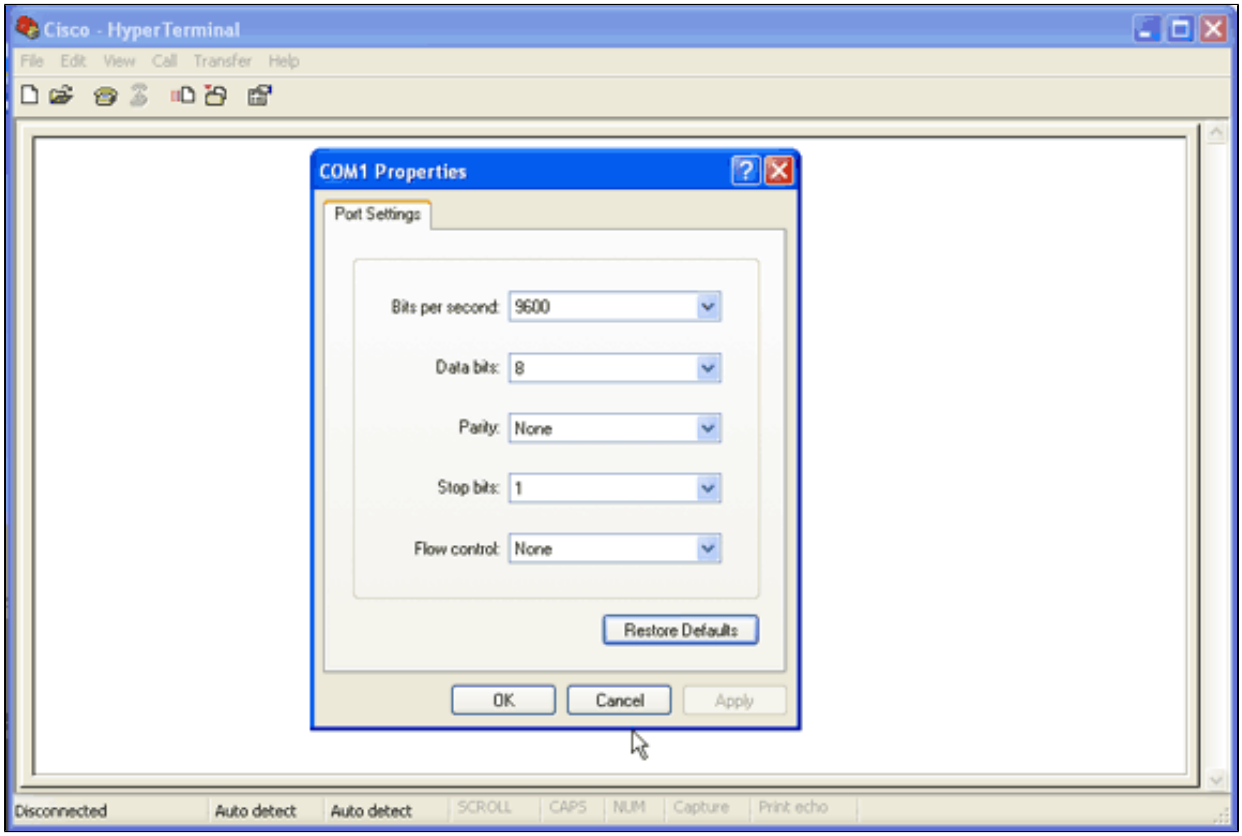
   d. Para restaurar la configuración del puerto predeterminado, haga clic en Restore Defaults.

      Nota: La mayoría de los productos de Cisco siguen la configuración de puerto predeterminada.

      Los parámetros predeterminados del puerto son:

      - Bits por segundo: 9600
      - Bits de datos: 8
      - Paridad: ninguna
      - Bits de detención: 1
      - Control de flujo: ninguno

Figura 3: Propiedades de COM1



En este punto, se establece la conexión Telnet o de consola y se le solicita un nombre de usuario y una contraseña.

Nota: El equipo Cisco Aironet asigna un nombre de usuario y una contraseña predeterminados de Cisco (distingue entre mayúsculas y minúsculas).

5. Para ejecutar los debugs, complete estos pasos:

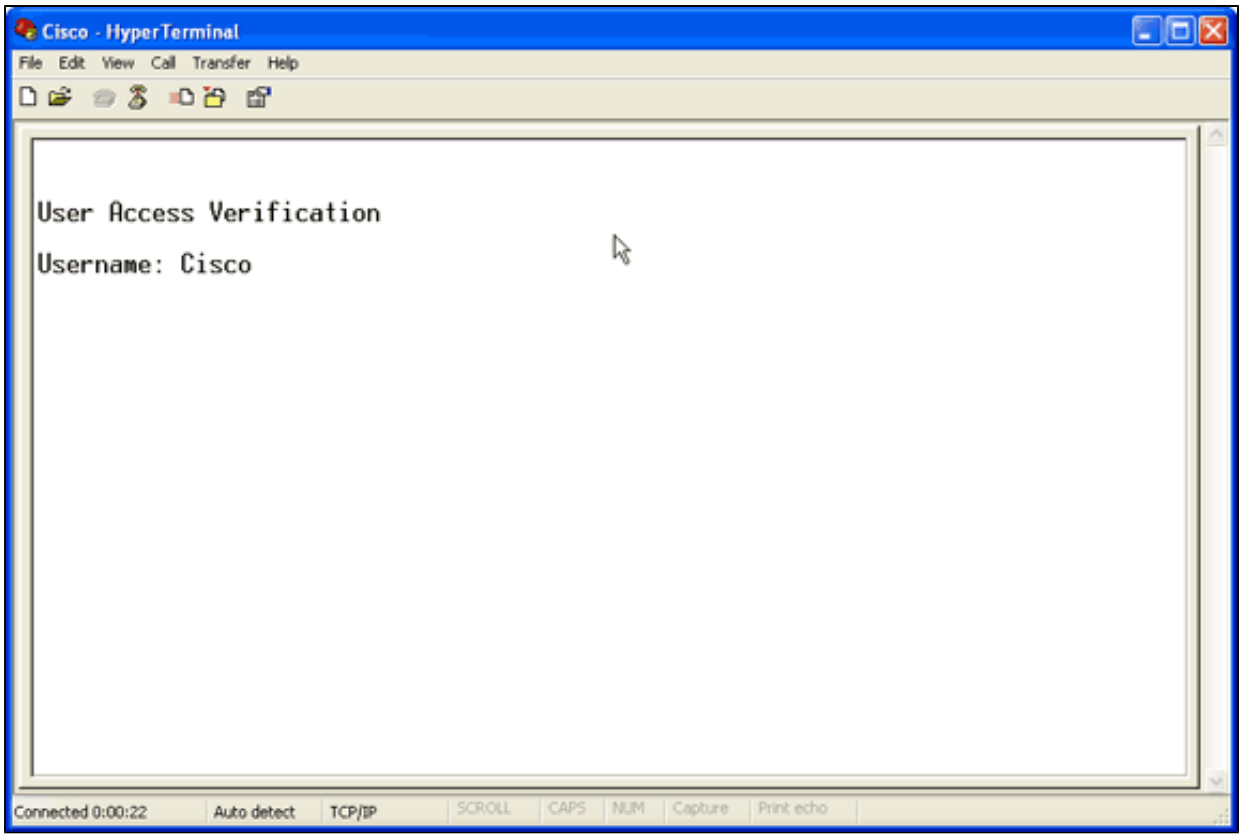
   a. Ejecute el comando enable para ingresar al modo privilegiado.

   b. Introduzca la contraseña de activación.

      Nota: Recuerde que la contraseña predeterminada para el equipo Aironet es Cisco (distingue entre mayúsculas y minúsculas).

      Nota: Para ver la salida de los debugs de una sesión Telnet, utilice el comando terminal monitor o el comando term mon para activar el monitor de terminal.

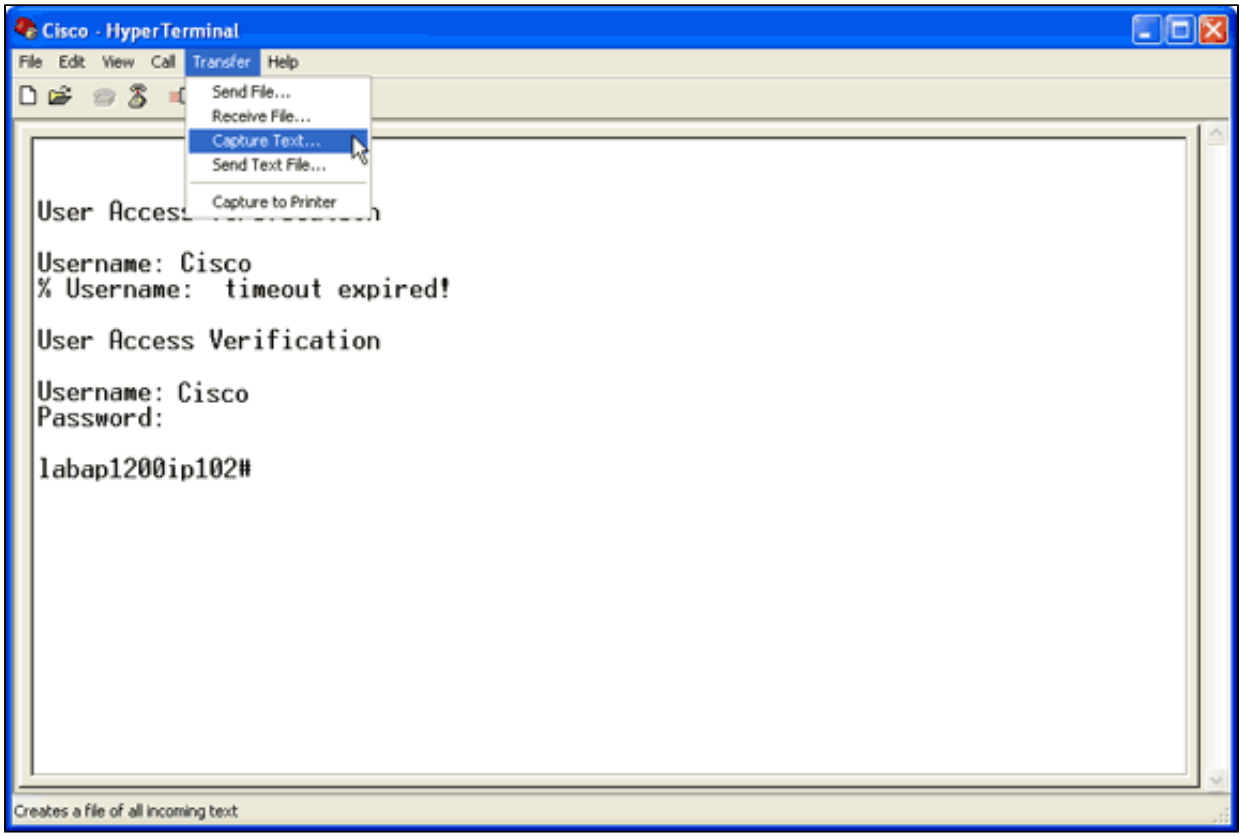
      Figura 4: Sesión de Telnet conectada



6. Después de establecer una conexión, complete estos pasos para recopilar una captura de pantalla:

   a. Elija Capture Text en el menú Transfer.

   Figura 5: Guardar una captura de pantalla



b. Cuando se abra un cuadro de diálogo que le solicite un nombre de archivo para la salida, introduzca un nombre de archivo.

7. Complete estos pasos para inhabilitar el ajuste de pantalla:

Nota: Puede leer las depuraciones más fácilmente cuando inhabilita el ajuste de pantalla.

a. En el menú HyperTerminal, elija File.

b. Elija Properties.

c. En la hoja de propiedades de la conexión, haga clic en la pestaña Settings.

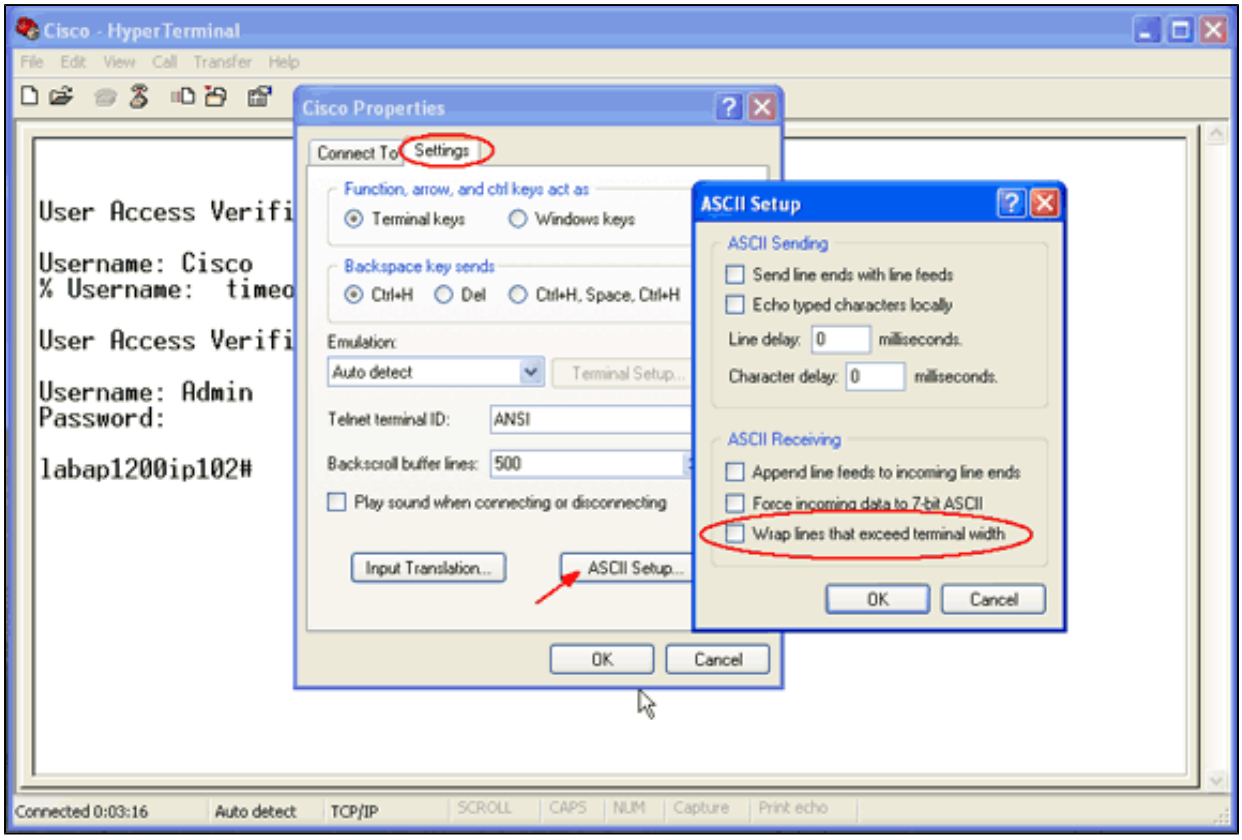
d. Haga clic en ASCII Setup.

e. Desmarque Ajustar líneas que excedan el ancho del terminal.

f. Para cerrar la configuración ASCII, haga clic en OK.

g. Para cerrar la hoja de propiedades de la conexión, haga clic en Aceptar.

Figura 6: Configuración de ASCII



Ahora que puede capturar cualquier resultado de la pantalla en un archivo de texto, las depuraciones que ejecute dependerán de lo que se negocie. Las siguientes secciones de este documento describen el tipo de conexión negociada proporcionada por los debugs.

EAP

Estas depuraciones son las más útiles para las autenticaciones EAP:

- debug radius authentication: las salidas de esta depuración comienzan con esta palabra: `RADIUS`.
- debug dot11 aaa authenticator process: las salidas de esta depuración comienzan con este texto: `dot11_auth_dot1x_`.
- debug dot11 aaa authenticator state-machine: las salidas de esta depuración comienzan con este texto: `dot11_auth_dot1x_run_rfsm`.

Estos debugs muestran:

- Elementos de los que se informa durante las partes RADIUS de un cuadro de diálogo de autenticación
- Las acciones que se realizan durante ese diálogo de autenticación
- Los diversos estados a través de los cuales transita el diálogo de autenticación

Este ejemplo muestra una autenticación correcta de EAP ligero (LEAP):

Ejemplo de Autenticación EAP Exitosa

```
<#root>

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]
```

Observe el flujo en las depuraciones **state-machine**. Hay una progresión a través de varios estados:

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY

   Nota: Mientras ambos negocian, puede haber varias iteraciones de CLIENT_WAIT y CLIENT_REPLY, así como de SERVER_WAIT y SERVER_REPLY.

6. SERVER_PASS

El comando **process** debug muestra cada paso individual a través de cada estado. Los debugs de **radius** muestran la conversación real entre el servidor de autenticación y el cliente. La manera más fácil de trabajar con los debugs EAP es observar la progresión de los mensajes de la máquina de estado a través de cada estado.

Cuando algo falla en la negociación, las depuraciones **state-machine** muestran por qué se detuvo

el proceso. Esté atento a mensajes similares a estos ejemplos:

- **CLIENT TIMEOUT**: este estado indica que el cliente no respondió dentro de una cantidad de tiempo apropiada. Esta falta de respuesta puede ocurrir debido a una de estas razones:
    - Hay un problema con el software cliente.
    - El valor de tiempo de espera del cliente EAP (del subseparador Autenticación EAP en Seguridad avanzada) ha caducado.

  Algunos EAP, especialmente los EAP protegidos (PEAP), tardan más de 30 segundos en completar la autenticación. Establezca este temporizador en un valor superior (entre 90 y 120 segundos).

  Este es un ejemplo de un intento de CLIENT TIMEOUT:

Ejemplo de CLIENT TIMEOUT

```
<#root>

Apr 12 17:51:09.373: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr 12 17:51:09.373: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0040.96a0.3758
Apr 12 17:51:09.374: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr 12 17:51:39.358: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,TIMEOUT

) for 0040.96a0.3758
Apr 12 17:51:39.358: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0040.96a0.3758
Apr 12 17:51:39.358: %DOT11-7-AUTH_FAILED:
    Station 0040.96a0.3758 Authentication failed
```

  Nota: Esté atento a los mensajes de error del sistema que sean similares a este mensaje:

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

  Nota: Estos mensajes de error pueden indicar un problema de radiofrecuencia (RF).

- Discordancia de secreto compartido entre el AP y el servidor RADIUS: en este registro de ejemplo, el servidor RADIUS no acepta la solicitud de autenticación del AP. El AP continúa enviando la solicitud al servidor RADIUS, pero el servidor RADIUS rechaza la solicitud porque el secreto compartido no coincide.

Para resolver este problema, asegúrese de verificar que el secreto compartido en el AP sea el mismo que se utiliza en el servidor RADIUS.

Discordancia secreta compartida entre el AP y el servidor RADIUS

```
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_DEAD:
    RADIUS server 10.10.1.172:1645, 1646 is not responding.
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server
    10.10.1.172:1645,1646 has returned.
Jun  2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758
    Authentication failed
```

- **server_timeout**: este estado indica que el servidor de autenticación no ha respondido en un período de tiempo adecuado. Este error de respuesta se debe a un problema en el servidor. Verifique que estas situaciones sean verdaderas:
    - El AP tiene conectividad IP al servidor de autenticación.

      Nota: Puede utilizar el comando ping para verificar la conectividad.
    - Los números de puerto de autenticación y cuentas son correctos para el servidor.

      Nota: Puede comprobar los números de puerto desde la ficha Administrador del servidor.
    - El servicio de autenticación se está ejecutando y funciona.

Este es un ejemplo de un intento de server_timeout:

Ejemplo de server_timeout

<#root>

```
Apr  8 20:02:55.469: dot11_auth_dot1x_start:
    in the dot11_auth_dot1x_start
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
Apr  8 20:02:55.470: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,EAP_START

) for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
    Started timer client_timeout 30 seconds
```

```
Apr  8 20:02:55.471: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.472: dot11_auth_parse_client_pak:
    id is not matching req-id:1resp-id:2, waiting for response
Apr  8 20:02:55.474: dot11_auth_parse_client_pak:
    Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_run_rfsm:
    Executing Action(

CLIENT_WAIT,CLIENT_REPLY

) for 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 20:02:55.475: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [248] 14
Apr  8 20:02:55.476: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [150] 2
Apr  8 20:02:55.476: RADIUS(00000031): Storing nasport 32 in rad_db
Apr  8 20:02:55.476: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.476: RADIUS/ENCODE(00000031): acct_session_id: 49
Apr  8 20:02:55.477: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.477: RADIUS(00000031): sending
Apr  8 20:02:55.477: RADIUS(00000031): Send Access-Request
    to 10.0.0.3:1234 id 21645/145, len 139
Apr  8 20:02:55.478: RADIUS:  authenticator B6 F7 BB 41 0E 9F 44 D1
    - 9A F8 E2 D7 5D 70 F2 76
Apr  8 20:02:55.478: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 20:02:55.478: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 20:02:55.478: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 20:02:55.478: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 20:02:55.478: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 20:02:55.478: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 20:02:55.478: RADIUS:  EAP-Message         [79]  14
Apr  8 20:02:55.479: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
    [?????aironet]
Apr  8 20:02:55.479: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless [19]
Apr  8 20:02:55.479: RADIUS:  NAS-Port            [5]   6   32
Apr  8 20:02:55.479: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 20:02:55.480: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 20:03:00.478: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:05.475: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:10.473: RADIUS:
    Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS:
    No response from (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response no app start; FAIL
Apr  8 20:03:15.470: RADIUS/DECODE:
    parse response; FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
```

```
    detailed aaa_status 1
Apr  8 20:03:15.471: dot11_auth_dot1x_run_rfsm:
    Executing Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 20:03:15.471: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 20:03:15.471: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- **SERVER_FAIL**: este estado indica que el servidor dio una respuesta de autenticación fallida basada en las credenciales del usuario. La depuración RADIUS que precede a esta falla muestra el nombre de usuario que se presentó al servidor de autenticación. Asegúrese de verificar el registro de intentos fallidos en el servidor de autenticación para obtener detalles adicionales sobre por qué el servidor denegó el acceso del cliente.

  Este es un ejemplo de un intento de SERVER_FAIL:

Ejemplo **SERVER_FAIL**

```
<#root>

Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Sending client 0002.8aa6.304f data to server
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
    Started timer server_timeout 60 seconds
Apr  8 17:46:13.605: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:46:13.605: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
    [labap1200ip1]
Apr  8 17:46:13.606: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:46:13.606: RADIUS(0000001D): Using existing nas_port 18
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS/ENCODE(0000001D): acct_session_id: 29
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS(0000001D): sending
Apr  8 17:46:13.607: RADIUS(0000001D): Send Access-Request
    to 10.0.0.3:1645 id 21645/97, len 176
Apr  8 17:46:13.607: RADIUS:  authenticator 88 82 8C BB DC 78 67 76
    - 36 88 1D 89 2B DC C9 99
Apr  8 17:46:13.607: RADIUS:  User-Name           [1]   14  "unknown_user"
Apr  8 17:46:13.607: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:46:13.608: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:46:13.608: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:46:13.608: RADIUS:  Service-Type        [6]   6   Login   [1]
Apr  8 17:46:13.608: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.608: RADIUS:  EAP-Message         [79]  46
Apr  8 17:46:13.608: RADIUS:  02 44 00 2C 11 01 00 18 02
    69 C3 F1 B5 90 52 F7    [?D?,?????i????R?]
Apr  8 17:46:13.609: RADIUS:
    B2 57 FF F0 74 8A 80 59 31 6D C7 30 D3 D0 AF 65
    [?W??t??Y1m?0???e]
Apr  8 17:46:13.609: RADIUS:   75 6E 6B 6E 6F 77 6E 5F 75 73 65 72
```

```
    [unknown_user]
Apr  8 17:46:13.609: RADIUS:  NAS-Port-Type       [61]  6   802.11
    wireless           [19]
Apr  8 17:46:13.609: RADIUS:  NAS-Port            [5]   6   18
Apr  8 17:46:13.610: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:46:13.610: RADIUS:  Nas-Identifier      [32]  16
    "labap1200ip102"
Apr  8 17:46:13.622: RADIUS: Received from id 21645/97
    10.0.0.3:1645,

Access-Reject

, len 56
Apr  8 17:46:13.622: RADIUS:  authenticator 55 E0 51 EF DA CE F7 78
    - 92 72 3D 97 8F C7 97 C3
Apr  8 17:46:13.622: RADIUS:  EAP-Message         [79]  6
Apr  8 17:46:13.623: RADIUS:   04 44 00 04                          [?D??]
Apr  8 17:46:13.623: RADIUS:  Reply-Message       [18]  12
Apr  8 17:46:13.623: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D  [Rejected??]
Apr  8 17:46:13.623: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.624: RADIUS(00000001D): Received from id 21645/97
Apr  8 17:46:13.624: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:46:13.624: RADIUS/DECODE: Reply-Message fragments,
    10, total 10 bytes
Apr  8 17:46:13.624: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: FAIL
Apr  8 17:46:13.625: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Apr  8 17:46:13.625: dot11_auth_dot1x_run_rfsm:
    xecuting Action(

SERVER_WAIT,SERVER_FAIL

) for 0002.8aa6.304f
Apr  8 17:46:13.625: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0002.8aa6.304f
Apr  8 17:46:13.626: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 20 seconds
Apr  8 17:46:13.626: dot11_auth_dot1x_send_client_fail:
    Authentication failed for 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
    Authentication failed
```

- No Response from Client: en este ejemplo, el servidor RADIUS envía un mensaje de pase al AP que el AP reenvía y luego asocia al cliente. Finalmente, el cliente no responde al AP. Por lo tanto, el AP lo desautentica después de alcanzar el máximo de reintentos.

No hay respuesta del cliente

```
<#root>

Sep 22 08:42:04: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
```

```
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 08:42:04: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Associated KEY_MGMT[NONE]
Sep 22 10:35:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:35:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,


Deauthenticating Station

 0040.96a0.3758
    Reason: Previous authentication no longer valid
```

El AP reenvía una respuesta de desafío get del radio al cliente. El cliente no responde y alcanza el número máximo de reintentos, lo que hace que EAP falle y que el AP desautentique al cliente.

No hay respuesta del cliente

```
<#root>

Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    Received server response: GET_CHALLENGE_RESPONSE
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
    found eap pak in server response
Sep 22 10:43:02: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:43:05: %DOT11-4-MAXRETRIES: Packet to client 0040.96a0.3758
    reached

max retries

, removing the client
Sep 22 10:43:05: Client 0040.96a0.3758 failed: reached maximum retries
```

Radius envía un mensaje de pase al AP, el AP reenvía el mensaje de pase al cliente, y el cliente no responde. El AP lo desautentica después de alcanzar el máximo de reintentos. El cliente luego intenta una nueva solicitud de identidad al AP, pero el AP rechaza esta solicitud porque el cliente ya ha alcanzado el máximo de reintentos.

No hay respuesta del cliente

```
<#root>

Sep 22 10:57:08: dot11_auth_dot1x_run_rfsm:
    Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Forwarding server message to client 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
    Started timer client_timeout 30 seconds
Sep 22 10:57:08: %DOT11-6-ASSOC: Interface Dot11Radio0,
    Station arlit1ad1hd6j91 0040.96a0.3758 Reassociated KEY_MGMT[NONE]
Sep 22 10:57:10: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached max retries, removing the client
Sep 22 10:57:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,
    Deauthenticating Station0040.96a0.3758 Reason:
    Previous authentication no longer valid
Sep 22 10:57:15: AAA/BIND(00001954): Bind i/f
Sep 22 10:57:15: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Sending identity request to 0040.96a0.3758
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
    Client 0040.96a0.3758 timer started for 30 seconds
Sep 22 10:57:15: %DOT11-4-MAXRETRIES: Packet to client
    0040.96a0.3758 reached

max retries

, removing the client
Sep 22 10:57:15: Client 0040.96a0.3758 failed: reached maximum retries
```

Las depuraciones **process** y/o **radius** que preceden inmediatamente al mensaje de la máquina de estado muestran los detalles de la falla.

Para obtener más información sobre cómo configurar EAP, consulte Autenticación EAP con servidor RADIUS.

Autenticación MAC

Estos debugs son los más útiles para la autenticación MAC:

- debug radius authentication: cuando se utiliza un servidor de autenticación externo, las salidas de esta depuración comienzan con esta palabra: `RADIUS`.
- debug dot11 aaa authenticator mac-authen: las salidas de esta depuración comienzan con este texto: `dot11_auth_dot1x_`.

Estos debugs muestran:

- Elementos de los que se informa durante las partes RADIUS de un cuadro de diálogo de autenticación
- La comparación entre la dirección MAC que se proporciona y la que se autentica en

Cuando se utiliza un servidor RADIUS externo con autenticación de dirección MAC, se aplican las depuraciones RADIUS. El resultado de esta conjunción es una visualización de la conversación real entre el servidor de autenticación y el cliente.

Cuando una lista de direcciones MAC se construye localmente en el dispositivo como una base de datos de nombre de usuario y contraseña, sólo los debugs **mac-authen** muestran resultados. A medida que se determina la coincidencia de dirección o la discordancia, se muestran estas salidas.

Nota: Introduzca siempre los caracteres alfabéticos de una dirección MAC en minúsculas.

Estos ejemplos muestran una autenticación MAC exitosa contra una base de datos local:

Ejemplo de Autenticación MAC Exitosa

```
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]
```

Este ejemplo muestra una autenticación MAC fallida contra una base de datos local:

Ejemplo de Autenticación MAC Fallida

```
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
```

Cuando falle la autenticación de una dirección MAC, compruebe la precisión de los caracteres introducidos en la dirección MAC. Asegúrese de que ha introducido caracteres alfabéticos en minúsculas en una dirección MAC.

Para obtener más información sobre cómo configurar la autenticación MAC, refiérase a Configuración de Tipos de Autenticación (Guía de Configuración de Cisco IOS Software para Puntos de Acceso Cisco Aironet, 12.2(13)JA).

WPA

Aunque el acceso Wi-Fi protegido (WPA) no es un tipo de autenticación, es un protocolo negociado.

- WPA negocia entre el AP y la tarjeta del cliente.
- La administración de claves WPA negocia después de que un servidor de autenticación autentique correctamente un cliente.
- WPA negocia una clave transitoria de par (PTK) y una clave transitoria de grupo (GTK) en un protocolo de enlace de cuatro direcciones.

Nota: Como WPA requiere que el EAP subyacente sea correcto, verifique que los clientes puedan autenticarse correctamente con ese EAP antes de utilizar WPA.

Estas depuraciones son las más útiles para las negociaciones WPA:

- debug dot11 aaa authenticator process: las salidas de esta depuración comienzan con este texto: `dot11_auth_dot1x_`.
- debug dot11 aaa authenticator state-machine: las salidas de esta depuración comienzan con este texto: `dot11_auth_dot1x_run_rfsm`.

En relación con las otras autenticaciones de este documento, las depuraciones WPA son fáciles de leer y analizar. Se debe enviar un mensaje PTK y recibir una respuesta apropiada. A continuación, se debe enviar un mensaje GTK y recibir otra respuesta apropiada.

Si los mensajes PTK o GTK no se envían, la configuración o el nivel de software en el AP pueden ser defectuosos. Si no se reciben las respuestas PTK o GTK del cliente, verifique la configuración o el nivel de software en el suplicante WPA de la tarjeta cliente.

Ejemplo de Negociación WPA Satisfactoria

```
<#root>

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#
```

Para obtener más información sobre cómo configurar WPA, consulte WPA Configuration Overview.

Autenticación HTTP/administrativa

Puede restringir el acceso administrativo al dispositivo a los usuarios que aparezcan en una base de datos de nombre de usuario y contraseña local o a un servidor de autenticación externo. El acceso administrativo es compatible con RADIUS y TACACS+.

Estas depuraciones son las más útiles para la autenticación administrativa:

- debug radius authentication o debug tacacs authentication: las salidas de esta depuración comienzan con una de estas palabras: `RADIUS` o `TACACS`.
- debug aaa authentication: los resultados de estas depuraciones comienzan con este texto: `AAA/AUTHEN`.
- debug aaa authorization: los resultados de estas depuraciones comienzan con este texto: `AAA/AUTHOR`.

Estos debugs muestran:

- Información proporcionada durante las partes RADIUS o TACACS de un diálogo de autenticación
- Las negociaciones reales para la autenticación y autorización entre el dispositivo y el servidor de autenticación

Este ejemplo muestra una autenticación administrativa exitosa cuando el atributo `Service-Type`

RADIUS se establece en Administrative:

Ejemplo de Autenticación Administrativa Exitosa con el Atributo Service-Type

```
<#root>

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
```

Este ejemplo muestra una autenticación administrativa exitosa cuando utiliza atributos específicos del proveedor para enviar una sentencia "priv-level":

Ejemplo de Autenticación Administrativa Exitosa con Atributo Específico del Proveedor

<#root>

```
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
```

El problema más común con la autenticación administrativa es la falla al configurar el servidor de autenticación para enviar los atributos de tipo de servicio administrativo o de nivel de privilegio apropiados. Este intento de ejemplo falló en la autenticación administrativa porque no se enviaron atributos de nivel de privilegio ni atributos de tipo de servicio administrativo:

Sin atributos de tipo de servicio o específicos del proveedor

```
<#root>

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=
```

Para obtener más información sobre cómo configurar la autenticación administrativa, refiérase a Administración del Punto de Acceso (Guía de Configuración de Cisco IOS Software para Puntos de Acceso Cisco Aironet, 12.2(13)JA).

Para obtener más información sobre cómo configurar los privilegios administrativos para los usuarios en el servidor de autenticación, consulte Ejemplo de Configuración: Autenticación Local para Usuarios del Servidor HTTP. Marque la sección que coincida con el protocolo de autenticación que utiliza.

Información Relacionada

- Guía de Configuración del Cisco IOS Software para los Puntos de Acceso Cisco Aironet, 12.2(13)JA
- Autenticación del EAP con servidor RADIUS
- Autenticación LEAP con el servidor RADIUS local
- Preguntas más Frecuentes sobre Aironet Wireless Security
- Ejemplo de Configuración de Wireless Domain Services AP como Servidor AAA
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).