Autenticaciones del debug

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 porciones de este documento que refieren a los Productos del no Cisco se basan en la experiencia del autor, no en la capacitación formal. Se piensan para su conveniencia y no como Soporte técnico. Para el Soporte técnico autoritario en los Productos del no Cisco, entre en contacto el Soporte técnico para ese producto.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación como se relaciona con las redes inalámbricas
- Comando line interface(cli) del software del ® del Cisco IOS
- Configuración de servidor de RADIUS

Componentes Utilizados

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

- Productos de red inalámbrica basados en software del Cisco IOS de cualquier modelo y versión

- Hyperterminal de Hilgraeve

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

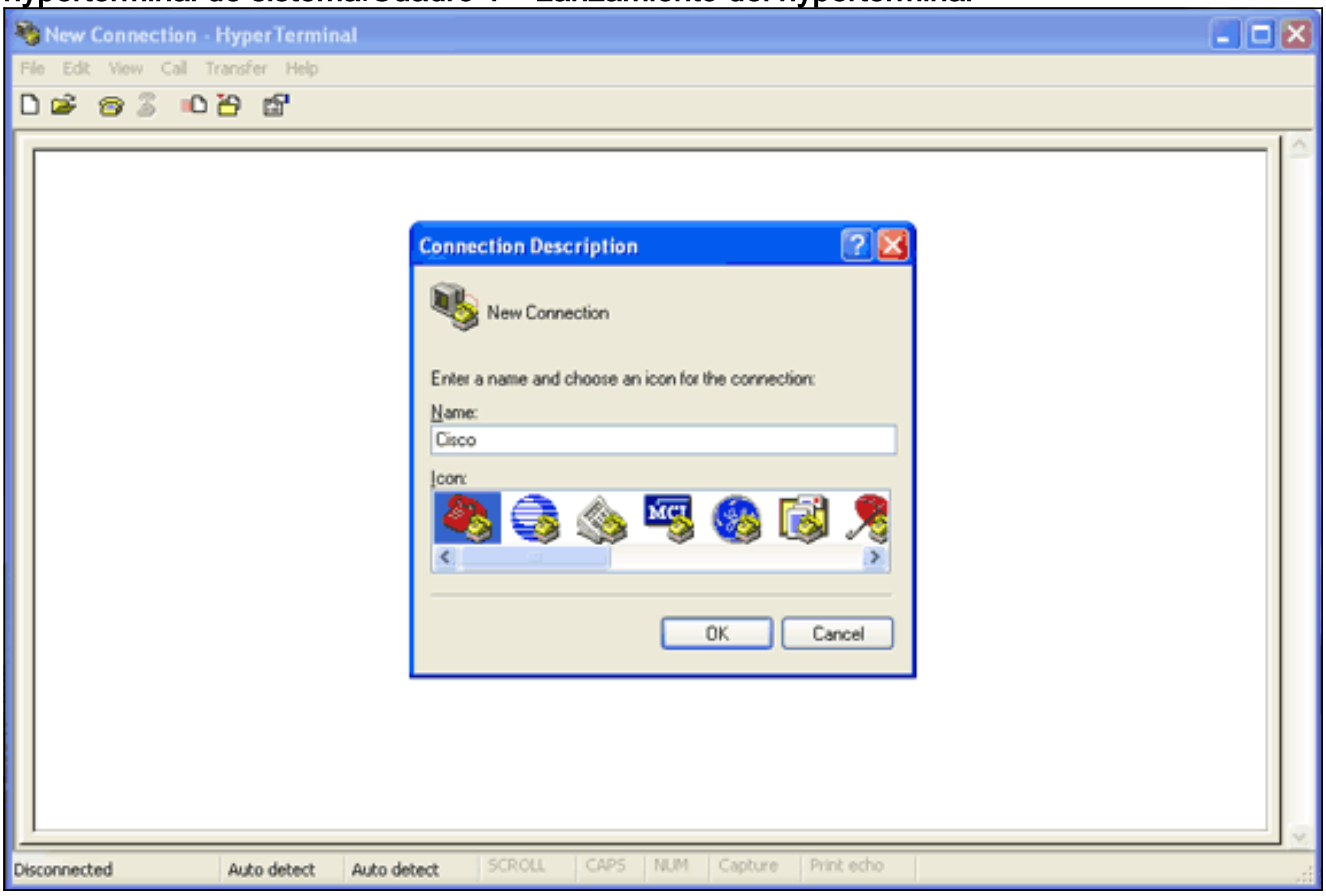
Capture los debugs

Si usted no puede capturar y analizar la información del debug, la información es inútil. La manera más fácil de capturar estos datos está con una función de la captura de pantalla que se incorpore a Telnet o a la Aplicación de comunicaciones.

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

Complete estos pasos para configurar el hyperterminal para comunicar con su punto de acceso o Bridge:

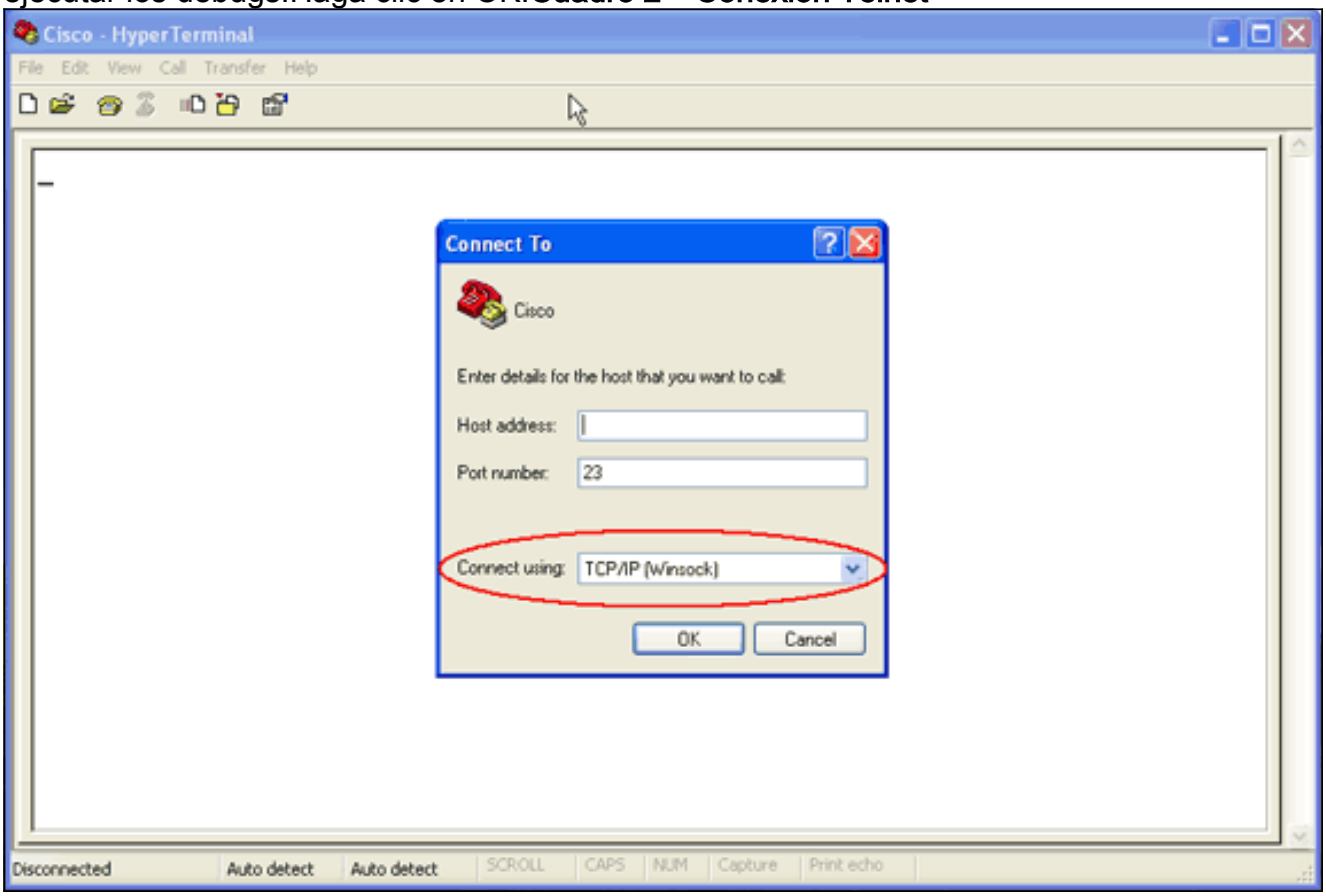
1. Para abrir el hyperterminal, elija **Start > Programs > las herramientas > las comunicaciones > hyperterminal de sistema**.**Cuadro 1 – Lanzamiento del hyperterminal**



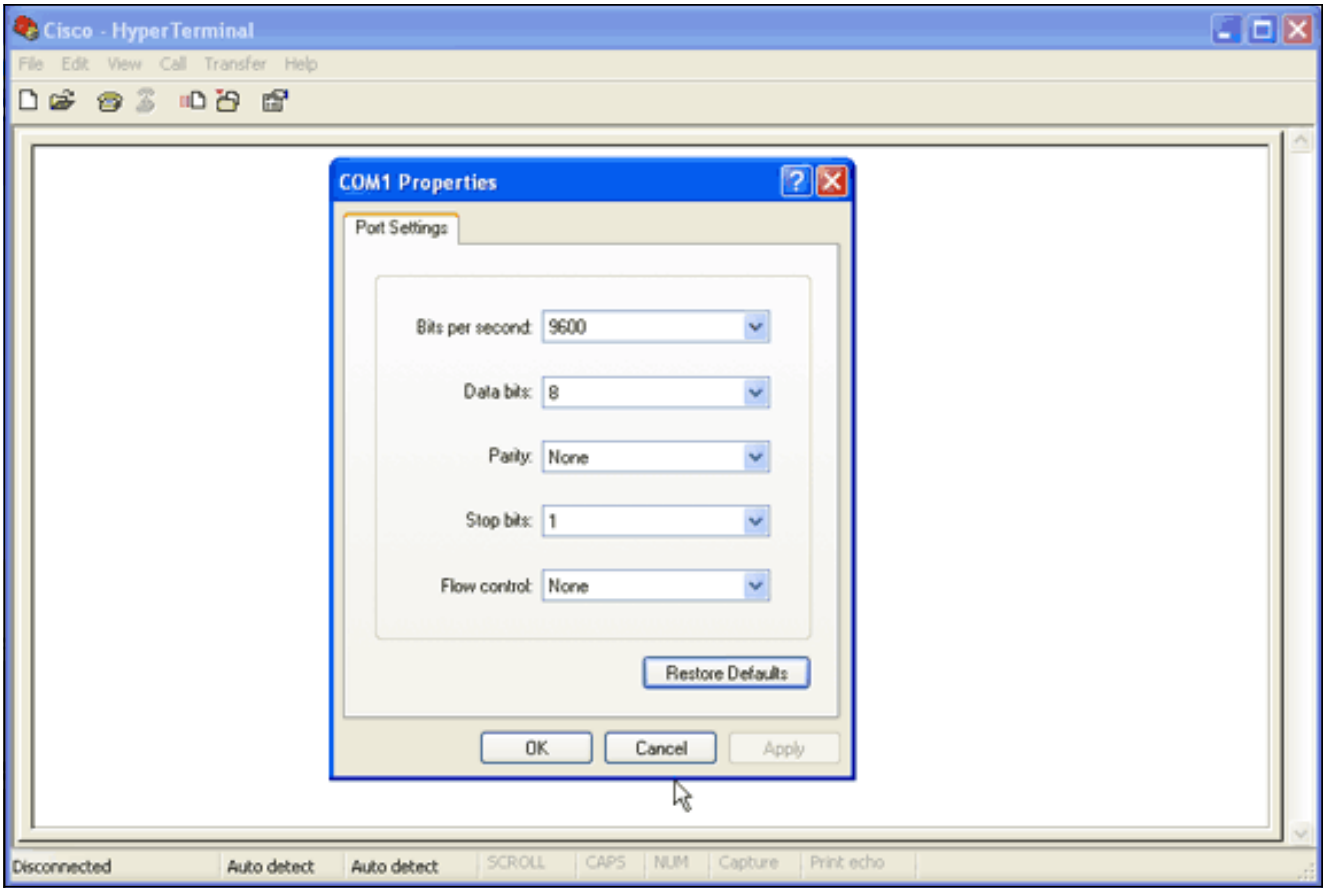
2. Cuando el hyperterminal se abre, complete estos pasos:Ingrese un nombre para la

conexión.Elija un icono.Haga clic en OK.

3. Para las conexiones Telnet, complete estos pasos:De la conexión usando el menú desplegable, elija el **TCP/IP**.Ingrese el IP Address del dispositivo donde usted quiere ejecutar los debugs.Haga clic en OK.**Cuadro 2 – Conexión Telnet**

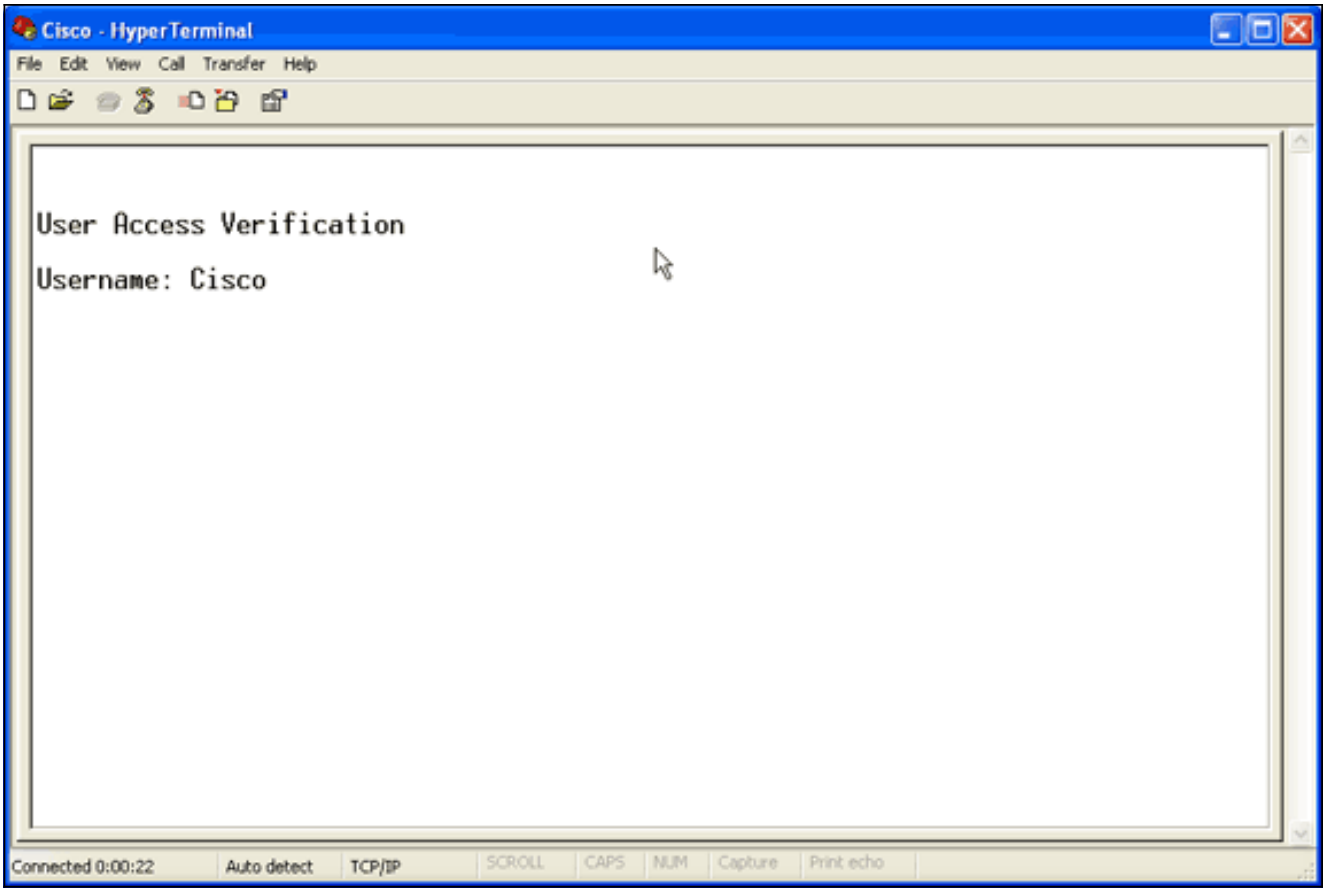


4. Para las conexiones de consola, complete estos pasos:De la conexión usando el menú desplegable, elija el puerto COM en donde el cable de la consola está conectado.Haga clic en OK.La hoja de propiedades para la conexión aparece.Fije la velocidad para la conexión al puerto de la consola.Para restablecer las configuraciones del puerto predeterminado, haga clic los **valores por defecto del Restore**.**Nota:** La mayoría de los Productos Cisco siguen las configuraciones del puerto predeterminado.Las configuraciones del puerto predeterminado son:Bits por segundo — 9600Bits de datos — 8Paridad — NingunosBits de detención — 1Control de flujo — Ningunos**Cuadro 3 – Propiedades COM1**

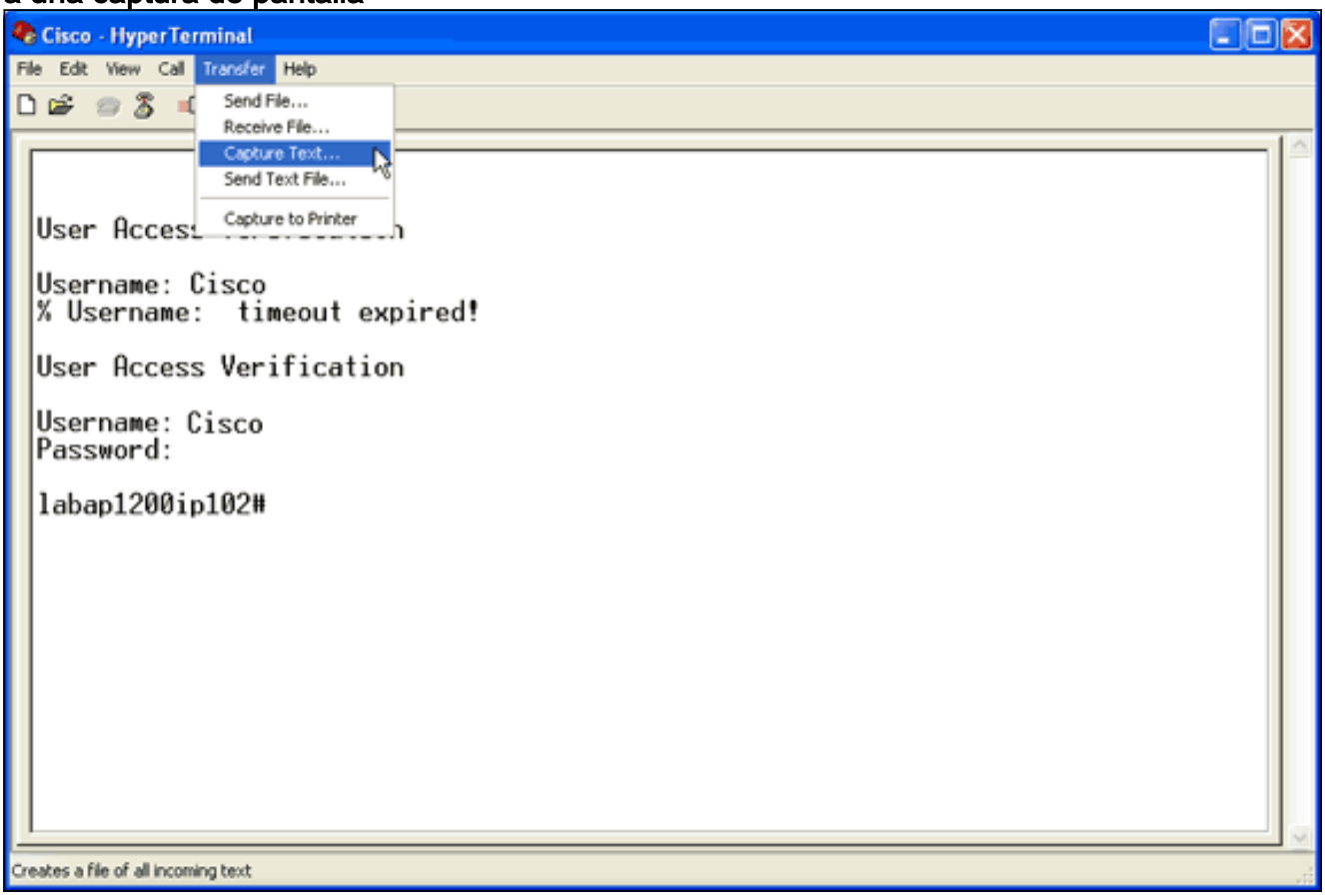


En este momento, Telnet o la conexión de consola establece, y le indican para un Nombre de usuario y una contraseña.**Nota:** El equipo Aironet de Cisco asigna un nombre de usuario predeterminado y la contraseña de *Cisco* (con diferenciación entre mayúsculas y minúsculas).

5. Para ejecutar los debugs, complete estos pasos:Publique el **comando enable** para ingresar al modo privilegiado.Ingrese la contraseña habilitada.**Nota:** Recuerde que la contraseña predeterminada para el equipo de Aironet es *Cisco* (con diferenciación entre mayúsculas y minúsculas).**Nota:** Para ver la salida de los debugs de una sesión telnet, utilice el **comando terminal monitor o term mon** para girar el monitor terminal.**Cuadro 4 – Sesión telnet conectada**



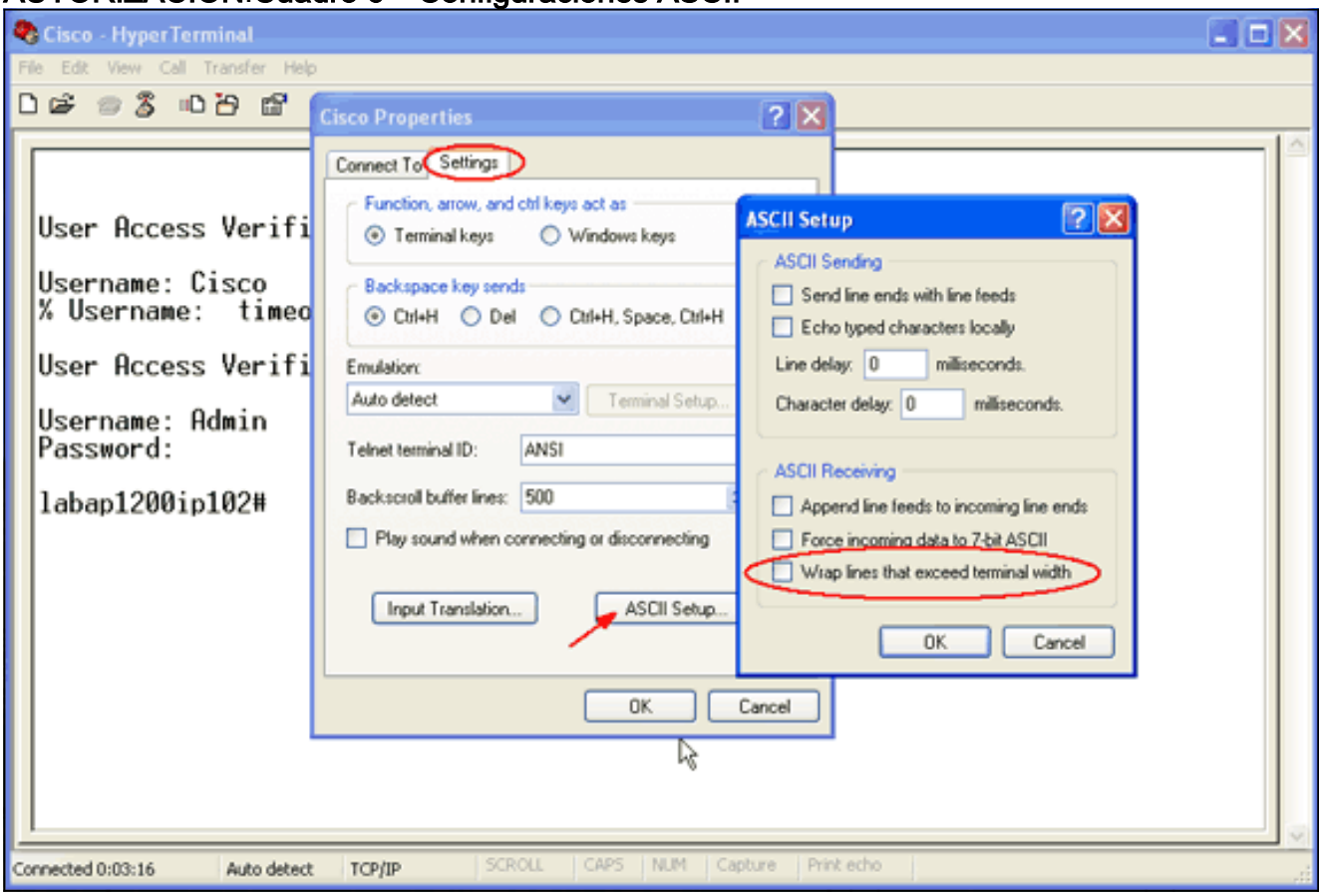
6. Después de que usted establezca una conexión, complete estos pasos para recoger a una captura de pantalla:Elija el **texto de la captura del** menú de la transferencia.**Cuadro 5 – Salve a una captura de pantalla**



Cuando un cuadro de diálogo se abre que le indica para un nombre del archivo para la salida, ingrese un nombre del archivo.

7. Complete estos pasos para inhabilitar el abrigo de la pantalla:**Nota:** Usted puede leer los

debugs más fácilmente cuando usted inhabilita el abrigo de la pantalla.Del menú HyperTerminal, elija el **archivo**.Elija las **propiedades**.En la hoja de propiedad de conexión, haga clic la lengueta de las **configuraciones**.Haga clic la **configuración ASCII**.Desmarque las **líneas del abrigo que exceden el ancho del terminal**.Para cerrar las configuraciones ASCII, haga clic la **AUTORIZACIÓN**.Para cerrar la hoja de propiedad de conexión, haga clic la **AUTORIZACIÓN**.Cuadro 6 – Configuraciones ASCII



Ahora que usted puede capturar cualquier resultado de pantalla a un archivo de texto, los debugs que usted ejecuta dependen se negocia de qué. Las siguientes secciones de este documento describen el tipo de conexión negociada proporcionada por los debugs.

EAP

Estos debugs son los más útiles para las autenticaciones EAP:

- **autenticación de RADIUS del debug** — Las salidas de este comienzo del debug con esta palabra: `RADIUS`.
- **proceso del authenticator aaa del dot11 del debug** — Las salidas de este comienzo del debug con este texto: `dot11_auth_dot1x_`.
- **estado-máquina del authenticator aaa del dot11 del debug** — Las salidas de este comienzo del debug con este texto: `dot11_auth_dot1x_run_rfsm`.

Demostración de estos debugs:

- Qué está señalada durante las porciones RADIUS de un diálogo de autenticación
- Medidas que se toman durante ese diálogo de autenticación
- Los diversos estados a través de los cuales las transiciones del diálogo de autenticación

Este ejemplo muestra una autenticación acertada de la luz EAP (SALTO):

Ejemplo acertado de la autenticación EAP

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]
```

Note el flujo en los debugs de la estado-**máquina**. Hay una progresión a través de varios estados:

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY**Nota:** Como los dos negocie, puede haber varias iteraciones de CLIENT_WAIT y CLIENT_REPLY, así como SERVER_WAIT y SERVER_REPLY.
6. SERVER_PASS

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

Cuando algo falla en la negociación, los debugs de la estado-**máquina** muestran porqué el proceso paró. Mire para los mensajes similares a estos ejemplos:

- **TIEMPO DE ESPERA AGOTADO DEL CLIENTE** — Este estado indica que el cliente no respondió dentro de una cantidad de tiempo apropiada. Este error responder puede ocurrir debido a una de estas razones:Hay un problema con el software de cliente.El valor de agotamiento del tiempo de los clientes EAP (del subtab de la autenticación EAP bajo Seguridad avanzada) ha expirado.Algunos EAP, determinado EAP protegido (PEAP), duran de 30 segundos para completar la autenticación. Fije este temporizador a un valor más alto (entre 90 y 120 segundos).Éste es un ejemplo de una tentativa del TIEMPO DE ESPERA AGOTADO DEL CLIENTE:**Nota:** Mire para cualquier mensaje de error del sistema que sea similar a este mensaje:`%DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached max retries, removing the client`**Nota:** Tales mensajes de error pueden indicar un problema del Radiofrecuencia (RF).
- **Discordancía del secreto compartido entre el AP y el servidor de RADIUS** — en este registro del ejemplo, el servidor de RADIUS no valida el pedido de autenticación del AP. El AP continúa enviando la petición al servidor de RADIUS, pero el servidor de RADIUS rechaza la petición porque se une mal el secreto compartido.Para resolver este problema, esté seguro de marcar que el secreto compartido en el AP es el mismo que se utiliza en el servidor de RADIUS.
- **server_timeout** — Este estado indica que el servidor de autenticación no respondió en una cantidad de tiempo apropiada. Este error responder ocurre debido a un problema en el servidor. Verifique que estas situaciones sean verdades:El AP tiene conectividad del IP al servidor de autenticación.**Nota:** Usted puede utilizar el **comando ping** para verificar la Conectividad.La autenticación y los números del puerto de contabilidad están correctos para el servidor.**Nota:** Usted puede marcar los números del puerto de la lengueta del administrador de servidor.El servicio de autenticación es corriente y funcional.Éste es un ejemplo de una tentativa del server_timeout:
- **SERVER_FAIL** — Este estado indica que el servidor dio una respuesta de la autenticación fallida basada en los credenciales de usuario. El debug RADIUS que precede este error muestra el Nombre de usuario que fue presentado al servidor de autenticación. Esté seguro de marcar el

login de los intentos fallidos el servidor de autenticación para los detalles adicionales en porqué el servidor negó el acceso al cliente.Éste es un ejemplo `SERVER_FAIL de una` tentativa:
- **Ninguna respuesta del cliente** — En este ejemplo, el servidor de RADIUS envía un mensaje del paso al AP que el AP adelante encendido y entonces él asocia al cliente. El cliente no responde eventual al AP. Por lo tanto, los deauthenticates AP él después de que alcance las cantidades de intentos máximas.El AP adelante una respuesta de seguridad del conseguir del radio al cliente. El cliente no responde y alcanza los Reintento máximo que hace el EAP fallar y el AP al deauthenticate el cliente.El radio envía un mensaje del paso al AP, el AP adelante el mensaje del paso al cliente, y el cliente no responde. Los deauthenticates AP él después de que alcance las cantidades de intentos máximas. El cliente entonces intenta una nueva petición de la identidad al AP, pero el AP rechaza esta petición porque el cliente ha alcanzado ya las cantidades de intentos máximas.

Los debugs del **`proceso`** y/o del **`radio`** que *preceden* inmediatamente la demostración del mensaje de la máquina de estado los detalles del error.

Para más información sobre cómo configurar el EAP, refiera a la autenticación EAP con el servidor de RADIUS.

Autenticación de MAC

Estos debugs son los más útiles para la autenticación de MAC:

- **autenticación de RADIUS del debug** — Cuando utilizan a un servidor de autenticación externa, las salidas de este debug comienzan con esta palabra: `RADIUS`.
- **mac-authen del authenticator aaa del dot11 del debug** — Las salidas de este debug comienzan con este texto: `dot11_auth_dot1x_`.

Demostración de estos debugs:

- Qué está señalada durante las porciones RADIUS de un diálogo de autenticación
- La comparación entre la dirección MAC se da que y la contra el cual se autentica

Cuando utilizan a un servidor RADIUS externo con la autenticación de la dirección MAC, los debugs RADIUS se aplican. 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 al dispositivo como un Nombre de usuario y base de datos de contraseñas, sólo los debugs del **`mac-authen`** muestran las salidas. Como se determina el emparejamiento o la discordancía del direccionamiento, visualización de estas salidas.

Nota: Ingrese siempre cualquier carácter alfabético en un MAC address en minúsculas.

Este los ejemplos muestran una autenticación de MAC acertada contra una base de datos local:

Ejemplo acertado de la autenticación de MAC

```
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 los ejemplos muestran una autenticación de MAC fallada contra una base de datos local:

Ejemplo fallado de la autenticación de MAC

```
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 una autenticación del MAC address falla, marque para saber si hay la exactitud de los caracteres que se ingresan en el MAC address. Esté seguro que usted ha ingresado cualquier carácter alfabético en un MAC address en minúsculas.

Para más información sobre cómo configurar la autenticación de MAC, refiera a configurar los tipos de autenticación (guía de configuración del Cisco IOS Software para los Puntos de acceso del Cisco Aironet, 12.2(13)JA).

WPA

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

- El WPA negocia entre el AP y la placa cliente.
- La administración de claves WPA negocia después de que a un servidor de autenticación autentique a un cliente con éxito.
- El WPA negocia una clave en parejas transitoria (PTK) y una clave transitoria de Groupwise (GTK) en un apretón de manos de cuatro terminales.

Nota: Porque el WPA requiere que el EAP subyacente sea acertado, verifique que los clientes puedan autenticar con éxito con ese EAP antes de que usted dedique el WPA.

Estos debugs son los más útiles para las negociaciones WPA:

- **proceso del authenticator aaa del dot11 del debug** — Las salidas de este comienzo del debug con este texto: `dot11_auth_dot1x_`.
- **estado-máquina del authenticator aaa del dot11 del debug** — Las salidas de este comienzo del debug con este texto: `dot11_auth_dot1x_run_rfsm`.

En relación con las otras autenticaciones en este documento, los debugs WPA son simples leer y analizar. Un mensaje PTK debe ser enviado y una contestación apropiada ser recibido. Después, un mensaje GTK debe ser enviado y otra respuesta apropiada ser recibido.

Si el PTK o los mensajes GTK no se envía, la configuración o el nivel de software en el AP puede

ser culpable. Si el PTK o las respuestas GTK del cliente no se recibe, marque la configuración o el nivel de software en el solicitante de WPA de la placa cliente.

Ejemplo de negociación WPA satisfactoria

```
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 más información sobre cómo configurar el WPA, refiera a la introducción a la configuración de WPA.

Autenticación Administrative/HTTP

Usted puede restringir el acceso administrativo al dispositivo a los usuarios que se enumeran en una base de datos del nombre de usuario local y contraseña o a un servidor de autenticación externa. El acceso administrativo se soporta con el RADIUS y el TACACS+.

Estos debugs son los más útiles para la autenticación administrativa:

- **autenticación de RADIUS del debug** o **autenticación de TACACS del debug** — Las salidas de este comienzo del debug con una de estas palabras: `Radius or tacacs`.
- **autenticación aaa del debug** — Las salidas de este comienzo de los debugs con este texto: `AAA/AUTHEN`.
- **debug aaa authorization** — Las salidas de este comienzo de los debugs con este texto: `AAA/AUTHOR`.

Demostración de estos debugs:

- Qué está señalada durante las porciones del radius or 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 acertada cuando el `atributo de RADIUS del tipo de servicio` se fija a `administrativo`:

Ejemplo acertado de la autenticación administrativa con el atributo de tipo de servicio

```
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 acertada cuando usted utiliza los atributos específicos del proveedor para enviar una declaración del “priv-nivel”:

Ejemplo acertado de la autenticación administrativa con el atributo específico del proveedor

```
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 el error configurar al servidor de autenticación para enviar el nivel de privilegio apropiado o los atributos de tipo de servicio administrativos. Esta tentativa del ejemplo falló la autenticación administrativa porque no se envió ningunos atributos del nivel de privilegio o los atributos de tipo de servicio administrativos:

Sin los atributos específicos del vendedor o de tipo de servicio

```
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 más información sobre cómo configurar la autenticación administrativa, refiera a administrar el Punto de acceso (guía de configuración del Cisco IOS Software para los Puntos de acceso del Cisco Aironet, 12.2(13)JA).

Para más información sobre cómo configurar el privilegio administrativo a los usuarios en el servidor de autenticación, refiera a la configuración de muestra: Autenticación local para los usuarios de servidor HTTP. Marque la sección que hace juego el protocolo de autenticación que usted utiliza.

Información Relacionada

- Guía de Configuración del Cisco IOS Software para los Puntos de Acceso Cisco Aironet, 12.2(13)JA
- Autenticación EAP con el servidor de RADIUS
- Autenticación LEAP con el servidor RADIUS local
- PREGUNTAS MÁS FRECUENTES SOBRE AIRONET WIRELESS SECURITY
- El dominio de red inalámbrica mantiene el AP como ejemplo de la configuración de servidor AAA
- Soporte Técnico y Documentación - Cisco Systems