Autenticación EAP en ACS 5.3 con los Puntos de acceso

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Configurar Configuración con el GUI Defina el servidor de la autenticación Configure ACS Configure el SSID Configuración con el CLI Verificación Troubleshooting estado-máquina del authenticator de la depuración dot11 aaa autenticación de RADIUS de la depuración

Introducción

Este documento describe una configuración de muestra de un punto de acceso basado en programas del ^{® del} Cisco IOS para la autenticación del Protocolo de Autenticación Extensible (EAP) de los usuarios de red inalámbrica contra una base de datos alcanzada por un servidor de RADIUS.

El AP puentea los paquetes inalámbricos del cliente en los paquetes atados con alambre destinados al servidor de la autenticación y vice versa. Porque el AP juega esto rol pasivo en EAP, esta configuración se utiliza con virtualmente todos los métodos EAP. Estos métodos incluyen, pero no se limitan a, EAP ligero (SALTO), EAP protegido (PEAP) - versión 2 del protocolo microsoft challenge handshake authentication (MSCHAP), la placa Token PEAP-genérica (GTC), autenticación adaptable de EAP vía el Tunelización seguro (RÁPIDO), Seguridad de la capa del EAP-transporte (TLS), y TLS EAP-hecho un túnel (TTL). Usted debe configurar apropiadamente el servidor de la autenticación para cada uno de estos métodos EAP.

Este documento describe cómo configurar el AP y al servidor de RADIUS, que es Cisco Secure Access Control Server (ACS) 5.3 en esta configuración de muestra.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Familiaridad con el GUI del software del Cisco IOS o el comando line interface(cli)
- Familiaridad con los conceptos de autenticación EAP

Componentes Utilizados

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

- Cisco Aironet 3602 Puntos de acceso que funciona con el Cisco IOS Software Release 15.2(2)JB
- Cisco Secure Access Control Server 5.3

Este ejemplo de la configuración asume que hay solamente un VLA N en la red.

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.

Configurar

Este documento utiliza esta configuración para el GUI y el CLI:

- La dirección IP del AP es 10.105.136.11.
- La dirección IP del servidor de RADIUS (el ACS) es 10.106.55.91.

Configuración con el GUI

Defina el servidor de la autenticación

Este procedimiento describe cómo definir el servidor de la autenticación y establecer una relación con él.

- 1. En el GUI AP, navegue a la **Seguridad > al administrador de servidor**.
- 2. En los servidores corporativos seccione, ingrese el IP address del servidor de la autenticación (10.106.55.91) en el campo del servidor.
- 3. Especifique el secreto compartido, el puerto de autenticación, y el puerto de las estadísticas. Usted puede utilizar los puertos 1813, 1814 o 1645, 1646.
- 4. Haga clic **se aplican** para crear la definición y poblar las listas desplegables.

- 5. En la sección de prioridades del servidor del valor por defecto, fije el campo de la prioridad 1 de la autenticación EAP a la dirección IP del servidor (**10.106.55.91**).
- 6. Haga clic en Apply (Aplicar).

-ili-ili- cisco	HOME NETWORK ASSOCIATION WERELESS	SECURITY SERVICES SOFTWARE EVENT LOD	5494	Configuration [Eng Legent
Committee .				Intel Const Carter
security	Corporate Servers			
Admin Access Encryption Manager SSID Manager Server Manager AP Authentication Intrusion Detection Local RADBUS Server Advance Sec_PRy	Current Server Lint FADLUS • 10.705 55 97 Delete	Server: Shared Secret: Authentication Part septional; Accounting Part septional; Constraints (constraints); Constraints (constraints); Constraints); Constraints (constraints); Constraints;	(Hodhame or IP Address)	Apply Concel
	Default Server Priorities			
	EAP Authentication	MAC Authentication	Accounting	
	Priority 1: 10 106 55 91 •	Priority 1: < NONE > *	Priority 1: < NONE > •	
	Priority 2 <none> •</none>	Priority 2. < NOVE > •	Priority 2 < NONE > •	
	Priority 3: *	Priprity 2: < NONE >	Priority 3: < NONE > *	
	Admin Authentication (FADR/S)	Admin Authentication (UACACS+)		
	Priority 1: < NONE > •	Priority 1: < NONE > *		
	Priority 2 <none> •</none>	Priority 2: < NONE > *		
	Priority 3: <none> •</none>	Priority 2: < NONE > *		
				Apply Cancel

Configure ACS

Si usted envía a los usuarios a un servidor de RADIUS externo, el AP necesita ser un cliente del Authentication, Authorization, and Accounting (AAA) para este servidor de RADIUS externo. Este procedimiento describe cómo configurar el ACS.

1. En el GUI seguro de Cisco ACS, **recursos de red del** tecleo. En ACS 5.3, los dispositivos se pueden agrupar por las ubicaciones.

cisco Cisco Secure	ACS	assadinin assidi (Primary) Log Out Acout Het
My Workspace Millsome	Welcome to Cisco Secure Access Control System	
Task Guide Guick Start Ivitial System Setup Policy Setup Setup Wy Account	Before You Begin Essential Reading to Get Started ACS Policy Model & Terninology 12	New in ACS 5 Managing Network Devices Cf Managing Users & Mertilles Cf Creating At Marianing Policies Cf
Son Network Resources Son Security Secu	Setting Started	D Tutorials & Other Resources

 Cree una ubicación. Bajo grupos de dispositivos de red, haga clic la ubicación. El tecleo crea la nueva ubicación. En el campo de nombre, ingrese un nombre de la ubicación (IOS_lab). Ingrese una descripción (LABORATORIO IOS) para esta ubicación. Seleccione al general todas las ubicaciones como la ubicación del padre. El tecleo somete para validar.

 St My Workspace 	Report Resources > Network Device Onoups > Location > Edit "Locations IOB_lat"				
- 🤯 Network Resources	Paulo deux deux				
 Network Device Orougs Location 	o Name: IOS_bb				
Device Type	Description: IOS LAB				
Network Devices and AAA Cients Defendt Network Device	o Parent All Locations Select				
External Proxy Servers	Required fields				
Users and Identity Stores					

3. Cree a un grupo para el IOS APs. Haga clic el tipo de dispositivo. El tecleo crea para crear a un nuevo grupo. En el campo de nombre, ingrese un nombre del grupo (IOS_APs). Ingrese una descripción (IOS APs en el LABORATORIO) para este grupo. Seleccione todos los tipos de dispositivo como el padre. El tecleo somete para validar.

😚 My Wasapace	Network Resources	Network Device Oroups > Device Type	Edit. 'Device Type Al Device Types IOS_APs'	
😝 Network Resources				
Network Device Drougs	Device Group	General		
Location	Name:	IOS_APs		
Device Type	Description:	IOS APs in the LAB		
Network Devices and AAA Clients		Al Device Types	Select	
External Proxy Servers	• = Required fe	ids		
38 Users and identity Stores	and the second second			

 Agregue el AP. Haga clic los dispositivos de red y a los clientes AAA. En el campo de nombre, ingrese el nombre de su IOS AP (AP). Ingrese una descripción para ese AP (IOS AP).

Bajo grupos de dispositivos de red, al lado del campo de la ubicación, haga clic **selecto**, controle el cuadro al lado de IOS_lab, y haga clic la **AUTORIZACIÓN** para validar. Bajo IP address, sea solo IP address se activa sure, y ingresan el IP address de su AP (10.105.136.11).

Bajo opciones de autenticación, controle el **RADIUS**. En el campo **secreto compartido**, ingrese un secreto (**Cisco**). Guarde los otros valores a sus valores por defecto. El tecleo **somete** para validar.

+ 🕤 My Workspace	Network Resources > Network	Devices and AAA Clients > Edit "Ish_AP"			
+ 😝 Network Resources					
 Network Device Groups 	o Name: 🐟 AP				
Location	Description 108 AP				
Device Type	Network Device Groups				
Party & Network Desize	Location	Al Locations IOS_lab	Select		
External Proxy Servers	Device Type	All Device Types KOS_APs	Select		
+ 🐉 Users and Identity Stores					
+ Qu Policy Elements	IP Address		Au	Authentication Options	
+ C Access Policies	Single IP Address	IP Range(s) By Mask		PAPALIS D	
Nostoring and Reports	O P. 10.105.136.11				
				Shared Secret Cisco	
 Share water (0, 1000) 				CsAport 1700	

5. Agregue las credenciales del usuario de red inalámbrica. Navegue a los usuarios y la identidad salva > los grupos de la identidad. El tecleo crea para crear a un nuevo grupo. En el campo de nombre, ingrese un nombre del grupo (EAP_Users). Ingrese una descripción (usuarios para la Tecnología inalámbrica EAP). El tecleo somete para validar.

+ 🚭 My Workspace	Users and identity Stores > identity Groups > Edit. "identityGroup AI Groups EAP_Users"
 Network Resources 	- Court
 B Users and Identity Stores 	Name EAP_Users
· Memaliferity Stores	Description. Users for EAP wineless
Users	Parent Al Drosps Seect
+ External Identity Stores	Required fields

6. Cree a un usuario en este grupo. Haga clic a los usuarios. El tecleo crea para crear a un usuario nuevo. En el campo de nombre, ingrese un username (radio). Asegúrese de que el estatus del usuario esté activado. Ingrese una descripción para el usuario (radio de la prueba). Al lado del campo del grupo de la identidad, haga clic selecto, controle el cuadro al lado de EAP_Users, y haga clic la AUTORIZACIÓN para validar.

Bajo la información de contraseña, ingrese el **<password>** en la contraseña y confirme los campos de contraseña. Porque este usuario necesita el acceso a la red pero no necesita el acceso a ningún dispositivo de Cisco para la Administración, no hay necesidad de una contraseña del permiso.

+ 😚 Ny Waterpace	Users and klendby Stores > Internal Identity Stores > Users > Create	
Soft Network Resources Soft Network Resources Monthy Orcups Internal Identity Stores Units Hasts	General General Status Erabled	
Edemaildently Stores LDNP Active Directory RSA Securit Directory RSA Securit Directory RADUS Idently Servers Conflicate Authorities Conflicate AuthoriticsIon Profile Identify Stare Sequences	Password Information Password Inust • Contail 4 - 32 characters • Password Type: Internal Users • Password • Confirm Password • • • • • • • • • • • • • • •	Enable Password Information Password must • Contain 4 - 33 characters Enable Password Confirm Password
Policy Elements Case Profices Mentoring and Reparts System Administration	Change password on rest login User Information There are no additional identity attributes defined for user recends er = Required fields	

- 7. El tecleo somete para validar. El usuario nuevo aparece en la lista, y el ACS está listo ahora.
- 8. Navegue a los elementos de la directiva > a la autorización y a los permisos > a los perfiles del acceso a la red > de la autorización para verificar que conceden el usuario el permiso de acceso. Debe haber un perfil de PermitAccess. Conceden los usuarios que reciben este perfil el acceso a la red.

 My Warkspace 	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles				
Network Resources	Authorization Profiles	Showing 1-2 of 2 50 + per page Ge			
B Users and klentity Stores	Fiber Match # 00 V				
 Pelicy Elements 	In the December				
 Session Conditions 	Name A Description				
Date and Time	MARTEST Mab WLC test users in Vian 30				
Custom • Network Conditions End Station Filters Device Filters	Permt Access				
Device Part Filters Authorization and Permissions • Network Access • Device Administration Shell Profiles Command Sets					

 Navegue a las políticas de acceso > a los servicios del acceso > al dispositivo Admin del valor por defecto para examinar la autorización. Asegúrese de que la identidad, la asignación del grupo, y la autorización estén controladas.

 My Workspace 	Access Policies > Access Benices > Defaul Device Amin > Edit. "Default Device Admin"
+ 🎲 Notwork Resources	
B Users and Identity Stores	General Allower Protocols
Policy Elements	Name: Default Device Admin
🔹 🛼 Access Policies	Descriptor: Default Device Administration Access Benvice
Access Services El Service Selection Failes O Secul Device Anno Idently Authenzation O Default Network Access Idently	Service Type: Device Administration * Policy Structure V Identity Change Mapping Authorization

10. Haga clic los **protocolos permitidos** tabulación, seleccione los cuadros para los métodos EAP requeridos, y el tecleo **somete** para validar.

• 🚭 Ny Watispace	Access Policies > Access Benices > Cetault Device Admin > Edit "Default Device Admin"
+ 😓 Network Resources	General Allowed Protocols
 B Users and Identity Stores Policy Elements 	Process Hist Laokap Authentisation Protocole
Access Policies Access Services Bervice Selection Rules	Alow PAPINSCI Z Alow CHAP
	 ■ Alaw MS-CHAPv1 ■ Alaw MS-CHAPv2
Authorization Authorization Authorization Max User Session Policy Max Session User Settings	Z Alaw EAP-MD6 Z Alaw EAP-TLS
Max Session Group Settings	
	PEAP Inter Methods Allow EAP-NLS Allow EAP-MS-CHAPv2

Configure el SSID

Este procedimiento describe cómo configurar el Service Set Identifier (SSID) en el AP.

1. En el GUI seguro de Cisco ACS, navegue a la **Seguridad** > al **administrador SSID**. Haga clic **nuevo**, ingrese el nombre SSID (**radio**), active ambas interfaces radio, y el tecleo **se aplica**.

cisco	HOME RETWORK SECONTION WIRELESS SECURITY SERVICES	SOLLWARE EVENTION		Saga Catfiguration Eng Lagout Editedi
Security	Hutsane ap			ap optime is 3 days, 4 hours, 47 minutes
Encryption Manager	Scourty: Global SSID Manager			
SSID Maxager	SSID Properties			#
Server Manager	Current SSID List			
Intrusion Detection	< NEW > A	SSD:	atius	
Local RADIUS Server	tedias	VLAN	KNONE S . Define VLANK	
Advance Security			Dathap 1:	
	*		Backup 2:	
			Backup 2	
		Band-Select:	C Band Select	
		Interface:	☑ Radis0-802 11M ^{2,40Hz} ☑ Radis1-002 11M ^{43Pb}	
		Network ID:	(0-4096)	

2. Navegue al **encargado de la Seguridad** > del **cifrado**, **AES** selecto **CCMP** como la cifra, y haga clic Aplicar-todo para aplicar este cifrado en ambas radios.



3. Navegue a la **Seguridad** > al **administrador SSID**, y seleccione el **radio** SSID. En la autenticación de cliente las configuraciones seccionan, controlan la **autenticación abierta**, selecta **con EAP de la** lista desplegable, y de la **red EAP del** control.

En el cliente la sección de administración de claves autenticada, **obligatorio** selecto de la lista desplegable de la administración de claves, controla el **permiso WPA**, y selecciona **WPAv2 de la** lista desplegable. Haga clic en Apply (Aplicar).

cisco	Howe Betwork Resocration wirelies Becalety	SERVICES SOFTWARE EVENTION		Sage Configuration Bing Logout Befreih
Security	Client Aufourtication Satings			
Admin Access Encryption Manager SSID Manager Server Manager AP Authentication Intrasien Detection	Methods Accepted: Coper Astheritication Shared Astheritication: Itaiwook EAP:	<pre>>>hEAP <no addition=""> <no addition=""> </no></no></pre>	×	
Local RADIUS Server Advance Security	Server Priorities: EAP Authentication Servers Use Outwarks <u>Extine Defaultion</u> Containing Priority 1: < <u>NONE > </u> Priority 2: < <u>NONE > </u> Priority 3: < <u>NONE > </u>		IIAC Authentication Servers Use Datases Determine Priority 1 < <u>NONE></u> Priority 2 < <u>NONE></u> Priority 3 < <u>NONE></u>	
	Client Authenticated Key Management			
	Key Management:	Navistory 💌	CCHM	1

4. Para difundir este SSID en ambas radios, encuentre la sección de las configuraciones del modo de invitado/de la infraestructura SSID en la misma página. Para ambas radios, fije el modo del faro para escoger BSSID, y para seleccionar el nombre SSID (radio) de la lista desplegable del solo modo de invitado SSID del conjunto. Haga clic en Apply (Aplicar).

Redio0.882.11N ^{2.4CH2} :		
Set Beacon Mode:	Single 8550 Set Single Guest Mode SSID Indus	
	O Multiple BSSID	
Set Infrastructure SSID	NONE > Force Infrastructure Devices to associate only to this SSID	
Redio1.802.11N ^{5GRz} :		
Set Beacon Mode:	Single BSSD Set Single Guest Mode SSD. Indius	
	© Multiple BSSID	
Set Infrastructure SSD	NONE > Force Infrastructure Devices to associate only to this SSID	
		Apply Cancel

5. Navegue a la **red** > al **interfaz de red** > a **Radio0-802.11n 2G.Hz** > las **configuraciones** > **permiso** para activar ambas interfaces radio.

6. Pruebe la Conectividad del cliente.

Configuración con el CLI

Notas:

Use la <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos usados en esta sección.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Ésta es la misma configuración hecha dentro del CLI:

```
show run
Building configuration...
Current configuration : 2511 bytes
!
! Last configuration change at 01:17:48 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
1
logging rate-limit console 9
enable secret 5 $1$1u04$jr7DG0DC5KZ6bVaSYUhck0
aaa new-model
!
1
aaa group server radius rad_eap
server 10.106.55.91
!
aaa group server radius rad_mac
1
aaa group server radius rad_acct
1
aaa group server radius rad_admin
1
aaa group server tacacs+ tac_admin
1
aaa group server radius rad_pmip
aaa group server radius dummy
1
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
```

```
1
1
1
aaa session-id common
ip cef
1
ip dhcp pool test
1
1
1
dot11 syslog
1
dot11 ssid radius
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa version 2
  guest-mode
!
!
crypto pki token default removal timeout 0
1
!
username Cisco password 7 0802455D0A16
1
1
bridge irb
!
1
1
interface Dot11Radio0
no ip address
 1
 encryption mode ciphers aes-ccm
 !
 ssid radius
 1
 antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
Ţ.
interface Dot11Radio1
 no ip address
 1
 encryption mode ciphers aes-ccm
 !
 ssid radius
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
```

```
1
interface GigabitEthernet0
no ip address
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
1
interface BVI1
ip address 10.105.136.11 255.255.255.128
1
ip default-gateway 10.105.136.1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.105.136.1
ip radius source-interface BVI1
1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.106.55.91 key 7 00271A1507545A545C606C
radius-server vsa send accounting
1
bridge 1 route ip
1
1
1
line con 0
line vty 0 4
transport input all
1
end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Conecte al cliente; después de la autenticación satisfactoria, éste es el resumen de la configuración que aparece en el GUI AP:

cisco	HOME METWORK ASSOCIAT	non womeness	proven previces portwo	WE EVENTION		Tage Configuration	on I Dud I Fritton I Bayers	
Home Summary > Easy Setup	Hostname op					**	gtime is 1 hour, 21 minutes	
	Association							
	Overts: 1	12		Instants-structure clients: 0				
	View IC Client IC Industruction class						Avera	
	Factor Rel. 1997 ATM							
	SSDraikes :							
	Device Type	Harmo	# Address	MACAderes	State	Parent	VLAN	
	unknowth	NONE	10105136116	\$1000.7175.218m4	6AP-Associated	set	none	

Nota: <u>La herramienta de interpretación de información de salida (disponible para clientes</u> registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

En el CLI, ingrese el comando show dot11 associations para confirmar la configuración:

802.11 Client Stations on Dot11Radio0:

SSID [radius] :

MAC AddressIP addressDeviceNameParentStatef8db.7f75.780410.105.136.116unknown-selfEAP-Assoc

Usted puede también ingresar el **comando show radius server-group all** para visualizar una lista de todos los grupos de servidores configurados del RADIO en el AP.

Troubleshooting

Este procedimiento describe cómo resolver problemas su configuración.

- 1. En la utilidad o el software del cliente-lado, cree un nuevo perfil o conexión con el mismo o los parámetros similares para asegurarse de que nada se ha corrompido en la configuración del cliente.
- 2. Los problemas del Radiofrecuencia (RF) pueden prevenir la autenticación satisfactoria. Temporalmente autenticación de la neutralización para eliminar esta posibilidad:

Del CLI, ingrese estos comandos:

ningunos eap_methods abiertos del eap de la autenticaciónningunos eap_methods de la redeap de la autenticaciónautenticación abierta

Del GUI, en la página del administrador SSID, uncheck la **red-EAP**, controle **abierto**, y fije la lista desplegable a **ninguna adición**.

Si el cliente se asocia con éxito, el RF no contribuye al problema de asociación.

3. Verifique que las contraseñas del secreto compartido estén sincronizadas entre el AP y el servidor de la autenticación. Si no, usted puede ser que reciba este mensaje de error:

Invalid message authenticator in EAP request **Del CLI, controle la línea**:

radius-server host x.x.x.x auth-port x acct-port x key <shared_secret> Del GUI, en la página del administrador de servidor, entre el secreto compartido de nuevo para el servidor apropiado en el campo del secreto compartido.

La entrada del secreto compartido para el AP en el servidor de RADIUS debe contener la misma contraseña del secreto compartido.

4. Elimine cualquier grupo de usuarios del servidor RADIUS. Los conflictos pueden ocurrir entre los grupos de usuarios definidos por el servidor de RADIUS y los grupos de usuarios en el dominio subyacente. Controle los registros del servidor de RADIUS para los intentos fallidos y para saber si hay las razones de los errores. Nota: Consulte <u>Información Importante sobre Comandos de Debug</u> antes de usar un **comando debug**.

Utilice estos comandos debug para investigar y visualizar las negociaciones entre los dispositivos:

- · ponga a punto la estado-máquina del authenticator dot11 aaa
- ponga a punto la autenticación de RADIUS
- debug aaa authentication

ponga a punto la estado-máquina del authenticator dot11 aaa

Este comando visualiza las divisiones importantes (o los estados) de la negociación entre el cliente y el servidor de la autenticación. Éste es un ejemplo de la salida de una autenticación satisfactoria:

```
ap#debug dot11 aaa authenticator state-machine
state machine debugging is on
ap#
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Sending identity
request to f8db.7f75.7804
*Mar 1 01:38:34.919: dot11_auth_dot1x_send_id_req_to_client: Client
f8db.7f75.7804 timer started for 30 seconds
*Mar 1 01:38:35.431: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:35.431: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 01:38:35.435: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.435: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:35.435: dot11 auth dot1x send response to client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:35.443: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:35.443: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 01:38:35.447: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:35.447: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
-----Lines Omitted for simplicity-----
*Mar 1 01:38:36.663: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.663: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.667: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,
CLIENT_REPLY) for f8db.7f75.7804
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Sending client
f8db.7f75.7804 data to server
*Mar 1 01:38:36.667: dot11_auth_dot1x_send_response_to_server: Started timer
```

server_timeout 60 seconds
*Mar 1 01:38:36.671: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,
SERVER_PASS) for f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Forwarding server
message to client f8db.7f75.7804
*Mar 1 01:38:36.671: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds
*Mar 1 01:38:36.719: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]

autenticación de RADIUS de la depuración

Este comando visualiza las negociaciones RADIUS entre el servidor y el cliente, que son puenteadas por el AP. Éste es un ejemplo de la salida de una autenticación satisfactoria:

ap#debug radius authentication

*Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6):Orig. component type = DOT11 *Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: ssid [347] 6 *Mar 1 01:50:50.635: RADIUS: 72 61 64 69 [radi] *Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: service-type [345] 4 1 *Mar 1 01:50:50.635: RADIUS: AAA Unsupported Attr: interface [222] 3 *Mar 1 01:50:50.635: RADIUS: 32 [2] *Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11 *Mar 1 01:50:50.635: RADIUS(000001F6): Config NAS IPv6: *Mar 1 01:50:50.635: RADIUS/ENCODE(000001F6): acct_session_id: 491 1 01:50:50.635: RADIUS(000001F6): Config NAS IP: 10.105.136.11 *Mar *Mar 1 01:50:50.635: RADIUS(000001F6): sending *Mar 1 01:50:50.635: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645 id 1645/73, len 140 *Mar 1 01:50:50.635: RADIUS: authenticator OF 74 18 0E F3 08 ED 51 -8B EA F7 31 AC C9 CA 6B *Mar 1 01:50:50.635: RADIUS: User-Name [1] 8 "radius" *Mar 1 01:50:50.635: RADIUS: Framed-MTU [12] 6 1400 1 01:50:50.635: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90: *Mar radius" *Mar 1 01:50:50.635: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804" *Mar 1 01:50:50.635: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 01:50:50.635: RADIUS: Message-Authenticato[80] 18 *Mar 1 01:50:50.635: RADIUS: E3 E1 50 F8 2B 22 26 84 C1 F1 76 28 79 70 5F 78 [P+"&v(yp_x] *Mar 1 01:50:50.635: RADIUS: EAP-Message [79] 13 1 01:50:50.635: RADIUS: 02 01 00 0B 01 72 61 64 69 75 73 *Mar [radius] *Mar 1 01:50:50.635: RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19] *Mar 1 01:50:50.635: RADIUS: NAS-Port [5] 6 282 *Mar 1 01:50:50.635: RADIUS: NAS-Port-Id [87] 5 "282" *Mar 1 01:50:50.635: RADIUS: NAS-IP-Address [4] 6 10.105.136.11 *Mar 1 01:50:50.635: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 01:50:50.635: RADIUS(000001F6): Sending a IPv4 Radius Packet *Mar 1 01:50:50.635: RADIUS(000001F6): Started 5 sec timeout *Mar 1 01:50:50.639: RADIUS: Received from id 1645/73 10.106.55.91:1645, Access -Challenge, len 94 *Mar 1 01:50:50.639: RADIUS: authenticator 5E A4 A7 B9 01 CC F4 20 -2E DO 2A 1A A4 58 05 9E *Mar 1 01:50:50.639: RADIUS: State [24] 32 *Mar 1 01:50:50.639: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35 [27SessionID=acs5] *Mar 1 01:50:50.639: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [1 /165489511/9;]

*Mar 1 01:50:50.639: RADIUS: EAP-Message [79] 24 *Mar 1 01:50:50.639: RADIUS: 01 DC 00 16 11 01 00 08 00 CB 2A 0A 74 B3 77 AF 72 61 64 69 75 73 [*twradius] *Mar 1 01:50:50.639: RADIUS: Message-Authenticato[80] 18 *Mar 1 01:50:50.643: RADIUS: CC 44 D5 FE FC 86 BC 2D B0 89 61 69 4F 34 D1 FF [D-ai04] *Mar 1 01:50:50.643: RADIUS(000001F6): Received from id 1645/73 1 01:50:50.643: RADIUS/DECODE: EAP-Message fragments, 22, total 22 bytes *Mar *Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6):Orig. component type = DOT11 *Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: ssid [347] 6 *Mar 1 01:50:50.647: RADIUS: 72 61 64 69 [radi] *Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: service-type [345] 4 1 *Mar 1 01:50:50.647: RADIUS: AAA Unsupported Attr: interface [222] 3 *Mar 1 01:50:50.647: RADIUS: 32 [2] *Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11 *Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IPv6: *Mar 1 01:50:50.647: RADIUS/ENCODE(000001F6): acct_session_id: 491 *Mar 1 01:50:50.647: RADIUS(000001F6): Config NAS IP: 10.105.136.11 *Mar 1 01:50:50.647: RADIUS(000001F6): sending *Mar 1 01:50:50.647: RADIUS(000001F6): Send Access-Request to 10.106.55.91:1645 id 1645/74, len 167 *Mar 1 01:50:50.647: RADIUS: authenticator C6 54 54 B8 58 7E ED 60 - F8 E0 2E 05 B0 87 3B 76 *Mar 1 01:50:50.647: RADIUS: User-Name [1] 8 "radius" *Mar 1 01:50:50.647: RADIUS: Framed-MTU [12] 6 1400 *Mar 1 01:50:50.647: RADIUS: Called-Station-Id [30] 26 "1C-E6-C7-E1-D8-90: radius" *Mar 1 01:50:50.647: RADIUS: Calling-Station-Id [31] 16 "f8db.7f75.7804" *Mar 1 01:50:50.647: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 01:50:50.647: RADIUS: Message-Authenticato[80] 18 *Mar 1 01:50:50.647: RADIUS: FE 15 7B DB 49 FE 27 C5 BC E2 FE 83 B9 25 8C 1F [{I'?] *Mar 1 01:50:50.647: RADIUS: EAP-Message [79] 8 *Mar 1 01:50:50.647: RADIUS: 02 DC 00 06 03 19 *Mar 1 01:50:50.647: RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19] *Mar 1 01:50:50.647: RADIUS: NAS-Port [5] 6 282 *Mar 1 01:50:50.647: RADIUS: NAS-Port-Id [87] 5 "282" *Mar 1 01:50:50.647: RADIUS: State [24] 32 *Mar 1 01:50:50.647: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35 [27SessionID=acs5] *Mar 1 01:50:50.647: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [1 /165489511/9;] *Mar 1 01:50:50.647: RADIUS: NAS-IP-Address [4] 6 10.105.136.11 *Mar 1 01:50:50.647: RADIUS: Nas-Identifier "ap" [32] 4 *Mar 1 01:50:50.647: RADIUS(000001F6): Sending a IPv4 Radius Packet *Mar 1 01:50:50.647: RADIUS(000001F6): Started 5 sec timeout *Mar 1 01:50:50.647: RADIUS: Received from id 1645/74 10.106.55.91:1645, Access -Challenge, len 78 *Mar 1 01:50:50.647: RADIUS: authenticator 0E 81 99 9E EE 39 50 FB - 6E 6D 93 8C 8E 29 94 EC *Mar 1 01:50:50.647: RADIUS: State [24] 32 *Mar 1 01:50:50.651: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35 [27SessionID=acs5] *Mar 1 01:50:50.651: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [1 /165489511/9;] *Mar 1 01:50:50.651: RADIUS: EAP-Message [79] 8 *Mar 1 01:50:50.651: RADIUS: 01 DD 00 06 19 21 [!] *Mar 1 01:50:50.651: RADIUS: Message-Authenticato[80] 18 *Mar 1 01:50:50.651: RADIUS: A8 54 00 89 1F 2A 01 52 FE FA D2 58 2F E5 F2 86 [T*RX/] *Mar 1 01:50:50.651: RADIUS(000001F6): Received from id 1645/74

*Mar 1 01:50:50.651: RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes *Mar 1 01:50:50.655: RADIUS/ENCODE(000001F6):Orig. component type = DOT11 *Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: ssid [347] 6 *Mar 1 01:50:50.655: RADIUS: 72 61 64 69 [radi] *Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: service-type [345] 4 1 *Mar 1 01:50:50.655: RADIUS: AAA Unsupported Attr: interface [222] 3 -----Lines Omitted for simplicity------[12^w\$qM{60] 11 *Mar 1 01:50:51.115: RADIUS: NAS-Port-Type [61] 6 802.11 wireless [19] *Mar 1 01:50:51.115: RADIUS: NAS-Port [5] 6 2.82 1 01:50:51.115: RADIUS: NAS-Port-Id [87] 5 *Mar "282" *Mar 1 01:50:51.115: RADIUS: State [24] 32 *Mar 1 01:50:51.115: RADIUS: 32 37 53 65 73 73 69 6F 6E 49 44 3D 61 63 73 35 [27SessionID=acs5] *Mar 1 01:50:51.115: RADIUS: 31 2F 31 36 35 34 38 39 35 31 31 2F 39 3B [1 /165489511/9;1 *Mar 1 01:50:51.115: RADIUS: NAS-IP-Address [4] 6 10.105.136.11 1 01:50:51.115: RADIUS: Nas-Identifier [32] 4 *Mar "ap" *Mar 1 01:50:51.115: RADIUS(000001F6): Sending a IPv4 Radius Packet *Mar 1 01:50:51.115: RADIUS(000001F6): Started 5 sec timeout *Mar 1 01:50:51.115: RADIUS: Received from id 1645/80 10.106.55.91:1645, Access -Challenge, len 115 *Mar 1 01:50:51.115: RADIUS: authenticator 74 CF 0F 34 1F 1B C1 CF -E9 27 79 D5 F8 9C 5C 50 *Mar 1 01:50:51.467: %DOT11-6-ASSOC: Interface Dot11Radio0, Station f8db.7f75.7804 Associated KEY_MGMT[WPAv2]

debug aaa authentication

Este comando visualiza las Negociaciones AAA para autenticación entre el dispositivo cliente y el servidor de la autenticación.

```
ap#debug aaa authentication
AAA Authentication debugging is on
ap#term mon
ap#
*Mar 1 01:55:52.335: AAA/BIND(000001F9): Bind i/f
*Mar
     1 01:55:52.859: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.867: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.875: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:52.895: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.219: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.379: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.395: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
     1 01:55:53.807: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar
*Mar 1 01:55:53.879: AAA/AUTHEN/PPP (000001F9): Pick method list 'eap_methods'
*Mar 1 01:55:53.939: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
f8db.7f75.7804 Associated KEY_MGMT[WPAv2]
```