Ejemplo de configuración de acceso Wi-Fi protegido (WPA) en una red inalámbrica unificada de Cisco

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Convenciones** Compatibilidad con WPA y WPA2 Configuración de la red Configuración de los dispositivos para el modo WPA2 Enterprise Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo Configuración de la WLAN para el modo de funcionamiento empresarial de WPA2 Configuración del servidor RADIUS para la autenticación de modo empresarial WPA2 (EAP-FAST) Configuración del cliente inalámbrico para el modo de funcionamiento de WPA2 Enterprise Configuración de los dispositivos para el modo WPA2 Personal Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar el acceso Wi-Fi protegido (WPA) en una red inalámbrica unificada de Cisco.

Prerequisites

Requirements

Asegúrese de tener conocimientos básicos de estos temas antes de intentar esta configuración:

- WPA
- Soluciones de seguridad para redes LAN inalámbricas (WLAN)Nota: Consulte <u>Descripción</u> <u>general de la seguridad de LAN inalámbrica de Cisco</u> para obtener información sobre las soluciones de seguridad de WLAN de Cisco.

Componentes Utilizados

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

- Punto de acceso ligero (LAP) Cisco serie 1000
- Controlador de LAN inalámbrica (WLC) Cisco 4404 que ejecuta el firmware 4.2.61.0
- Adaptador de cliente Cisco 802.11a/b/g que ejecuta firmware 4.1
- Aironet Desktop Utility (ADU) que ejecuta firmware 4.1
- Servidor Cisco Secure ACS versión 4.1

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Compatibilidad con WPA y WPA2

Cisco Unified Wireless Network es compatible con las certificaciones Wi-Fi Alliance WPA y WPA2. WPA fue introducido por Wi-Fi Alliance en 2003. WPA2 fue introducido por Wi-Fi Alliance en 2004. Todos los productos con certificación Wi-Fi para WPA2 deben ser interoperables con productos con certificación Wi-Fi para WPA.

WPA y WPA2 ofrecen un alto nivel de garantía a los usuarios finales y los administradores de red de que sus datos seguirán siendo privados y de que el acceso a sus redes estará restringido a los usuarios autorizados. Ambos tienen modos de funcionamiento personal y empresarial que satisfacen las distintas necesidades de los dos segmentos de mercado. El modo empresarial de cada uno utiliza IEEE 802.1X y EAP para la autenticación. El modo personal de cada uno utiliza una clave precompartida (PSK) para la autenticación. Cisco no recomienda el modo personal para implementaciones empresariales o gubernamentales porque utiliza una PSK para la autenticación de usuarios. PSK no es seguro para entornos empresariales.

WPA aborda todas las vulnerabilidades WEP conocidas en la implementación de seguridad IEEE 802.11 original, lo que aporta una solución de seguridad inmediata a las WLAN en entornos empresariales y de pequeña oficina/oficina doméstica (SOHO). WPA utiliza TKIP para la encriptación.

WPA2 es la última generación en seguridad Wi-Fi. Es la implementación interoperable de la Wi-Fi Alliance del estándar IEEE 802.11i ratificado. Implementa el algoritmo de cifrado AES recomendado por el Instituto Nacional de Normas y Tecnología (NIST) mediante el modo de recuento con el protocolo de código de autenticación de mensajes en cadena para el bloqueo de cifrado (CCMP). WPA2 facilita el cumplimiento gubernamental de FIPS 140-2.

Comparación de los tipos de modo WPA y WPA2

	WPA	WPA2
Modo empresarial	Autenticaci	 Autenticaci
(empresas, gobierno,	ón: IEEE	ón: IEEE
educación)	802.1X/EA	802.1X/EA

	P • Cifrado: TKIP/MIC	P • Cifrado: AES- CCMP
Modo personal (SOHO, doméstico/personal)	 Autenticaci ón: PSK Cifrado: TKIP/MIC 	 Autenticaci ón: PSK Cifrado: AES- CCMP

En el modo de funcionamiento empresarial, tanto WPA como WPA2 utilizan 802.1X/EAP para la autenticación. 802.1X proporciona a las WLAN una autenticación sólida y mutua entre un cliente y un servidor de autenticación. Además, 802.1X proporciona claves de cifrado dinámicas por usuario y por sesión, lo que elimina la carga administrativa y los problemas de seguridad relacionados con las claves de cifrado estáticas.

Con 802.1X, las credenciales utilizadas para la autenticación, como las contraseñas de inicio de sesión, nunca se transmiten sin cifrar o sin cifrado a través del medio inalámbrico. Aunque los tipos de autenticación 802.1X proporcionan una autenticación sólida para las LAN inalámbricas, se necesitan TKIP o AES para el cifrado, además de 802.1X, ya que el cifrado WEP 802.11 estándar es vulnerable a los ataques a la red.

Existen varios tipos de autenticación 802.1X, cada uno de los cuales proporciona un enfoque diferente de la autenticación, al tiempo que se basa en el mismo marco y EAP para la comunicación entre un cliente y un punto de acceso. Los productos Cisco Aironet admiten más tipos de autenticación EAP 802.1X que cualquier otro producto WLAN. Entre los tipos admitidos se incluyen:

- <u>Cisco LEAP</u>
- EAP-autenticación flexible a través de tunelación segura (EAP-FAST)
- EAP-seguridad de la capa de transporte (EAP-TLS)
- Protocolo de autenticación extensible protegido (PEAP)
- EAP-TLS con túnel (EAP-TTLS)
- EAP-módulo de identidad del suscriptor (EAP-SIM)

Otra ventaja de la autenticación 802.1X es la gestión centralizada de los grupos de usuarios de WLAN, incluida la rotación de claves basada en políticas, la asignación de claves dinámicas, la asignación de VLAN dinámica y la restricción de SSID. Estas funciones giran las claves de cifrado.

En el modo de funcionamiento personal, se utiliza una clave previamente compartida (contraseña) para la autenticación. El modo personal sólo requiere un punto de acceso y un dispositivo cliente, mientras que el modo empresarial normalmente requiere un servidor RADIUS u otro servidor de autenticación en la red.

Este documento proporciona ejemplos para configurar WPA2 (modo Enterprise) y WPA2-PSK (modo Personal) en una red Cisco Unified Wireless.

Configuración de la red

En esta configuración, un Cisco 4404 WLC y un Cisco 1000 Series LAP se conectan a través de

un switch de capa 2. Un servidor RADIUS externo (Cisco Secure ACS) también está conectado al mismo switch. Todos los dispositivos están en la misma subred. El punto de acceso (LAP) se registra inicialmente en el controlador. Es necesario crear dos LAN inalámbricas, una para el modo WPA2 Enterprise y otra para el modo WPA2 Personal.

La WLAN en modo WPA2-Enterprise (SSID: WPA2-Enterprise) utilizará EAP-FAST para autenticar los clientes inalámbricos y AES para el cifrado. El servidor Cisco Secure ACS se utilizará como servidor RADIUS externo para autenticar los clientes inalámbricos.

La WLAN en modo WPA2-Personal (SSID: WPA2-PSK) utilizará WPA2-PSK para la autenticación con la clave previamente compartida "abcdefghijk".



Debe configurar los dispositivos para esta configuración:

WLC Management IP address: WLC AP Manager IP address: Wireless Client IP address:	10.77.244.204 10.77.244.205 10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Configuración de los dispositivos para el modo WPA2 Enterprise

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Siga estos pasos para configurar los dispositivos para el modo de funcionamiento de WPA2 Enterprise:

- 1. Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo
- 2. Configuración de la WLAN para la autenticación de modo empresarial WPA2 (EAP-FAST)
- 3. Configuración del cliente inalámbrico para el modo WPA2 Enterprise

Configure el WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario mediante EAP-FAST y proporciona acceso a los clientes inalámbricos.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

- 1. Elija **Seguridad** y **Autenticación RADIUS** en la GUI del controlador para mostrar la página Servidores de Autenticación RADIUS. Luego, haga clic en **Nuevo** para definir un servidor RADIUS.
- Defina los parámetros del servidor RADIUS en la página RADIUS Authentication Servers > New. Estos parámetros incluyen:Dirección IP de servidor RADIUSsecreto compartidonúmero de puertoEstado del servidorEste documento utiliza el servidor ACS con una dirección IP de 10.77.244.196.

					Sage Co	nfiguration <u>P</u> ing	Logout Befresh
cisco	MONITOR WLANS CONTRO	LLER WIRELESS	ECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication S	ervers > New				< Back	Apply
General	Server Index (Priority)	1 .					
 RADIUS Authentication 	Server IPAddress	10.77.244.196					
TACACS+ LDAP	Shared Secret Format	ASCII ·					
Local Net Users MAC Filtering	Shared Secret	•••••					
User Login Policies AP Policies	Confirm Shared Secret	****					
Local EAP	Key Wrap	(Designed for FIPS)	customers a	and requires a key	wrap compliant	RADIUS server)	
Priority Order	Dort Number	1012					
▶ Access Control Lists	Port Number	1012					
Wireless Protection Policies	Server Status	Enabled 💌					
Web Auth	Support for RFC 3576	Enabled 💌					
► Advanced	Server Timeout	2 seconds					
	Network User	Enable					
	Management	Enable					
	IPSec	Enable					

3. Haga clic en Apply (Aplicar).

Configuración de la WLAN para el modo de funcionamiento empresarial de WPA2

A continuación, configure la WLAN que utilizarán los clientes para conectarse a la red inalámbrica. El SSID de WLAN para el modo empresarial WPA2 será WPA2-Enterprise. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN y sus parámetros relacionados:

- 1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs.Esta página enumera las WLANs que existen en el controlador.
- 2. Haga clic en Nuevo para crear un nuevo WLAN.

 Introduzca el nombre SSID de WLAN y el nombre Profile en la página WLANs > New. A continuación, haga clic en Aplicar. Este ejemplo utiliza WPA2-Enterprise como SSID

allalla							Sa <u>v</u> e Co	onfiguration Ping	Logout Bef
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs>	New						< Back	Apply
WLANS WLANS	Туре		WLAN						
Advanced	Profile Na	me	WPA2-Ent	erprise					
	WLAN SSI	D	WPA2-Ent	erprise					

- 4. Una vez que haya creado una nueva WLAN, aparecerá la página WLAN > Edit para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, políticas de seguridad, políticas de QOS y parámetros avanzados.
- 5. En Políticas generales, marque la casilla de verificación Status para habilitar la



- 6. Si desea que el AP difunda el SSID en sus tramas de baliza, marque la casilla de verificación **Broadcast SSID**.
- Haga clic en la ficha Security (Seguridad). En Layer 2 Security, elija WPA+WPA2. Esto activa la autenticación WPA para la WLAN.

	Sage Configuration Bing Logout Befresh
WLANS	WLANs > Edit Apply General Security QoS Advanced
WLANS WLANS Advanced	Layer 2 Layer 3 AAA Servers
	Static WEP Parameters 802.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 0) Type Key Size Key Index Encryption Key
	WEP not set 1 ASCII Allow Shared Key Enabled CKIP Parameters Enabled
	B02.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Key Format not set 1 ASCII
	Foot Notes
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MFP is not active unless WPA2 is configured

 Desplácese hacia abajo por la página para modificar los parámetros WPA+WPA2. En este ejemplo, se seleccionan la política WPA2 y el cifrado AFS

.ANS	WLANS > Edit < Back Ap General Security QoS Advanced
MLANs dvanced	Layer 2 Layer 3 AAA Servers 802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0)
	Key Size Key Index Encryption Key Key Format not set 1 ASCII
	MMH Mode Enabled Key Permutation Enabled 802.1X Parameters Image: Construction of the second
	002.11 Data Encryption Type Key Size @ WEP 104 bits •
	WPA Policy
	WPA2 Encryption R AES TKIP Auth Key Mgmt 802.1X
	1 1
	Foot Notes I CKIP is not supported by IOxx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clien 5 Client MPP is not active unless WPA2 is configured

- 9. En Administración de claves de autenticación, elija **802.1x**.Esto habilita WPA2 usando autenticación 802.1x/EAP y cifrado AES para la WLAN.
- 10. Haga clic en la pestaña **AAA Servers**. En Servidores de autenticación, elija la dirección IP del servidor correspondiente.En este ejemplo, 10.77.244.196 se utiliza como servidor

ADIUS.		
արտիս	Save Configuration Ping Logo	ut <u>B</u> efre
CISCO	MONITOR MUANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
LANs	WLANs > Edit < Back	Apply
	General Security QoS Advanced	
WLANs	Laver 2 Laver 3 AAA Servers	
Advanced		
	Select AAA servers below to override use of default servers on this WLAN	
	Radius Servers LDAP Servers	
	Authentication Servers Accounting Servers Server 1 None 💌	
	Enabled Server 2 None	
	Server 19:10.77.244.196, Port:1812 • None • Server 3 None •	
	Server None None I	
	Server None V None V	
	3 Invite 21	
	Local EAP Authentication	
	Local EAP Authentication L Enabled	
	Foot Notes	
	1 CKIP is not supported by 10xx model APs	
	2 Web Folicy cannot be used in combination with IFsec. 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication	
	4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded 5 Client MFP is not active unless WPA2 is configured	clients)

11. Haga clic en Apply (Aplicar). Nota: Éste es el único parámetro EAP que debe configurarse en el controlador para la autenticación EAP. Todas las demás configuraciones específicas de EAP-FAST deben realizarse en el servidor RADIUS y en los clientes que deben autenticarse.

Configuración del servidor RADIUS para la autenticación de modo empresarial WPA2 (EAP-FAST)

En este ejemplo, Cisco Secure ACS se utiliza como servidor RADIUS externo. Realice estos pasos para configurar el servidor RADIUS para la autenticación EAP-FAST:

- 1. Crear una base de datos de usuarios para autenticar clientes
- 2. Agregue el WLC como cliente AAA al servidor RADIUS

.

3. <u>Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con el</u> <u>Aprovisionamiento de PAC en banda anónimo</u>Nota: EAP-FAST se puede configurar con aprovisionamiento de PAC en banda anónimo o con aprovisionamiento de PAC en banda autenticado. En este ejemplo se utiliza el aprovisionamiento de PAC en banda anónimo. Para obtener información detallada y ejemplos sobre la configuración de EAP FAST con aprovisionamiento de PAC en banda anónimo y aprovisionamiento en banda autenticado, consulte Ejemplo de Configuración de Autenticación EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo.

Creación de una Base de Datos de Usuario para Autenticar Clientes EAP-FAST

Complete estos pasos para crear una base de datos de usuario para los clientes EAP-FAST en ACS. Este ejemplo configura el nombre de usuario y la contraseña del cliente EAP-FAST como Usuario1 y Usuario1, respectivamente.

1. En ACS GUI en la barra de navegación, seleccione **User Setup**. Cree un nuevo usuario inalámbrico, y luego haga clic en **Add/Edit** para ir a la página Edit de este



 En la página User Setup Edit (Edición de la configuración de usuario), configure Real Name (Nombre real) y Description (Descripción), así como los parámetros de Password (Contraseña), como se muestra en este ejemplo.Este documento utiliza ACS Internal Database para la autenticación de contraseña.

kess http://127.0	.0.1:1065/	- 61
Cisco Svorems	User Setup	
alb alb	Edit	Help
User Setup Setup Setup	User: User1 (New User)	Account Disabled Oxisting & Oremann Supplementary User Info Password Avdientication Group to which the user is assigned
Network Configuration System Configuration	Supplementary User Info Real Name Description	Callback Client 3D Advanced SetSings Advanced SetSings Network Access Restrictions Nan Seasions Usage Operan Access to hable Overvised able Covervised able
Administration Centrol Control Control Posture Posture Validation Network Access Profiles	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	Advanced TACACS+ Settings TACACS+ Enable Parsword TACACS+ Enable Parsword TACACS+ Dutheand Parsword TACACS+ Shell Command Authorization Command Authorization for Network Device Nanagement Applications TACACS+ Unknown Services TACACS+ Unknown Services RADIUS Attributes RADIUS Yeador-Specific Attributes
Reports and Activity	Checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account. [Back to Top]
	Confirm Password Submit Cancel	Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the connect user account from the database, click Delete . When asked to confirm your action, click OK .

- 3. Elija ACS Internal Database del cuadro desplegable Password Authentication.
- 4. Configure todos los demás parámetros requeridos y haga clic en Submit.

Agregue el WLC como cliente AAA al servidor RADIUS

Complete estos pasos para definir el controlador como un cliente AAA en el servidor ACS:

- 1. Haga clic en **Network Configuration** desde la GUI de ACS. Bajo la sección Add AAA client de la página Network Configuration, haga clic en **Add Entry** para agregar el WLC como cliente AAA al servidor RADIUS.
- En la página AAA Client (Cliente AAA), defina el nombre del WLC, la dirección IP, el secreto compartido y el método de autenticación (RADIUS/Cisco Airespace). Consulte la documentación del fabricante para otros servidores de autenticación no ACS.

Cisco Systems	Network Configuration	
alb_alb_	Edit	Help
User Setup Setup Setup Shared Profile	Add AAA Client	AAA Cleast Bestname AAA Cleast IP Address Shared Scort Network Device Group BA005 Key Wrae Anthenic In Union
Network Configuration System Configuration	AAA Client IP Address	Oxtension and a comm Single Connect TACAS+ AAA Client Leg Undate/Watchdeg Packets from th AAA Client Leg RADIUS Tunneling Packets from th AAA Client
Administration	Shared Secret cisco RADIUS Key Wrap	 Realisce RADIUS Part info with Usernat from this AAA Client Match Franzed IP-Address with user IP address for accounting packets from th AAA Client
Posture Validation	Key Encryption Key Message Authenticator Code Key Key Input Format C ASCII Hexadecimal	AAA Client Hostname
Network Access Profiles	Authenticate Using RADIUS (Cisco Airespace)	The AAA Clean Hostbaine is the name assigned to the AAA client. [Back to Tep]
Online Decementation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
	Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client Match Framed-IP-Address with user IP address for accounting packets from	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each

Nota: La clave secreta compartida que configure en el WLC y el servidor ACS deben coincidir. El secreto compartido distingue entre mayúsculas y minúsculas.

3. Haga clic en Enviar+Aplicar.

Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con el Aprovisionamiento de PAC en banda anónimo

Aprovisionamiento anónimo en banda

Este es uno de los dos métodos de aprovisionamiento en banda en los que el ACS establece una conexión segura con el cliente de usuario final con el fin de proporcionar al cliente una nueva PAC. Esta opción permite un intercambio de señales TLS anónimo entre el cliente de usuario final y ACS.

Este método funciona dentro de un túnel de protocolo de acuerdo de clave Diffie-Hellman (ADHP) autenticado antes de que el par autentique el servidor ACS.

Entonces, el ACS requiere la autenticación EAP-MS-CHAPv2 del usuario. Cuando la autenticación de usuario es exitosa, el ACS establece un túnel Diffie-Hellman con el cliente de usuario final. El ACS genera una PAC para el usuario y la envía al cliente de usuario final en este túnel, junto con información sobre este ACS. Este método de aprovisionamiento utiliza EAP-MSCHAPv2 como método de autenticación en la fase cero y EAP-GTC en la fase dos.

Dado que se ha aprovisionado un servidor no autenticado, no es posible utilizar una contraseña de texto sin formato. Por lo tanto, sólo se pueden utilizar las credenciales MS-CHAP dentro del túnel. MS-CHAPv2 se utiliza para probar la identidad del par y recibir una PAC para sesiones de

autenticación adicionales (EAP-MS-CHAP se utilizará sólo como método interno).

Complete estos pasos para configurar la autenticación EAP-FAST en el servidor RADIUS para el aprovisionamiento anónimo en banda:

1. Haga clic en **System Configuration** de la GUI del servidor RADIUS. En la página System Configuration , elija **Global Authentication**

in Edit Very Fa	varias Tools Help	-10- tinis ¹⁰ Oc
dress a http://127.	0.0.1:1065/	• D @
Cisco Svorens	System Configuration	
User Setup Setup Setup Setup Setup Setup Setup Setup Suprem Configuration Suprem Configuration Suprem Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Reserved Reserved Configuration Configuration Reserved Configuration Configuration Reserved Configuration Co	Stat	Help Service Central Acts Income Control Acts Income Control Acts Income Control Acts Income Control Acts Income Acts Incom Acts Income Acts Incom Acts Income Act

 Desde la página de configuración de Autenticación Global, haga clic en Configuración EAP-FAST para ir a la página de configuración de EAP-FAST.

CiscoSecure ACS - N	Nicrosoft Internet Explorer	
ger gok yew rg Address a http://127.0	vontes Loos (Pep)	viii 🦉 🙀
Cisco Systems	System Configuration	
(D) Ultra	EAP Configuration	? Hap
Setup Group Setup Shared Profile Components Net work Configuration Startem Startem	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Select one or more of the following options:	Use this page to specify settings for various authentication protocols. EAP Configuration PEAP EAP-FAST EAP-FAST EAP-FAST EAP-FAST EAP-FAST AP EAP Request Tameout
Configuration Interface Interface Interface Configuration Control Contro Control Control Control Control	Certificate SAN comparison Certificate CN comparison Certificate Binary comparison EAP-TLS session timeout (minutes): 120 Cisco client initial message: PEAP session timeout (minutes): 120	MS-CHAP Configuration EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2234). EAP is layered on top of another protocol such as LUDP, 802.1% or RADEUS and supports multiple "authentication" types. It subtract Trop1
Reports and Activity	Enable Fast Reconnect: E EAP-FAST EAP-FAST Configuration	PEAP DEAD is the outer layer protocol for the secure tunnel.
	EAP-TLS C Allow EAP-TLS Select one or more of the following options: Certificate SAN comparison	Alexer AEAP is a cartificate-based authentication protocol. AEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
e)	Submit Submit + Restart Cancel	Internet
🐮 Start 🔂 🥭	CiscoSecure ACS - Mic	👮 7:58 PM

3. En la página EAP-FAST Settings (Parámetros de EAP-FAST), marque la casilla de verificación **Allow EAP-FAST** para activar EAP-FAST en el servidor RADIUS.

ElscoSecure ACS - M	Scrosoft Internet Explorer	LIDIX
Ele Edt Yew Far	roniters Iools Help	Links 🍟 🦧
Address a http://127.0	0.0.1:1065/	💌 🛃 Go
Cisco Systems	System Configuration	X
	EAP-FAST Configuration	A Help A
User Setup	EAD EAD Rothings	EAP-FAST Configuration Page
Setup	EAP-FAST Settings	Use this page to configure EAP-FAST authentication settings.
Shareditrofile Components Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	Allow EAP-FAST Active master key TTL Retired master key TTL Imonths Tunnel PAC TTL Imonths Client initial message: Authority ID Info: Reduebacs Authority ID Info: Allow anonymous in-band PAC provisioning Allow authenticated in-band PAC provisioning Require client on authenticated provisioning Require client certificate for provisioning	EAP-FAST Settings Cleant initial measures Antherity ID Infe Allow anthentics the and PAC provisioning Allow anthentic attain Allow anthentic attain Allow anthentic method EAP-FAST settings EAP-FAST settings EAP-FAST Settings Actual EAP-FAST—To enable EAP-FAST authentication, select this check box.
Reports and Contine	Allow Machine Authentication Machine PAC TTL 1 weeks Allow Stateless session resume Authorization PAC TTL 1 hours Allowed inner methods EAP-GTC EAP-MSCHAPV2 EAP-TLS Submit Submit + Restart Cancel	 Active Master Key TIL - Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated. Retired master key TIL - Enter a value for the amount of time that PACs generated using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access using a PAC based on a retired master key, ACS sends a new PAC to the end-user client. Tennel PAC TIL - Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC has net expired, new PAC creation and assignment is automatic. If the master key used to generate the tonnel PAC empired, automatic or manual growinsoning must be used to provide the end-user client with a new PAC.
		internet
start 🕜 🥭	CiscoSecure ACS - Mic	9 7:58 PM

- 4. Configure los valores TTL (Time-to-Live) de clave maestra activa/retirada como desee o establézcalos en el valor predeterminado, como se muestra en este ejemplo.Consulte Claves Maestras para obtener información sobre las claves Maestras Activas y Retiradas. Consulte también las claves maestras y los TTL PAC para obtener más información.El campo Información de ID de autoridad representa la identidad textual de este servidor ACS, que un usuario final puede utilizar para determinar con qué servidor ACS se autenticará. Rellenar este campo es obligatorio.El campo Mensaje de visualización inicial del cliente especifica un mensaje que se enviará a los usuarios que se autentiquen con un cliente EAP-FAST. La longitud máxima es de 40 caracteres. Un usuario sólo verá el mensaje inicial si el cliente de usuario final admite la visualización.
- 5. Si desea que ACS realice el aprovisionamiento de PAC en banda anónimo, marque la casilla de verificación **Permitir el aprovisionamiento de PAC en banda anónimo**.
- 6. Métodos internos permitidos: esta opción determina qué métodos EAP internos se pueden ejecutar dentro del túnel EAP-FAST TLS. Para el aprovisionamiento en banda anónimo, debe habilitar EAP-GTC y EAP-MS-CHAP para la compatibilidad con versiones anteriores. Si selecciona Permitir el aprovisionamiento de PAC en banda anónimo, debe seleccionar EAP-MS-CHAP (fase cero) y EAP-GTC (fase dos).

Configuración del cliente inalámbrico para el modo de funcionamiento de WPA2 Enterprise

El siguiente paso consiste en configurar el cliente inalámbrico para el modo de funcionamiento WPA2 Enterprise.

Complete estos pasos para configurar el cliente inalámbrico para el modo WPA2 Enterprise.

- Desde la ventana Aironet Desktop Utility, haga clic en Profile Management > New para crear un perfil para el usuario WLAN WPA2-Enterprise.Como se mencionó anteriormente, este documento utiliza el nombre WLAN/SSID como WPA2-Enterprise para el cliente inalámbrico.
- Desde la ventana Profile Management, haga clic en la pestaña General y configure el nombre del perfil, el nombre del cliente y el nombre SSID como se muestra en este ejemplo. A continuación, haga clic en Acentar

rofile Management	?
General Security Advar	nced
Profile Settings	
Profile Name	x WPA2-Enterprise
Client Name	x Wireless-Client1
Network Names	
SSID1	: WPA2-Enterprise
SSID2	2 []
SSIDS	k []
<u> </u>	
	OK Cancel

 Haga clic en la ficha Security y seleccione WPA/WPA2/CCKM para activar el modo de funcionamiento de WPA2. En WPA/WPA2/CCKM EAP Type (Tipo de EAP WPA/WPA2/CCKM), seleccione EAP-FAST. Haga clic en Configure para configurar el ajuste EAP-FAST.

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: EAP-FAST	
WPA/WPA2 Passphrase		
○ 802.1x	802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)		
○ None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗘 sec	
	OK C	ancel

4. En la ventana Configure EAP-FAST, marque la casilla de verificación **Allow Automatic PAC Provisioning**. Si desea configurar el aprovisionamiento de PAC anónimo, EAP-MS-CHAP se utilizará como el único método interno en la fase cero.

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
<	>
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
✓ No Network Connection Unless User Is Logged In	
	OK Cancel

- 5. Elija Nombre de usuario y Contraseña MSCHAPv2 como método de autenticación en el cuadro desplegable Método de autenticación EAP-FAST. Haga clic en Configure (Configurar).
- En la ventana Configurar nombre de usuario y contraseña de MSCHAPv2, elija la configuración de nombre de usuario y contraseña adecuada.En este ejemplo se elige Pedir automáticamente nombre de usuario y contraseña.

rusted Root Certification Au	uthorities	
(Any>		~
Jser Name and Password S	Settings	
💿 Use Temporary Use	r Name and Password	
Use Windows I	User Name and Password	
Automatically P Manually Promi	rompt for User Name and Password	
- · ·	•	
OUse Saved User Nar	me and Password	
User Name:	Administrator	
Password:		
Confirm Password:		
Confirm Password: Domain:		

mismo nombre de usuario y la misma contraseña deben registrarse en ACS. Como se mencionó anteriormente, este ejemplo utiliza User1 y User1 respectivamente como nombre de usuario y contraseña. Además, tenga en cuenta que se trata de un aprovisionamiento en banda anónimo. Por lo tanto, el cliente no puede validar el certificado del servidor. Debe asegurarse de que la casilla de verificación Validar identidad de servidor no está activada.

7. Click OK.

Verificación del modo de funcionamiento de WPA2 Enterprise

Complete estos pasos para verificar si su configuración del modo WPA2 Enterprise funciona correctamente:

- 1. En la ventana Aironet Desktop Utility, seleccione el perfil **WPA2-Enterprise** y haga clic en **Activate** para activar el perfil del cliente inalámbrico.
- 2. Si ha habilitado MS-CHAP ver2 como su autenticación, el cliente solicitará el nombre de

usuario	У	la

Enter Wireless Network Password 🗙				
Please enter your EA network	P-FAST username and password to log on to the wireless			
User Name :	User1			
Password :	•••••			
Log on to :				
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter			
Profile Name :	WPA-Enterprise			
	OK Cancel			

contraseña.

3. Durante el procesamiento EAP-FAST del usuario, el cliente le pedirá que solicite PAC del servidor RADIUS. Al hacer clic en **Sí**, se inicia el aprovisionamiento de PAC.

EAP-FAST Authentication	×
You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?	
Yes No	

4. Después del aprovisionamiento correcto de PAC en la fase cero, se siguen las fases uno y dos, y tiene lugar un procedimiento de autenticación correcto.Una vez realizada la autenticación correctamente, el cliente inalámbrico se asocia a WLAN WPA2-Enterprise. Esta es la captura de pantalla:

Cisco Aironet Desktop Utility	y - Current Profile: WPA2-E	nterprise 🛛 🖓 🔀
Action Options Help		
Current Status Profile Management	Diagnostics	
CISCO SYSTEMS		
nullinullin. Profile Name:	WPA2-Enterprise	
Link Status:	Authenticated	Network Type: Infrastructure
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based Authentication:	EAP-FAST	Data Encryption: AES
IP Address:	10.77.244.221	
Signal Strength:		Good
		Advanced

También puede verificar si el servidor RADIUS recibe y valida la solicitud de autenticación del cliente inalámbrico. Verifique los informes Passed Authentications and Failed Attempts en el servidor ACS para lograr esto. Estos informes están disponibles en Informes y actividades en el servidor ACS.

Configuración de los dispositivos para el modo WPA2 Personal

Siga estos pasos para configurar los dispositivos para el modo de funcionamiento WPA2-Personal:

- 1. Configuración de la WLAN para la autenticación en modo WPA2 Personal
- 2. Configuración del cliente inalámbrico para el modo WPA2 Personal

Configuración de la WLAN para el modo de funcionamiento WPA2 Personal

Debe configurar la WLAN que los clientes utilizarán para conectarse a la red inalámbrica. El SSID de WLAN para el modo WPA2 Personal será WPA2-Personal. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN y sus parámetros relacionados:

- 1. Haga clic en **WLANs** de la GUI del controlador para mostrar la página WLANs.Esta página enumera las WLANs que existen en el controlador.
- 2. Haga clic en Nuevo para crear un nuevo WLAN.
- Introduzca el nombre SSID de WLAN, el nombre de perfil y la ID de WLAN en la página WLAN > New (WLAN > Nuevo). A continuación, haga clic en Aplicar. Este ejemplo utiliza WPA2-Personal como SSID.

						Sa <u>r</u> e Co	nfiguration <u>P</u> ing	Logout Befresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN						
Advanced	Profile Name	WPA2-Per	sonal					
	WLAN SSID	WPA2-Per	sonal					

- 4. Una vez que haya creado una nueva WLAN, aparecerá la página WLAN > Edit para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, políticas de seguridad, políticas de QOS y parámetros avanzados.
- 5. En Políticas generales, marque la casilla de verificación Status para habilitar la WLAN.
- 6. Si desea que el AP difunda el SSID en sus tramas de baliza, marque la casilla de verificación **Broadcast SSID**.
- Haga clic en la ficha Security (Seguridad). En Layer Security, seleccione WPA+WPA2.Esto activa la autenticación WPA para la WI AN

cisco		OLLER WIRELESS	SECURITY	MANAGEMENT	Saye Co COMMANDS	nfiguration (<u>Ping</u> HELP	Logout Bef
LANS WLANS	WLANs > Edit General Security C	oS Advanced				< Back	Apply
WLANS Advanced	Layer 2 Layer 3	WPA2					^
	Static WEP Parameters	Filtering					
	802.11 Data Encryption	Current Key: Type Key Size WEP not set	104 bits WEI	P Static Key (Key 1 Encryption Key	ndex = 0)	Key Format	
	Allow Shared Key Authentication	Enabled					
	802.11 Data Encryption	Current Key: 0 b	its CKIP Key ((Key Index= 0)			
		not set • 1 •	Index Encr	yption Key		ASCII ·	
	*						<u>×</u>
	Foot Notes I CKIP is not supported by 10: 2 Web Policy cannot be used it 3 H-REAP Load Switching is no 4 When client exclusion is ena 5 Client MPP is not active unles	cr model APs n combination with IPsec, bled, a Timeout Value o is WPA2 is configured	c CRANITE aut f zero means	hentication infinity (will requir	e administrative	override to reset excl	uded clients;

- 8. Desplácese hacia abajo por la página para modificar los parámetros **WPA+WPA2**.En este ejemplo, se seleccionan la política WPA2 y el cifrado AES.
- 9. En Auth Key Mgmt, elija **PSK** para habilitar WPA2-PSK.
- 10. Introduzca la clave precompartida en el campo correspondiente, como se muestra a continuación.

cisco	Sage Configuration > Bing Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS MLANS	WLANs > Edit < Back Apply General Security QoS Advanced Layer 2 Layer 3 AAA Servers Key Size Key Index Encryption Key Key Format not set I I ASCII MMH Mode Enabled Key Permutation Enabled B02.1X Parameters 802.11 Date Encryption Type Key Size @ WEP 104 bits Image Security
	WPA Policy WPA2 Policy WPA2 Encryption ALES TKIP Auth Key Mgmt PSK PSK Format ASCII ************************************

Nota: La clave previamente compartida utilizada en el WLC debe coincidir con la configurada en los clientes inalámbricos.

11. Haga clic en Apply (Aplicar).

Configuración del cliente inalámbrico para el modo WPA2 Personal

El siguiente paso consiste en configurar el cliente inalámbrico para el modo de funcionamiento WPA2-Personal.

Complete estos pasos para configurar el cliente inalámbrico para el modo WPA2-Personal:

- 1. Desde la ventana Aironet Desktop Utility, haga clic en **Profile Management > New** para crear un perfil para el usuario WLAN WPA2-PSK.
- Desde la ventana Profile Management, haga clic en la pestaña General y configure el nombre del perfil, el nombre del cliente y el nombre SSID como se muestra en este ejemplo. A continuación, haga clic en Aceptar.

Profile Management		? 🗙
General Security Advance	ed	
Profile Settings Profile Name: Client Name:	WPA2-Personal Wireless-Client2	
Network Names SSID1: SSID2: SSID3:	WPA2-Personal	
	ОК	Cancel

 Haga clic en la ficha Security y seleccione WPA/WPA2 Passphrase para activar el modo de funcionamiento de WPA2-PSK. Haga clic en Configure para configurar la clave previamente compartida WPA-PSK.

Profile Management			? 🔀
General Security Advanced			
- Set Security Options			
○ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	
WPA/WPA2 Passphrase			
○ 802.1x	802.1x EAP Type:	LEAP	
O Pre-Shared Key (Static WEP)			
◯ None			
Configure			
	Limit Time for Finding Domain	Controller To: 0	tec sec
Group Policy Delay:	60 😂 sec		
		<u> Service and a</u>	
			OK Cancel

4. Introduzca la clave previamente compartida y haga clic en **Aceptar**.

Configure WPA/WPA2 Passphrase				
Enter a WPA/WPA2 passphrase (8 to 63 ASCII or 64 hexadecimal characters)				
abcdefghijkl				
	OK Cancel			

Verificación del modo de funcionamiento de WPA2-Personal

Complete estos pasos para verificar si su configuración del modo WPA2-Enterprise funciona correctamente:

- 1. Desde la ventana de Aironet Desktop Utility, seleccione el perfil **WPA2-Personal** y haga clic en **Activar** para activar el perfil del cliente inalámbrico.
- 2. Una vez que se activa el perfil, el cliente inalámbrico se asocia a la WLAN tras una autenticación exitosa.Esta es la captura de pantalla:

🖻 Cisco Aironet Desktop Utility - Current Profile: WPA2-Personal 🛛 🔗 🔀					
Action Options Help					
Current Status Profile Management	Diagnostics				
CISCO SYSTEMS					
Profile Name:	WPA2-Personal				
Link Status:	Authenticated	Network Type: Infrastructure			
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149			
Server Based Authentication:	None	Data Encryption: AES			
IP Address:	10.77.244.221				
Signal Strength:		Good			
		Advanced			

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Estos comandos debug serán útiles para resolver problemas de configuración:

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

 debug dot1x events enable: habilita la depuración de todos los eventos dot1x. A continuación se presenta un ejemplo de resultado de depuración basado en una autenticación exitosa:Nota: Algunas de las líneas de esta salida se han movido a la segunda línea debido a limitaciones de espacio.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....
```

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43) Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from

mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for

```
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for
tation 00:40:96:af:3e:93 (RSN 0)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- debug dot1x packet enable: habilita la depuración de mensajes de paquetes 802.1x.
- debug aaa events enable: habilita la salida de depuración de todos los eventos aaa.

Información Relacionada

- <u>WPA2: acceso Wi-Fi protegido 2</u>
- Ejemplo de Configuración de Autenticación EAP-FAST con Controladores LAN Inalámbricos y Servidor RADIUS Externo
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Introducción a la configuración WPA
- Soporte de Productos de Red Inalámbrica
- 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).