

Acceso convergido 5760, 3850, y EAP-FAST del WLC de las 3650 Series con el ejemplo de configuración del servidor RADIUS interno



ID del Documento: 117664

Actualizado: De abril el 18 de 2014

Contribuido por Surendra BG, ingeniero de Cisco TAC.



[Descarga PDF](#)



[Imprimir](#)

[Feedback](#)

Productos Relacionados

- [Wireless, LAN \(WLAN\)](#)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Información general sobre configuración](#)

[Configure el WLC con el CLI](#)

[Configure el WLC con el GUI](#)

[Verificación](#)

[Troubleshooting](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento describe cómo configurar Cisco convergió acceso 5760, 3850, y reguladores del Wireless LAN de las 3650 Series (WLCs) para actuar como servidores de RADIUS que realicen la autenticación de Protocol Flexible de autenticación ampliable de Cisco vía el protocolo seguro (EAP-FAST, en este ejemplo) para la autenticación de cliente.

Utilizan generalmente a un servidor RADIUS externo para autenticar a los usuarios, que no es una solución factible en algunos casos. En estas situaciones, un WLC convergido del acceso puede actuar como servidor de RADIUS, donde autentican a los usuarios contra la base de datos local que se configura en el WLC. Esto se llama una característica local del servidor de RADIUS.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente esta configuración:

- [®] GUI o CLI del Cisco IOS con el acceso convergido 5760, 3850, y WLC de las 3650 Series
- Conceptos del Protocolo de Autenticación Extensible (EAP)
- Configuración del Service Set Identifier (SSID)
- RADIUS

Componentes Utilizados

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

- Versión 3.3.2 ([NGWC] del WLC de las Cisco 5760 Series del Wiring Closet de la última generación)
- Lightweight Access Point de las Cisco 3602 Series (AP)
- Microsoft Windows XP con el supplicant de Intel PROset
- Cisco Catalyst 3560 Series Switches

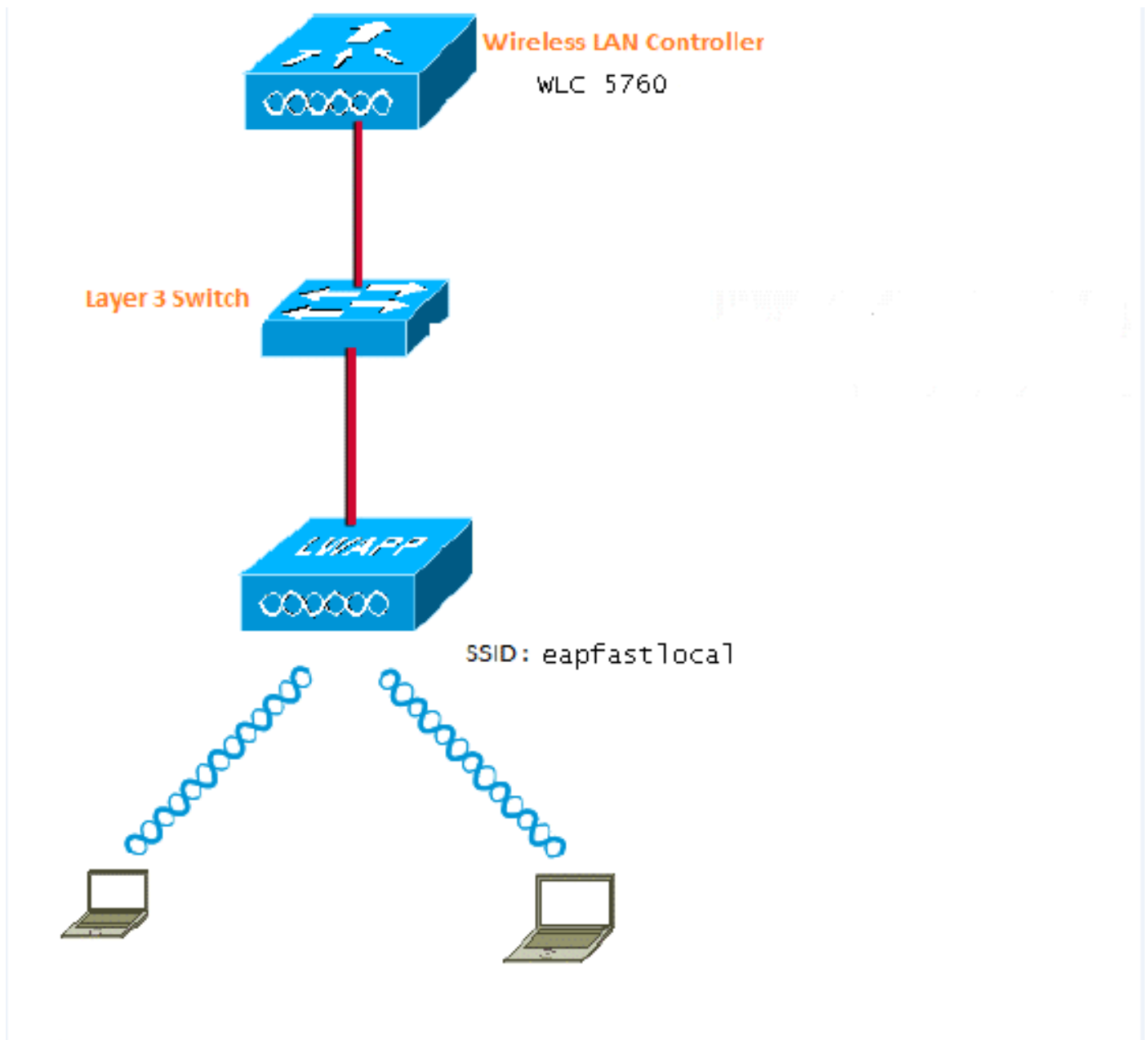
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Note: Use la [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Esta imagen proporciona un ejemplo de un diagrama de la red:



Información general sobre configuración

Esta configuración se completa en dos pasos:

1. Configure el WLC para el método EAP local y los perfiles relacionados de la autenticación y autorización con el CLI o el GUI.
2. Configure la red inalámbrica (WLAN) y asocie la lista de métodos que tiene los perfiles de la autenticación y autorización.

Configure el WLC con el CLI

Complete estos pasos para configurar el WLC con el CLI:

1. Habilite el modelo AAA en el WLC:

```
aaa new-model
```

2. Defina la autenticación y autorización:

```
aaa local authentication eapfast authorization eapfast
```

```
aaa authentication dot1x eapfast local  
aaa authorization credential-download eapfast local  
aaa authentication dot1x default local
```

3. Configure el perfil local EAP y el método (el EAP-FAST se utiliza en este ejemplo):

```
eap profile eapfast  
method fast  
!
```

4. Configure los parámetros avanzados del EAP-FAST:

```
eap method fast profile eapfast  
description test  
authority-id identity 1  
authority-id information 1  
local-key 0 cisco123
```

5. Configure la red inalámbrica (WLAN) y asocie el perfil de la autorización local a la red inalámbrica (WLAN):

```
wlan eapfastlocal 13 eapfastlocal  
client vlan VLAN0020  
local-auth eapfast  
session-timeout 1800  
no shutdown
```

6. Configure la infraestructura para soportar la conectividad del cliente:

```
ip dhcp snooping vlan 12,20,30,40,50  
ip dhcp snooping  
!  
ip dhcp pool vlan20  
network 20.20.20.0 255.255.255.0  
default-router 20.20.20.251  
dns-server 20.20.20.251
```

```
interface TenGigabitEthernet1/0/1  
switchport trunk native vlan 12  
switchport mode trunk  
ip dhcp relay information trusted  
ip dhcp snooping trust
```

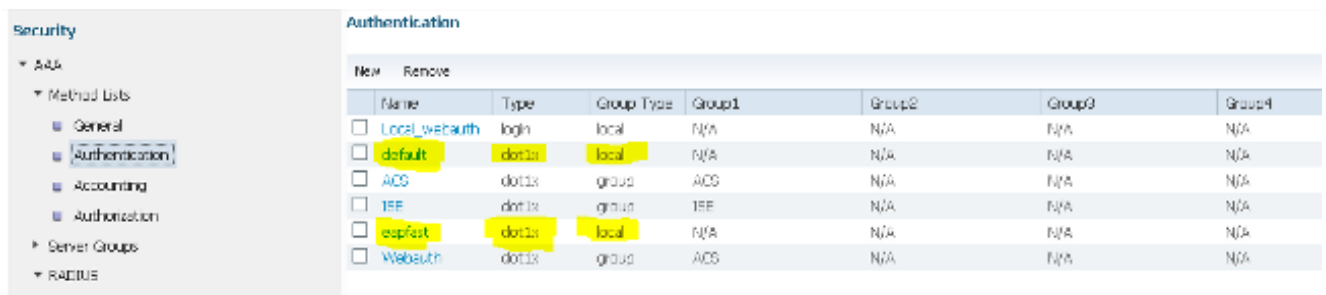
Configure el WLC con el GUI

Complete estos pasos para configurar el WLC con el GUI:

1. Configure la lista de métodos para la autenticación:

Configure el tipo del **eapfast** como **dot1x**.

Configure el Tipo de grupo del **eapfast** como **Local**.

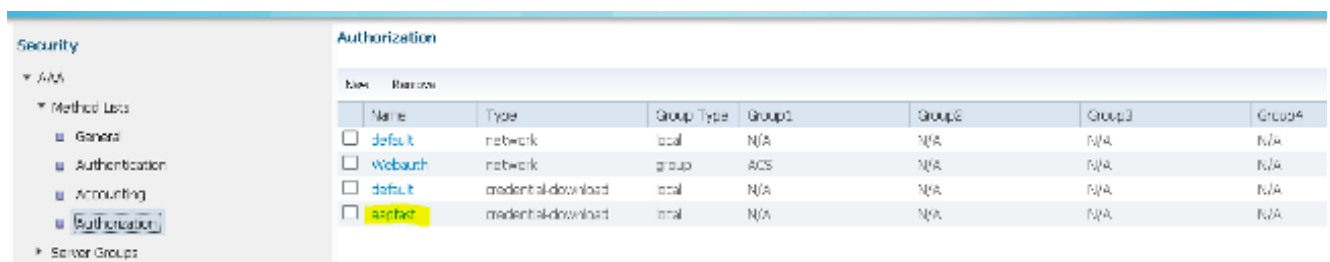


New		Remove					
Name	Type	Group Type	Group1	Group2	Group3	Group4	
<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A	
<input type="checkbox"/> TEF	dot1x	group	TEF	N/A	N/A	N/A	
<input type="checkbox"/> eapfast	dot1x	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> Webauth	dot1x	group	ACS	N/A	N/A	N/A	

2. Configure la lista de métodos para la autorización:

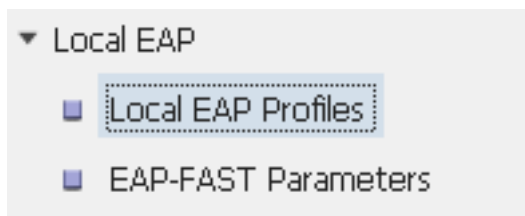
Configure el tipo del **eapfast** como **Credencial-descarga**.

Configure el Tipo de grupo del **eapfast** como **Local**.



New		Remove					
Name	Type	Group Type	Group1	Group2	Group3	Group4	
<input type="checkbox"/> default	network	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> Webauth	network	group	ACS	N/A	N/A	N/A	
<input type="checkbox"/> default	credential-download	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> eapfast	credential-download	local	N/A	N/A	N/A	N/A	

3. Configure el perfil local EAP:



4. Cree un nuevo perfil y seleccione el tipo EAP:



New		Remove			
Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP	
<input type="checkbox"/> eapfast	Disabled	Enabled	Disabled	Disabled	

El nombre del perfil es **eapfast** y el tipo seleccionado EAP es **EAP-FAST**:

Local EAP Profiles

Local EAP Profiles > Edit

Profile Name	eapfast
LEAP	<input type="checkbox"/>
EAP-FAST	<input checked="" type="checkbox"/>
EAP-TLS	<input type="checkbox"/>
PEAP	<input type="checkbox"/>
Trustpoint	<input type="checkbox"/>

5. Configure los parámetros de método del EAP-FAST:

EAP-FAST Method Parameters

New Remove

	Profile Name	Description
<input type="checkbox"/>	eapfast	test

La clave del servidor se configura como **cisco123**.

EAP-FAST Method Profile

EAP-FAST Method Profile > **Edit**

Profile Name	eapfast
Server Key	●●●●●●●●
Confirm Server Key	●●●●●●●●
Time to live (secs)	86400
Authority ID	1
Authority ID Information	1
Description	test

6. Marque la casilla de verificación del **control del auth del sistema del dot1x** y seleccione el **eapfast** para las listas de métodos. Esto le ayuda a realizar la autenticación EAP local.

Security	General
▼ AAA	
▼ Method Lists	
■ General	Dot1x System Auth Control <input checked="" type="checkbox"/>
■ Authentication	Local Authentication Method List ▼
■ Accounting	Authentication Method List eapfast ▼
■ Authorization	Local Authorization Method List ▼
▶ Server Groups	Authorization Method List eapfast ▼
▼ RADIUS	

7. Configure la red inalámbrica (WLAN) para la encriptación AES WPA2:

WLAN
WLAN > **Edit**

General Security QOS AVC Advanced

Profile Name eapfastlocal
 Type WLAN
 SSID eapfastlocal
 Status
 Security Policies [WPA2][Auth(802.1x)]
 (Modifications done under security tab will appear after applying the changes.)
 Radio Policy All ▾
 Interface/Interface Group(G) VLAN0020 ▾
 Broadcast SSID
 Multicast VLAN Feature

WLAN
WLAN > **Edit**

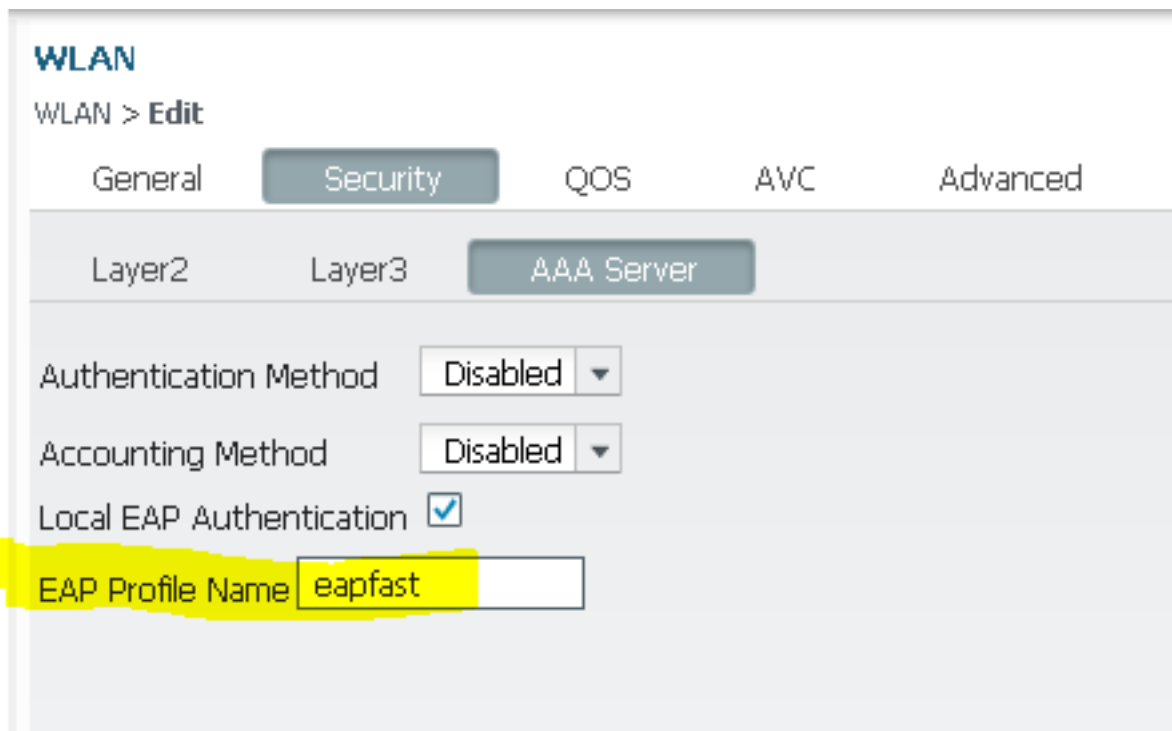
General Security QOS AVC Advanced

Layer2 Layer3 AAA Server

Layer 2 Security WPA + WPA2 ▾
 MAC Filtering
 Fast Transition
 Over the DS
 Reassociation Timeout 20

WPA+WPA2 Parameters
 WPA Policy
 WPA2 Policy
 WPA2 Encryption AES TKIP
 Auth Key Mgmt 802.1x ▾

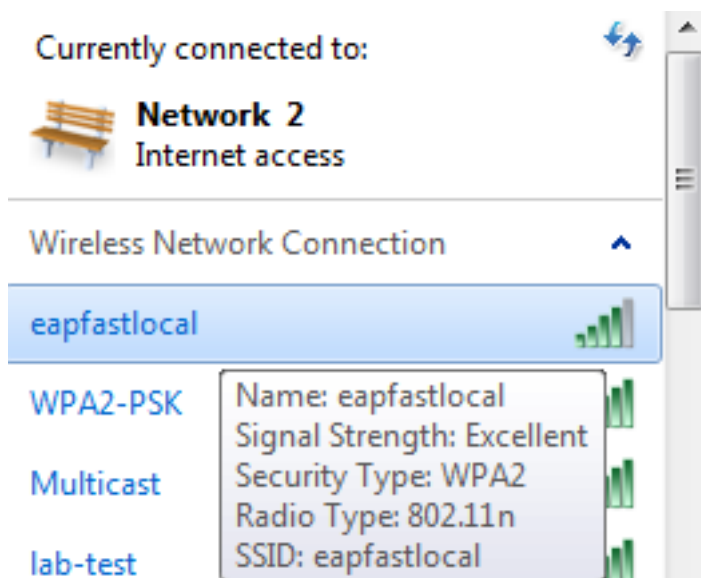
8. En la lengüeta del **servidor de AAA**, asocie el **eapfast** del nombre del perfil EAP a la red inalámbrica (WLAN):



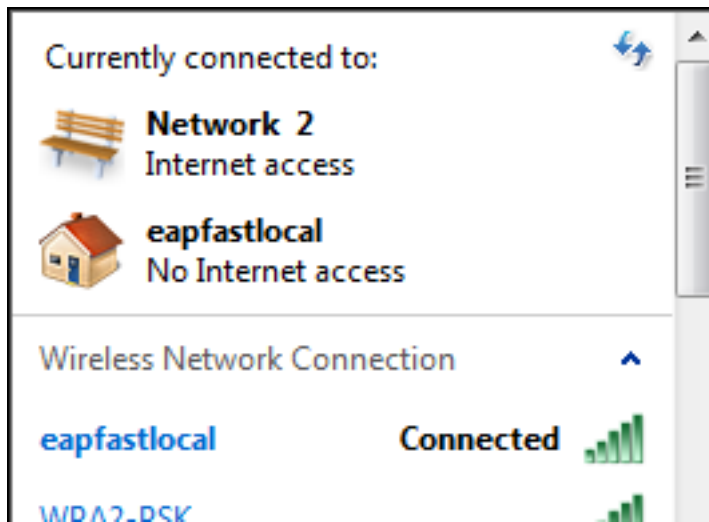
Verificación

Complete estos pasos para verificar que su configuración trabaja correctamente:

1. Conecte al cliente con la red inalámbrica (WLAN):



2. Verifique que aparezca el popup protegido de las credenciales del acceso (PAC) y que usted debe validar para autenticar con éxito:



Troubleshooting

Cisco recomienda que usted utiliza las trazas para resolver problemas los problemas inalámbricos. Las trazas se guardan en el buffer circular y no son hace un uso intensivo del procesador.

Permita a estas trazas para obtener los registros del auth de la capa 2 (L2):

- fije el debug llano grupo-Tecnología inalámbrica-seguro de la traza
- fije el filtro grupo-Tecnología inalámbrica-seguro mac0021.6a89.51ca de la traza

Permita a estas trazas para obtener los registros de eventos del DHCP:

- fije el debug llano de los eventos DHCP de la traza
- fije el mac 0021.6a89.51ca del filtro de los eventos DHCP de la traza

Aquí están algunos ejemplos de las trazas acertadas:

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
mobile on AP c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
override for station 0021.6a89.51ca - vapId 13, site 'default-group',
interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
Interface Policy for station 0021.6a89.51ca - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0
```

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
57ca4000000048, uid 42, capwap id 50b94000000012, Flag 4, Audit-Session ID
0a6987b253468efb0000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca,
ID list 0x00000000

[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): method: Dot1X, method list: none, aaa id:
0x0000002A

**[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): eap profile: eapfast**

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTH_START for 0xF700000A

[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering request state

[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Sending EAPOL packet

[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
Platform changed src mac of EAPOL packet

[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
EAPOL packet sent to client 0xF700000A

[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:idle request action

[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 5) from mobile

**[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start
from mobile**

[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA: EAPOL-Start -
EAPOL start message from mobile as mobile is in Authenticating state, restart
authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering response state

[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Response sent to the server from 0xF700000A

[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:ignore response action

[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202

[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req

[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for
0021.6a89.51ca with handle FE000052, list 630007B2

[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Received Authz Success for the client 0xF700000A (0021.6a89.51ca)

[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTHZ_SUCCESS on Client 0xF700000A

[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering authenticated state

[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded

[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache

[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache

[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca **Starting key exchange with
mobile - data forwarding is disabled**

[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: **Sending EAPOL message
to mobile, WLAN=13 AP WLAN=13**

```
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
PTK_START state (msg 2) from mobile
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission
timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
PTKINITNEGOTIATING state (msg 4) from mobile

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca)
client (0x57ca400000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak
with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with
SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 255.255.255.0
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak
with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with
SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
```

¿Era este documento útil? [Sí ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: De abril el 18 de 2014

ID del Documento: 117664