

Ejemplo de Configuración de WLC EAP-FAST de acceso convergente serie 5760, 3850 y 3650 con servidor RADIUS interno

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Información general sobre configuración](#)

[Configure el WLC con la CLI](#)

[Configure el WLC con la GUI](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Cisco Converged Access 5760, 3850 y 3650 Series Wireless LAN Controllers (WLC) para actuar como servidores RADIUS que realizan Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST, en este ejemplo) para la autenticación de cliente.

Normalmente, se utiliza un servidor RADIUS externo para autenticar a los usuarios, lo que en algunos casos no es una solución factible. En estas situaciones, un WLC de acceso convergente puede actuar como un servidor RADIUS, donde los usuarios se autentican contra la base de datos local configurada en el WLC. Esto se denomina función de servidor RADIUS local.

Prerequisites

Requirements

Cisco recomienda tener conocimientos sobre estos temas antes de intentar esta configuración:

- GUI o CLI de Cisco IOS[®] con WLC de acceso convergente serie 5760, 3850 y 3650
- Conceptos de protocolo de autenticación extensible (EAP)
- Configuración del identificador de conjunto de servicios (SSID)
- RADIUS

Componentes Utilizados

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

hardware.

- Cisco 5760 Series WLC versión 3.3.2 (armario de cableado de última generación [NGWC])
- Punto de acceso ligero (AP) de la serie Cisco 3602
- Microsoft Windows XP con suplicante Intel PROset
- Cisco Catalyst 3560 Series Switches

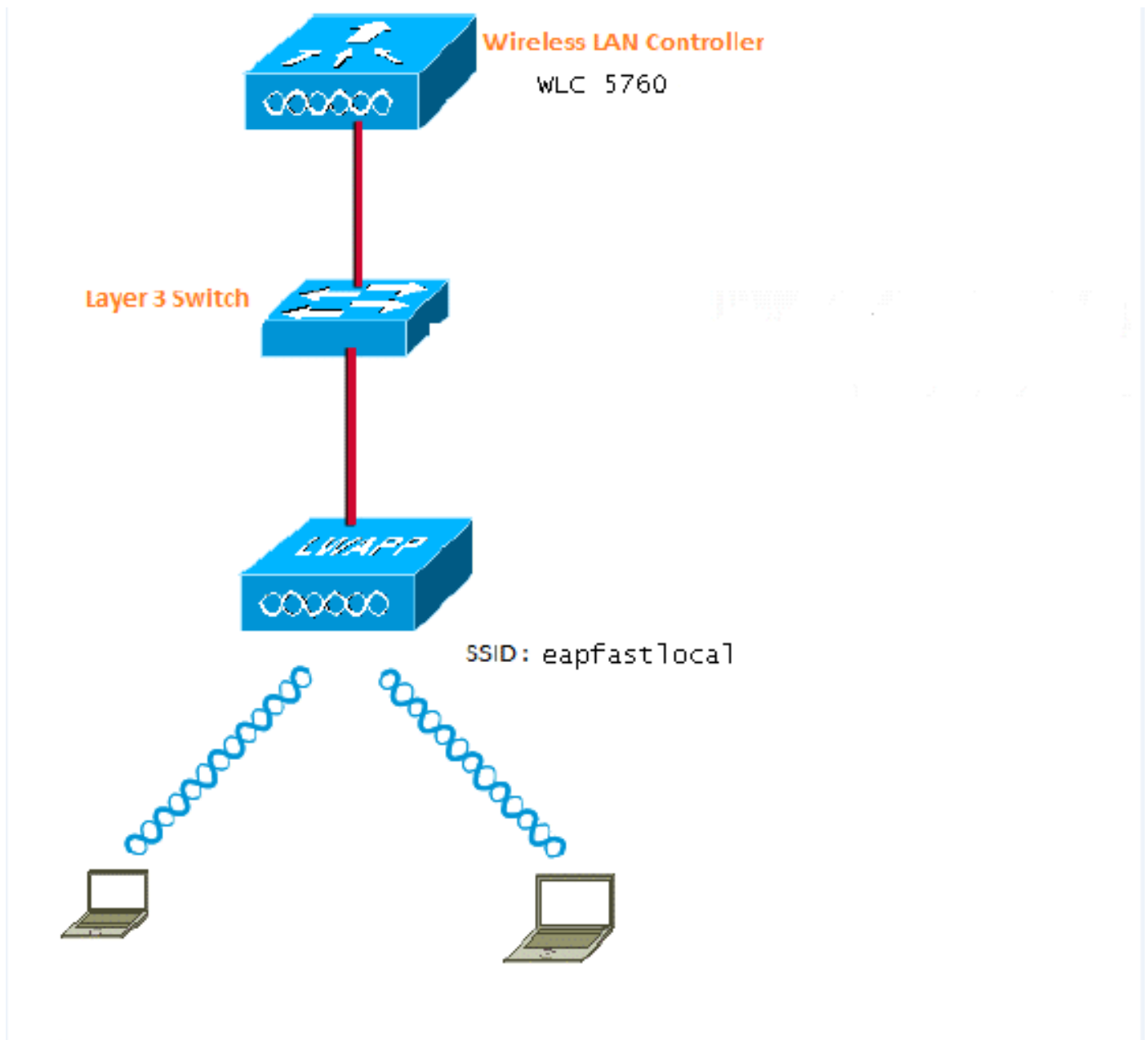
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Nota: 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 red:



Información general sobre configuración

Esta configuración se completa en dos pasos:

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

Configure el WLC con la CLI

Complete estos pasos para configurar el WLC con la 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 EAP local y el método (en este ejemplo se utiliza EAP-FAST):

```
eap profile eapfast
```

```
method fast
```

```
!
```

4. Configure los parámetros avanzados EAP-FAST:

```
eap method fast profile eapfast
```

```
description test
```

```
authority-id identity 1
```

```
authority-id information 1
```

```
local-key 0 cisco123
```

5. Configure la WLAN y asigne el perfil de autorización local a la 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
```

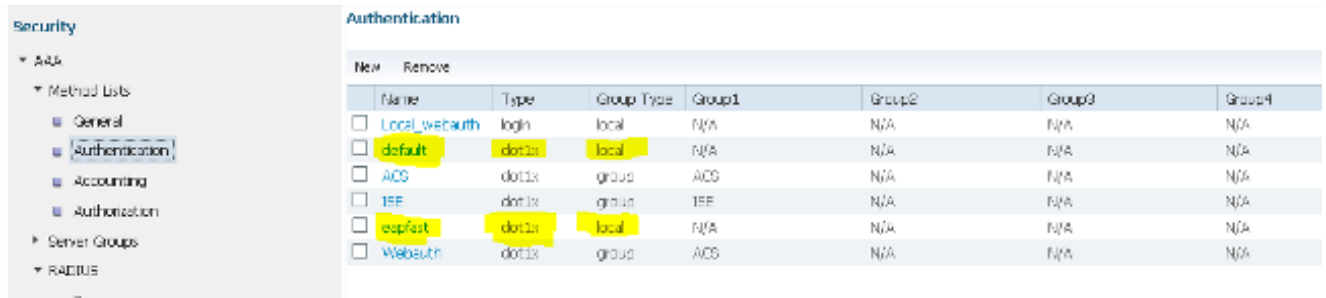
Configure el WLC con la GUI

Complete estos pasos para configurar el WLC con la GUI:

1. Configure la lista de métodos para la autenticación:

Configure el tipo **eapfast** como **Dot1x**.

Configure el Tipo de Grupo **eapfast** como **Local**.

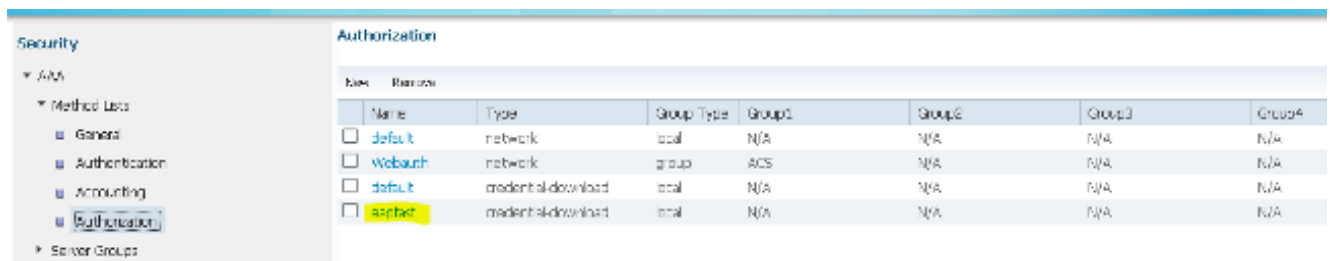


Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A
<input type="checkbox"/> TEF	dot1x	group	TEF	N/A	N/A	N/A
<input type="checkbox"/>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

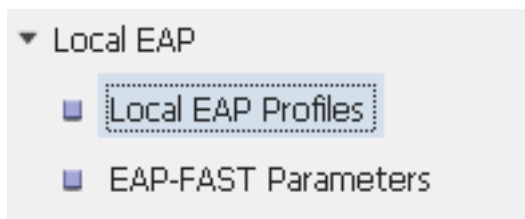
Configure el tipo **eapfast** como **Credential-Download**.

Configure el Tipo de Grupo **eapfast** como **Local**.



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 EAP local:



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



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 EAP seleccionado 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 del Método EAP-FAST:

EAP-FAST Method Parameters

New Remove

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

La clave de 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 **Dot1x System Auth Control** y **seleccione 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 WLAN para la encriptación WPA2 AES:

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**

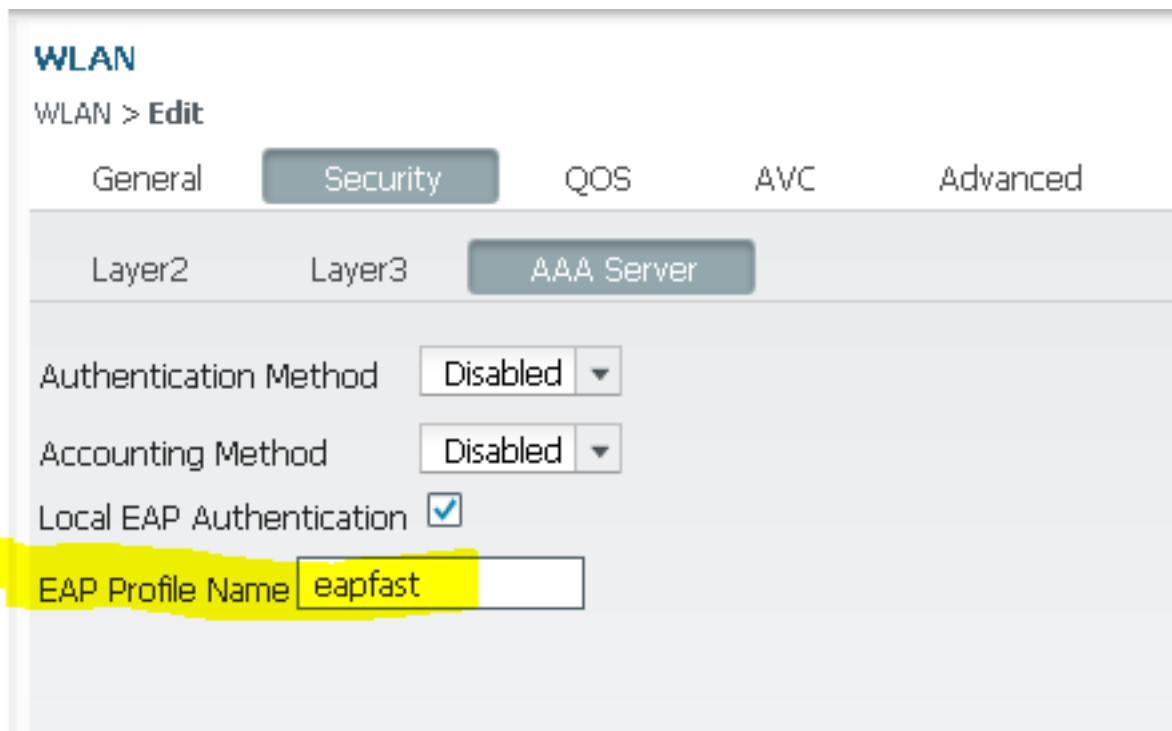
General Security QOS AVC Advanced

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 ▾

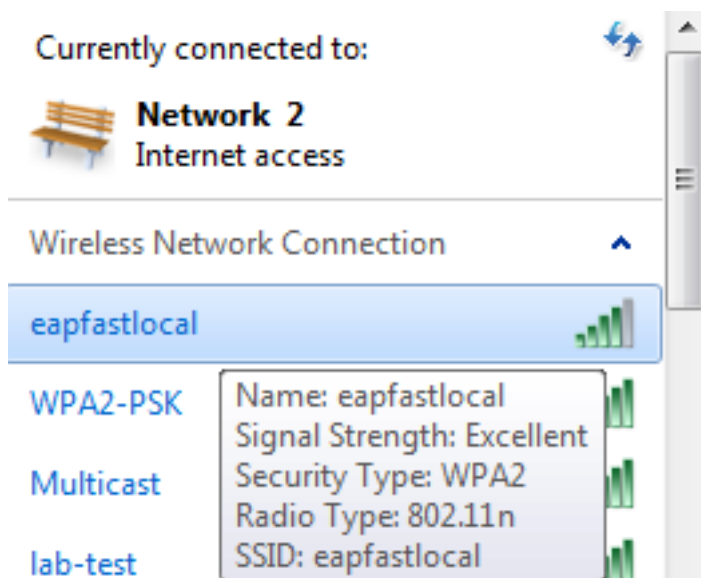
8. En la pestaña **Servidor AAA**, mapee la función EAP Profile Name **fast** a la WLAN:



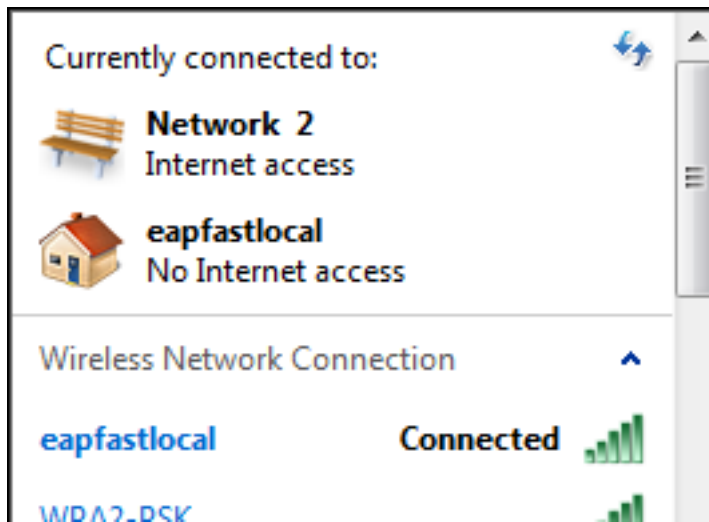
Verificación

Complete estos pasos para verificar que su configuración funcione correctamente:

1. Conecte el cliente a la WLAN:



2. Verifique que aparezca la ventana emergente Credenciales de acceso protegido (PAC) y que debe aceptar para autenticar correctamente:



Troubleshoot

Cisco recomienda que utilice seguimientos para resolver problemas de red inalámbrica. Los seguimientos se guardan en el búfer circular y no hacen un uso intensivo del procesador.

Habilite estos seguimientos para obtener los registros de autenticación de Capa 2 (L2):

- **set trace group-wireless-secure level debug**
- **set trace group-wireless-secure filter mac0021.6a89.51ca**

Habilite estos seguimientos para obtener los registros de eventos DHCP:

- **set trace dhcp events level debug**
- **set trace dhcp events filter mac 0021.6a89.51ca**

A continuación se muestran algunos ejemplos de trazas exitosas:

```
[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 (0x57ca4000000048): 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**