

Exemple de configuration EAP-FAST avec serveur RADIUS interne pour les WLC EAP-FAST d'accès convergé des gammes 5760, 3850 et 3650

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Présentation de la configuration](#)

[Configurer le WLC avec l'interface de ligne de commande](#)

[Configurer le WLC avec l'interface graphique utilisateur](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer les contrôleurs de réseau local sans fil (WLC) de la gamme Cisco Converged Access 5760, 3850 et 3650 afin d'agir en tant que serveurs RADIUS qui exécutent l'authentification flexible Cisco Extensible Authentication Protocol via Secure Protocol (EAP-FAST, dans cet exemple) pour l'authentification client.

Généralement, un serveur RADIUS externe est utilisé pour authentifier les utilisateurs, ce qui n'est pas une solution possible dans certains cas. Dans ces situations, un WLC d'accès convergé peut agir en tant que serveur RADIUS, où les utilisateurs sont authentifiés par rapport à la base de données locale configurée dans le WLC. Il s'agit d'une fonctionnalité de serveur RADIUS local.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- Interface graphique ou CLI Cisco IOS® avec le WLC Converged Access 5760, 3850 et 3650
- Concepts EAP (Extensible Authentication Protocol)
- Configuration SSID (Service Set Identifier)
- RADIUS

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 5760 version 3.3.2 (armoire de câblage nouvelle génération [NGWC])
- Point d'accès léger (AP) de la gamme Cisco 3602
- Microsoft Windows XP avec Intel PROset Supplican
- Commutateurs Cisco Catalyst, série 3560

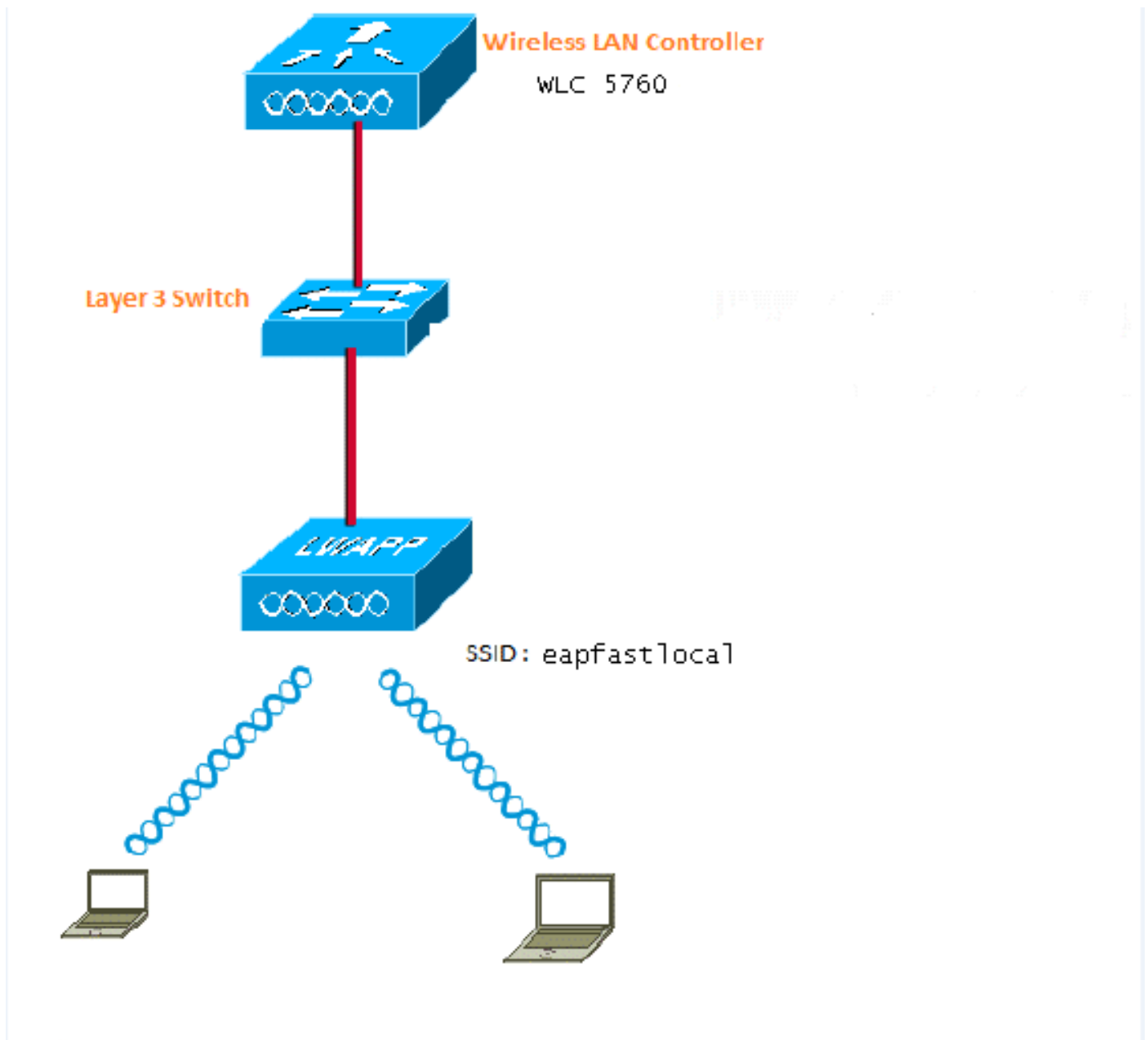
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Note: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Cette illustration donne un exemple de diagramme de réseau:



Présentation de la configuration

Cette configuration est effectuée en deux étapes :

1. Configurez le WLC pour la méthode EAP locale et les profils d'authentification et d'autorisation associés avec l'interface de ligne de commande ou l'interface utilisateur graphique.
2. Configurez le WLAN et mappez la liste de méthodes qui possède les profils d'authentification et d'autorisation.

Configurer le WLC avec l'interface de ligne de commande

Complétez ces étapes afin de configurer le WLC avec l'interface de ligne de commande :

1. Activez le modèle AAA sur le WLC :

```
aaa new-model
```

2. Définissez l'authentification et l'autorisation :

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

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

3. Configurez le profil EAP local et la méthode (EAP-FAST est utilisé dans cet exemple) :

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

4. Configurez les paramètres avancés EAP-FAST :

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

5. Configurez le WLAN et associez le profil d'autorisation local au WLAN :

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

6. Configurez l'infrastructure afin de prendre en charge la connectivité du client :

```
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
```

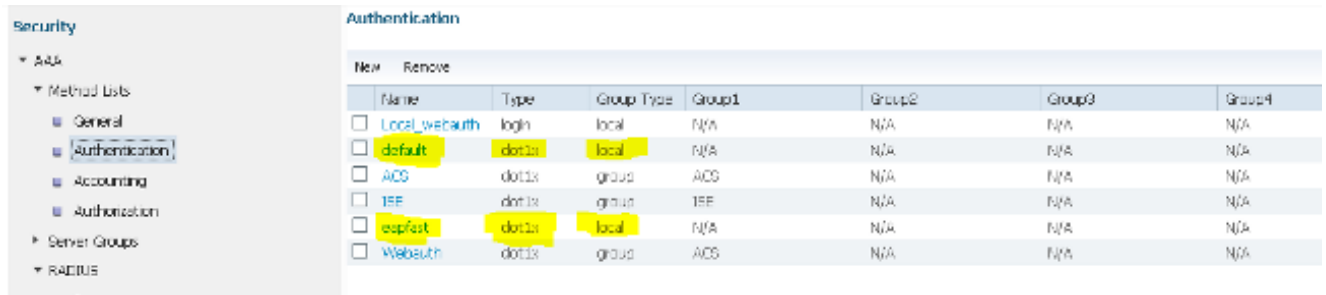
Configurer le WLC avec l'interface graphique utilisateur

Complétez ces étapes afin de configurer le WLC avec l'interface utilisateur graphique :

1. Configurez la liste des méthodes pour l'authentification :

Configurez le type **eapfast** en **Dot1x**.

Configurez le type de groupe **eapfast** en tant que **Local**.

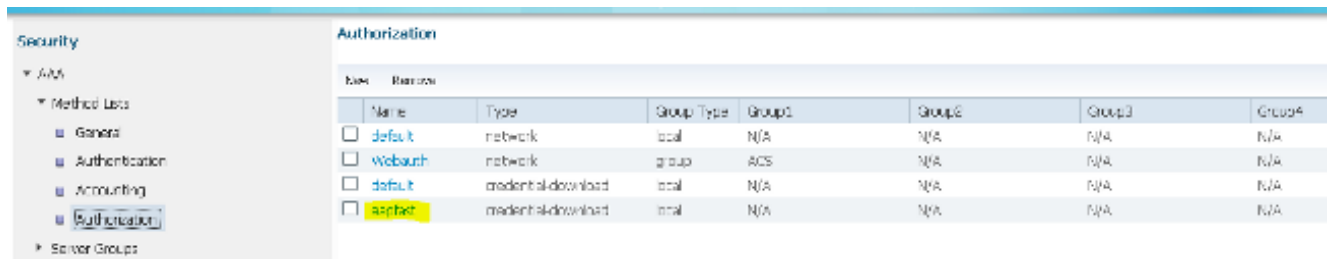


New		Remove					
Name	Type	Group Type	Group1	Group2	Group3	Group4	
<input type="checkbox"/> Local_Webauth	login	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A	
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A	
<input type="checkbox"/> TEF	dot1x	group	TEF	N/A	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. Configurez la liste des méthodes pour l'autorisation :

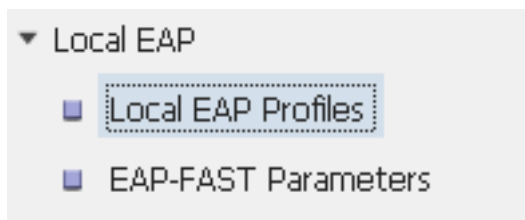
Configurez le type **eapfast** en tant que **Credential-Download**.

Configurez le type de groupe **eapfast** en tant que **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. Configurez le profil EAP local :



4. Créez un nouveau profil et sélectionnez le type EAP :



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

Le nom du profil est **rapide** et le type EAP sélectionné est **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. Configurez les paramètres de la méthode EAP-FAST :

EAP-FAST Method Parameters

New Remove

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

La clé de serveur est configurée en tant que **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. Cochez la case **Contrôle d'authentification système Dot1x** et sélectionnez **apfast** pour les listes de méthodes. Cela vous aide à effectuer l'authentification EAP locale.

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. Configurez le WLAN pour le cryptage 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**

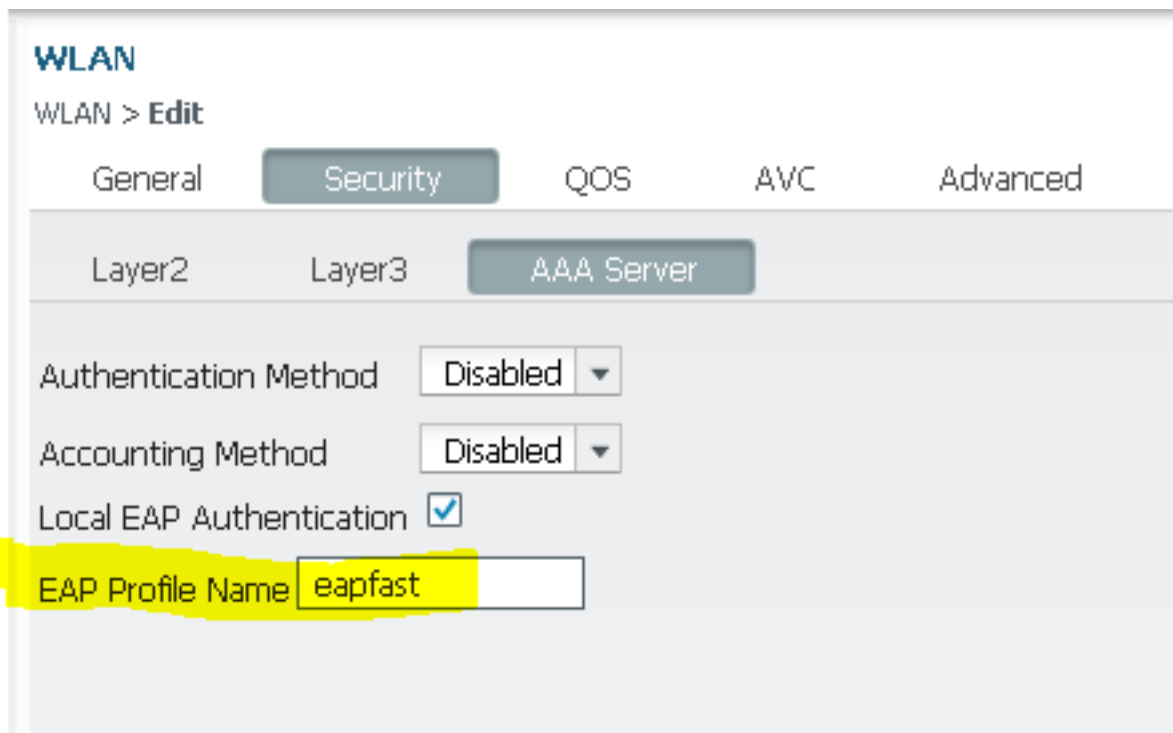
General Security QOS AVC Advanced

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 ▾

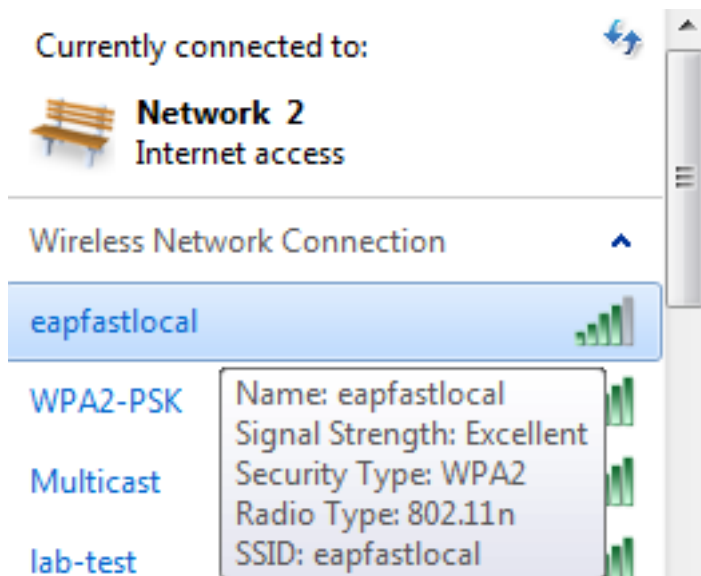
8. Dans l'onglet **Serveur AAA**, mappez le nom de profil EAP **eapfast** au WLAN :



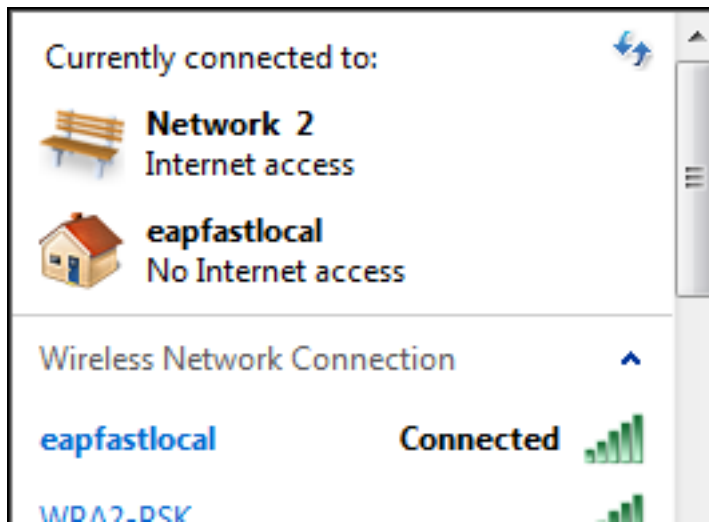
Vérification

Complétez ces étapes afin de vérifier que votre configuration fonctionne correctement :

1. Connectez le client au WLAN :



2. Vérifiez que la fenêtre des informations d'identification et de connexion d'accès protégé (PAC) s'affiche et que vous devez accepter pour pouvoir authentifier :



Dépannage

Cisco vous recommande d'utiliser des traces afin de dépanner les problèmes sans fil. Les traces sont enregistrées dans la mémoire tampon circulaire et ne nécessitent pas de processeur.

Activez ces traces afin d'obtenir les journaux d'authentification de couche 2 (L2) :

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

Activez ces traces afin d'obtenir les journaux des événements DHCP :

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

Voici quelques exemples de traces réussies :

```
[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**