

使用內部RADIUS伺服器的融合接入5760、3850和3650系列WLC EAP-FAST配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態概觀](#)

[使用CLI設定WLC](#)

[使用GUI設定WLC](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何設定Cisco Converged Access 5760、3850和3650系列無線LAN控制器(WLC)以充當RADIUS伺服器，這些伺服器執行Cisco可擴充驗證通訊協定 — 透過安全通訊協定的彈性驗證（在本範例中為EAP-FAST），以進行使用者端驗證。

通常使用外部RADIUS伺服器來驗證使用者身分，在某些情況下，這不是可行的解決方案。在這些情況下，融合存取WLC可以充當RADIUS伺服器，以便使用者對WLC中設定的本機資料庫進行驗證。此功能稱為本地RADIUS伺服器功能。

必要條件

需求

思科建議您在嘗試此設定之前瞭解以下主題：

- 採用融合接入5760、3850和3650系列WLC的Cisco IOS® GUI或CLI
- 可擴充驗證通訊協定(EAP)概念
- 服務組識別碼(SSID)配置
- RADIUS

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5760系列WLC版本3.3.2 (下一代配線間[NGWC])
- Cisco 3602系列輕量型存取點(AP)
- Microsoft Windows XP與英特爾PROset請求方

- Cisco Catalyst 3560 系列交換器

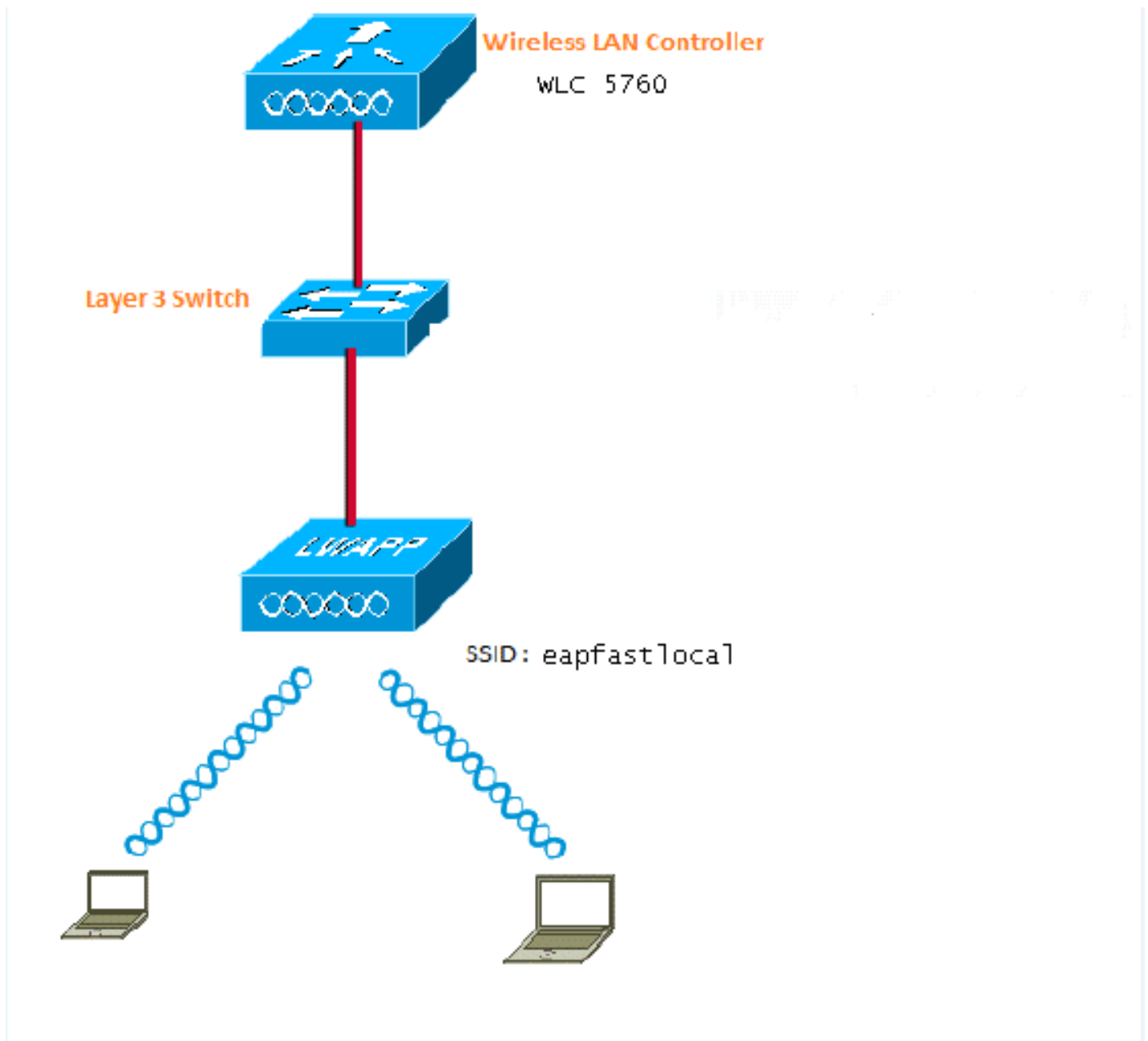
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用[命令查詢工具](#)（僅供已註冊客戶使用）可獲取本節中使用的命令的更多資訊。

網路圖表

此圖提供網路圖示範例：



組態概觀

此配置分兩步完成：

1. 使用CLI或GUI為本地EAP方法和相關的身份驗證和授權配置檔案配置WLC。
2. 配置WLAN並對映具有身份驗證和授權配置檔案的方法清單。

使用CLI設定WLC

完成以下步驟，以便使用CLI設定WLC:

1. 在WLC上啟用AAA型號：

```
aaa new-model
```

2. 定義身份驗證和授權：

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

```
aaa authentication dot1x eapfast local
```

```
aaa authorization credential-download eapfast local
```

```
aaa authentication dot1x default local
```

3. 配置本地EAP配置檔案和方法（本示例中使用了EAP-FAST）：

```
eap profile eapfast
```

```
method fast
```

```
!
```

4. 配置高級EAP-FAST引數：

```
eap method fast profile eapfast
```

```
description test
```

```
authority-id identity 1
```

```
authority-id information 1
```

```
local-key 0 cisco123
```

5. 配置WLAN並將本地授權配置檔案對映到WLAN:

```
wlan eapfastlocal 13 eapfastlocal
```

```
client vlan VLAN0020
```

```
local-auth eapfast
```

```
session-timeout 1800
```

```
no shutdown
```

6. 配置基礎設施以支援客戶端連線：

```
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

```

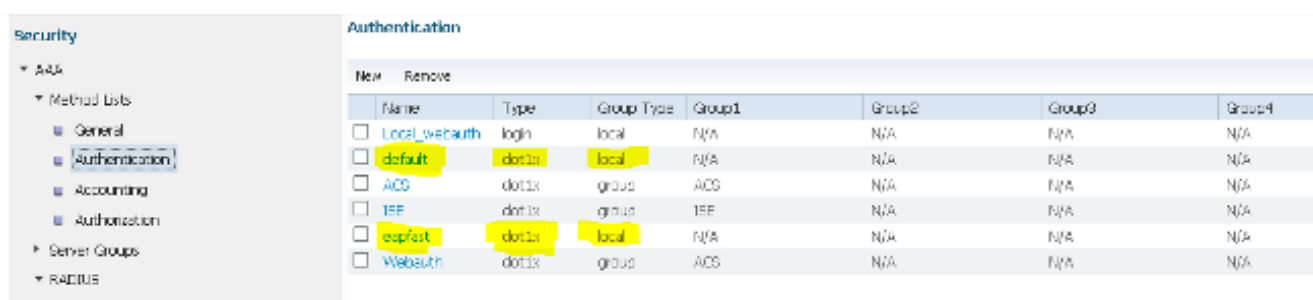
使用GUI設定WLC

完成以下步驟，以便使用GUI設定WLC:

1. 配置身份驗證的方法清單：

將eapfast型別配置為Dot1x。

將eapfast組型別配置為Local。

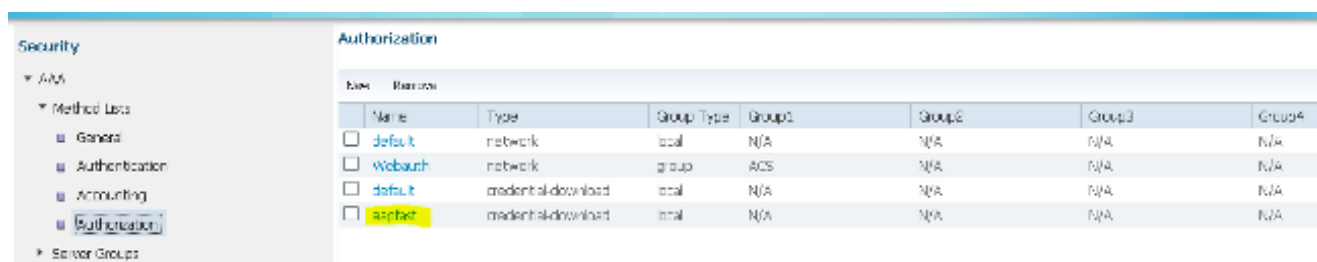


Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A
<input type="checkbox"/> IEF	dot1x	group	IEF	N/A	N/A	N/A
<input type="checkbox"/> 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. 配置用於授權的方法清單：

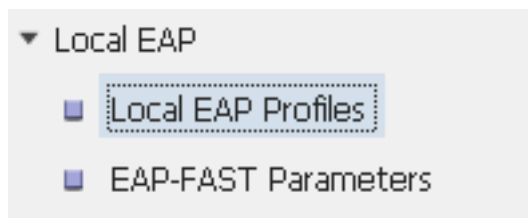
將eapfast型別配置為Credential-Download。

將eapfast組型別配置為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. 配置本地EAP配置檔案：



4. 建立新配置檔案並選擇EAP型別：

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

配置檔名稱為eapfast，選擇的EAP型別為EAP-FAST:

Local EAP Profiles
Local EAP Profiles > Edit

Profile Name

LEAP

EAP-FAST

EAP-TLS

PEAP

Trustpoint

5. 配置EAP-FAST方法引數：

EAP-FAST Method Parameters

New Remove

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

伺服器金鑰配置為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. 選中**Dot1x System Auth Control**覈取方塊，然後選擇**eapfast**作為Method Lists。這有助於您執行本地EAP身份驗證。

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. 為WPA2 AES加密配置WLAN:

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**

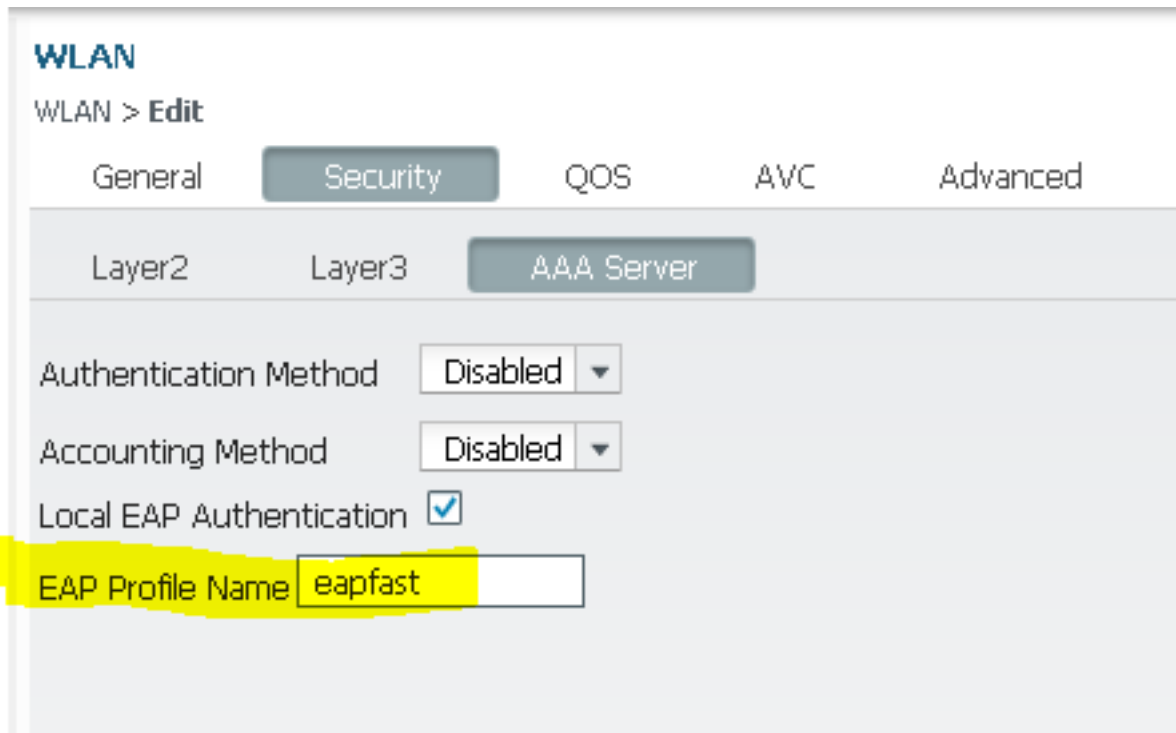
General Security QOS AVC Advanced

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 ▾

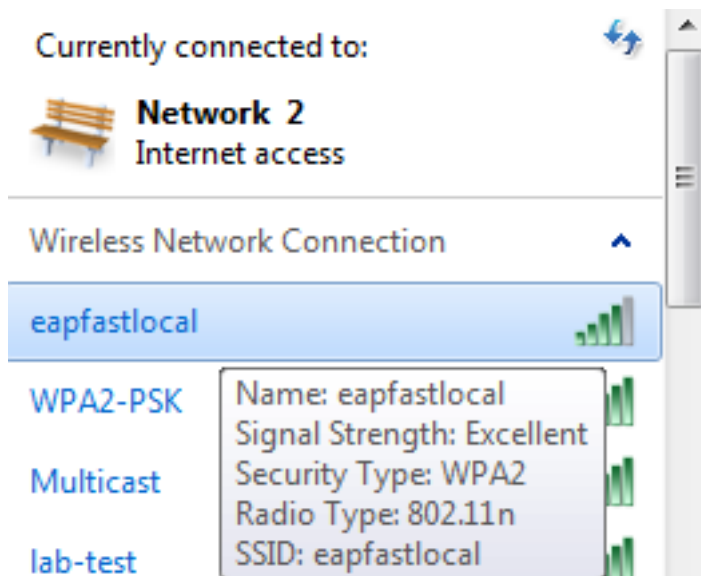
8. 在AAA Server 頁籤上，將EAP配置檔名稱eapfast對映到WLAN:



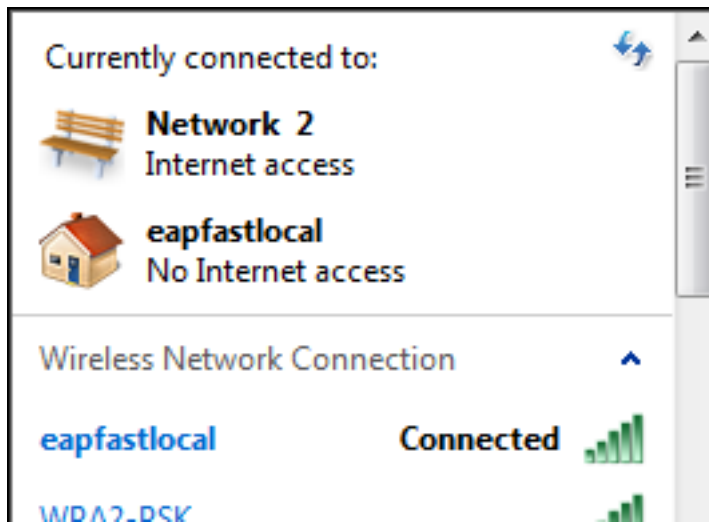
驗證

完成以下步驟，確認您的組態是否正常運作：

1. 將使用者端連線到WLAN:



2. 驗證是否顯示「Protected Access Credentials(PAC)」彈出視窗，並且您必須接受才能成功進行身份驗證：



疑難排解

思科建議您使用追蹤來排解無線問題。跟蹤儲存在循環緩衝區中，不佔用大量處理器。

啟用這些追蹤以取得第2層(L2)驗證日誌：

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

啟用這些跟蹤以獲取DHCP事件日誌：

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

以下是一些成功跟蹤的示例：

```
[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**