

内部 RADIUS サーバで使用するコンバージド アクセス 5760、3850、および 3650 シリーズ WLS EAP-FAST の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定の概要](#)

[CLIによるWLCの設定](#)

[GUIを使用したWLCの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、クライアント認証用にCisco Extensible Authentication Protocol-Flexible Authentication(EAP-FAST)を実行するRADIUSサーバとして動作するように、Cisco Converged Access 5760、3850、および3650シリーズワイヤレスLANコントローラ(WLC)を設定する方法について説明します。

通常、ユーザを認証するために外部RADIUSサーバが使用されます。これは、場合によっては実行可能なソリューションではありません。このような状況では、コンバージドアクセスWLCはRADIUSサーバとして機能し、WLCで設定されているローカルデータベースに対してユーザが認証されます。これは、ローカル RADIUS サーバ機能と呼ばれます。

前提条件

要件

この設定を開始する前に、次の項目に関する知識を得ておくことを推奨します。

- コンバージドアクセス5760、3850、および3650シリーズWLCを使用したCisco IOS® GUIまたはCLI
- Extensible Authentication Protocol(EAP)の概念
- サービス セット ID (SSID) の設定
- RADIUS

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 5760シリーズWLCリリース3.3.2(次世代ワイヤリングクローゼット(NGWC))
- Cisco 3602シリーズLightweightアクセスポイント(AP)
- Microsoft Windows XP と Intel PROset サプリカント
- Cisco Catalyst 3560 シリーズ スイッチ

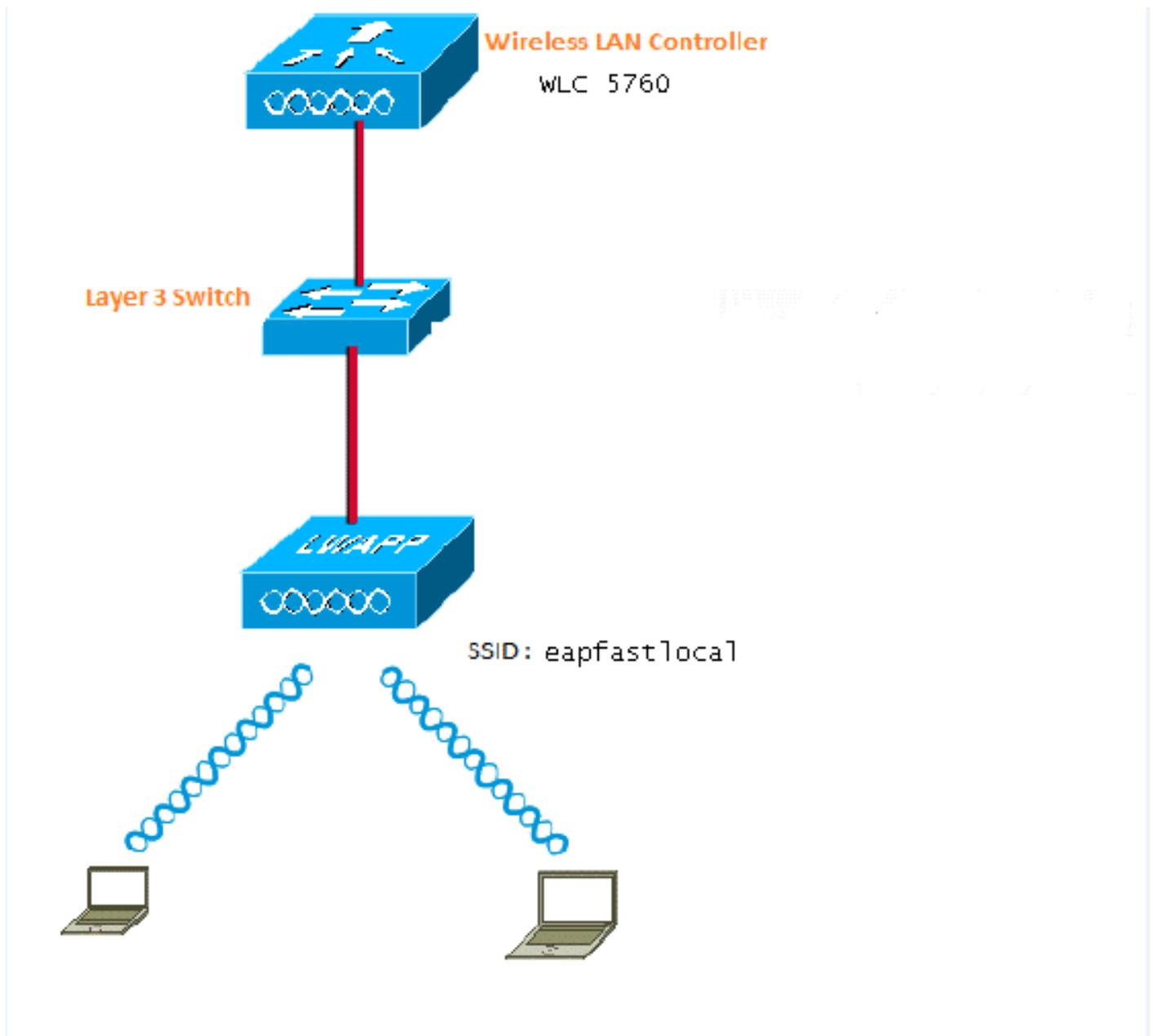
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

注：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

次の画像は、ネットワーク ダイアグラムの例を示しています。



設定の概要

この設定は、次の2つの手順で行います。

1. CLIまたはGUIを使用して、ローカルEAP方式および関連する認証および許可プロファイル用にWLCを設定します。
2. WLANを設定し、認証および認可プロファイルを持つ方式リストをマッピングします。

CLIによるWLCの設定

CLIを使用してWLCを設定するには、次の手順を実行します。

1. WLCでAAAモデルを有効にします。

```
aaa new-model
```

2. 認証と認可を定義します。

```
aaa local authentication eapfast authorization eapfast

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

3. ローカルEAPプロファイルと方式を設定します (この例ではEAP-FASTを使用します)。

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

4. 高度なEAP-FASTパラメータを設定します。

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

5. WLANを設定し、ローカル認可プロファイルをWLANにマッピングします。

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

6. クライアント接続をサポートするようにインフラストラクチャを設定します。

```
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
```

GUIを使用したWLCの設定

GUIを使用してWLCを設定するために次の手順を実行します。

1. 認証の方式リストを設定します。

eapfastタイプをDot1xとして設定します。

[Fast Group Type]を[Local]に設定します。



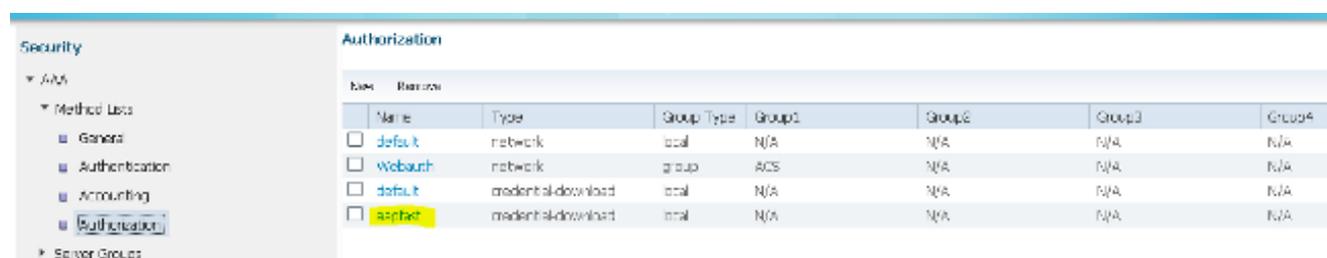
The screenshot shows the 'Security' configuration page with the 'Authentication' tab selected. The left sidebar shows a tree view with 'Authentication' highlighted. The main area displays a table with columns: Name, Type, Group Type, Group1, Group2, Group3, and Group4. The 'eapfast' row is highlighted in yellow.

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"/> TFF	dot1x	group	TFF	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. 認可の方式リストを設定します。

[Fast Type]を[Credential-Download]に設定します。

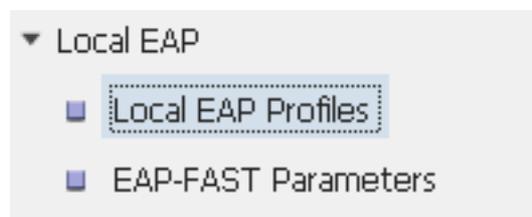
[Fast Group Type]を[Local]に設定します。



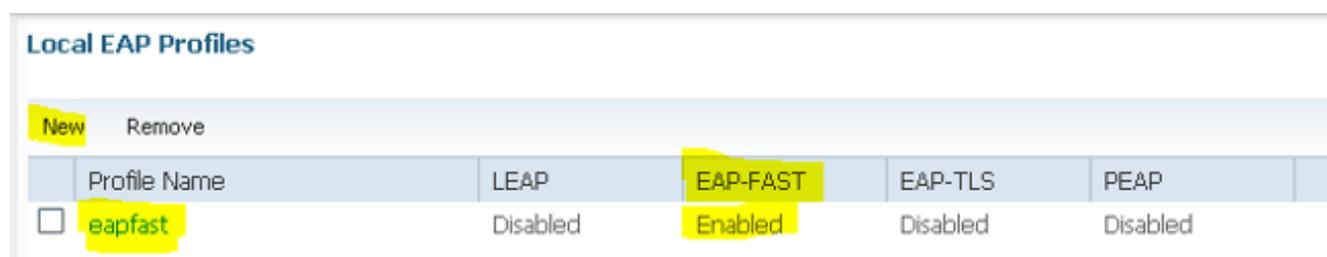
The screenshot shows the 'Security' configuration page with the 'Authorization' tab selected. The left sidebar shows a tree view with 'Authorization' highlighted. The main area displays a table with columns: Name, Type, Group Type, Group1, Group2, Group3, and Group4. The 'eapfast' row is highlighted in yellow.

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. ローカルEAPプロファイルを設定します。



4. 新しいプロファイルを作成し、EAPの種類を選択します。



The screenshot shows the 'Local EAP Profiles' configuration page. The 'eapfast' profile is highlighted in yellow. The 'EAP-FAST' column is also highlighted in yellow.

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

プロファイル名はeapfastで、選択したEAPタイプはEAP-FASTです。

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. EAP-FAST方式パラメータを設定します。

EAP-FAST Method Parameters

New Remove

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

サーバキーはCisco123として設定されています。

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. [Dot1x System Auth Control]チェックボックスをオンにし、[Method Lists]に[eapfast]を選択します。これにより、ローカルEAP認証を実行できます。

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. WPA2 AES暗号化のWLANを設定します。

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**

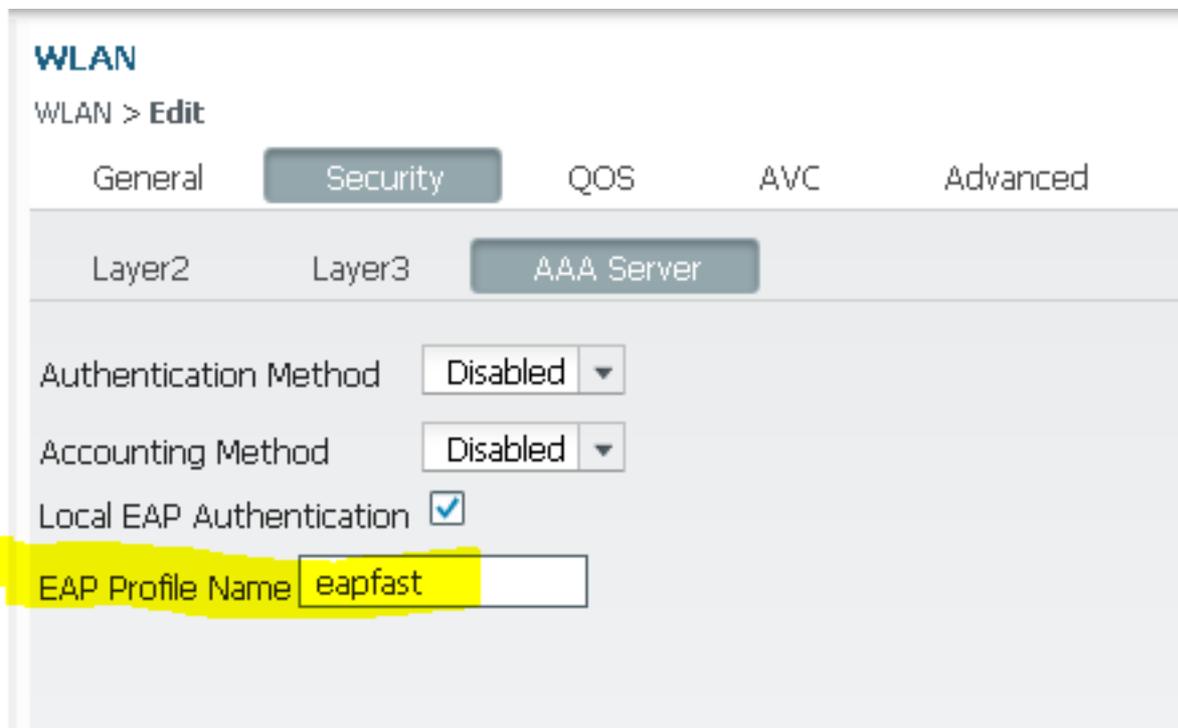
General Security QOS AVC Advanced

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 ▾

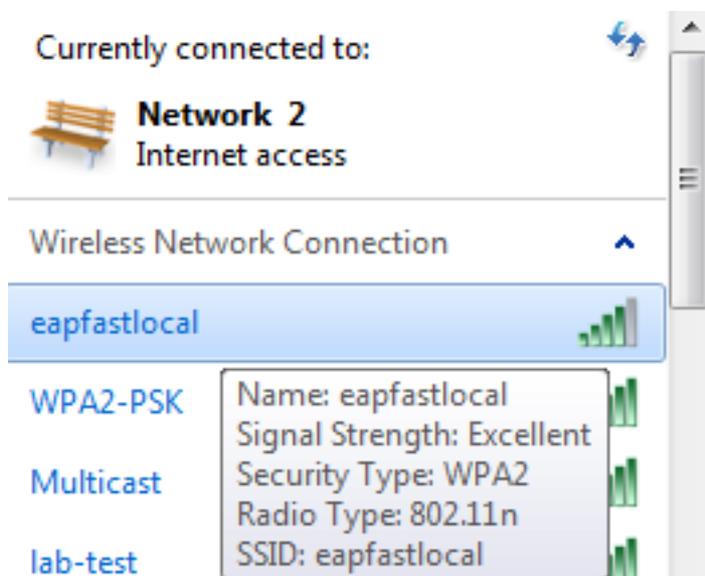
8. [AAA Server]タブで、[EAP Profile Name]をWLANにマップします。



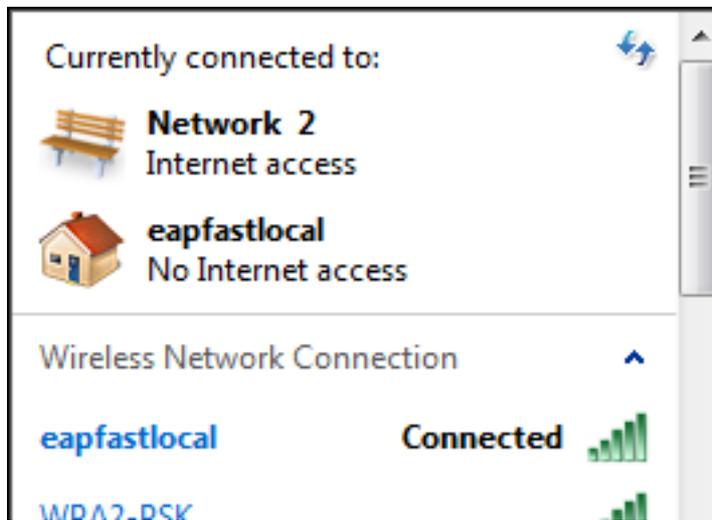
確認

設定が正しく動作していることを確認するには、次の手順を実行します。

1. クライアントをWLANに接続します。



2. Protected Access Credentials(PAC)ポップアップが表示され、認証を正常に行うには受け入れる必要があることを確認します。



トラブルシューティング

無線の問題のトラブルシューティングを行う際はトレースを使用することを推奨します。トレースは循環バッファに保存されているため、プロセッサに負荷はかかりません。

レイヤ2(L2)認証ログを取得するには、次のトレースを有効にします。

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

DHCPイベントログを取得するには、次のトレースを有効にします。

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

成功したトレースの例を次に示します。

```
[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