

# Acesso convergido 5760, 3850, e 3650 Series WLC EAP-FAST com exemplo de configuração do raio de servidor interno



ID do Documento: 117664

Atualizado em: abril 18, 2014

Contribuído por Surendra BG, engenheiro de TAC da Cisco.



[Transferência PDF](#)



[Imprimir](#)

[Feedback](#)

## Produtos Relacionados

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

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Visão geral sobre a configuração](#)

[Configurar o WLC com o CLI](#)

[Configurar o WLC com o GUI](#)

[Verificar](#)

[Troubleshooting](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento descreve como configurar Cisco convergiu acesso 5760, 3850, e controladores do Wireless LAN do 3650 Series (WLC) a fim atuar como os servidores Radius que executam a autenticação Protocolo flexível da autenticação extensível de Cisco através do protocolo seguro (EAP-FAST, neste exemplo) para a autenticação do cliente.

Um servidor de raio externo é usado geralmente a fim autenticar usuários, que não seja uma solução possível em alguns casos. Nestas situações, um acesso convergido WLC pode atuar como um servidor Radius, onde os usuários sejam autenticados contra o base de dados local que é configurado no WLC. Isto é chamado uma característica local do servidor Radius.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos antes que você tente esta configuração:

- <sup>®</sup> GUI ou CLI do Cisco IOS com o acesso convergido 5760, 3850, e 3650 Series WLC
- Conceitos do Extensible Authentication Protocol (EAP)
- Configuração do Service Set Identifier (SSID)
- RADIUS

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Liberação 3.3.2 do Cisco 5760 Series WLC ([NGWC] do armário de fiação da próxima geração)
- Access Point (AP) do peso leve do Cisco 3602 Series
- Microsoft Windows XP com o suplicante de Intel PROset
- Cisco Catalyst 3560 Series Switches

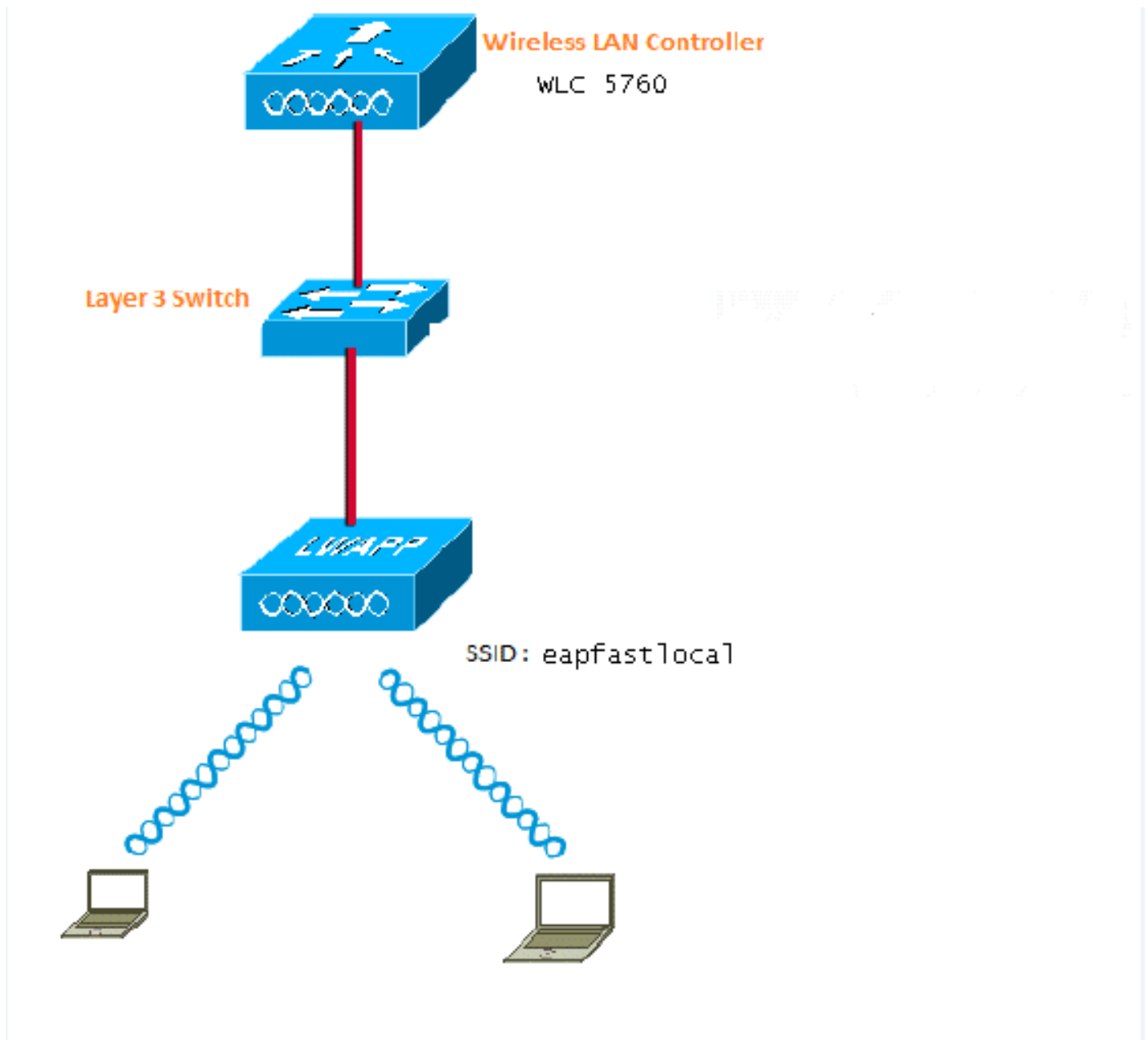
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Nota: Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

### Diagrama de Rede

Esta imagem fornece um exemplo de um diagrama da rede:



## Visão geral sobre a configuração

Esta configuração é terminada em duas etapas:

1. Configurar o WLC para o método de EAP local e os perfis relacionados da authentication e autorização com o CLI ou o GUI.
2. Configurar o WLAN e trace a lista de método que tem os perfis da authentication e autorização.

## Configurar o WLC com o CLI

Termine estas etapas a fim configurar o WLC com o CLI:

1. Permita o modelo AAA no WLC:

```
aaa new-model
```

2. Defina a authentication e autorização:

```
aaa local authentication eapfast authorization eapfast

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

3. Configurar o perfil local EAP e o método (EAP-FAST é usado neste exemplo):

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

4. Configurar os parâmetros EAP-FAST avançados:

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

5. Configurar o WLAN e trace o perfil da autorização local ao WLAN:

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

6. Configurar a infraestrutura a fim apoiar a conectividade de 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
```

## Configurar o WLC com o GUI

Termine estas etapas a fim configurar o WLC com o GUI:

1. Configurar a lista de método para a autenticação:

Configurar o tipo do **eapfast** como o **dot1x**.

Configurar o tipo de grupo do **eapfast** como o **Local**.

Security		Authentication						
AAA		New Remove						
Method Lists		Name	Type	Group Type	Group1	Group2	Group3	Group4
General		<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A
Authentication		<input type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A
Accounting		<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A
Authorization		<input type="checkbox"/> TSE	dot1x	group	TSE	N/A	N/A	N/A
Server Groups		<input type="checkbox"/> eapfast	dot1x	local	N/A	N/A	N/A	N/A
RADIUS		<input type="checkbox"/> Webauth	dot1x	group	ACS	N/A	N/A	N/A

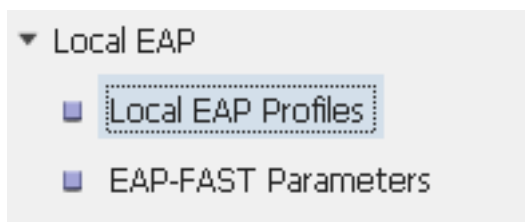
2. Configurar a lista de método para a autorização:

Configurar o tipo do **eapfast** como a Credencial-transferência.

Configurar o tipo de grupo do **eapfast** como o **Local**.

Security		Authorization						
AAA		New Remove						
Method Lists		Name	Type	Group Type	Group1	Group2	Group3	Group4
General		<input type="checkbox"/> default	network	local	N/A	N/A	N/A	N/A
Authentication		<input type="checkbox"/> Webauth	network	group	ACS	N/A	N/A	N/A
Accounting		<input type="checkbox"/> default	credential-download	local	N/A	N/A	N/A	N/A
Authorization		<input type="checkbox"/> eapfast	credential-download	local	N/A	N/A	N/A	N/A
Server Groups								

3. Configurar o perfil local EAP:



4. Crie um perfil novo e selecione o tipo EAP:

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

O nome de perfil é **eapfast** e o tipo selecionado EAP é **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. Configurar os parâmetros EAP-FAST do método:

### EAP-FAST Method Parameters

New Remove

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

A chave de servidor é configurada como o **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. Verifique a caixa de verificação do **controle do AUTH do sistema do dot1x** e selecione o **eapfast** para as listas de método. Isto ajuda-o a executar a autenticação de EAP local.

<b>Security</b>	<b>General</b>
▼ 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. Configurar o WLAN para a criptografia de 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

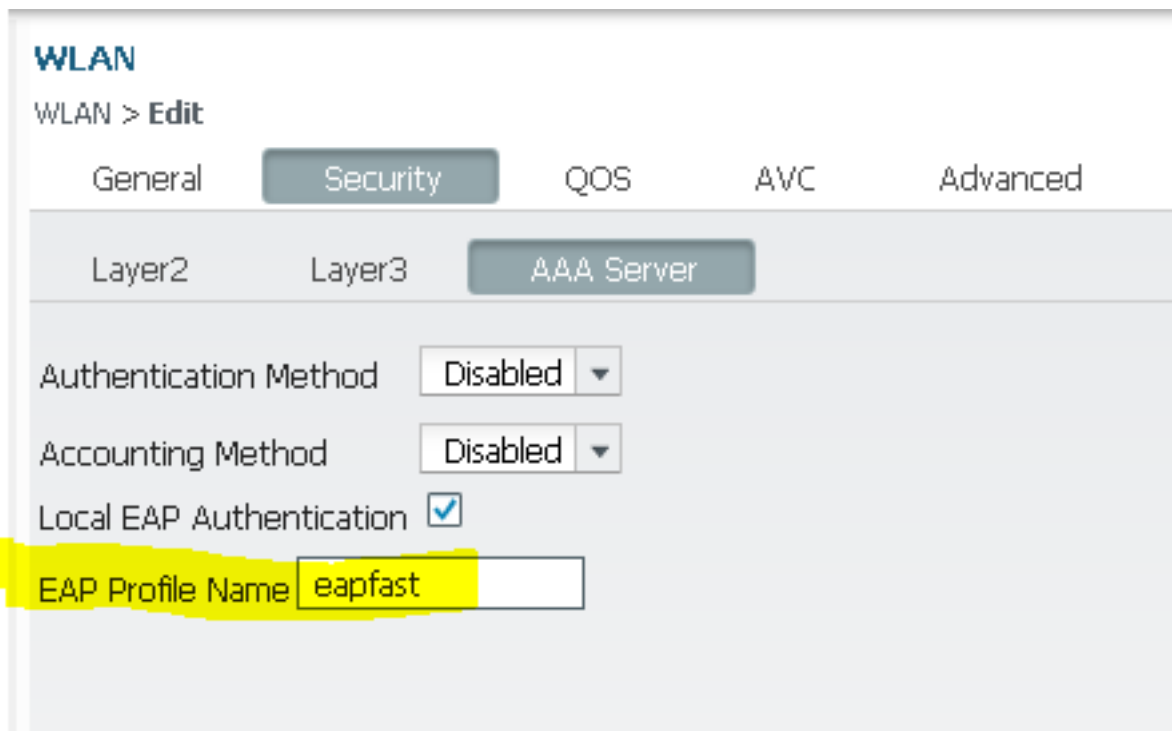
Layer2 Layer3 AAA Server

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. Na aba do **servidor AAA**, trace o **eapfast** do nome de perfil EAP ao WLAN:

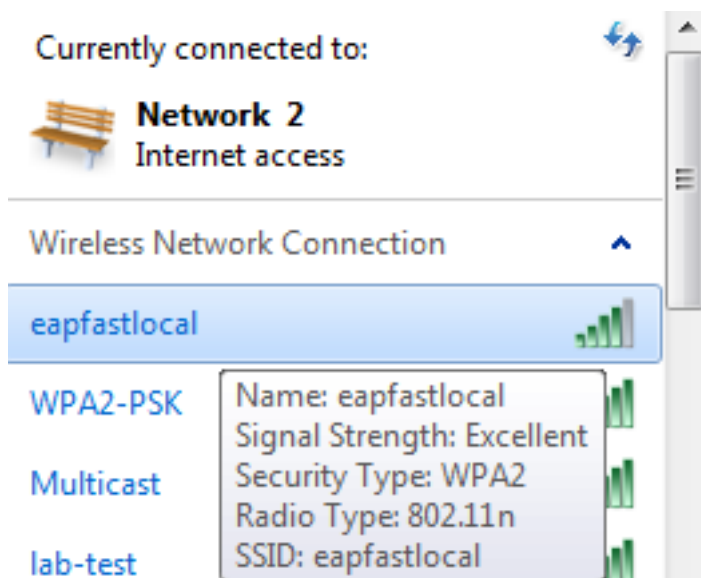




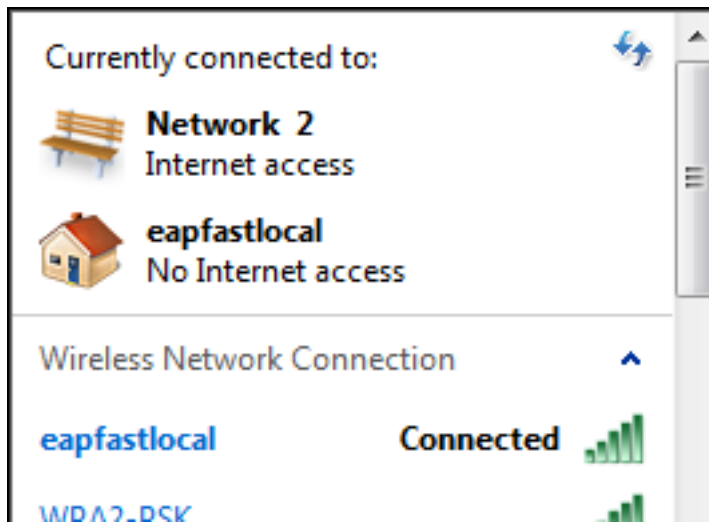
## Verificar

Termine estas etapas a fim verificar que sua configuração trabalha corretamente:

1. Conecte o cliente ao WLAN:



2. Verifique que o pop-up protegido das credenciais do acesso (PAC) aparece e que você deve aceitar a fim autenticar com sucesso:



## Troubleshooting

Cisco recomenda que você use traços a fim de pesquisar defeitos em edições wireless. Os traços salvam no buffer circular e não são utilização de processador.

Permita estes traços a fim de obter os logs do AUTH da camada 2 (L2):

- o nível grupo-Sem fio-seguro do traço ajustado debuga
- ajuste o filtro grupo-Sem fio-seguro mac0021.6a89.51ca do traço

Permita estes traços a fim de obter os logs de eventos DHCP:

- os eventos ajustados DHCP do traço em nível debugam
- ajuste o Mac 0021.6a89.51ca do filtro dos eventos DHCP do traço

Estão aqui alguns exemplos de traços bem sucedidos:

```
[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
```

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

## Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: abril 18, 2014

ID do Documento: 117664