

与内部RADIUS服务器配置示例的聚合的访问5760，3850和3650系列WLC EAP-FAST

TAC

文档ID117664

已更新：四月18，2014

贡献用Surendra BG，Cisco TAC工程师。



[下载 pdf文档](#)



[打印](#)

[反馈](#)

相关产品

- [无线，LAN \(WLAN\)](#)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置概述](#)

[配置与CLI的WLC](#)

[配置与GUI的WLC](#)

[验证](#)

[故障排除](#)

[相关的思科支持社区讨论](#)

简介

本文描述如何配置Cisco聚合的访问5760，3850和3650系列无线局域网控制器(WLCs)为了作为通过安全协议的RADIUS服务器(EAP-FAST执行Cisco扩展验证灵活协议验证，在本例中)客户端验证的。

通常外部RADIUS服务器用于为了验证用户，在某些情况下不是可行解决方案。在这些情况下，一聚合的访问WLC能作为RADIUS服务器，用户验证本地数据库在WLC配置。此功能称为本地

RADIUS 服务器功能。

[先决条件](#)

[要求](#)

Cisco 建议您在尝试进行此配置之前了解下列主题：

- Cisco IOS GUI或CLI与聚合的访问5760，3850和3650系列WLC
- 可扩展的认证协议(EAP)概念
- 服务集标识(SSID)配置
- RADIUS

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- Cisco 5760系列WLC版本3.3.2 (下一代配线间[NGWC])
- Cisco 3602系列轻量级接入点(AP)
- 有英特尔PROset请求方的Microsoft Windows XP
- Cisco Catalyst 3560 系列交换机

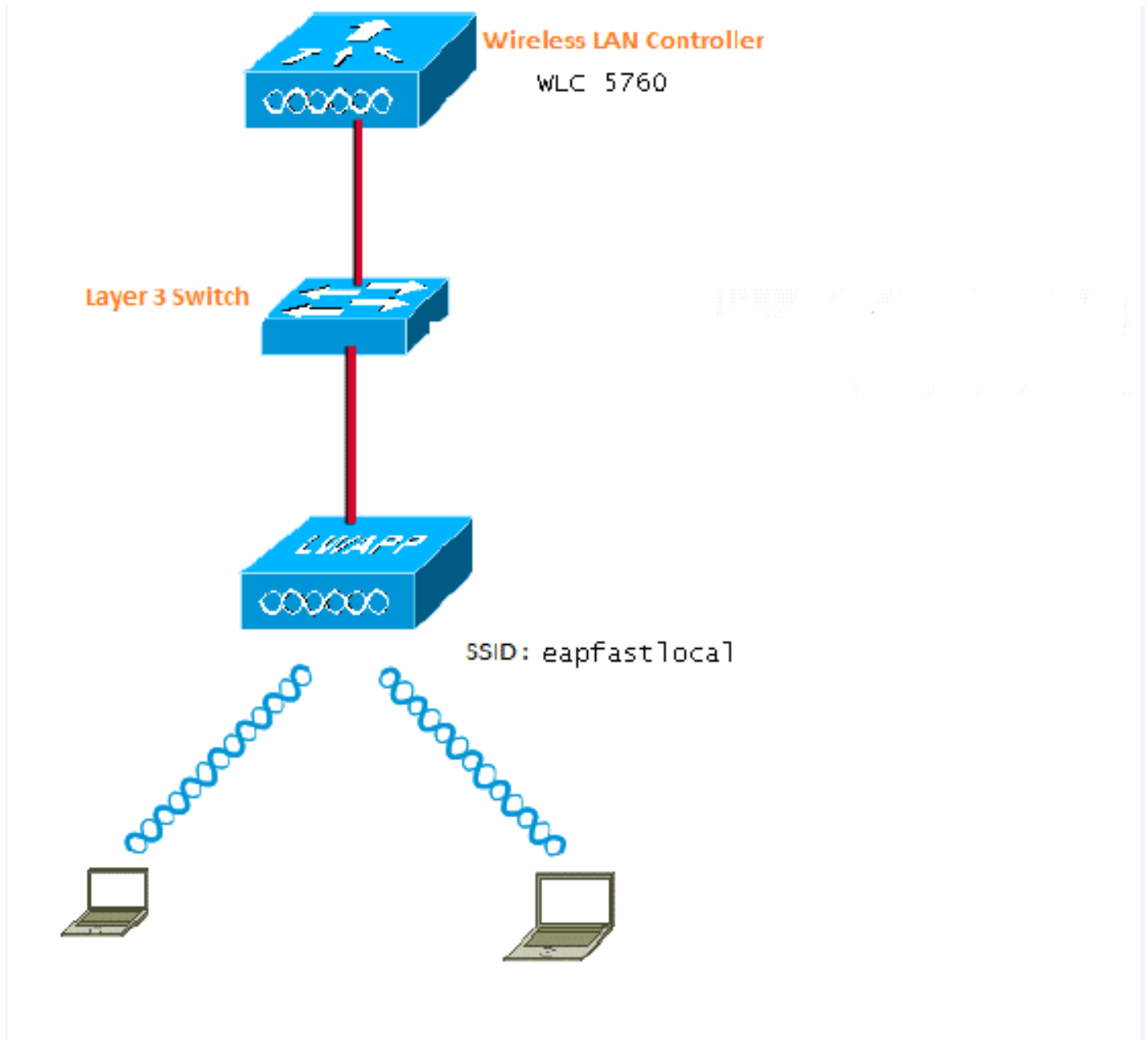
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[配置](#)

注意：使用[命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

[网络图](#)

此镜像提供网络图的示例：



配置概述

此配置在两个步骤完成：

1. 配置本地EAP方法的WLC和与CLI或GUI的相关认证和授权配置文件。
2. 配置WLAN并且映射有认证和授权配置文件的方法列表。

配置与CLI的WLC

完成这些步骤为了配置与CLI的WLC：

1. 启用在WLC的AAA型号：

```
aaa new-model
```

2. 定义认证和授权：

```
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 profile和方法(EAP-FAST用于此示例) :

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

4. 配置先进的EAP-FAST参数 :

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

5. 配置WLAN并且映射本地授权配置文件对WLAN :

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

6. 配置基础设施为了支持客户端连接 :

```
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
```

配置与GUI的WLC

完成这些步骤为了配置与GUI的WLC :

1. 配置验证的方法列表 :

配置eapfast类型作为Dot1x。

配置eapfast组类型作为本地。

Security		Authentication																																																																					
<ul style="list-style-type: none"> AAA <ul style="list-style-type: none"> Method Lists <ul style="list-style-type: none"> General Authentication Accounting Authorization Server Groups RADIUS 		<table border="1"> <thead> <tr> <th colspan="2">New Remove</th> <th>Name</th> <th>Type</th> <th>Group Type</th> <th>Group1</th> <th>Group2</th> <th>Group3</th> <th>Group4</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td></td> <td>Local_webauth</td> <td>login</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>default</td> <td>dot1x</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>ACS</td> <td>dot1x</td> <td>group</td> <td>ACS</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>ISE</td> <td>dot1x</td> <td>group</td> <td>ISE</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>eapfast</td> <td>dot1x</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>Webauth</td> <td>dot1x</td> <td>group</td> <td>ACS</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>							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"/>		ISE	dot1x	group	ISE	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
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"/>		ISE	dot1x	group	ISE	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																																																															

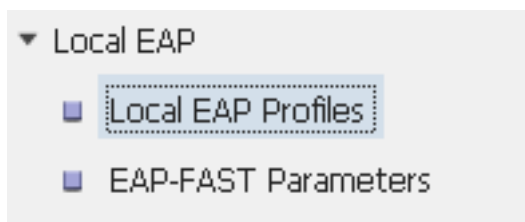
2. 配置授权的方法列表：

配置eapfast类型作为凭证下载。

配置eapfast组类型作为本地。

Security		Authorization																																																			
<ul style="list-style-type: none"> AAA <ul style="list-style-type: none"> Method Lists <ul style="list-style-type: none"> General Authentication Accounting Authorization Server Groups 		<table border="1"> <thead> <tr> <th colspan="2">New Remove</th> <th>Name</th> <th>Type</th> <th>Group Type</th> <th>Group1</th> <th>Group2</th> <th>Group3</th> <th>Group4</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td></td> <td>default</td> <td>network</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>Webauth</td> <td>network</td> <td>group</td> <td>ACS</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>default</td> <td>credential-download</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> <td>eapfast</td> <td>credential-download</td> <td>local</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>							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
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. 配置本地Eap profile：



4. 创建新配置文件并且选择EAP类型：

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

配置文件名称是eapfast，并且选定EAP类型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. 配置EAP-FAST方法参数：

EAP-FAST Method Parameters

New Remove

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

服务器密钥配置作为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. 检查Dot1x系统验证控制复选框并且选择方法列表的eapfast。这帮助您进行本地EAP验证。

Security	General
▼ AAA	
▼ Method Lists	
■ General	
■ Authentication	
■ Accounting	
■ Authorization	
▶ Server Groups	
▼ RADIUS	
	Dot1x System Auth Control <input checked="" type="checkbox"/>
	Local Authentication Method List ▼
	Authentication Method List eapfast ▼
	Local Authorization Method List ▼
	Authorization Method List eapfast ▼

7. 配置WPA2 AES加密的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**

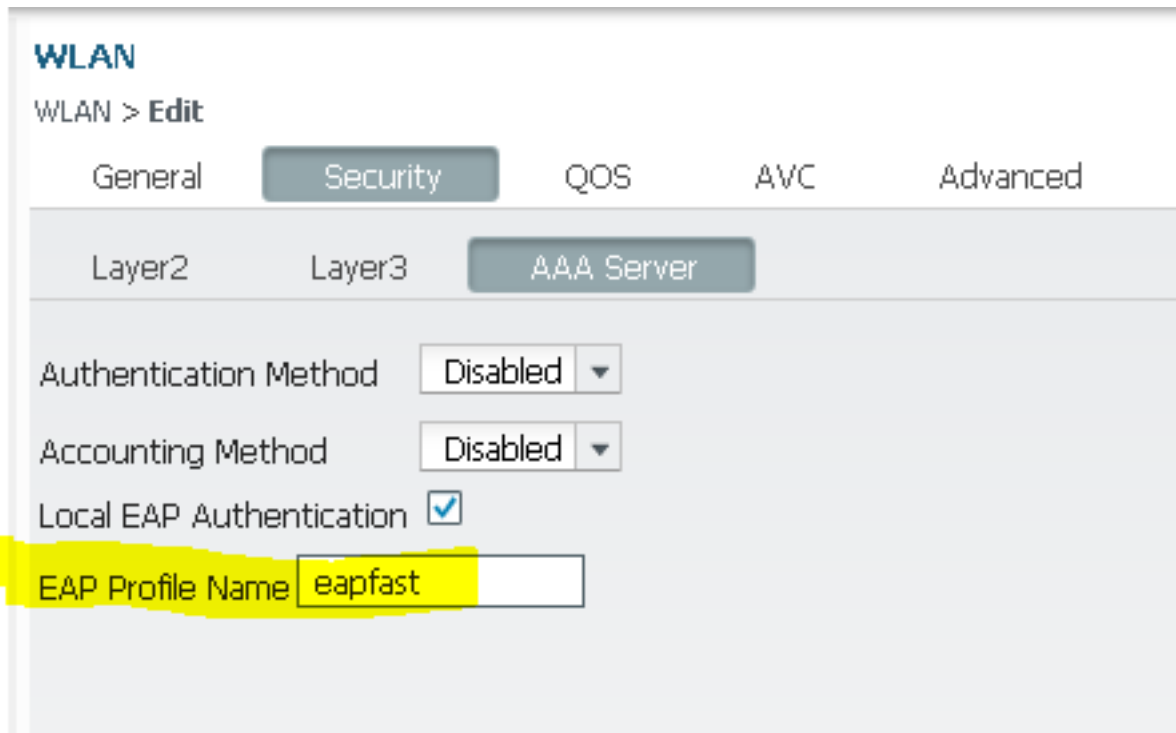
General Security QOS AVC Advanced

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 ▾

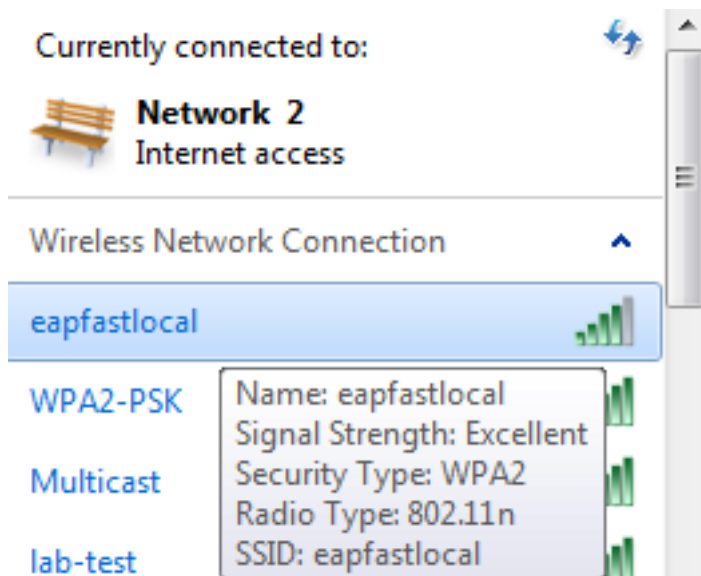
8. 在AAA服务器选项卡，请映射Eap profile名称eapfast对WLAN：



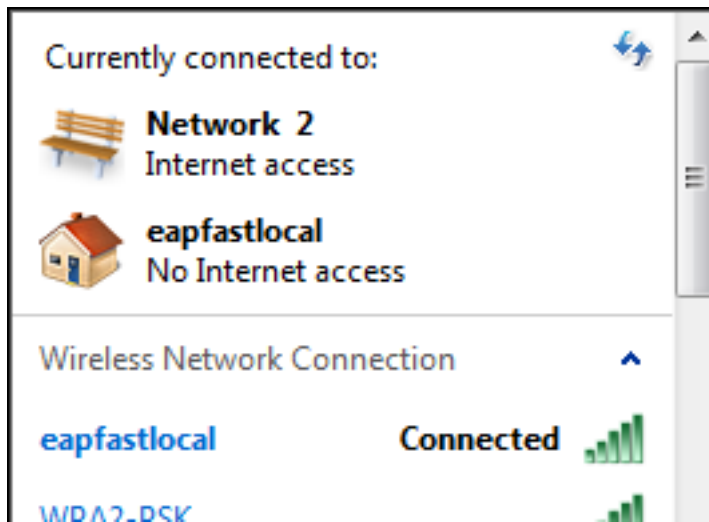
验证

完成这些步骤为了验证您的配置适当地工作：

1. 联络客户端对WLAN：



2. 验证受保护的访问凭证(PAC)弹出式出现，并且您必须接受为了成功验证：



故障排除

思科建议您使用跟踪为了排除故障无线问题。跟踪在圆的缓冲区保存并且不是密集的处理程序。

使这些跟踪为了获取Layer2 (L2)验证日志：

- 设置trace组无线安全级别调试
- 设置trace组无线安全过滤器mac0021.6a89.51ca

使这些跟踪为了获取DHCP事件日志：

- 设置trace dhcp事件级别调试
- 设置trace dhcp事件过滤器mac 0021.6a89.51ca

这是成功的跟踪一些示例：

```
[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
```

```
[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
```

本文档是否是有用？[有](#) [没有](#)

感谢您的反馈。

[打开通信案例](#)（需要[思科服务合同](#)。）

相关的思科支持社区讨论

[思科支持社区](#)是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 [Cisco Technical Tips Conventions](#)。

已更新：四月18，2014

文档ID117664