Converged Access 5760, 3850, and 3650 Series WLC EAP-FAST with Internal RADIUS Server Configuration Example

Contents

Introduction Prerequisites Requirements Components Used Configure Network Diagram Configuration Overview Configure the WLC with the CLI Configure the WLC with the GUI Verify Troubleshoot

Introduction

This document describes how to configure the Cisco Converged Access 5760, 3850, and 3650 Series Wireless LAN Controllers (WLCs) in order to act as RADIUS servers that perform Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST, in this example) for client authentication.

Usually an external RADIUS server is used in order to authenticate users, which is not a feasible solution in some cases. In these situations, a Converged Access WLC can act as a RADIUS server, where users are authenticated against the local database that is configured in the WLC. This is called a Local RADIUS Server feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt this configuration:

- Cisco IOS[®] GUI or CLI with the Converged Access 5760, 3850, and 3650 Series WLC
- Extensible Authentication Protocol (EAP) concepts
- Service Set Identifier (SSID) configuration
- RADIUS

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5760 Series WLC Release 3.3.2 (Next Generation Wiring Closet [NGWC])
- Cisco 3602 Series Lightweight Access Point (AP)
- Microsoft Windows XP with Intel PROset Supplicant
- Cisco Catalyst 3560 Series Switches

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.

Configure

Note: Use the <u>Command Lookup Tool</u> (<u>registered</u> customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This image provides an example of a network diagram:



Configuration Overview

This configuration is completed in two steps:

- 1. Configure the WLC for the local EAP method and the related authentication and authorization profiles with the CLI or GUI.
- 2. Configure the WLAN and map the method list that has the authentication and authorization profiles.

Configure the WLC with the CLI

Complete these steps in order to configure the WLC with the CLI:

1. Enable the AAA model on the WLC:

aaa new-model

2. Define the authentication and authorization:

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

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

3. Configure the local EAP profile and the method (EAP-FAST is used in this example):

```
eap profile eapfast
method fast
```

4. Configure the advanced EAP-FAST parameters:

```
eap method fast profile eapfast
description test
authority-id identity 1
authority-id information 1
local-key 0 cisco123
Configure the W/LAN and men the local outherization profile to the W/LAN
```

5. Configure the WLAN and map the local authorization profile to the WLAN:

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

6. Configure the infrastructure in order to support the client connectivity:

```
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
```

Configure the WLC with the GUI

Complete these steps in order to configure the WLC with the GUI:

1. Configure the method list for Authentication:

Configure the **eapfast** Type as **Dot1x**.

Configure the eapfast Group Type as Local.

Security	Authentication	Authentication					
* Ada	New Renove	New Renove					
▼ Method Lists	Name	Type	Group Type	Goup1	Group2	Group3	Group4
General	Local_webat	rth login	local	N/A	N/A	N/A	N/0A
 [Authentication] 	default	dot1a	local	N/A	N/A	N/A	N/CA
 Accounting 	ACS A	dotix	group	ACS	N/A	N/A	N/CA
 Authorization: 	15E	dot12	graup	15E	N/A	N/A	N/CA.
h Concern Concern	 eapfast 	dotis	local	N/A	N/A	N/A	N/04
 Server Groups 	Webauth	dotix	graup	ACS	N/A	N/A	N/04
▼ R4FIUS							

2. Configure the method list for Authorization:

Configure the eapfast Type as Credential-Download.

Configure the eapfast Group Type as Local.

Security	Authorization						
* 686	New Recover						
 Method Lists 	Name	Туре	Group Type	Group1	Group2	Group3	Group4
 General 	default	network	local	N/A	N/A	N/A	N/A
 Authentication 	Webauth	network	0.01b	ACS	N/A	N/A	N/A
 Accounting 	default	medential-download	local	N/A	N/A	$\mathbb{N}_{t}^{k}A_{t}$	N/A
 Sutherization) 	asptast	medential-download	local	N/A	N/A	NA	N/A
 Server Groups 							

3. Configure the Local EAP profile:



4. Create a new profile and select the EAP type:

Loc	al EAP Profiles				
Net	w Remove				
	Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
	eapfast	Disabled	Enabled	Disabled	Disabled

The Profile Name is **eapfast** and the selected EAP type is **EAP-FAST**:

Local EAP Profiles Local EAP Profiles > Edit	
Profile Name	eapfast
LEAP	
EAP-FAST	
EAP-TLS	
PEAP	
Trustnoint	

5. Configure the EAP-FAST Method Parameters:

EAP-FAST Method Parameters	
New Remove	
Profile Name	Description
🗆 eapfast	test

The Server Key is configured as **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. Check the **Dot1x System Auth Control** check box and select **eapfast** for the Method Lists. This helps you to perform the local EAP authentication.

Security	General	General		
▼ AAA				
 Method Lists 	Dot1x System Auth Control	\checkmark		
🗉 General	Local Authentication	Method List 💌		
Authentication	Authentication Method List	eapfast 💌		
Accounting	Local Authorization	Method List 💌		
Authorization				
Server Groups	Authorization Method List	eapfast 💌		
▼ RADIUS				

7. Configure the WLAN for WPA2 AES encryption:

WLAN > Edit				
General S	ecurity	QOS	AVC	Advanced
Profile Name		eapfastlocal		
Туре		WLAN		
SSID		eapfastlocal		
Status		✓		
Security Policies		[WPA2][Auth((Modification	302.1x)] Is done und	er security tab will appear after applying the changes.)
Radio Policy		All 👻		
Interface/Interface G	roup(G)	VLAN0020	•	
Broadcast SSID		\checkmark		
Multicast VLAN Featu	re			

WLAN

WLAN > Edit					
General	Security	QOS	AVC	Advanced	
Layer2	Layer3	AAA Server			
Layer 2 Security	WPA + WPA2	Ŧ			
MAC Filtering					
Fast Transition					
Over the DS					
Reassociation Ti	imeout 20				
WPA+WPA2 F	Parameters				
WPA Policy 🗌					
WPA2 Policy	/				
WPA2 Encryp	ition 🗹 AES 🕻	🗆 ткір			
Auth Key Mgm	t 802.1x 💌				

8. On the **AAA Server** tab, map the EAP Profile Name **eapfast** to the WLAN:

WLAN WLAN > Edit				
General	Security	QOS	AVC	Advanced
Layer2	Layer3	AAA Server		
Authentication Accounting Met Local EAP Auth EAP Profile Nam	Method Disa thod Disa entication 🗹 ne eapfast	bled 💌		

Verify

Complete these steps in order to verify that your configuration works properly:

1. Connect the client to the WLAN:



2. Verify that the Protected Access Credentials (PAC) popup appears and that you must accept in order to successfully authenticate:



Troubleshoot

Cisco recommends that you use traces in order to troubleshoot wireless issues. Traces are saved in the circular buffer and are not processor intensive.

Enable these traces in order to obtain the Layer 2 (L2) auth logs:

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

Enable these traces in order to obtain the DHCP events logs:

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

Here are some examples of successful traces:

[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 0x0000000 [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 (0x57ca400000048): 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