

FlexConnect Wireless Branch Controller Deployment Guide

Last Updated: July, 2018

Introduction

This document describes how to deploy a Cisco Flex Connect AP. The purpose of this document is to:

- Explain various network elements of the Cisco FlexConnect solution, along with their communication flow.
- Provide general deployment guidelines for designing the Cisco FlexConnect wireless branch solution.

The Cisco WLCs can manage Flex Connect wireless access points in up to 2000 branch locations and allows IT managers to configure, manage, and troubleshoot up to 6000 access points (APs) and 64,000 clients from the data center. The Cisco Flex Connect deployments support secure guest access, rogue detection for Payment Card Industry (PCI) compliance, and in-branch (locally switched) Wi-Fi voice and video.

The following table highlights the FC scalability differences between the Flex 3504, 5520, 8540, Mobility Express and vWLC controllers:



Additional Scale Specifications	WLC 3504	WLC5520	WLC8540	ME	vWLC-Small	vWLC-Large
Maximum Access Points	150	1500	6000	100	200	3000
Maximum Clients	3000	20000	64000	2000	6000	32000
Maximum # of AP Groups	150	1500	6000	50	200	3000
Max Flex Connect Groups	100	1500	2000	1	100	1500
Max # of VLANs	4094	4095	4095	16		
MaxWLANs	512	512	512	16		
Max # interfaces	512	1500	1500	n/a		
Maximum RFID's	1500	25000	50000	2000	6000	25000
Maximum Rogue APs	600	24000	24000	200	800	12000
Maximum Rogue Clients	150	32000	32000	400	3000	16000
Maximum APs in one RRM/RF group	1000	3000	6000	100	400	5000
NBAR Max Profiles	16	16	16	n/a		
NBAR Max Rules single profile	32	32	32	n/a		
NBAR Max # FlowTable Entries	160000	320000	320000	n/a		
Maximum L2 ACL rules per L2 ACL	16	16	16	n/a		
Maximum L2 ACLs allowed	64	64	64	n/a		
Max # L3 ACLs (ipv4/ipv6)	64/64	64/64	64/64	n/a		
Max # of Rules in L3 ACL IP/DNS	64/64	64/64	64/64	64/32		
Max # of Radius servers supported (unique)	16	16	16	6		
Max Bonjour Service Providers	16000	16000	16000	n/a		
Max FC groups with max APs per group	100	100	100	1	100	100

Supported Access Points

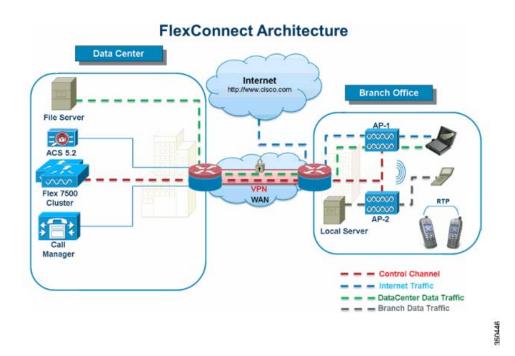
Access Points

- Wave-1 APs: 3700, 2700, 1700, 702, 702W, 1530, 1570
- Wave-2 APs: 1800 series, 2800 series, 3800 series, 4800 series (starting rel 8.7.5); 1540, 1560

1

FlexConnect Architecture

Figure 1



Typical Wireless Branch Topology

FlexConnect is a wireless solution for branch office and remote office deployments. The FlexConnect solution enables the customer to:

- Centralize control and manage traffic of APs from the Data Center.
- Distribute the client data traffic at each Branch Office.
 - Each traffic flow is going to its final destination in the most efficient manner.

Controllers Supporting FlexConnect Mode

• Cisco WLC 3504, 5520, 8500 Series, vWLC

Advantages of Centralizing Access Point Control Traffic

- Single pane of monitoring and troubleshooting.
- Ease of management.

I

- Secured and seamless mobile access to Data Center resources.
- Reduction in branch footprint.
- Increase in operational savings.

Advantages of Distributing Client Data Traffic

- No operational downtime (survivability) against complete WAN link failures or controller unavailability.
- Mobility resiliency within branch during WAN link failures.
- Increase in branch scalability. Supports branch size that can scale up to 100 APs and 250,000 square feet (5000 sq. feet per AP).

The Cisco FlexConnect solution also supports Central Client Data Traffic, but it is limited to Guest data traffic only. This next table describes the restrictions on WLAN L2 security types only for non-guest clients whose data traffic is also switched centrally at the Data Center.

 Table 1
 L2 Security Support for Centrally Switched Non-Guest Users

WLAN L2 Security	Туре	Result
None	N/A	Allowed
WPA + WPA2	802.1x	Allowed
	ССКМ	Allowed
	802.1x + CCKM	Allowed
	PSK	Allowed
802.1x	WEP	Allowed
Static WEP	WEP	Allowed
WEP + 802.1x	WEP	Allowed
СКІР	-	Allowed

<u>Note</u>

These authentication restrictions do not apply to clients whose data traffic is distributed at the branch.

WLAN L3 Security	Туре	Result
Web Authentication	Internal	Allowed
	External	Allowed
	Customized	Allowed
Web Pass-Through	Internal	Allowed
	External	Allowed
	Customized	Allowed
Conditional Web Redirect	External	Allowed
Splash Page Web Redirect	External	Allowed

For more information on Flexconnect external webauth deployment, please refer to Flexconnect External WebAuth Deployment Guide

For more information on HREAP/FlexConnect AP states and data traffic switching options, refer to Configuring FlexConnect.

FlexConnect Modes of Operation

FlexConnect Mode	Description
Connected	A FlexConnect is said to be in Connected Mode when its CAPWAP control plane back to the controller is up and operational, meaning the WAN link is not down.
Standalone	Standalone mode is specified as the operational state the FlexConnect enters when it no longer has the connectivity back to the controller. FlexConnect APs in Standalone mode will continue to function with last known configuration, even in the event of power failure and WLC or WAN failure.

For more information on FlexConnect Theory of Operations, refer to the H-Reap/FlexConnect Design and Deployment Guide.

WAN Requirements

ſ

FlexConnect APs are deployed at the Branch site and managed from the Data Center over a WAN link. The maximum transmission unit (MTU) must be at least 500 bytes.

Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	64 Kbps	300 ms	5	25
Data	640 Kbps	300 ms	50	1000
Data	1.44Mbps	1 sec	50	1000
Data + Voice	128 Kbps	100 ms	5	25
Data + Voice	1.44Mbps	100 ms	50	1000
Monitor	64 Kbps	2 sec	5	N/A
Monitor	640 Kbps	2 sec	50	N/A



It is highly recommended that the minimum bandwidth restriction remains 12.8 Kbps per AP with the round trip latency no greater than 300 ms for data deployments and 100 ms for data + voice deployments.

For large deployments with scale for max APs per branch = 100 and max clients per branch = 2000.

Key Features

Adaptive wIPS, Context Aware (RFIDs), Rogue Detection, Clients with central 802.1X auth and CleanAir.

Test Results

For 100 APs, 2000 Clients, 1000 RFIDs, 500 Rogue APs, and 2500 Rogue Clients (Features above turned on):

Recommended BW = 1.54 Mbps

Recommended RTT latency = 400 ms

Test Results

For 100 APs, 2000 Clients, no rogue, and no RFIDs. (Features above turned off).

Recommended BW = 1.024 Mbps

Recommended Latency = 300 ms

Wireless Branch Network Design

The rest of this document highlights the guidelines and describes the best practices for implementing secured distributed branch networks. FlexConnect architecture is recommended for wireless branch networks that meet these design requirements.

I

Primary Design Requirements

- Branch size that can scale up to 100 APs and 250,000 square feet (5000 sq. feet per AP)
- Central management and troubleshooting
- No operational downtime
- Client-based traffic segmentation
- · Seamless and secured wireless connectivity to corporate resources
- PCI compliant
- Support for guests

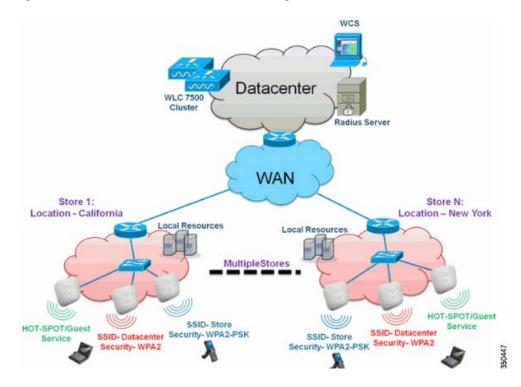


Figure 2 Wireless Branch Network Design

Overview

Branch customers find it increasingly difficult and expensive to deliver full-featured scalable and secure network services across geographic locations. In order to support customers, Cisco is addressing these challenges by introducing the FlexConnect deployment mode.

The FlexConnect solution virtualizes the complex security, management, configuration, and troubleshooting operations within the data center and then transparently extends those services to each branch. Deployments using FlexConnect are easier for IT to set up, manage and, most importantly, scale.

Advantages

I

- Increase scalability with 6000 AP support.
- Increased resiliency using FlexConnect Fault Tolerance.
- Increase segmentation of traffic using FlexConnect (Central and Local Switching).
- Ease of management by replicating store designs using AP groups and FlexConnect groups.

Features Addressing Branch Network Design

The rest of the sections in the guide captures feature usage and recommendations to realize the network design shown in Figure 2.

Primary Features	Highlights				
AP Groups	Provides operational/management ease when handling multiple branch sites. Also, gives the flexibility of replicating configurations for similar branch sites.				
FlexConnect Groups	FlexConnect Groups provide the functionality of Local Backup Radius, CCKM/OKC fast roaming, and Local Authentication.				
Fault Tolerance	Improves the wireless branch resiliency and provides no operational downtime.				
ELM (Enhanced Local Mode for Adaptive wIPS)	Provide Adaptive wIPS functionality when serving clients without any impact to client performance.				
Client Limit per WLAN	Limiting total guest clients on branch network.				
AP Pre-image Download	Reduces downtime when upgrading your branch.				
Auto-convert APs in FlexConnect	Functionality to automatically convert APs in FlexConnect for your branch.				
Guest Access	Continue existing Cisco's Guest Access Architecture with FlexConnect.				

Table 3	Features

<u>Note</u>

Flexconnect APs implemented with WIPS mode can increase bandwidth utilization significantly based on the activity being detected by the APs. If the rules have forensics enabled, the link utilization can go up by almost 100 Kbps on an average.

Feature Matrix

Refer to FlexConnect Feature Matrix for a feature matrix for the FlexConnect feature.

AP Groups

After creating WLANs on the controller, you can selectively publish them (using access point groups) to different access points in order to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among

several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing, Engineering or Operations) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration.

This document uses AP groups to simplify network administration when managing multiple stores across geographic locations. For operational ease, the document creates one AP-group per store to satisfy these requirements:

- Centrally Switched SSID Data center across all stores for Local Store Manager administrative access.
- Locally Switched SSID Store with different WPA2-PSK keys across all stores for hand-held scanners.

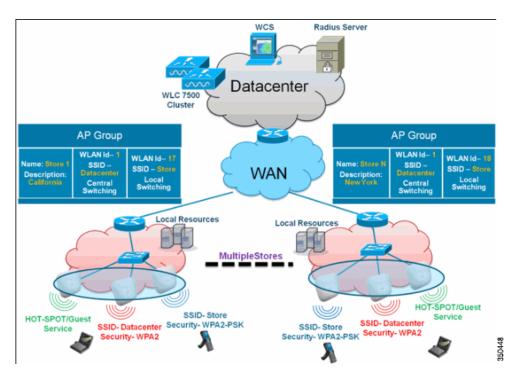


Figure 3 Wireless Network Design Reference Using AP Groups

Configurations from WLC

I

Complete the following steps:

Step 1 On the WLANs > New page, enter Store1 in the Profile Name field, enter store in the SSID field, and choose 17 from the ID drop-down list.

<u>Note</u>

WLAN IDs 1-16 are part of the default group and cannot be deleted. In order to satisfy our requirement of using same SSID store per store with a different WPA2-PSK, you need to use WLAN ID 17 and beyond because these are not part of the default group and can be limited to each store.

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	Sage Configuration Eing Logout Eef EEEDBACK	resh.
WLANs	WLANs > New				< Back Apply	-
WLANS	Туре	WLAN M				
Advanced	Profile Name	Store1				
	SSID	store				
	ID	17 🛩				
	ID	17 🚿				

Step 2 Under WLAN > Security, choose PSK from the Auth Key Mgmt drop-down list, choose ASCII from the PSK Format drop-down list, and click Apply.

1

uluili. cisco	MONITOR WLAN: CONTROLLER WIREL	LESS SECURITY MANAGEMENT	COMMANDS HELP	Sage Configuration Bing EEEDBACK	Logout <u>R</u> efresh
WLANs	WLANs > Edit			< Back	Αρρίγ
WLANS	General Security QoS Advan	ced			
Advanced	Layer 2 Layer 3 AAA Servers				
	Layer 2 Security 6 WPA+WPA2	×			
	WPA+WPA2 Parameters				
	WPA Policy				
	WPA2 Policy				
	WPA2 Encryption PAES	KIP			
	Auth Key Mgmt PSK	~			
	PSK Format ASCII M				

Step 3 Click **WLAN > General**, verify the Security Policies change, and check the **Status** box to enable the WLAN.

սիսիս	Sage Configuration _ Eng _ Logout _ Befre
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit Apply
WLANS	General Security QoS Advanced
Advanced	Profile Name Store1
	Type WLAN
	SSID store
	Stetus 🗹 Enabled
	Security Policies [WPA2][Auth(PSK)]
	(Modifications done under security tab will appear after applying the changes.)
	Radio Policy All
	Interface/Interface management v
	Multicest Vian Feature 🔲 Enabled
	Broadcast SSID

Step 4 Repeat steps 1, 2 and 3 for new WLAN profile Store2, with SSID as store and ID as 18.

ahaha									Sage Configur	ration Eing I	Logout <u>B</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		
WLANs	WLANs >	New								< Back	Apply
WLANS WLANS	Туре		WLAN	~							
Advanced	Profile Na	ine	Store	2							
	SSID		store								
	ID		18	× 1							
	_										

 cisco	Sage Configuration [Eng] Lagout Befresh Monitor <u>Wilans</u> Controller Wireless Security Management Commands Help Eeedback
WLANs	WLANs > Edit Apply
WLANS	General Security QuS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer Z Security WPA+WPA2 MMAC Filtering WPA+WPA2 Parameters
	WPA Policy WPA Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt PSK Format



Step 5

I

Create and enable the WLAN profile with Profile Name DataCenter, SSID DataCenter and ID 1.

NoteOn creation, WLAN IDs from 1-16 are automatically part of the default-ap-group.

Step 6 Under WLAN, verify the status of WLAN IDs 1, 17 and 18.

 cisco	MONITOR	<u>W</u> LANs		WIRELESS SECURITY	MANAGEMENT	COMMANDS		age Configuration EDBACK	Eing	Logout Bel
WLANs	WLANs								Entr	ies 1 - 3 o
WLANS WLANS	Current Filter: None [Change Filter] Create New M Go									
AP Groups	WLAN 10) Туре	Profile Name	e w	AN SSID		dmin Status	Security Policies	•	
		WLAN	DataCenter	De	taCenter	t	nabled	[WPA + WPA2][Au	/h(802.1	×)] 🗖
	17	WLAN	Store1	sta	ire		nabled	[WPA2][Auth(PSK)	1	
					ire		nabled	[WPA2][Auth(PSK		

- Step 7 Click WLAN > Advanced > AP group > Add Group.
- **Step 8** Add AP Group Name as **Store1**, same as WLAN profile **Store1**, and Description as the Location of the Store. In this example, California is used as the location of the store.
- Step 9 Click Add when done.

uluilu cisco	MONITOR WLANS CONTROLL	ER WIRELESS SECURITY	Management Commands	нејр	Sage Configuration Eing	, Logout <u>R</u> efresh
WLANS WLANS WLANS Advanced AP Groups	AP Groups Add New AP Group				Entries 0 - 0 of 0	Add Group
	AP Group Name Store1 Description California Add Can	cel				
	AP Group Name	AP Group Descri				

Step 10 Click Add Group and create the AP Group Name as Store2 and the description as New York.

Step 11 Click Add.

ahaha				Sage Configuration Ping Logout	Befresh
CISCO	MONITOR WLANS CONTROLLE	R WIRELESS SECURITY MANAGEMEN	T COMMANDS HELP	EEEOBACIC	
WLANS WLANS	AP Groups			Entries 1 - 1 of 1	Group
* Advanced	Add New AP Group AP Group Name Store2				
AP Groups	Description New York				
	Add Canc	et			
	AP Group Name	AP Group Description			
	Store1	California			
	default-group				

Step 12 Verify the group creation by navigating to WLAN > Advanced > AP Groups.

	MONITOR WLANS	CONTROLLER WIRELE	SS <u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	Sage Configuration Ping EEEDBACK	Logout <u>R</u> efresh
WLANs	AP Groups						Entries 1 - 2 of 2	Add Group
WLANS	AP Group Name		AP Group Desc	ription				
 Advanced 	Storel		California					
AP Groups	Store2		New York					
	default-group							

- **Step 13** Click AP Group Name **Store1** to add or edit the WLAN.
- Step 14 Click Add New to select the WLAN.
- Step 15 Under WLAN, from the WLAN SSID drop-down, choose WLAN ID 17 store(17).
- Step 16 Click Add after WLAN ID 17 is selected.
- Step 17 Repeat steps (14 -16) for WLAN ID 1 DataCenter(1). This step is optional and needed only if you want to allow Remote Resource access.

.ı ı.ı ı. cısco	Saga Configuration (Eng. Lagout MONITOR <u>W</u> LANIS <u>C</u> ONTROLLER WIRELESS SECURITY MEMAGEMENT COMMANDS HELP EEEDBACK	Befresh
WLANs	Ap Groups > Edit 'Store1'	ck
WLANS WLANS Advanced AP Groups	General WLANS APs Add New	^
	WLAN SSID Dottelial State: 1 Interficio DataCenter(1) //monthic DataCenter(1) /monthic stare(1) Store 2 /monthic State /monthic Enabled Add Cancel	
	WLAN WLAN Interface/Interface NAC ID SSID Group(C) State	

Step 18 Go back to the WLAN > Advanced > AP Groups screen.

Step 19 Click AP Group Name Store2 to add or edit WLAN.

- Step 20 Click Add New to select the WLAN.
- Step 21 Under WLAN, from WLAN SSID drop-down, choose WLAN ID 18 store(18).
- Step 22 Click Add after WLAN ID 18 is selected.
- **Step 23** Repeat steps 14 -16 for WLAN ID 1 DataCenter(1).

. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MAN	Saye Configuration _ Bing _ Lagout _ Befresh AGEMENT COMMANDS HELP _ EEEDBACK
WLANs	Ap Groups > Edit "Store2"	< Back
WLANS WLANS	General WLANS APs	
Advanced AP Groups		Add New
	Add New WLAN SSID Unterface DataCenter(1) Interface Group(0) store(127) Store 1 Group(0) NAC State Add Cancel WLAN WLAN Interface/Interface NAC State	

Adding multiple WLAN profiles with the same SSID under a single AP group is not permitted.

The pag	ge at https://172.20.227.174 says:	X
1	Failed to add interface entry management	
	ОК	
Note A	Adding APs to the AP group is not captured	in this
	ccess network services.	III tills

Summary

ſ

- AP groups simplify network administration.
- Troubleshooting ease with per branch granularity
- Increased flexibility

FlexConnect Groups

Note

In most typical branch deployments, it is easy to foresee that client 802.1X authentication takes place centrally at the Data Center. Because the above scenario is perfectly valid, it raises these concerns:

• How can wireless clients perform 802.1X authentication and access Data Center services if WLC fails?

- How can wireless clients perform 802.1X authentication if WAN link between Branch and Data Center fails?
- Is there any impact on branch mobility during WAN failures?
- Does the FlexConnect Solution provide no operational branch downtime?

FlexConnect Group is primarily designed and should be created to address these challenges. In addition, it eases organizing each branch site, because all the FlexConnect access points of each branch site are part of a single FlexConnect Group.

Note FlexConnect Groups are not analogous to AP Groups.

Primary Objectives of FlexConnect Groups

Backup RADIUS Server Failover

You can configure the controller to allow a FlexConnect access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. In order to increase the resiliency of the branch, administrators can configure a primary backup RADIUS server or both a primary and secondary backup RADIUS server. These servers are used only when the FlexConnect access point is not connected to the controller.

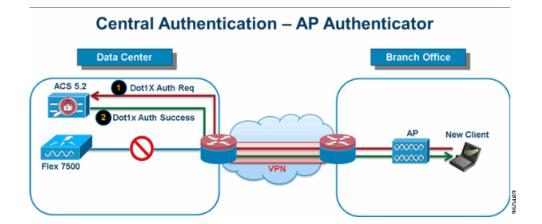


Backup RADIUS accounting is not supported.

Local Authentication

Before the 7.0.98.0 code release, local authentication was supported only when FlexConnect is in Standalone Mode to ensure client connectivity is not affected during WAN link failure. With the 7.0.116.0 release, this feature is now supported even when FlexConnect access points are in Connected Mode.

Figure 4 Central Dot1X Authentication (FlexConnect APs Acting as Authenticator)



As shown in Figure 4, branch clients can continue to perform 802.1X authentication when the FlexConnect Branch APs lose connectivity with the WLC. As long as the RADIUS/ACS server is reachable from the Branch site, wireless clients will continue to authenticate and access wireless services. In other words, if the RADIUS/ACS is located inside the Branch, then clients will authenticate and access wireless services even during a WAN outage.



With Local Authentication turned on, the AP will always authenticate the clients locally, even when it is in connected mode. When Local Authentication is disabled, the controller will authenticate clients to the Central RADIUS server when the FlexConnect AP is in connected mode. When the AP is in Standalone mode, the AP will authenticate clients to the Local RADIUS / Local EAP on AP configured on the FlexConnect Group.

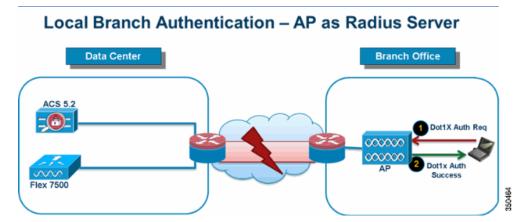


This feature can be used in conjunction with the FlexConnect backup RADIUS server feature. If a FlexConnect Group is configured with both backup RADIUS server and local authentication, the FlexConnect access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the Local EAP Server on FlexConnect access point itself (if the primary and secondary are not reachable).

Dot1X Authentication (FlexConnect APs Acting as Local-EAP Server)

Local EAP (Local Authentication Continuation)

Figure 5



- You can configure the controller to allow a FlexConnect AP in standalone or connected mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured users. The controller sends the static list of user names and passwords to each FlexConnect access point of that particular FlexConnect Group when it joins the controller. Each access point in the group authenticates only its own associated clients.
- This feature is ideal for customers who are migrating from an autonomous access point network to a lightweight FlexConnect access point network and are not interested in maintaining a large user database, or adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

• As shown in Figure 5, if the RADIUS/ACS server inside the Data Center is not reachable, then FlexConnect APs automatically acts as a Local-EAP Server to perform Dot1X authentication for wireless branch clients.

CCKM/OKC Fast Roaming

- FlexConnect Groups are required for CCKM/OKC fast roaming to work with FlexConnect access points. Fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The FlexConnect access points need to obtain the CCKM/OKC cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that might associate, sending the CCKM/OKC cache for all 100 clients is not practical. If you create a FlexConnect Group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM/OKC cache is distributed among those four access points only when the clients associate to one of them.
- This feature along with Backup Radius and Local Authentication (Local-EAP) ensures **no operational downtime** for your branch sites.



CCKM/OKC fast roaming among FlexConnect and non-FlexConnect access points is not supported.

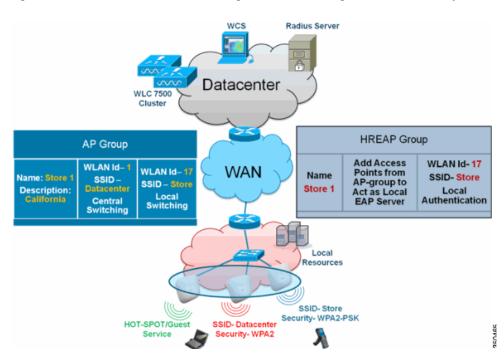


Figure 6 Wireless Network Design Reference Using FlexConnect Groups

FlexConnect Group Configuration from WLC

Complete the steps in this section in order to configure FlexConnect groups to support Local Authentication using LEAP, when FlexConnect is either in Connected or Standalone mode. The configuration sample in Figure 6 illustrates the objective differences and 1:1 mapping between the AP Group and FlexConnect group.

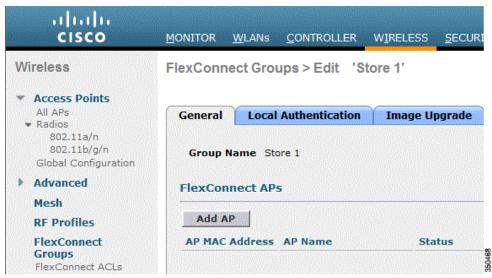
- Step 1 Click New under Wireless > FlexConnect Groups.
- **Step 2** Assign Group Name Store 1, similar to the sample configuration as shown in Figure 6.
- **Step 3** Click **Apply** when the Group Name is set.

ſ



Step 4 Click the Group Name **Store 1** that you just created for further configuration.

		<u>M</u> ONITOR <u>W</u> LANS <u>C</u> CNTROLLER W <u>I</u> RELESS <u>S</u> ECURI	ITY
	Wireless	FlexConnect Groups	
	 Access Points All APs Radios 802.11a/n 802.11h/g/n Global Configuration 	Group Name Store 1	
	Advanced		
	Mesh		
	RF Profiles		
	FlexConnect Groups		350467
Step 5	Click Add AP.		



Step 6 Check the **Enable AP Local Authentication** box in order to enable Local Authentication when the AP is in Standalone Mode.



Step 20 shows how to enable Local Authentication for Connected Mode AP.

- Step 7 Check the Select APs from current controller box in order to enable the AP Name drop-down menu.
- **Step 8** Choose the AP from the drop-down that needs to be part of this FlexConnect Group.
- **Step 9** Click **Add** after the AP is chosen from the drop-down.
- **Step 10** Repeat steps 7 and 8 to add all the APs to this FlexConnect group that are also part of AP-Group Store 1. See Figure 6 to understand the 1:1 mapping between the AP-Group and FlexConnect group.

If you have created an AP-Group per Store (Figure 3), then ideally all the APs of that AP-Group should be part of this FlexConnect Group (Figure 6. Maintaining 1:1 ratio between the AP-Group and FlexConnect group simplifies network management.

ululu cisco	<u>M</u> onitor <u>w</u> lans <u>c</u> ontroller	W <u>i</u> reless <u>s</u> ecuri
Wireless	FlexConnect Groups > Edit 'S	store 1'
Access Points		
All APs Radios	General Local Authentication	Image Upgrade
802.11a/n 802.11b/g/n Global Configuration	Group Name Store 1	
Advanced	FlexConnect APs	
Mesh		
RF Profiles	Add AP	
FlexConnect Groups	Select APs from current controller	
FlexConnect ACLs	AP Name	AP3500 -
▶ 802.11a/n	Ethernet MAC	00:22:90:e3:37:df
802.11b/g/n		Add Cancel
Media Stream		
		Status

Step 11 Click Local Authentication > Protocols and check the Enable LE

Step 12 Click **Apply** after the check box is set.

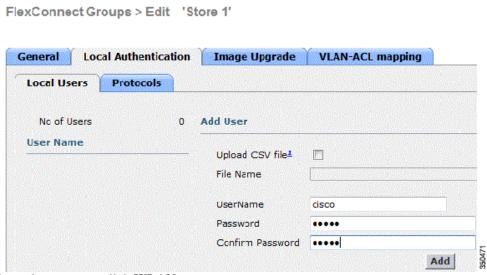
Note

ſ

If you have a backup controller, make sure the FlexConnect groups are identical and AP MAC address entries are included per FlexConnect group.

neral Local Authentication	Image Upgrade VLAN-ACL mapping
ocal Users Protocols	
AP	
Enable LEAP Authentication ²	
AP FdSt	
Enable EAP Fast Authentication ²	
	Enable Auto key generation
Enable EAP Fast Authentication ²	
Enable EAP Fast Authentication ²	
Enable EAP Fast Authentication ² Server Key (in hex)	Enable Auto key generation

- Step 13 Under Local Authentication, click Local Users.
- **Step 14** Set the UserName, Password and Confirm Password fields, then click **Add** in order to create user entry in the Local EAP server residing on the AP.
- Step 15 Repeat step 13 until your local user name list is exhausted. You cannot configure or add more than 100 users.
- Step 16 Click Apply after step 14 is completed and the No of Users count is verified.



Step 17 From the top pane, click WLANs.

Step 18 Click WLAN ID 17. This was created during the AP Group creation. See Figure 3.

cisco	MONITOR	WLANS (ONTROLLER	WIRELESS	SECURITY	MANAGEI
WLANs	WLANs					
WI ANS WLANS	Current Fi	lter: None	[Cha	inge Eilter] [Clé	ear Filter]	
Advanced		ID Type	Profile N	lame	w	LAN SSID
	□ 2	WEAN	Guest		G	uest g
	□ <u>17</u>	WLAN	Store-1		St	tore

- Step 19 Under WLAN > Edit for WLAN ID 17, click Advanced.
- **Step 20** Check the **FlexConnect Local Auth** box in order to enable Local Authentication in Connected Mode.



e Local Authentication is supported only for FlexConnect with Local Switching.

<u>Note</u>

Always make sure to create the FlexConnect Group before enabling Local Authentication under WLAN.

WLANs > E	lit 'Store-1'
-----------	---------------

I

Γ

General	Security	QoS		Advai	nced)	
P2P Bloc	king Action		Disab	led			
Client Ex	clusion ²		🔽 En	abled	60 Tim	eout	t Value (secs)
Maximun	n Allowed Clier	nts 🚨 🛛	0				
Static IP	Tunneling 11		🔲 En	abled			
Wi-Fi Dir	ect Clients Poli	су	Disab	oled 🖯	-		
Maximun Per AP R	n Allowed Clier adio	its	200				
Off Channe	l Scanning De	efer					
Scan De	fer Priority	0 1	2	3 4	5	6	7
Scan Del (msecs)	fer Time	100					
FlexConne	ct						
FlexConr 2	nect Local Swite	ching	С е	inable	1		
FlexConr	nect Local Auth	<u>12</u>	🔽 e	nabled	ł		
Learn Cli	ient IP Address	5	E E	nabled	ł		

NCS and Cisco Prime also provides the FlexConnect Local Auth check box in order to enable Local Authentication in Connected Mode as shown here:

Properties	>	WLAN Configuration Deta	ails : 1 > WLANs > WLAN Configuration :
System	>		
WLANs	~	General Security (QoS Advanced
Han Configuration			
H Groups		HexConnect Local Switching	Enable
FlexConnect	>	FlexConnect Local Auth 🔍	Enable
Security	>	Learn Client IP Address	Enable
Access Points	>	Session Timeout	Enable
802.11	>	Coverage Hole Detection Aironet IF	Enable Enable
802.11a/n	>	IPv6 2	Enable
802.11b/g/n	> >	Diagnostic Channel 🙎	Enable
Mesh	>	Override Interface ACL	IPv4 NONE
Ports	>	Peer to Peer Blocking 🔍	Disable
Management	>	Wi-Fi Direct Clients Policy	Disabled
Location	>	Client Exclusion 4 Timeout Value	60 (secs)

1

NCS and Cisco Prime also provides facility to filter and monitor FlexConnect Locally Authenticated clients as shown here:

(i	Ilome Monitor	Configure	✓ Services		Adr	nnistration	
Tile	nts and Users						
S	ucubeshoot 🍐 lest	r 🔹 🛣 Disable	-Remove	More 🔹 😨 Irad	Clents	So Identify	Hinknown Users
	MAC Address	IP Address	The line	User Name	lype	Vendor	Device Name
0	00:22:90:1b:17:42		IPv1	Unknown	-	Cisco	WCS_SW 0.1.0.23
0	1c:df:0f:66:86:58		IPv4	Unknown	61	Cisco	WC5_SW-9.1.0.2
0	00:21:6a:97:9b:bc		₽v4	hust/vikatta		Intel	oeap-laiwar-2
0	00:22:90:15:96:48		IPv4	Unknown	4	LISCO	WCS_SW-9.1.0.2
0	00:22:90:1b:17:8c		₽v1	Unknown	-	Cisco	WCS_SW 0.1.0.2
Q	00:25:0b:4d:77:c4		IPv4	Unknown	5	Cisco	WCS_SW-9.1.0.2
0	c4:7d:4f:3a:c5:d5		TPv4	Unknown	-	CISCO	WCS_SW-9.1.0.2
0	00:21:a0:d5:03:c4		IPv4	Unknown	-	Cisco	WCS_SW-9.1.0.2
U	f8:66:f2:67:7f:50		IPv4	Unknown	5	Cisco	WCS_SW-9.1.0.2
0	00:1f:ca:b0:01:b4		IPv4	Unknown		Ciscu	WCS_SW-9.1.0.2
0	88:43:e1:d1:df:02		IPv4	Unknown	-	Cisco	WCS_SW-9.1.0.2
0	00:22:bd:1b:e2:b5		IPv1	Unknown	R	Cisco	WCS_SW 0.1.0.2
0	f3:66:f2:ab:1e:69		₽v4	Unknown	5	Cisco	WC5_SW-9.1.0.2
0	00:10:58:JU:b4:4e		₽v4	Unknown	8	Ciscu	WCS_SW-9.1.0.2 oeap-tawar-2
0	00:1e:/atbb:21:8d			ssimm		Cisco	oeap-tawar-2

AND THE REAL PROPERTY OF	OT-DOMAIN	root 🔹 Log O	ut 📿 🖓	
				Total 299 😽 🕼 🕻
			Show	Associated Clients 👻 🏹
Location	VLAN	Status	Interface	
Unknown	109	Associated	Gi1/0/34	
Unknown	109	Associated	Gi1/0/26	
Root Area	310	Associated	data	Manage Preset Filters
Unknown	109	Associated	Gi1/0/36	2.4GHz Clients 5GHz Clients
Unknown	109	Associated	Gi1/0/32	
Unknown	109	Associated	Gi1/0/30	
Unknown	109	Associated	Gi1/0/13	
Unknown	109	Associated	Gi1/0/27	Associated Clients
Unknown	109	Associated	Gi1/0/12	Clients known by ISE
Unknown	109	Associated	Gi1/0/15	Clients detected by MSE
Unknown	109	Associated	Gi1/0/28	Clients detected in the last 24 hours
Unknown	109	Associated	Gi1/0/14	Clients with Problems
Unknown	109	Associated	Gi1/0/9	Excluded Clients
Unknown	109	Associated	Gi1/0/29	FlexConnect Locally Authenticated
Root Area	311	Associated	voice	New clients detected in last 24 hours

Γ

Verification Using CLI

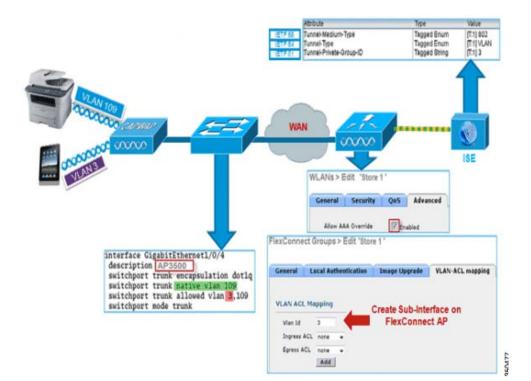
Client authentication state and switching mode can quickly be verified using this CLI on the WLC:

(Cisco	Controller) > show client detail 00:24:d7:24	p:7c:0c
Client	MAC Address	00:24:d7:2b:7c:0c
Client	Username	N/A
AP MAC	Address	d0:57:4c:08:e6:70
Client	State	Associated
H-REAP	Data Switching	Local
H-REAP	Authentication	Local

FlexConnect VLAN Override

In the current FlexConnect architecture, there is a strict mapping of WLAN to VLAN, and thus the client getting associated on a particular WLAN on FlexConnect AP has to abide by a VLAN which is mapped to it. This method has limitations, because it requires clients to associate with different SSIDs in order to inherit different VLAN-based policies.

From 7.2 release onwards, AAA override of VLAN on individual WLAN configured for local switching is supported. In order to have dynamic VLAN assignment, AP would have the interfaces for the VLAN pre-created based on a configuration using existing WLAN-VLAN Mapping for individual FlexConnect AP or using ACL-VLAN mapping on a FlexConnect group. The WLC is used to pre-create the sub-interfaces at the AP.



Summary

- AAA VLAN override is supported from release 7.2 for WLANs configured for local switching in central and local authentication mode.
- AAA override should be enabled on WLAN configured for local switching.
- The FlexConnect AP should have VLAN pre-created from WLC for dynamic VLAN assignment.
- If VLANs returned by AAA override are not present on AP client, they will get an IP from the default VLAN interface of the AP.

Procedure

Γ

Complete these steps:

Step 1 Create a WLAN for 802.1x authentication.

eneral	Security	QoS Advanced	
Layer 2	Layer 3	AAA Servers	
Layer 2	Security 🧧 🔤	WPA+WPA2	
	2 Paramete	2MAC Filtering	
WPA Po			
-		\checkmark	
WPA2 P	olicy		
	ncryption		

Step 2 Enable AAA override support for local switching WLAN on the WLC. Navigate to WLAN GUI > WLAN > WLAN ID > Advance tab.

Allow AAA Override	Enabled		DHCP	
Coverage Hole Detection Enable Session Timeout	Enabled		DHCP Server	verride
Enable Session Timeout	Session Timeout (secs)		DHCP Addr. Assignment	equired
Aironet IE	Enabled		Management Frame Protection (
Diagnostic Channel	Enabled			
Override Interface ACL	participation of the second	IPv6	MFP Client Protection 4 Option	al 📉
PDD Blocking Asting	None V Disabled V	None	DTIM Period (in beacon intervals)
P2P Blocking Action			and a second	
Client Exclusion 2	Enabled 50 Timeout Value (secs)	1	802.11a/n (1 - 255) 1	
Maximum Allowed Clients			802.11b/g/n (1 - 255) 1	1
Static IP Tunneling	Enabled		NAC	
Wi-Fi Direct Clients Policy	Disabled 💌		NAC State None 👻	
Maximum Allowed Clients	200		Load Balancing and Band Select	
Per AP Radio			Client Load Balancing	
Off Channel Scanning Defe	r		Client Band Select Z	
Scan Defer Priority 0	1 2 3 4 5 6 7		Passive Client	
E			Passive Client	
Scan Defer Time			Voice	
(msecs)	00		Media Session Snooping	Enable
lexConnect			Re-anchor Roamed Voice Clients	
			the anonor roamed voice clients	Enable

1

Step 3 Add the AAA server details on the controller for 802.1x authentication. In order to add the AAA server, navigate to **WLC GUI > Security > AAA > Radius > Authentication > New**.

* AAA General	Server Index	1
RADIUS Authentication	Server Address	
Accounting	Shared Secret Format	ASCII V
Fallback FTACACS+	Shared Secret	***
LDAP Local Net Users	Confirm Shared Secret	•••
MAC Filtering Disabled Clients	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
User Login Policies AP Policies	Port Number	1812
Password Policies	Server Status	Enabled 💌
Local EAP	Support for RFC 3576	Enabled 💌
Priority Order	Server Timeout	2 seconds
Certificate	Network User	Enable
Access Control Lists	Management	Enable
Wireless Protection Policies	IPSec	Enable

Step 4 The AP is in local mode by default, so covert the mode to FlexConnect mode. Local mode APs can be converted to FlexConnect mode by going to **Wireless > All APs**, and click the Individual AP.

General	Credentials	Interfaces	High Availability	Inventory	Advanced	
ieneral				Versions		
AP Name	A	P3500		Primary Soft	ware Version	7.2.1.69
Location	de	fault location		Backup Soft	ware Version	7.2.1.72
AP MAC	Address cc	:ef:48:c2:35:57		Predownload	Status	None
Base Rad	fio MAC 2c	:3f:38:f6:98:b0		Predownload	ed Version	None
Admin St	atus Er	nable 💌		Predownload	Next Retry Time	NA
AP Mode	6	exConnect 👻		Predownload	Retry Count	NA
AP Sub M	lode No	one 💌		Boot Version		12.4.23.0
Operation	nal Status RE	G		IOS Version		12.4(20111122:141426)
Port Num	iber 1			Mini IOS Ver	sion	7.0.112.74
Venue G	roup Ur	nspecified	~	IP Config		
Venue Ty	vpe Ur	nspecified 💌		IP Address		10.10.10.132
Venue Na	ame			Static IP		
Language	1					
Network Interface	Spectrum 00	45BA896226F411	7D98BA920FBA8A16	Time Statistics	5	
interrace	Ney			UP Time		0 d, 00 h 01 m 14 s
				Controller As	sociated Time	0 d, 00 h 00 m 14 s
				Controller As	sociation Latency	0 d, 00 h 00 m 59 s

Step 5 Add the FlexConnect APs to the FlexConnect group.

Navigate under WLC GUI > Wireless > FlexConnect Groups > Select FlexConnect Group > General tab > Add AP.

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping		
	ame Store 1		۸۸۸		
dd AP			Primary Radius Server	None	*
	Ps from current controller		Secondary Radius Server	None	*
Add AP Select A AP Nam		AP3500		None	100
Select A	e		Secondary Radius Server	None	1999

Step 6 The FlexConnect AP should be connected on a trunk port and WLAN mapped VLAN and AAA overridden VLAN should be allowed on the trunk port.

	gabitEthernet1/0/4
	AP3500
	trunk encapsulation dotlq
	trunk native vlan 109
	trunk allowed vlan 3,109
switchport	node trunk

ſ

Note

In this configuration, VLAN 109 is used for WLAN VLAN mapping and VLAN 3 is used for AAA override.

Step 7 Configure WLAN to VLAN Mapping for the FlexConnect AP. Based on this configuration, the AP would have the interfaces for the VLAN. When the AP receives the VLAN configuration, corresponding dot11 and Ethernet sub-interfaces are created and added to a bridge-group. Associate a client on this WLAN and when the client associates, its VLAN (default, based on the WLAN-VLAN mapping) is assigned.

Navigate to WLAN GUI > Wireless > All APs, click the specific AP > FlexConnect tab, and click VLAN Mapping.

AP Na	me	AP3500	
Base F	Radio MAC	2c:3f:38:f6:98:b0	
	SSID		VLAN
1	Store 1		109

Step 8 Create a user in the AAA server and configure the user to return VLAN ID in IETF Radius attribute.

		Attribute	Туре	Value	
I	ETF 65	Tunnel-Medium-Type	Tagged Enum	[T:1] 802	1
1	ETF 64	Tunnel-Type	Tagged Enum	[T:1] VLAN	
1	ETF 81	Tunnel-Private-Group-ID	Tagged String	[T:1] 3	50485

Step 9 In order to have dynamic VLAN assignment, the AP would have the interfaces for the dynamic VLAN pre-created based on the configuration using existing WLAN-VLAN Mapping for the individual FlexConnect AP or using ACL-VLAN mapping on FlexConnect group.

In order to configure AAA VLAN on the FlexConnect AP, navigate to WLC GUI > Wireless > FlexConnect Group, click the specific FlexConnect group > VLAN-ACL mapping, and enter VLAN in the Vlan ID field.

I

General	Local Authentication	Image Upgrade	VLAN-ACL mapping
VI AN ACL	Mapping		
TENIT ACE			
Vlan Id	3		
	3		
Vlan Id	3 CL none V		

- **Step 10** Associate a client on this WLAN and authenticate using the user name configured in the AAA server in order to return the AAA VLAN.
- Step 11 The client should receive an IP address from the dynamic VLAN returned via the AAA server.
- **Step 12** In order to verify, click **WLC GUI > Monitor > Client**, click the specific client MAC address in order to check the client details.

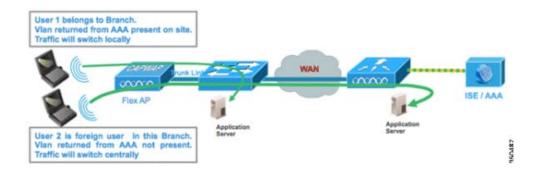
Limitations

- Cisco Airespace-specific attributes will not be supported and IETF attribute VLAN ID will only be supported.
- A maximum of 16 VLANs can be configured in per-AP configuration either via WLAN-VLAN Mapping for individual FlexConnect AP or using ACL-VLAN mapping on the FlexConnect group.

FlexConnect VLAN Based Central Switching

In controller software releases 7.2, AAA override of VLAN (Dynamic VLAN assignment) for locally switched WLANs will put wireless clients to the VLAN provided by the AAA server. If the VLAN provided by the AAA server is not present at the AP, the client is put to a WLAN mapped VLAN on that AP and traffic will switch locally on that VLAN. Further, prior to release 7.3, traffic for a particular WLAN from FlexConnect APs can be switched Centrally or Locally depending on the WLAN configuration.

From release 7.3 onwards, traffic from FlexConnect APs can be switched Centrally or Locally depending on the presence of a VLAN on a FlexConnect AP.



Summary

Traffic flow on WLANs configured for Local Switching when Flex APs are in Connected Mode:

- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the Flex AP database, traffic will switch centrally and the client will be assigned this VLAN/Interface returned from the AAA server provided that the VLAN exists on the WLC.
- If the VLAN is returned as one of the AAA attributes and that VLAN is not present in the Flex AP database, traffic will switch centrally. If that VLAN is also not present on the WLC, the client will be assigned a VLAN/Interface mapped to a WLAN on the WLC.

- If the VLAN is returned as one of the AAA attributes and that VLAN is present in the FlexConnect AP database, traffic will switch locally.
- If the VLAN is not returned from the AAA server, the client will be assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

Traffic flow on WLANs configured for Local Switching when Flex APs are in Standalone Mode:

- If the VLAN returned by an AAA server is not present in the Flex AP database, the client will be put to default VLAN (that is, a WLAN mapped VLAN on Flex AP). When the AP connects back, this client will be de-authenticated and will switch traffic centrally.
- If the VLAN returned by an AAA server is present in the Flex AP database, the client will be put into a returned VLAN and traffic will switch locally.
- If the VLAN is not returned from an AAA server, the client will be assigned a WLAN mapped VLAN on that FlexConnect AP and traffic will switch locally.

Procedure

Complete these steps:

Step 1 Configure a WLAN for Local Switching and enable AAA override.

eneral Security	QoS Advanced
Allow AAA Override	🗹 Enabled
Coverage Hole Detection	Enabled
Enable Session Timeout	Session Timeout (secs)
Aironet IE	Enabled
Diagnostic Channel	Enabled
Override Interface ACL	IPv4 None V IPv6 None S
P2P Blocking Action	Disabled 💌
Client Exclusion ³	Enabled 60 Timeout Value (secs)
Maximum Allowed Clients ^g	0
Static IP Tunneling 💶	Enabled
Wi-Fi Direct Clients Policy	Disabled 💌
Maximum Allowed Clients Per AP Radio	200
lexConnect	

General Sec	urity QoS	Ad	vanced		
Allow AAA Ove	rride 🔽	Enabled			
Coverage Hole		Enabled			
Enable Session		1800	Timeout (secs)		
Aironet IE	ΨE	nabled			
Diagnostic Cha	nnel 📃 E	nabled			
Override Interf	ace ACL IPv	1 None	~	IPv6	None N
P2P Blocking A	ction Di:	abled	~		
Client Exclusion	. <u>3</u>	nabled	60 Timeout Value	e (secs)	
Maximum Allow Clients [@]	o o				
Static IP Tunne	ing 💶 🛛 🗖 E	nabled			
Wi-Fi Direct Cli Policy	Dis	abled	~		
Maximum Allow Clients Per AP	20)			
FlexConnect					
FlexConnect Lo Switching ²	cal 🔽	Enable	d		
FlexConnect Lo	cal Auth 💶 📋	Enable	d		
Learn Client IP	Address 5	Enable	d		
Vlan based Cer	ntral 🔽	Enable			

Step 2 Enable Vlan based Central Switching on the newly created WLAN.

I

Γ

Step 3 Set AP Mode to **FlexConnect.**

	All APs >	Details for	AP_3500E
--	-----------	-------------	----------

General Credent	ials Interfaces	High Availability
ieneral		
AP Name	AP_3500E	
Location		
AP MAC Address	o4:7d:4f:3a:07:74	
Base Radio MAC	o4:7d:4f:53:24:e0	
Admin Status	Enable 💌	
AP Mode	FlexConnect	
AP Sub Mode	local FlexConnect	
Operational Status	monitor	
Port Number	Rogue Detector Sniffer	
Venue Group	Bridge SE-Connect	~

Step 4 Make sure that the FlexConnect AP has some sub-interface present in its database, either via WLAN-VLAN Mapping on a particular Flex AP or via configuring VLAN from a Flex group. In this example, VLAN 63 is configured in WLAN-VLAN mapping on Flex AP.

1

cisco		<u>W</u> LANs		WIRELESS	
Wireless	All APs > A	P_3500	DE > VLAN Ma	ppings	
Access Points	AP Name	4	AP_3500E		
♥ Radios 802.11a/n	Base Radio	MAC d	4:7d:4f:53:24:e0		
802.11b/g/n Global Configuration	WLAN Id S	SID			VLAN ID
Advanced		tore 1' :			63
Mesh					1.2.2
RF Profiles	Centrally sy	vitched	Wlans		
FlexConnect Groups FlexConnect ACLs	WLAN Id	ficone a	SSID	VLAN ID	
▶ 802.11a/n	AP level VL	AN ACL	Mapping		
▶ 802.11b/g/n	Vlan Id		ess ACL	Egress A	CL
Media Stream	63	none		none 💌	
Country	Group leve	I VLAN A	CL Mapping		
	Vlan Id	Ingr	ess ACL	Egress A	CL

Step 5 In this example, VLAN 62 is configured on WLC as one of the dynamic interfaces and is not mapped to the WLAN on the WLC. The WLAN on the WLC is mapped to Management VLAN (that is, VLAN 61).

սիսիս cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>o</u> mmands	HELP	EEEDBACK	ł
Controller	Interfaces	s								
General Inventory	Interface	Name		/LAN Identifier	IP Address	Interface T	ype Dynam	iic AP M	anagement	
Interfaces	dyn		(52	9.6.62.10	Dynamic	Disable	d		ŀ
Interface Groups	manageme	ent.		51	9.6.61.2	Static	Enabled	ł		

Step 6

ſ

Associate a client to the WLAN configured in Step 1 on this Flex AP and return VLAN 62 from the AAA server. VLAN 62 is not present on this Flex AP, but it is present on the WLC as a dynamic interface so traffic will switch centrally and the client will be assigned VLAN 62 on the WLC. In the output captured here, the client has been assigned VLAN 62 and Data Switching and Authentication are set to Central.

Summary				
Access Points				
Cisco CleanAir	Client Properties		AP Properties	
 Statistics CDP 	MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
Rogues	IPv4 Address	9.6.62.100	AP Name	AP_3500E
Redundancy	IPv6 Address		AP Type	802.11a
Clients			WLAN Profile	'Store 1'
Multicast			Data Switching	Central
			Authentication	Central
			Status	Associated
			Association ID	1
			802.11 Authentication	Open System
			Reason Code	3
			Status Code	0
	Client Type	Regular	CF Pollable	Not Implemented
	User Name	betauser	CF Poll Request	Not Implemented
	Port Number	1	Short Preamble	Not Implemented
	Interface	dyn	PBCC	Not Implemented
	VLAN ID	62	Channel Agility	Not Implemented

- **Note** Observe that although WLAN is configured for Local Switching, the Data Switching field for this client is Central based on the presence of a VLAN (that is, VLAN 62, which is returned from the AAA server, is not present in the AP Database).
- **Step 7** If another user associates to the same AP on this created WLAN and some VLAN is returned from the AAA server which is not present on the AP as well as the WLC, traffic will switch centrally and the client will be assigned the WLAN mapped interface on the WLC (that is, VLAN 61 in this example setup), because the WLAN is mapped to the Management interface which is configured for VLAN 61.

ient Properties		 AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.61.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile 'St	ore 1'
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	3
		Status Code	0
Client Type	Regular	CF Pollable	Not Implemented
User Name	betauser2	CF Poll Request	Not Implemented
Port Number	1	Short Preamble	Not Implemented
Interface	management	PBCC	Not Implemented
VLAN ID	61	Channel Agility	Not Implemented

Observe that although WLAN is configured for Local Switching, the Data Switching field for this client is Central based on the presence of a VLAN. That is, VLAN 61, which is returned from the AAA server, is not present in the AP Database but is also not present in the WLC database. As a result, the client is assigned a default interface VLAN/Interface which is mapped to the WLAN. In this example, the WLAN is mapped to a management interface (that is, VLAN 61) and so the client has received an IP address from VLAN 61.

Step 8 If another user associates to it on this created WLAN and VLAN 63 is returned from the AAA server (which is present on this Flex AP), the client will be assigned VLAN 63 and traffic will switch locally.

Clients > Detail			
Client Properties		AP Properties	
MAC Address	00:40:96:b8:d4:be	AP Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central

Limitations

• VLAN Based Central Switching is only supported on WLANs configured for Central Authentication and Local Switching.

1

• The AP sub-interface (that is, VLAN Mapping) should be configured on the FlexConnect AP.

FlexConnect ACL

With the introduction of ACLs on FlexConnect, there is a mechanism to cater to the need of access control at the FlexConnect AP for protection and integrity of locally switched data traffic from the AP. FlexConnect ACLs are created on the WLC and should then be configured with the VLAN present on the FlexConnect AP or FlexConnect group using VLAN-ACL mapping which will be for AAA override VLANs. These are then pushed to the AP.



Summary

- Create FlexConnect ACL on the controller.
- Apply the same on a VLAN present on FlexConnect AP under AP Level VLAN ACL mapping.
- Can be applied on a VLAN present in FlexConnect Group under VLAN-ACL mapping (generally done for AAA overridden VLANs).
- While applying ACL on VLAN, select the direction to be applied which will be "ingress", "egress" or "ingress and egress".

Procedure

Complete these steps:

Step 1 Create a FlexConnect ACL on the WLC. Navigate to WLC GUI > Security > Access Control List > FlexConnect ACLs.

Step 3 Configure the ACL Name.

Step 2

I

ccess Control Lists > New	< Back	Apply
ccess Control List Name Flex-ACL-Ingress		

Step 4 Click Apply.

Step 5 Create rules for each ACL. In order to create rules, navigate to WLC GUI > Security > Access Control List > FlexConnect ACLs, and click the above created ACL.

Acci	ess Con	trol Lists > Edit						< Back	Add New Rule
Gene	e ral is List Nam	e Flex-ACL-	Ingrass						
	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP		

Step 6 Click Add New Rule.

Access Contro	ol Lists > Rules > New			< Back	Apply
Sequence	1				
Source	IP Address 💌	IP Address 0.0.0.0	Netmask 0.0.0.0		
Destination	IP Address 💌	IP Address 0.0.0.0	Netmask 0.0.0.0		
Protocol	Any 🗸				
DSCP	Any 💌				
Action	Deny 💌				350500
	figure the rules as pe	r the requireme	ent. If the permi	it anv rule is i	ot configure

te Configure the rules as per the requirement. If the permit any rule is not configured at the end, there is an implicit deny which will block all traffic.

- **Step 7** Once the FlexConnect ACLs are created, it can be mapped for WLAN-VLAN mapping under individual FlexConnect AP or can be applied on VLAN-ACL mapping on the FlexConnect group.
- Step 8 Map FlexConnect ACL configured above at AP level for individual VLANs under VLAN mappings for individual FlexConnect AP. Navigate to WLC GUI > Wireless > All AP, click the specific AP > FlexConnect tab > VLAN Mapping.

AP Name		AP3500			
Base Rad	lio MAC	2c:3f:38:f6:	98:b0		
WLAN Id	SSID				VLAN ID
1	Store 1				109
entrally	switche	d Wlans			
0.23		d Wlans		1	VLAN ID
WLAN Id		d Wlans			VLAN IE N/A
WLAN Id 2	SSID Store 3	ed Wlans			0.00035000
WLAN Id 2	SSID Store 3	L Mapping		Egress ACL	0.00035000

Step 9 FlexConnect ACL can also be applied on VLAN-ACL mapping in the FlexConnect group. VLANs created under VLAN-ACL mapping in FlexConnect group are mainly used for dynamic VLAN override.

eneral L	ocal Authentication	Image Upgrade	VLAN-ACL mapping
AN ACL M	apping		
Vlan Id	0		
Ingress ACL	Flex-ACL-Egress V		
Egress ACL	Flex-ACL-Egress		
	Add		

Limitations

ſ

- A maximum of 512 FlexConnect ACLs can be configured on WLC.
- Each individual ACL can be configured with 64 rules.
- A maximum of 32 ACLs can be mapped per FlexConnect group or per FlexConnect AP.
- At any given point in time, there is a maximum of 16 VLANs and 32 ACLs on the FlexConnect AP.

FlexConnect Split Tunneling

In WLC releases prior to 7.3, if a client connecting on a FlexConnect AP associated with a centrally switched WLAN needs to send some traffic to a device present in the local site/network, they need to send traffic over CAPWAP to the WLC and then get the same traffic back to the local site over CAPWAP or using some off-band connectivity.

From release 7.3 onwards, **Split Tunneling** introduces a mechanism by which the traffic sent by the client will be classified based on packet contents **using Flex ACL**. Matching packets are switched locally from Flex AP and the rest of the packets are centrally switched over CAPWAP.

From release 8.8 onwards, Split Tunneling is also supported on Wave-2 802.11ac based AP as noted in the beginning of this guide. Matching packets are switched locally from Flex AP and the rest of the packets are centrally switched over CAPWAP.

The Split Tunneling functionality is an added advantage for OEAP AP setup where clients on a Corporate SSID can talk to devices on a local network (printers, wired machine on a Remote LAN Port, or wireless devices on a Personal SSID) directly without consuming WAN bandwidth by sending packets over CAPWAP. Split tunneling is not supported on OEAP 600 APs. Flex ACL can be created with rules in order to permit all the devices present at the local site/network. When packets from a wireless client on the Corporate SSID matches the rules in Flex ACL configured on OEAP AP, that traffic is switched locally and the rest of the traffic (that is, implicit deny traffic) will switch centrally over CAPWAP.

The Split Tunneling solution assumes that the subnet/VLAN associated with a client in the central site is not present in the local site (that is, traffic for clients which receive an IP address from the subnet present on the central site will not be able to switch locally). The Split Tunneling functionality is designed to switch traffic locally for subnets which belong to the local site in order to avoid WAN bandwidth consumption. Traffic which matches the Flex ACL rules are switched locally and NAT operation is performed changing the client's source IP address to the Flex AP's BVI interface IP address which is routable at the local site/network.



Summary

- The Split Tunneling functionality is supported on WLANs configured for Central Switching advertised by Flex APs only.
- The DHCP required should be enabled on WLANs configured for Split Tunneling.
- The Split Tunneling configuration is applied per WLAN configured for central switching on per Flex AP or for all the Flex APs in a FlexConnect Group.

Procedure

Γ

Complete these steps:

Step 1 Configure a WLAN for Central Switching (that is, **Flex Local Switching** should not be enabled).

General	Security	QoS	Advanced	1	
Coverag	A Override e Hole Detectio ession Timeout	180	bled	(secs)	
Aironet 1	E	Enab			
Diagnost	tic Channel	Enab	led		
Override	Interface ACL	IPv4 N	lone 💌		IPv6 None N
P2P Bloc	king Action	Disabl	ed	~	
Client E>	clusion ³	Enab	led 60 Timeou	t Value (secs)	
Maximur Clients 🔮	n Allowed	0]		
Static IP	Tunneling 👭	Enab	led		
Wi-Fi Dir Policy	ect Clients	Disabl	ed 💌	Electronic and	
	n Allowed er AP Radio	200			l Switching be enabled
FlexConne	ct			/	

Step 2 Set DHCP Address Assignment to **Required.**

General	Security	QoS Advan	d			
Allow AA	A Override	Enabled			DHCP	
Coverag	e Hole Detectio	n 🗹 Enabled			DHCP Server	Override
Enable S	ession Timeout	1800 Session Tim	ut (secs)		DHCP Addr. Assignment	Require
Aironet I	E	Enabled			Management Frame Prot	
Diagnost	ic Channel	Enabled				ection (PPP)
Override	Interface ACL	IPv4 None M		IPv6 None 💌	MFP Client Protection	Optional N

General	Credenti	als	Interfac	ces	High Availability
General					
AP Name		AP_3	3500E		
Location					
AP MAC	Address	04:7	d:4f:3a:07	7:74	
Base Rad	lio MAC	o4:7	d:4f:53:24	4:e0	
Admin St	atus	Enat	ole 💌		
AP Mode		Flex	Connect	~	
AP Sub M	lode	loca Flex	l Connect	_	
Operation	nal Status	mon		r	
Port Num	ber	Snift	fer		
Venue Gi	roup	Brid SE-0	ge Connect		~

All APs > Details for AP_3500E

Step 4 Configure FlexConnect ACL with a permit rule for traffic which should be switched locally on the Central Switch WLAN. In this example, the FlexConnect ACL rule is configured so it will alert ICMP traffic from all the clients which are on the 9.6.61.0 subnet (that is, exist on the Central site) to 9.1.0.150 to be switched locally after the NAT operation is applied on Flex AP. The rest of the traffic will hit an implicit deny rule and be switched centrally over CAPWAP.

350506

ı. cısco	Mont	TOR	<u>W</u> LANs		LER	WIRELESS	5	ECURITY	MANAGEMENT	COMMANDS	неџр	EEEDBACK
Wireless	Acce	ess Co	ntrol Li	ists > Edi	t							
Access Points All APs	Gene	eral										
 Radios 802.11a/n 802.11b/g/n 	Acces	s List Na	me	Fle	x-A(CL						
Global Configuration	Seq	Action	Sour	ce IP/Masi		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	
Advanced Mesh	1	Permit	9.6.6	1.0		9.1.0.150	/	ICMP	Any	Any	Any	٠
RF Profiles					_		_					
FlexConnect Groups FlexConnect ACLs												

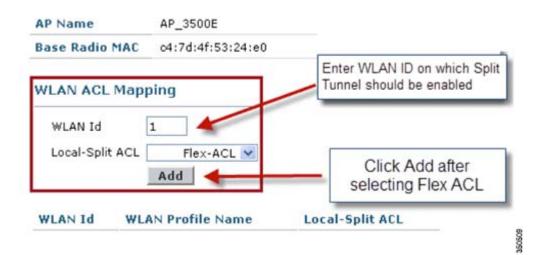
Step 5 This created FlexConnect ACL can be pushed as a Split Tunnel ACL to individual Flex AP or can also be pushed to all the Flex APs in a Flex Connect group.

Complete these steps in order to push Flex ACL as a Local Split ACL to individual Flex AP:

a. Click Local Split ACLs.

ululu cisco		<u>w</u> lans <u>c</u> ont	ROLLER WIRE	LESS SECURITY	MANAGEMENT	COMMANDS HE	ELP EEEDBACK
Wireless	All APs > D	Details for AP	3500E				
Access Points All APs	General	Credentials	Interfaces	High Availability	y Inventory	FlexConnect	Advanced
♥ Radios 802.11a/n 802.11b/g/n Global Configuration	VLAN Su	pport					
Advanced	Native V	LAN ID	57 VL	AN Mappings			
Mesh	FlexCon	nect Group Name	Not Configure	d			
RF Profiles	Destables	tication Access	Control Links				
FlexConnect Groups FlexConnect ACLs		WebAuthenticatio			-		8
▶ 802.11a/n	Local Spl	lit ACLE	And in case of the local division of the loc				350508

- **b.** Select **WLAN Id** on which Split Tunnel feature should be enabled, choose **Flex-ACL**, and click **Add**.
 - All APs > AP_3500E > ACL Mappings



c. Flex-ACL is pushed as Local-Split ACL to the Flex AP.

I

WLAN ACL Mapping WLAN Id 0 Local-Split ACL Flex-ACL Add	AP Name		AP_3500E	
WLAN Id 0 Local-Split ACL Flex-ACL	Base Radio	MAC	o4:7d:4f:53:24:e0	
Local-Split ACL Flex-ACL	WLAN ACI	Mapp	bing	
	WLAN Id	[0	
Add	Local-Spl	t ACL [Flex-ACL 💌	
			Add	
		LAN P	rofile Name	Local-Split ACL
WLAN Id WLAN Profile Name Local-Split ACL	1	Store 1'		Flex-ACL

Complete these steps in order to push Flex ACL as Local Split ACL to a FlexConnect Group:

a. Select the WLAN Id on which the Split Tunneling feature should be enabled. On the **WLAN-ACL mapping** tab, select FlexConnect ACL from the FlexConnect group where particular Flex APs are added, and click **Add**.

1

Wireless	FlexConnect Groups > Edit	Flex-Group'			
Access Points All AP1 Redios	General Local Authentication	Image Upgrade	AAA YLAN-ACL mepping	WLAN-ACL mapping	WebPolicies
002.11a/n 002.11b/g/h Global Configuration Advanced	Web Auth ACL Mopping		Local Split ACL Map		a NID on which Split Id be enabled
Mesh RF Profiles FlexConnect Groups	WLAN Jd 0 WebAuth ACL Flex-ACL W		WLAN 1d 1 Local Split ACL	Flex-ACL Click ADD / ACL	after selecting Flex
> 002.11a/n	WLAN Id WLAN Profile Name	WebAuth ACL	WLAN Ed WLAN F	rufile Name Loca	dSplit ACL

b. The Flex-ACL is pushed as LocalSplit ACL to Flex APs in that Flex group.

W	ireless	FlexConne	ect Groups > Edit	Flex-Group*			
•	Access Points All APs Radies 802.11a/h	General	Local Authentication	Image Upgrade	AAA YLAN-ACL mapping	WLAN-ACL mapping	WebPalicies
	002.11b/g/n Global Centiguration	Web Aut	h ACL Mapping		Local Split ACL M	apping	
1	Advanced Mesh	WLAN Id	0		WLAN Id 0		
	RF Profiles	WebAut			Local Split ACL	Flex-ACL M	
	FlexConnect Groups FlexConnect ACLa		Add			Add	
•	802.11a/n	WLAN Id	WLAN Profile Name	WebAuth ACI	WLAN Id WLAN	N Profile Name Loci	Her-ACL V
	802.11b/g/n				1 'Stor	e 1'	Flex-ACL V

Limitations

- Flex ACL rules should not be configured with permit/deny statement with same subnet as source and destination.
- Traffic on a Centrally Switched WLAN configured for Split Tunneling can be switched locally only when a wireless client initiates traffic for a host present on the local site. If traffic is initiated by clients/host on a local site for wireless clients on these configured WLANs, it will not be able to reach the destination.
- Split Tunneling is not supported for Multicast/Broadcast traffic. Multicast/Broadcast traffic will switch centrally even if it matches the Flex ACL.

Fault Tolerance

FlexConnect Fault Tolerance allows wireless access and services to branch clients when:

- FlexConnect Branch APs lose connectivity with the primary controller.
- FlexConnect Branch APs are switching to the secondary controller.
- FlexConnect Branch APs are re-establishing connection to the primary controller.

FlexConnect Fault Tolerance, along with Local EAP as outlined above and PEAP/EAP-TLS authentication on FlexConnect AP with release 7.5, together provide zero branch downtime during a network outage. This feature is enabled by default and cannot be disabled. It requires no configuration on the controller or AP. However, to ensure Fault Tolerance works smoothly and is applicable, this criteria should be maintained:

- WLAN ordering and configurations have to be identical across the primary and backup controllers.
- VLAN mapping has to be identical across the primary and backup controllers.
- Mobility domain name has to be identical across the primary and backup controllers.

Summary

- FlexConnect will not disconnect clients when the AP is connecting back to the same controller provided there is no change in configuration on the controller.
- FlexConnect will not disconnect clients when connecting to the backup controller provided there is no change in configuration and the backup controller is identical to the primary controller.
- FlexConnect will not reset its radios on connecting back to the primary controller provided there is no change in configuration on the controller.

Limitations

- Supported only for FlexConnect with Central/Local Authentication with Local Switching.
- Centrally authenticated clients require full re-authentication if the client session timer expires before the FlexConnect AP switches from Standalone to Connected mode.
- FlexConnect primary and backup controllers must be in the same mobility domain.

Client Limit per WLAN

Along with traffic segmentation, the need for restricting the total client accessing the wireless services arises. For example, limiting total Guest Clients from branch tunneling back to the Data Center.

In order to address this challenge, Cisco is introducing Client Limit per WLAN feature that can restrict the total clients allowed on a per WLAN basis.

Primary Objective

- Set limits on maximum clients
- Operational ease



• This is not a form of QoS.

By default, the feature is disabled and does not force the limit.

Limitations

This feature does not enforce client limit when the FlexConnect is in Standalone state of operation. Any configuration mismatch across WLCs in any of below will result in radio reset at AP:

- 1. Flexconnect group (all possible configs)
- 2. WLAN to WLAN mapping per AP / AP Group / WLAN
- 3. Radio related configs (rates / power) etc.
- **4**. WLAN configurations

WLC Configuration

Complete these steps:

Step 1 Select the Centrally Switched WLAN ID 1 with SSID **DataCenter**. This WLAN was created during THE AP Group creation. See Figure 3.

- **Step 2** Click the **Advanced** tab for WLAN ID 1.
- Step 3 Set the client limit value for the Maximum Allowed Clients text field.
- Step 4 Click Apply after the text field for Maximum Allowed Clients is set.

General Security QoS Advanced		^
Allow AAA Override Enabled Coverage Hole Detection P Enabled Enable Sessien Timeout P Enabled Enable Sessien Timeout (secs) Aironet IE P Enabled Diagnostic Channel Enabled IPv6 Enable Ž Override Interface ACL P2P Blocking Action Client Exclusion Ž Client S Client S	DHCP DHCP Server OHCP Addr. Assignment Required Management Frame Protection (MFP) MFP Client Protection Optional OTIM Period (in beacon intervals) 02.11a/n (1 - 255) 002.11b/g/n (1 - 255) NAC NAC NAC NAC OOB State Enabled Posture State Enabled Load Balancing and Band Select	
Scan Defer Time(msecs) 100	Client Load Balancing Client Band Select	~
Foot Notes	34	>
2 H-REAP Local Switching is not supported with IPsec, CRANITE authenti 3 When client exclusion is enabled, a Timeout Value of zero means infin 4 Client MP is not active unless WA21 is configured 5 Learn Client IP is configurable only when HREAP Local Switching is ena 4 WMM and open or AES security should be enabled to support higher 1. 7 Multicast Should Be Enabled For IPV6. 8 Band Select is configurable only when Radio Policy is set to 'All'. 9 Value zero implies there is no restriction on maximum clients allowed 10 MAC Filtering is not supported with HREAP Local subhenciation	ity (will require administrative override to reset excluded clients) bled	

Default for Maximum Allowed Clients is set to 0, which implies there is no restriction and the feature is disabled.

Configuration through Cisco Prime

ſ

In order to enable this feature from the Cisco Prime, go to **Configure > Controllers > Controller IP >** WLANs > WLAN Configuration > WLAN Configuration Details.

Properties General Security QcS Advacced HotSpot Policy Configuration System		Home	Monitor T Configure	Servic	ces 🔻 Reports 🔻 Admini	istration 🔻	
Security Security Enable PecConnect PecConnect Enable 20 VLAN Configuration Alrind E of Enable PecConnect Local Auth D Enable 21 VLAN Configuration Alrind E of Enable PecConnect Local Auth D Enable 21 VLAN Configuration Percenter of Enable Learn Clerit P Address Enable 22 VLAN Configuration Percenter Diagnostic Channel (P Enable Learn Clerit P Address Enable 24 PERCONNECT Diagnostic Channel (P Enable Central DHCP Processing Enable 3602.111 Override Interfice ACL Pr4 NNNE Override Interfice ACL Pr4 802.111 VHAT Direct Electron (PFP) Diable Override INFC Enable 802.111/n Client Exclusion (P Diable DHCP DHCP 802.111/n Client Exclusion (P Diable DHCP DHCP 802.111/n Client Exclusion (P Diable DHCP DHCP 802.111/n Timeout Value 60 (sco) MPP Client Protection (MPP)	Properties	General Security	QoS Advanced	HotS	pot Policy Configuration	1	
WLAKE V Joseph (Indoor Perconnect Local Switching) Enable 2/ WLAN Configuration Coverage into Datation (Enable If Enable Perconnect Local Switching) Enable 2/ WLAN Configuration Allonet IE If Enable Perconnect Local Switching Enable 2/ Policy Configuration Disposition Enable UAN Bade Central Switching Enable 3/ Policy Configuration Disposition Enable UAN Bade Central Switching Enable 3/ Policy Configuration Disposition Finable Central INCP Processing Enable 3/ Policy Configuration Disposition Finable Ownide Interface ACL Pr4 NORE Ownide INCP Processing Enable 3/ Policy Configuration Disposition Disposition Enable NoT+Art Enable 3/ Policy Configuration VM-Polet Elections Policy Disbel = 0 NoT+Art Enable 3/ Policy Configuration Central Election Policy Disbel = 0 NoT+Art Enable 3// Policy Configuration Central Election Policy Disbel = 0 DitCP Ownide Polic	System				DesCannad		
Air ond: E off Enable PecConnect Local Auth (*) Enable A Groups Proj. Configuration Proj. (*) Enable Lam Client IP Address (*) Enable BrackConnect Diagnostic Channel (*) Enable Lam Client IP Address (*) Enable BrackConnect Diagnostic Channel (*) Enable Lam Client IP Address (*) Enable Security Override Interface ALL Proj. (*) Enable Override Interface ALL Proj. (*) Security Override Interface ALL Proj. (*) Notifie DNS Enable Security Override Interface ALL Proj. (*) Notifie DNS Enable S02.11 Verif Direct Elociting (*) Disable 0 Notifie DNS Enable S02.113/n Client Exclusion (*) of Enable DHCP Server Override S02.114/n Timeouch Value 60 (secc) Merogenerat Frame Protection (VFP) Application Visibility And Control Nobility Acchors 0 Merogenerat Frame Protection (VFP) Application Visibility And Control Nobility Acchors 0	WLANs					Enable	
Policy Configuration Disposition Enable VLNI Based Central Switching Enable ReaConnext > Deprodict Channel (?) Intable Central INHCP Processing Enable Security > Poet to Peer Blocking (?) Disable Central INHCP Processing Enable 802.111 > Wri-R Direct Clearls Policy Disable Disable Direc Direc 802.114/n > Wri-R Direct Clearls Policy Disable Direc Direc Direc 802.114/n > Cleart Exclusion (?) off Enable Direc Server Override 802.114/n Cleart Exclusion (?) off Enable Direc Server Override 802.114/n Cleart Exclusion (?) off Enable Direc Server Override 802.114/n Cleart Exclusion (?) off Enable Direc Server Override Required Timoock Value 60 (secs) Management frame Protection (MPP) Application Visibility And Control Mobility Anchors 0 Lead Balancing on Blad Select Porage Controller Mappings 0 Lead Balancing on Enable Client Load Balancing on Enable Nangagement > Off Cannel Scarring Defer Client Bad Select Enable Off Cannel Scarri	WLAN Configuration				FlexConnect Local Auth @	Enable	
Perconnect Disponsitic Channel I/2 Enable Central DHCP Processing Enable Security Verride Interface ACL IP-4 INOR Override INES Enable Security Verride Interface ACL IP-4 INOR Override INES Enable Security Verride Interface ACL IP-4 INOR Override INES Enable Security Verride Interface ACL IP-4 INOR Override INES Enable Security Verride Interface ACL IP-4 INOR Override INES Enable Security Verride Interface ACL Interface ACL Interface ACL Interface ACL Security Verride Interface ACL Interface ACL Interface ACL Interface ACL Security Verride Interface ACL Interface ACL Interface ACL Interface ACL Security Verride Interface ACL Interface ACL Interface ACL Interface ACL Security Verride Interface ACL Interface ACL Interface ACL Interface ACL Security And Control Verride	AP Groups	IPv6 2	Enable		Learn Client IP Address	C Enable	
File/Connect > Overhole Interface ACL P-4 NONE • Security > Poet to Peer Blocking % Interface ACL P-4 NONE • B02.11 > Wi-R Direct Clients Policy Disabled • Direct Direct Direct B02.11 > Wi-R Direct Clients Policy Disabled • Direct Direct Direct B02.114/n > Client Exclusion % off Enable Direct Direct Direct Direct B02.118/n > Client Exclusion % off Enable Direct Direct Direct Direct B02.118/n > Client Exclusion % off Enable Direct Server O override B02.118/n > Timox Value 60 (secs) Harsgement France Production (MPP) Application Visibility And Contonity > Mobility Anchors 0 MPP Client Production % Enable Netfow > Porago-Controller Mappings 0 Load Balancing Enable Ports - Parative Client Enable Client Load Balancing Enable Nongement > Off Channel Scanning Defer Noc Noc	Policy Configuration	Dissocitic Channel	Fnable		VLAN Based Central Switching	Enable	
Access Points > Peer to Peer Blocking ⁽¹⁾ Disble ⁽²⁾ MAT PAT Enable BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Clients Policy Disble ⁽²⁾ Direct Override BC2.11 > Wi-F Direct Direct Override BC2.11 > Wi-F Direct Override BC2.11 > Wi-F Direct Direct Direct Override BC2.11 > Wi-F Direct Direct Direct Override BC2.11 > Wi-F Direct Dire	RexConnect			•	Central DHCP Processing	Enable	
Access Points > Peet to poet Bocking (?) Disable C) 802.11 > Wi-Fi Direct Clents Policy Disable C) 802.111/n > Wi-Fi Direct Clents Policy Disable D) 802.111/n > Clent Exclusion(?) ef Entatle D) 802.111/n > Clent Exclusion(?) ef Entatle D) 802.111/n > Timeout Value 60 (sco) Application Vability And Control > Reamum Clents (?) 0 Methow > Fording Current Policy 0 Methow > Policy Exclusion 0 Policy Parative Client Entable Client Exclusion(?) Parative Client Entable Client Exclusion(?) Entable Noticy Parative Client Entable Client Exclusion(?) Entable Policy Parative Client Entable Client Load Balancing Enable Noticy Off Charmel Scarting Defer Olient Enable Enable Other Charmel Scarting Defer No.6 No.6	Security						
802.11 Wi-Fi Direct Clients Policy Direbhed Direbhed </td <td>Access Points</td> <td>Peer to Peer Blocking 2</td> <td>Disable \$</td> <td></td> <td></td> <td>Enable</td> <td></td>	Access Points	Peer to Peer Blocking 2	Disable \$			Enable	
802.114/n Client Exclusion [®] If Enable DHCP Address Assignment If Required 802.116/n Timock Value 60 (scc) Management Frame Protection (MFP) Application Vability And Control Maximum Clients ¹⁰ 0 Management Frame Protection (MFP) Methow Nobility Anchors 0 Enable MPD Client Protection (MFP) Methow Portigo Control Mobility Anchors 0 Enable Ports Parave Client Enable Client Load Balancing Enable Management 2 Off Channel Scanning Defer Client Biol Select Enable Off Channel Scanning Defer NAC NAC NAC Enable	802.11	Wi-Fi Direct Clients Policy	Disabled \$			Override	
Application Valshilty And Control Application Valshilty And Control Mesh Potson Mesh Potson Pots Pots Pasive Client Potson Pots Pasive Client Potson Pots Pasive Client Potson Pots Pasive Client Potson Pots Potson Po	802.11a/n	Client Exclusion	S Enable			Required	
Netflow Mobility Anchois Image: Controller Muppings Member Mail Member Muppings Member Muppings Member Muppings Image: Controller Muppings Image: Controller Muppings Control Muppings Controller Muppings Contr	802.11b/g/n	Timeout Value	60 (secs)		Management Frame Protection	n (MFP)	
Netflow > Mobility Acctors 0 MPP Guilt Protocol 1 Mesh > Forsign Controller Nuppings 0 Load Balancing and Band Select Ports > Passive Client Enable Client Load Balancing and Band Select Management > Off Channel Scanning Defer Client Band Select Enable Nacc > MPP Vision 1 Enable Dient Load Balancing and Band Select	Application Visibility And Control	Maximum Clients	0		MED Client Destantion	Enabled	
Meeh Product Vactorials U Load Balancing and Band Select Ports > Product Collect Mappings 0 Load Balancing and Band Select Ports > Prostive Cilent Enable Client Load Balancing Enable Managament > Off Channel Scanning Defer Client Band Select Enable Load Defense Off Channel Scanning Defer Client Band Select Enable	Netflow					1	
Ports Passive Client Enable Client Load Balancing Enable Management Off Channel Scanning Defer Olient Band Select Enable Location NAC NAC NAC	Mesh					iat	
Management Off Channel Scanning Defer Olient Band Select Enable Location > NAC NAC NAC	Ports				Plant Lord Palacity		
Location > NAC	Management						
	Location	on channel dealining belo					
Router Advertisement > Scan Defer Priority 0 1 2 3 4 5 6 7 NAC State None \$	Router Advertisement	Scan Defer Priority	0 1 2 3 4 5 6 7		NAC State	(None 🛊	
Scan Defer Time 100 (ms) Voice DTIM Period ⁽²⁾ Client Profiling	Redundancy		100 (ms)				

Peer-to-Peer Blocking

In controller software releases prior to 7.2, peer-to-peer (P2P) blocking was only supported for central switching WLANs. Peer-to-peer blocking can be configured on WLAN with any of these three actions:

- Disabled Disables peer-to-peer blocking and bridged traffic locally within the controller for clients in the same subnet. This is the default value.
- Drop Causes the controller to discard packets for clients in the same subnet.
- Forward Up-Stream Causes the packet to be forwarded on the upstream VLAN. The devices above the controller decide what action to take regarding the packet.

From release 7.2 onwards, peer-to-peer blocking is supported for clients associated on local switching WLAN. Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP.



Summary

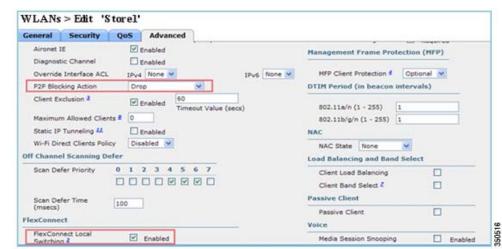
- Peer-to-peer Blocking is configured per WLAN
- Per WLAN, peer-to-peer blocking configuration is pushed by WLC to FlexConnect APs.
- Peer-to-peer blocking action configured as drop or upstream-forward on WLAN is treated as peer-to-peer blocking enabled on FlexConnect AP.

Procedure

Complete these steps:

Step 1 Enable peer-to-peer blocking action as **Drop** on WLAN configured for FlexConnect Local Switching.

I



Step 2 Once the P2P Blocking action is configured as **Drop** or **Forward-Upstream** on WLAN configured for local switching, it is pushed from the WLC to the FlexConnect AP. The FlexConnect APs will store this information in the reap config file in flash. With this, even when FlexConnect AP is in standalone mode, it can apply the P2P configuration on the corresponding sub-interfaces.

Limitations

- In FlexConnect, solution P2P blocking configuration cannot be applied only to a particular FlexConnect AP or sub-set of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports P2P upstream-forward. However, this will not be supported in the FlexConnect solution. This is treated as P2P drop and client packets are dropped instead of forwarded to the next network node.
- Unified solution for central switching clients supports P2P blocking for clients associated to different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

AP Pre-Image Download

This feature allows the AP to download code while it is operational. The AP pre-image download is extremely useful in reducing the network downtime during software maintenance or upgrades.

Summary

I

- Ease of software management
- Schedule per store upgrades: NCS or Cisco Prime is needed to accomplish this.
- Reduces downtime

Procedure

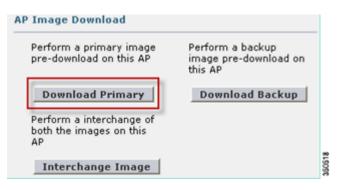
Complete these steps:

Step 1 Upgrade the image on the primary and backup controllers.

Navigate under WLC GUI > Commands > Download File to start the download.

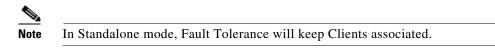
Code	¥
TFTP 💌	
10	
6	
AS_5500_7_0_112_52.aes	
	TFTP V

- Step 2 Save the configurations on the controllers, but do not reboot the controller.
- **Step 3** Issue the AP pre-image download command from the primary controller.
 - a. Navigate to WLC GUI > Wireless > Access Points > All APs and choose the access point to start pre-image download.
 - **b.** Once the access point is chosen, click the **Advanced** tab.
 - c. Click Download Primary to initiate pre-image download.



```
*Sep
              903: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
Image
              not found in flash, predownloading.
examining image...
extracting info (326 bytes)
Image info:
   Version Suffix: k9w8-.wnbu_j_mr.201009101910
   Image Name: c1250-k9w8-mx.wnbu_j_mr.201009101910
   Version Directory: c1250-k9w8-mx.wnbu_j_mr.201009101910
   Ios Image Size: 5530112
   Total Image Size: 5550592
   Image Feature: WIRELESS LAN|LWAPP
   Image Family: C1250
   Wireless Switch Management Version:
Extracting files...
c1250-k9w8-mx.wnbu_j_mr.201009101910/ (directory) 0 (bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_1.img (13696 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W5.bin (17372 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9w8-mx.wnbu_j_mr.20100910
1910 (5322509 bytes)!!!!!
*Sep 13 21:25:43.747: Loading file /c1250-pre
                                                                   35051
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/8001.img (172792 bytes)!!!!!!!!
1111
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/W2.bin (4848 bytes)!
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/info (326 bytes)
extracting c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250_avr_2.img (10880 bytes)!
extracting info.ver (326 bytes)
New software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910
archive download: takes 138 seconds
New backup software image installed in flash:/c1250-k9w8-mx.wnbu_j_mr.2010091019
10/c1250-k9w8-mx.wnbu_j_mr.201009101910
Reading backup version from flash:/c1250-k9w8-mx.wnbu_j_mr.201009101910/c1250-k9
w8-mx.wnbu_j_mr.201009101910done.
Reboot the controllers after all the AP images are downloaded.
```

The APs now fall back to Standalone mode until the controllers are rebooting.



Once the controller is back, the APs automatically reboot with the pre-downloaded image. After rebooting, the APs re-join the primary controller and resume client's services.

Limitations

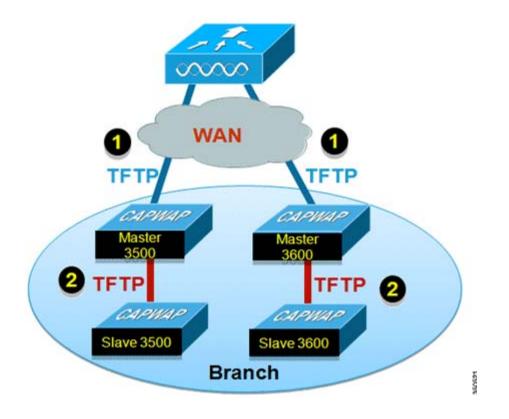
Step 4

• Works only with CAPWAP APs.

FlexConnect Smart AP Image Upgrade

The pre-image download feature reduces the downtime duration to a certain extent, but still all the FlexConnect APs have to pre-download the respective AP images over the WAN link with higher latency.

Efficient AP Image Upgrade will reduce the downtime for each FlexConnect AP. The basic idea is only one AP of each AP model will download the image from the controller and will act as Primary/Server, and the rest of the APs of the same model will work as Secondary/Client and will pre-download the AP image from the primary. The distribution of AP image from the server to the client will be on a local network and will not experience the latency of the WAN link. As a result, the process will be faster.



Summary

- Primary and Secondary APs are selected for each AP Model per FlexConnect Group
- Primary downloads image from WLC
- · Secondary downloads image from Primary AP
- Reduces downtime and saves WAN bandwidth

Procedure

Complete these steps:

Step 1Upgrade the image on the controller.Navigate to WLC GUI > Commands > Download File in order to begin the download.

SCH02

Download file to Controller	
File Type	Code
Transfer Mode	TFTP 💌
Server Details	
IP Address	
Maximum retries	10
Timeout (seconds)	6
File Path	
File Name	AS_5500_7_2_1_72.aes

- **Step 2** Save the configurations on the controllers, but do not reboot the controller.
- **Step 3** Add the FlexConnect APs to FlexConnect group.

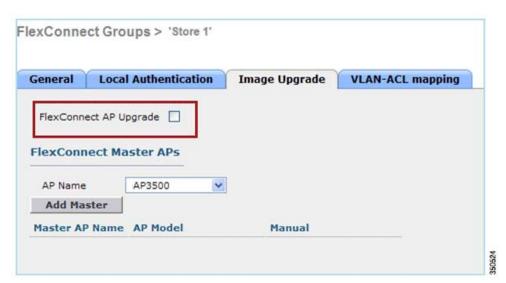
Γ

Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > General tab > Add AP.

350522

eneral	Local Authentication	Image Upgrade	VLAN-ACL mapping		
Group N	ame Store 1				
lexCon	nect APs		AAA		
dd AP			Primary Radius Server	None	
	Ps from current controller	8	Secondary Radius Serve	r None	~
		-	Enable AP Local Authenti	cation	
AP Nam	e i	AR3500			

Step 4 Click the FlexConnect AP Upgrade check box in order to achieve efficient AP image upgrade.
 Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab.



- **Step 5** The Primary AP can be selected manually or automatically:
 - a. In order to manually select the Primary AP, navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab > FlexConnect Master APs, and select AP from the drop-down list, and click Add Master.

General	Local Authentica	tion Image Upgrade	VLAN-ACL mapping	
FlexConn	ect AP Upgrade 🔽			
Slave Ma	ximum Retry Count	44		
Upgrade	Image	Backup 💌	FlexConnect Upgrade	
FlexCon	nect Master APs			
AP Name	AR3500	~		
Add Ma	ster			
	P Name	AP Model	Manual	12000
Master A				

<u>Note</u>

Only one AP per model can be configured as Primary AP. If Primary AP is configured manually, the Manual field will be updated as yes.

I

b. In order to automatically select Primary AP, navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect Group > Image Upgrade tab, and click FlexConnect Upgrade.

General	Local Authentica	tion Image	Upgrade	VLAN-ACL mapping	
FlexConn	ect AP Upgrade 🗹				
Slave Ma	ximum Retry Count	44			
Upgrade	Image	Backup 💌		FlexConnect Upgrade	
FlexConr	AP3500-1	~			
Add Ma					
Master Al	P Name	AP Model		Manual	
	500-1	c3500I		no	

Step 6 In order to start efficient AP image upgrade for all the APs under a specific FlexConnect group, click **FlexConnect Upgrade**.

If Primary AP is selected automatically, the Manual field will be updated as no.

Navigate to WLC GUI > Wireless > FlexConnect Groups, select FlexConnect group > Image Upgrade tab and click FlexConnect Upgrade.

neral	Local Authentica	tion Image Upgrade	VLAN-ACL mapping
			-
exConn	ect AP Upgrade 🔽		
ale factoria a	ect AP Upgrade 🔽 ximum Retry Count	44	

Note

- **Note** Secondary Maximum Retry Count is the number of attempts (44 by default) in which the secondary AP will make in order to download an image from the Primary AP, after which it will fall back to download the image from the WLC. It will make 20 attempts against WLC in order to download a new image after which the administrator has to re-initiate the download process.
- Step 7 Once FlexConnect Upgrade is initiated, only the Primary AP will download the image from the WLC. Under All AP page, Upgrade Role will be updated as Master/Central which means Primary AP has downloaded the image from the WLC which is at the central location. The Secondary AP will download the image from the Primary AP which is at the local site and is the reason under All AP page Upgrade Role will be updated as Slave/Local.

In order to verify this, navigate to WLC GUI > Wireless.

AP Name	AP Model	AP MAC	Download Status	Upgrade Role (Master/Slave)	
AP3600	AIR-CAP3602I-A-K9	44:d3:ca:42:31:62	None		
AP3500	AIR-CAP3502I-A-K9	cc:ef:48:c2:35:57	Complete	Slave/Local	
AP3500-1	AIR-CAP3502I-A-K9	c4:71:fe:49:ed:5e	Complete	Master/Central	

Step 8

Reboot the controllers after all the AP images are downloaded. The APs now fall back to Standalone mode until the controllers are rebooting.



In Standalone mode, Fault Tolerance will keep Clients associated.

Once the controller is back, the APs automatically reboot with the pre-downloaded image. After rebooting, the APs re-join the primary controller and resume the client's services.

Limitations

- Primary AP selection is per FlexConnect group and per AP model in each group.
- Only 3 secondary APs of same model can upgrade simultaneously from their primary AP and rest of the secondary APs will use the random back-off timer to retry for the Primary AP in order to download the AP image.
- In the instance that the Secondary AP fails to download the image from the Primary AP for some reason, it will go to the WLC in order to fetch the new image.
- This works only with CAPWAP APs.
- Smart AP image upgrade does not work when the Primary AP is connected over CAPWAPv6.

Auto Convert APs in FlexConnect Mode

The WLC provides these two options to convert the AP mode to FlexConnect:

- Manual mode
- Auto convert mode

Manual Mode

This mode is available on all the platforms and allows the change to take place only on per AP basis.

- 1. Navigate to WLC GUI > Wireless > All APs and choose the AP.
- 2. Select FlexConnect as the AP Mode, then click Apply.
- **3.** Changing the AP mode causes the AP to reboot.

All APs > Details for AP3500

General	Credentials	Interfaces	High Availability
General			
AP Name	AP3	500	
Location	defa	ault location	
AP MAC Add	lress 00:	22:90:e3:37:df	
Base Radio I	MAC 00:	22:bd:d1:71:30	
Admin Statu	s Dis	able 👻	
AP Mode	loca	al 👻	
AP Sub Mod	e loca	cConnect	
Operational	Status mor	nitor	
Port Number		ue Detector fer	
Venue Grou	P Brid	lge Connect	•

This option is also available on all the current WLC platforms.

Auto Convert Mode

This mode triggers the change on all the connected APs. It is recommended that FlexConnect WLC is deployed in a different mobility domain than existing WLC campus controllers before you enable this CLI:

• This feature is also supported on the 8510, 5520 and 8540 controllers.

```
(Cisco Controller) >config ap autoconvert ?
```

disable.....Disables auto conversion of unsupported mode APs to supported modes
when AP joins
flexconnect.....Converts unsupported mode APs to flexconnect mode when AP joins
monitor....Converts unsupported mode APs to monitor mode when AP joins
(Cisco Controller) >

Step 1 The Auto-conversion feature is disabled by default, which can be verified by using this **show** command:

(Cisco Controller) >show ap autoconvert

AP Autoconvert Disabled

Non-supported AP modes = Local Mode, Sniffer, Rogue Detector and Bridge.

AP Mode	FlexConnect
AP Sub Mode	local
	FlexConnect
Operational Status	Rogue Detector
Port Number	Sniffer
	Bridge
Venue Group	SE-Connect

This option is currently available only via CLIs.

Step 2 Performing config ap autoconvert flexconnect CLI converts all the APs in the network with non-supported AP mode to FlexConnect mode. Any APs that are already in FlexConnect or Monitor Mode are not affected.

```
(Cisco Controller) >config ap autoconvert flexconnect
(Cisco Controller) >show ap autoconvert
AP Autoconvert ..... FlexConnect
(Cisco Controller) >
```

Step 3 Performing **config ap autoconvert monitor** CLI converts all the APs in the network with non-supported AP mode to Monitor mode. Any APs that are already in FlexConnect or Monitor mode are not affected.

(Cisco Controller >config ap autoconvert monitor (Cisco Controller) >show ap autoconvert

AP Autoconvert Monitor

There is no option to perform both **config ap autoconvert flexconnect** and **config ap autoconvert monitor** at the same time.

FlexConnect WGB/uWGB Support for Local Switching WLANs

From release 7.3 onwards, WGB/uWGB and wired/wireless clients behind WGBs are supported and will work as normal clients on WLANs configured for local switching.

After association, WGB sends the IAPP messages for each of its wired/wireless clients, and Flex AP will behave as follows:

- When Flex AP is in connected mode, it forwards all the IAPP messages to the controller and the controller will process the IAPP messages the same as Local mode AP. Traffic for wired/wireless clients will be switched locally from Flex APs.
- When AP is in standalone mode, it processes the IAPP messages, wired/wireless clients on the WGB
 must be able to register and de-register. Upon transition to connected mode, Flex AP will send the
 information of wired clients back to the controller. WGB will send registration messages three times
 when Flex AP transitions from Standalone to Connected mode.

Wired/Wireless clients will inherit WGB's configuration, which means no separate configuration like AAA authentication, AAA override, and FlexConnect ACL is required for clients behind WGB.



Summary

- No special configuration is required on WLC in order to support WGB on Flex AP.
- Fault Tolerance is supported for WGB and clients behind WGB.
- WGB is supported on an IOS AP: 3700, 2700, 1700, 702, 702W, 1530, 1570.
- Starting with release 8.8 WGB will be supported on the Wave-2 APs 2800, 3800 and 1562.

Procedure

I

Complete these steps:

Step 1 No special configuration is needed in order to enable WGB/uWGB support on FlexConnect APs for WLANs configured for local switching as WGB. Also, clients behind WGB are treated as normal clients on local switching configured WLANs by Flex APs. Enable **FlexConnect Local Switching** on a WLAN.

General	Security	QoS A	dvanced		
Coverag Enable S Aironet Diagnos Override P2P Bloc Client E: Maximu Clients Static IF Wi-Fi Dir Policy Maximu	tic Channel Interface ACL king Action colusion 3 n Allowed Tunneling 11 ect Clients n Allowed fer AP Radio stSpot ation	1800	d on Timeout (secs) d d e V f 60 Timeout Valu	IPv6	None 💌

1

Step 2 Set AP Mode to **FlexConnect.**

All APs > Details for AP_3500E

General 👔	Credentia	als In	terfaces	High Availabilit
eneral				
AP Name		AP_3500	E	
Location				
AP MAC A	ddress	o4:7d:4f	:3a:07:74	
Base Radi	o MAC	o4:7d:4f	:53:24:e0	
Admin Sta	tus	Enable	*	
AP Mode		FlexCon	nect 🔽	
AP Sub Me	ode	local FlexCon	nect	-
Operation	al Status	monitor	and the state of the	
Port Numb	er	Rogue D Sniffer	etector	
Venue Gro	pup	Bridge SE-Coni	nect	~

Step 3 Associate WGB with wired clients behind this configured WLAN.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEOBACK				
Clients											
Current Filter	None	Change Filter] [Clear Filter]								
Client MAC Addr	AD No.										
Chent MAL AGOF	AP Name		WLAN	Profile	WLAN SSID		Protocol	Status	Auth	Fort	WGB
00:40:95-58:d4-be			WLAN "Store		WLAN SSID "Store 1"		Protocol N/A	Status Associated	Auth Yes	Fort 1	WG8 No
				÷ 1'							

Step 4

In order to check the details for WGB, go to Monitor > Clients, and select WGB from the list of clients.

Clients > Detail				
lient Properties		AP Pro	operties	
MAC Address	o4:7d:4f:3a:08:10	AP A	Address	o4:7d:4f:53:24:e0
IPv4 Address	9.6.63.102	AP N	lame	AP_3500E
IPv6 Address		AP T	ype	802.11an
		WLA	N Profile	'Store 1'
		Data	Switching	Local
		Auth	entication	Central
		Statu	us	Associated
		Asso	ciation ID	1
		802.:	11 Authentication	Open System
		Reas	son Code	1
		Statu	us Code	0
Client Type	WGB		ollable	Not Implemented
Number of Wired Cli	ent(s) 2	CF P	oll Request	Not Implemented

Step 5 In order to check the details of the wired/wireless clients behind WGB, go to **Monitor > Clients**, and select the client.

ient Properties		AP Properties	
MAC Address	00:50:b6:09:e5:3b	AP Address	o4:7d:4f:53:24:el
IPv4 Address	9.6.63.100	AP Name	AP_3500E
IPv6 Address		AP Type	802.11a
		WLAN Profile	'Store 1'
		Data Switching	Local
		Authentication	Central
		Status	Associated
		Association ID	0
		802.11 Authenticatio	on Open System
		Reason Code	1
		Status Code	0
Client Type	WGB Client	CF Pollable	Not Implemented
WGB MAC Address	o4:7d:4f:3a:08:10	CF Poll Request	Not Implemented

Clients > Detail

ſ

Limitations

- Wired clients behind WGB will always be on the same VLAN as WGN itself. Multiple VLAN support for clients behind WGB is not supported on Flex AP for WLANs configured for Local Switching.
- A maximum of 20 clients (wired/wireless) are supported behind WGB when associated to Flex AP on WLAN configured for local switching. This number is the same as what we have today for WGB support on Local mode AP.
- Web Auth is not supported for clients behind WGB associated on WLANs configured for local switching.

Support for an Increased Number of Radius Servers

Prior to release 7.4, the configuration of RADIUS servers at the FlexConnect group was done from a global list of RADIUS servers on the controller. The maximum number of RADIUS servers, which can be configured in this global list, is 17. With an increasing number of branch offices, it is a requirement to be able to configure a RADIUS server per branch site. In release 7.4 onwards, it will be possible to configure Primary and Backup RADIUS servers per FlexConnect group which may or may not be part of the global list of 17 RADIUS authentication servers configured on the controller.

An AP specific configuration for the RADIUS servers will also be supported. The AP specific configuration will have greater priority than the FlexConnect group configuration.

The existing configuration command at the FlexConnect Group, which needs the index of the RADIUS server in the global RADIUS server list on the controller, will be deprecated and replaced with a configuration command, which configures a RADIUS server at the Flexconnect Group using the IP address of the server and shared secret.

Summary

- Support for configuration of Primary and Backup RADIUS servers per FlexConnect group, which may or may not be present in the global list of RADIUS authentication servers.
- The maximum number of unique RADIUS servers that can be added on a WLC is the number of FlexConnect groups that can be configured on a given platform times two. An example is one primary and one secondary RADIUS server per FlexConnect group.
- Software upgrade from a previous release to release 7.4 will not cause any RADIUS configuration loss.
- The deletion of the primary RADIUS server is allowed without having to deleting the secondary RADIUS server. This is consistent with the present FlexConnect group configuration for the RADIUS server.

Procedure

Step 1 Mode of configuration prior to release 7.4.

A maximum of 17 RADIUS servers can be configured under the AAA Authentication configuration.

I

CISCO	MONETON			WRELESS ST	and the second second	GEMENT COMMAND	IS HELP PERCHAN		
Security	RADIUS	5 Authenticat	tion Serv	ers					Apply New-
AAA General - RADDUS Authentication		atien 30 Type ⁴ S Ray Way		NAC Address	d requires a key	who compliant RADI2/5	aarver)		
Adducting	MAC D	winnter	Hyphet	(8)					
TAEACS+ LOAP Local Ret Linese	Natwork	Hanaperson	Server Index	Server Address	Part	1PBec	Advis Status		
MAC Fibeling	M		1	1234	1812	Disabled	Emailded		
Disabled Olerts	10	8	2	1.2.3.4	2	Disabled	Enabled		
User Lagre Polonis AP Polonis	H.	6	3	1.2.2.4		Disabled	Enabled		
Personal Policies	10	68	4	1.2.3.4	4	Disabled	Evabled	•	
Local EAP	H	-	5	1.2.3.4	8	Disabled	Enabled		
	H	8	6	1.2.3.4	6	Disabled	Evabled		
Priority Order	H	95	1	1.2.3.4	7	Disabled	Enabled		
Certificate	M	ef		1234		Disabled	Enabled		
Access Centrel Lists	66	ef -		1.3.3.4	*	Disabled	Enabled		
Wireless Protection	M		22	1234	10	Disabled	Enabled		
Policies	10		22	1.2.3.4	11	Disabled	Enabled		
Web Auth		8	.12	5.2.3.4	12	Disabled	Enabled		
Trustlec SXP	6		13	1.2.3.4	13	Disabled	Enabled		
Advanced	8	6	16	1.2.3.4	14	Disabled	Enabled	•	
	- 61	*	.13	1.2.3.4	18	Disabled	Evabled		
	H		10	1.2.3.4	36	Disabled	Enabled		
	18	a	12	1.2.3.4	17	Disabled	Enabled		

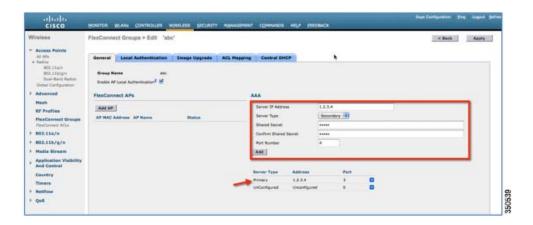
Step 2 Primary and Secondary RADIUS servers can be associated with a FlexConnect Group using a drop-down list comprising of RADIUS servers configured on the AAA Authentication page.

Vireless	FlexConnect Groups > Edit 'abc'			e Back Apply
Access Prints All Ab Sallas BEL1310 BEL1310ph Ubbel Configuration Advanced Mesh Bis/Context Groups PiecContext Groups Disclosed Gold B01.110/0 B01.110/0/11 Media Stream	General Least Authentication Inage Upgrade Group Name sic PiesConnect APs Add Am Alf MAC Address AP Name Blates	AAA VLAN-ACL mapping WLAN-ACL ma AAA AAA Ahmer Radus Sovie Societien Radus Sovie Societien Radus Sovie Societien Radus Sovie	(P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)12 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P (P1234.5m)2 (P) (P (P1234.5m)2 (P)	
Country Timers QoS			P1.3.2.3, Prot.5 P1.2.2.4, Prot.5 P1.3.2.4, Prot.5 P1.3.3.4, P1.5 P1.3.3.4, P1.5 P1.3.5 P1.5 P1.5 P1.5 P1.5 P1.5 P1.5 P1.5 P1	

Step 3 Mode of configuration at FlexConnect Group in release 7.4.

ſ

Primary and Secondary RADIUS servers can be configured under the FlexConnect Group using an IP address, port number and Shared Secret.



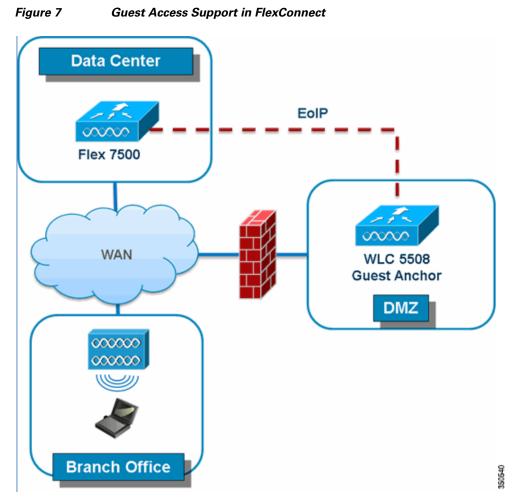
Limitations

- Software downgrade from release 7.4 to a previous release will retain the configuration but with some limitations.
- Configuring a primary/secondary RADIUS server when a previous one is configured will cause the older entry to be replaced by the new one.

Enhanced Local Mode (ELM)

ELM is supported on the FlexConnect solution. Refer to the best practices guide on ELM for more information.

Guest Access Support in FlexConnect



FlexConnect WLC will allow and continue to support creation of EoIP tunnel to your guest anchor controller in DMZ. For best practices on the wireless guest access solution, refer to the Guest Deployment Guide.

Support for PEAP and EAP-TLS Authentication

FlexConnect AP can be configured as a RADIUS server for LEAP and EAP-FAST client authentication. In standalone mode and also when local authentication feature is enabled on the WLANs, FlexConnect AP will do dot1x authentication on the AP itself using the local radius. With controller release 7.5, PEAP and EAP-TLS EAP methods are also supported.

EAP-TLS

Certificate Generation for EAP-TLS

The following steps are needed on the WLC and the client in order to authenticate the client to the FlexConnect AP using EAP-TLS authentication.

On WLC:

- **1**. Generate device certificate for the WLC.
- 2. Get device certificate signed by CA server.
- **3**. Generate CA certificate from the CA server.
- 4. Import device and CA certificate into the WLC in .pem format.

On Client:

- **1**. Generate client certificate.
- 2. Get client certificate signed by CA server.
- **3**. Generate CA certificate from the CA server.
- 4. Install client and CA certificate on the client.

Detailed steps on how to accomplish the above steps are listed in Document-100590 (http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008093f1b9.sh tml)

igure 8	Document 100590	
Products & Services Local EAP Au Configuration		s LAN Controller with EAP-FAST and LDAP Server
Document ID: 100590		
Generate a Device C Downloading the De- linstall the Root Certi Generate the Root Certi Configure LOAP Serve Creating Users on th Configure the User (Using LDP to Identify t Configure the User (Using LDP to Identify t Configure the User (Verify Yroubjeshoot	Local EAD Authentication Method on the WLC refificate for the WLC ficate of PKI into the WLC ficate of PKI into the WLC certificate for the Client on the WLC e e for the WLC f e Domain Controller or LDAP Access he User Attributes	

Configuration of EAP-TLS on FlexConnect AP

1. Create WLAN for Local Switching and Local Authentication.

In the example below, two WLANs have been created, one for EAP-TLS and the other for PEAP authentication.

I

1

/LANs	WLANs	NS CONTROLLER WIRELE	SS SECURITY MANAGEMENT COMI	MANDS HELP	FEEDBACK	
LANS	WLANS					
WLANS WLANS	Current Filter:	None (Change Filter)	[Clear_Filter]		Create New Go	1
Advanced	WLAN ID TY	pe Profile Name	WLAN SSID	Admin Status	Security Policies	
	Di W	LAN enley	enjoy	Enabled	[WPA21(Auth/802.1X1]	
	D 4 W	LAN ciscowic-peap	ciscowic-peap	Enabled	[WPA2][Auth(802.1X)]	0
	0 5 W	LAN ciscowic-eaptis	ciscowic-eaptis	Enabled	[WPA2][Auth(802.1X)]	

Figure 9 WLAN Configuration for PEAP and EAP-TLS

2. Enable FlexConnect Local Switching and FlexConnect Local Auth

/LANs	WLANs > Edit 'ciscowic	-peap*			
WLANs WLANs Advanced	General Security (Scan Defer Priority Scan Defer Time(msecs) PlacConnect PlacConnect Local Switching ² PlacConnect Local Auth ⁴²	Policy-Mapping U 1 2 3 4 5 5 7 	Advanced	Media Session Snooping Re-anchor Roamed Voice Clients KTS based CAC Policy Radius Client Profiling DERP Profiling HTTP Profiling	Enabled Enabled Enabled Enabled
	Learn Client IP Address [#] Vian based Central Switching ^{##}	Enabled		Local Client Profiling DHCP Profiling HTTP Profiling	0
	Central DHCP Processing	Enabled		PHIP	
	Override DNS	Enabled		PHIP Mobility Type	None 1
	NAT-PAT	Enabled		PMIP Profile PMIP Realm	None 1
				mDNS mDNS Snooping	Enabled

Figure 10 WLANs for Local Switching and Local Authentication

3. Enable AP Local Authentication.

Enable the **Enable AP Local Authentication** check box on the FlexConnect groups edit page. Radius Servers on the FlexConnect group must be 'Unconfigured'. If any RADIUS servers are configured on the FlexConnect group, the AP tries to authenticate the wireless clients using the RADIUS servers first. AP Local Authentication is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

Figure 11 FlexConnect Group Configuration for AP Local Authentication

cisco	MONITOR WLANS	CONTROLLER V	RELESS SECURITY	MUNAGEMENT	CQHOW	NDS HELP	FEEDBACK			10 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -
Wireless	FlexConnect Group	ps > Edit 'ab	o"							App
Access Points At APs Radius	General Local A	luthentication	Image Upgrade	ACL Mapping	Centro	I DHCP W	IAN VLAN map;	aing		
802.13a/n/ac 802.13b/g/n Duel-Band Radice Global Configuration	Group Name Enable AP Local Auth	abc entication 8 🖬								
Advanced	FlexConnect APs					AAA				
Mesh RF Profiles	Add AP					Server IP Add	-855	(
FlexConnect Groups	AP MAC Address	AP Name	State			Server Type Shared Secret		Primary 4	9	-0
+ 802.11a/n/ac	fc:99:47:50:19:9f	AP_3600	Asso	sated		Confirm Share				-
002.11b/g/n						Port Number		1812		
Hedia Stream						Add				
Application Visibility And Control										
Country						Server Type	Address	Pert		
Timers					-	UnConfigured	Unconfigured Unconfigured	0		
Netflow						a secondaria	and a second second		-	
+ QoS										

- **4.** Selecting EAP methods will now have two more options, PEAP and EAP-TLS under the FlexConnect group with the existing LEAP and EAP-FAST options.
 - **a.** Current controller release supports downloading of EAP device and root (CA) certificates to the controller and the same is stored in PEM format on the flash.

Commands	Download file to Controller			
Download File Upload File Reboot Config Boot	File Type Certificate Password Transfer Mode Server Details	Vendor Device Certificate	Ĩ	
Reset to Factory Default Set Time Login Banner	IP Address Maximum retries Timeout (seconds) File Path File Name	10 6 / ciscowicdev.pem		3

Figure 12 Downloading Vendor Device Certificate



cisco	Monitor Wlans Controller Wireless Security Management Commands Help Feedback
Commands Download File Upload File Reboot Config Boot	Download file to Controller
 Scheduled Reboot Reset to Factory Default Set Time 	IP Address Maximum retries 10 Timeout (seconds) 6 File Path /
Login Banner	File Name: discowicca.pem

- **b.** With release 7.5, these certificates will be used for authenticating clients using EAP-TLS. Both the device and root certificates will be downloaded to all the FlexConnect APs in the FlexConnect group if the EAP-TLS method is enabled, and the same is used at the AP to authenticate the clients.
- **c.** When a new AP joins the group, certificates will be pushed to the AP along with other configurations. The user has to download the EAP device and Root certificates to controller prior to enabling EAP-TLS on the FlexConnect group.
- **d.** Upon receiving a certificate message from the controller, the AP will import these certificates, store them in memory and use them for authenticating clients.
- e. EAP TLS Certificate Download option is provided to push any updated certificates to the AP.

eneral Local Authen	tication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping
Local Users Protoco	Is				
EAP Fast					
Enable EAP Fast Authentication ² Server Key (in hex)	Enabl	e Auto key generation		-	
	_			(Confirm server key)	
Authority ID (in hex)		636f000000000000000000		(commissive key)	
Authority Info	Cisco A	_ID		1	
PAC Timeout (2 to 4095 days)					
PEAP					
Enable PEAP Authentication ²	V				
EAP TLS					

Figure 14 Enabling PEAP and EAP TLS on AP Local Authentication under FlexConnect Group

Certificate Files on AP

Four files are downloaded to the AP, when EAP-TLS is enabled.

- eapdev.pem.ca This is the CA (root) certificate.
- eapdev.pem.crt –This is the public certificate of the device.
- eapdev.pem.prv This is the RSA private key of the device.
- eapdevpwd This is the password file to protect the private key.

Figure 15 Files Stored in the Flash on AP

2	-rwx	65056	Feb	28	2013	15:48:41	+88:08	event.log
3	drwx	64	Feb	26	2013	04:04:36	+00:00	configs
7	-rwx	1513	Feb	28	2013	18:37:11	+00:00	eapdev.pem.ca
54	-rwx	1704	Feb	28	2013	18:37:11	+00:00	eapdev.pem.crt
56	-rwx	963	Feb	28	2013	18:37:11	+00:00	eapdev.pem.prv
61	-rwx		Feb	28	2013	18:37:11	+88:88	eapdevpwd

Client Configuration

ſ

Configure the wireless profile for EAP-TLS by selecting EAP Type **EAP-TLS** and specifying the Trusted Root certificate Authorities and the client certificate.

Figure 16 Wireless Profile for EAP-TLS

WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	EAP-TLS	~
O WPA/WPA2 Passphrase			
O 802.1x	802.1x EAP Type:	EAP-TLS	15
O Pre-Shared Key (Static WEP)			
O None			
Configure	Allow Association to Mixed Co	ela	
	Limit Time for Finding Domain	Controller To:	o sec
Group Policy Delay	60 🗢 sec		

I

Figure 17 Validate Server Identity

Configure EAP-TLS	? 🛛
Use Machine Information for Domain Logon	
Validate Server Identity Trusted Root Certification Authorities sskcert Select a Certificate Administrator [Issued by: sskcert 11/22/2012]	~
Server/Domain Name	
Always Do User Authentication	OK Cancel

Once the client is connected, Server Based Authentication will reflect EAP-TLS.

on Options	Help		
	Profile Management	Diagnostics	
CISCO SYSTE			
ահրուսի	Profile Name:	ciscowlc-eaptls	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 48
Server	Based Authentication	EAP-TLS	Data Encryption: AES
_	IP Address:	9.5.56.102	
	Signal Strength:		Excellent
			Advanced

Figure 18 Client Authentication using EAP-TLS

Client Certificates

Γ

I

The Trusted Root and Client Certificates can be viewed as follows (These are the certificates as generated earlier)

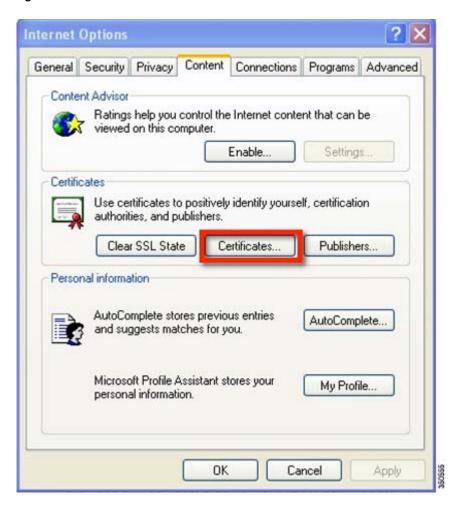


Figure 19 Certificates on Client

Issued To	Issued By	Expiratio	Friendly Name	^
SecureSign RootCA1	SecureSign RootCA1	9/15/2020	Japan Certificati	17
SecureSign RootCA2		9/15/2020	Japan Certificati	
SecureSign RootCA3	SecureSign RootCA3	9/15/2020	Japan Certificati	
SERVICIOS DE CER	SERVICIOS DE CERTI	3/10/2009	SERVICIOS DE C	
SIA Secure Client CA	SIA Secure Client CA	7/9/2019	Societa Interban	
STA Secure Server CA	STA Secure Server CA	7/9/2019	Societa Interhan	12
Esskcert	sskcert	4/5/2017	<none></none>	
Swisskey Root CA		1/1/2016	Swisskey Root CA	1.
TC TrustCenter Cla	TC TrustCenter Class	1/1/2011	TC TrustCenter	~
Export	Remove		Advanc	ced
stificate intended summer				
tificate intended purpose	5			

Figure 20 Trusted Root (CA) Certificate on Client

I

Γ

ided purpose:	<all></all>			_	1994)	-
sonal Other Pe	ople Interr	mediate Certifica	tion Authorities	Truste	ed Root Certifi	cation 4
Issued To		sued By	Expiratio	D	Friendly Name	-
Administrator	ssi	cert	11/22/20	013 -	<none></none>	
nport E	xport]	Remove]		A	dvanced.
nport E		Remove]		A	dvanced.
tificate intended	purposes	Remove) hentication		A	dvanced.

Figure 21 Trusted Client Certificate

Show Commands

The EAP type of the client will be reflected on the WLC and can be seen in the output of **show client detail**

IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
Layer2 ACL Name	
Layer2 ACL Applied Status. The	Unavailable
Client Type	
mDNS Status	Disabled
mDNS Profile Name	none
No. of mDNS Services Advertised	Θ
Policy Type	WPA2 6 Downloads
Authentication Key Management	802.1x
Encryption Cipher	CCMP (AES)
Protected Management Frame	
Management Frame Protection	No
ЕАР Туре	EAP-TLS
r Lexconnect Data Switching	
FlexConnect Dhcp Status	
FlexConnect Vlan Based Central Switching	
FlexConnect Authentication	
Quarantine VLAN	0 56
Access VLAN	56

Figure 22 EAP Type for Client Authenticated using EAP-TLS

EAP-PEAP

PEAP (EAP-MSCHAPv2 and EAP-GTC) EAP Type is supported with release 7.5 and Users need to be added on the WLC as shown below. A maximum of 100 users can be added per FlexConnect group.

User Creation

ſ

eral Loc	al Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping		
cal Users	Protocols						
No of Users	1			Add User			
ser Name				Upload CSV file			
				File Name			Browse
				UserName			
				Password Confirm Password	d	_	
						Add	
Remove /	All Users						

Figure 23 User Addition for Local Authentication

Client Configuration

Selecting EAP Type EAP-MSCHAPv2 or GTC can configure the wireless profile for EAP-PEAP.

1

eral Security Advanced			-
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type	PEAP (EAP-MSCHAP V2)	~
WPA/WPA2 Passphrase 802.1x	802 1x EAP Type:	PEAP (EAP MSCHAP V2)	141
Pre-Shared Key (Static WEP) None			
Configue	Allow Association to Moved Co Profile Locked Limit Time for Finding Domain	-	1
Group Policy Delay:	60 🗢 sec		

Figure 24 Wireless Profile for EAP-PEAP (EAP-MSCHAPv2)

Users created on the controller need to be configured on the client.

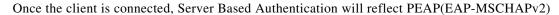
ifigure PEAP (EAP-MSCI	
Use Machine Information fo	r Domain Logon
Validate Server Identity	
rusted Floot Certification Auth	orities
(Any>	
When connecting, use:	
O Certificate	
User Name and Password	—
Use Windows User Name User Information for PEAP (I	and Password EAP-MSCHAP V2) Authentication
User Name:	Approxition of the second seco
Password:	••••••
Confirm Password:	••••••
Ad	vanced OK Cancel

Figure 25 User Name and Password for PEAP

Γ

Options Help			
ent Status Profile Manageme	ent Diagnostics		
aitel		<u>^</u> (New
spittunnel blizzard		(Modify
eniov			Remove
ciscowlc-peap ciscowlc-eaptls		~ (Activate
etals			
Network Type:	Infrastructure	(Import
Security Mode: Network Name 1 (SSID1):	Disabled splittunnel	(Export
Network Name 2 (SSID2)	<empty></empty>	i i	Scan
Network Name 3 (SSID3):	<empty></empty>		
Auto Select Profiles			Order Profiles

Figure 26 Cisco Aironet Desktop Utility Profile Management



1

Figure 27 Client Authentication using PEAP(EAP-MSCHAPv2)

	Profile Management	Diagnostics	
ISCO SYSTE		ciscowlc-peap	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 48
Server	Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES
_	IP Address:	9.5.56.102	
	Signal Strength:		Excellent

Once the client is authenticated, the EAP Type can be seen under the Client Detail page.

cisco		s CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
Summary Access Points Cisco CleanAir Statistics	Clients > Detai	C Statistics						
	Security Infor	mation						
CDP Rogues Redundancy Clients Sleeping Clients Multicast Applications	Security Policy Completed Policy Type Auth Key Mgmt Encryption Cipl EAP Type SNMP NAC Stat Radius NAC Stat Radius NAC Stat CTS Security G AAA Override A Acoverride Status	er CCMP (A PEAP e Access te RUN oup Tag Not Appl CL Name none	ES) icable					
	Applied Status AAA Override F	ex ACL none						
	AAA Override F Applied Status	ex ACL Unavaila	ble					
	Redirect URL	none						

Figure 28 Web GUI Client Details

Show Commands

ſ

The EAP type of the client will be reflected on the WLC and can be seen in the output of **show client detail**

IPv6 ACL Applied Status.	Unavailable
ayer2 ACL Name	
ayer2 ACL Applied Status	
Client Type	
nDNS Status	Disabled
nDNS Profile Name	
No. of mDNS Services Advertised	
Policy Type	WPA2
Authentication Key Management	802.1x
Encryption Cipher	
Protected Management Frame	No
Management Frame Protection	No
EAP Type	PEAP
rexconnect bata switching	
FlexConnect Dhcp Status	
FlexConnect Vlan Based Central Switching	
ElexConnect Authentication	Local
Quarantine VLAN	Θ
ccess VLAN	56

Figure 29 EAP Type of Client Authenticated using PEAP

CLI Support for PEAP and EAP-TLS on FlexConnect APs

Two new CLIs have been added to configure PEAP and EAP-TLS from the controller.

config flexconnect	group	<groupname></groupname>	radius	ap	peap	<enable th="" <=""><th>disable></th></enable>	disable>
config flexconnect	group	<groupname></groupname>	radius	ap	eap-tls	<enable td="" <=""><td>disable></td></enable>	disable>

A CLI for certificate download has been added as well.

config flexconnect group <groupName> radius ap eap-cert download



Configurations at the AP can be seen from the console.

Figure 30 CLI Commands on AP Console



The following commands can be used to troubleshoot this feature:

```
debug eap all
debug aaa authentication
debug dot11 aaa authenticator all
debug aaa api
debug aaa subsys
debug dot11 aaa dispatcher
debug aaa protocol local
debug radius
debug aaa dead-criteria transaction
```

Guidelines

- FlexConnect AP should be in standalone mode or configured for Local authentication.
- Certificates must be present on the AP for EAP-TLS to work.

WLAN-VLAN mapping at FlexConnect Group Level

Prior to release 7.5, WLAN to VLAN mapping was done on a per AP basis.

With increasing number of APs in a deployment, there is a need to provide the capability of adding WLAN to VLAN maps from the FlexConnect group. This will be supported in release 7.5.

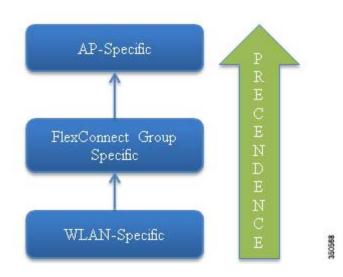
This will push the WLAN to VLAN mapping to all the APs present in the FlexConnect group. The FlexConnect level configuration will have a higher precedence compared to the WLAN-VLAN mapping configured on the WLAN.

WLAN-VLAN Mapping Inheritance

- WLAN level WLAN-VLAN mapping has the lowest precedence.
- Higher precedence mapping will override the mapping of lower precedence
- AP level WLAN-VLAN mapping has the highest precedence
- On deletion of a higher precedence mapping, the next highest precedence mapping will take effect.

The following figure depicts the order of precedence as it refers to WLAN-VLAN mapping at the WLAN, FlexConnect group and at the AP.

Figure 31 Flow of Inheritance



GUI Configuration

ſ

1. Create WLAN for Local Switching

Figure 32 WLAN for Local Switching

uluilu cisco VLANs	MONITOR WLANs	WLANS O	ONTROLLER WIRELESS	SECURITY MANAGEMENT CC	MMANDS HELP	FEEDBACK	
WLANS WLANS	Current Filter	n None	(Change Filter) (C	sar.Filter]		Create New Co	
Advanced	WLAN ID	Туре	Profile Name	WLAN SSID	Admin Status	Security Policies	
	0.4	WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]	0
	01	WLAN	ciscowic-peap	ciscowic-peap	Enabled	[WPA2][Auth(802.1X)]	
	0 5	WLAN	ciscowic-eaptis	ciscowic-eaptls	Enabled	[WPA2][Auth(802.1X)]	

1



General Security	QoS Policy-Mapping	Advanced	Passive Citeric	
Off Channel Scanning Defer			Passive Client	0
Scan Defer Priority	01234567		Voice	_
			Media Session Snooping	Enabled
Scan Defer Time(msecs)	100		Re-anchor Roamed Voice Clients	Enabled
lexConnect			KTS based CAC Policy	Enabled
FlexConnect Local	Enabled		Radius Client Profiling	
Switching 2			DHCP Profiling	
FlexConnect Local Auth	Enabled		HTTP Profiling	
Learn Client IP Address	Enabled		Local Client Profiling	
Vian based Central Switching	Enabled		DHCP Profiling	
Central DHCP Processing	Enabled		HTTP Profiling	
Override DNS	Enabled		PMIP	
NAT-PAT	Enabled		PMIP Mobility Type	None
1011-1111			PMIP Profile	None 🔹

The WLAN is mapped to the management VLAN 56.

eneral	Security	QoS	Policy-Mapping	Advanced			
Profile Na	ame	enjoy					
Туре		WLAN					
SSID		enjoy					
Status		🗹 Enat	bled				
Security Policies		[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)					
Radio Po	licy	All	:				
Interface Group(G	e/Interface)	manag	ement 🔹				
Multicast	Vian Feature	Enabled					
Broadcas	st SSID	Senabled					
NAS-ID		Aparajit	ta_Primary_5500				

Figure 34 WLAN Mapped to VLAN 56 Management Interface



P Name	AP_3600			
ase Radio MAC	34:a8:4e:e7:5b:c0			
Make AP Specifi	c 🗘 Go			
WLAN Id SSID		VLAN ID		Inheritance
				Inheritance Wlan-specifi
Id SSID		ID	NAT-PAT	

When a client connects to this WLAN, it will get an IP in VLAN 56.

ſ

Figure 36

Cisco Aironet Desktop Utility	y - Current Profile: enjoy		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	enjoy		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 108	
Server Based Authentication:	LEAP	Data Encryption: AES	
IP Address:	9.5.56.102		
Signal Strength:		Excellent	
		Advanced	

Client in VLAN 56

2. Create WLAN-VLAN mapping under FlexConnect Groups. This capability is the new feature in release 7.5.

1

Figure 37 WLAN Mapped to VLAN 57 under FlexConnect Group

	Local Authentication	n Image Upgrade	ACL Mapping Central DHC	P WLAN VLAN mapping
	AN Mapping			
WLAN Id				
Vlan Id	1 Add			
LAN Id	WLAN Profile Name	Vian 57	1.	
-				

WLAN-VLAN mappings can be viewed per AP from the VLAN Mappings page

eneral Credential	s Interfa	ices	High Availability	Inventory	FlexConnect	Advanced
VLAN Support		Ø				
Native VLAN ID	56		VLAN Mappings			
FlexConnect Group Name	2	abc				
eAuthentication Access	Control Lists					
External WebAuthentication Local Solit ACLs Central DHCP Processing						
External WebAuthentication		-				
External WebAuthentication						

Figure 38 VLAN Mappings at AP

In this example, the WLAN is mapped to VLAN 57 on the FlexConnect Group, since the Group-specific mappings take precedence over WLAN-specific mappings.

Figure 39 WLAN 1 Mapped to VLAN 57 as Per Group-Specific Configuration Inheritance

P Nam	8	AP_3600			
Base Ra	dio MAC	34:a8:4e:e7:5b:c0			
C					
Make WLAN Id	AP Specific SSID	Go	VLAN ID	NAT-PAT	Inheritance
WLAN	I	Go		NAT-PAT	Inheritance Group-speci
WLAN	SSID		ID		

The client is assigned an IP address in VLAN 57.

ſ

Figure 40

Cisco Airone	et Desktop Utility	y - Current Profile: enjoy	? 🛛
Action Options	Help		
Current Status	Profile Management	Diagnostics	
CISCO SYSTEM			
ահրուսիր	Profile Name:	enjoy	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 108
Server B.	ased Authentication:	LEAP 9.5.57.100	Data Encryption: AES
	Signal Strength:		
			Advanced

Client in VLAN 57

3. To create a WLAN-VLAN mapping at the AP, select Make AP Specific under VLAN Mappings.

1

Once this is done, the WLAN is mapped to VLAN 58 since AP-specific mappings take precedence over Group-specific and WLAN-specific mappings.

Figure 41 WLAN Mapped to VLAN 58 as Per AP-Specific Mapping Inheritance

AP	Name		AP_3600			
Ba	se Radi	io MAC	34:a8:4e:e7:5b:c0			
ľ	Make A	AP Specific	Go			
	Make A WLAN Id	AP Specific	Go	VLAN ID	NAT-PAT	Inheritance
	WLAN		Go		NAT-PAT	Inheritance AP-specific
	WLAN Id	SSID		ID		

The client is assigned an IP address in VLAN 58.

tion Options Help	
Current Status Profile Management Diagnostics	
CISCO SYSTEMS AUDITUM Profile Name: enjoy	
Link Status: Authenticated	Network Type: Infrastructure
Wireless Mode: 5 GHz 54 Mbps	Current Channel: 108
Server Based Authentication: LEAP	Data Encryption: AES
Signal Strength:	

Figure 42 Client in VLAN 58

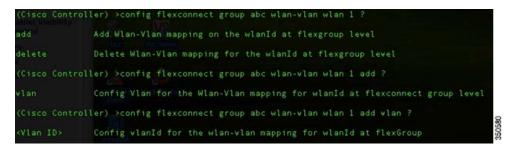
CLI Configuration

I

The following CLIs have been added as part of this feature:

- config flexconnect group <group> wlan-vlan wlan <wlan-id> add vlan <vlan-id>
- config flexconnect group <group> wlan-vlan wlan <wlan-id> delete
- config ap flexconnect vlan remove wlan <wlan_id> <ap_name>

Figure 43 WLAN-VLAN Configuration at FlexConnect Group from CLI



The command **show flexconnect group detail** can be used to see the WLAN-VLAN mapping for the FlexConnect group

(Cisco Control	ler)⇒show flexco	nnect grou	p detail ab	c			
Number of AP's	in Group: 1						
fc:99:47:60:f9	1:9f AP_3600	Joined					
Efficient AP I	mage Upgrade	Disabled					
Master-AP-Mac	Master-AP-Name			Model	Manual		
Group Radius S Type	Servers Settings: Server Address	Port					
Primary Secondary	Unconfigured Unconfigured	Unconfig Unconfig					
LEAP Auth EAP-TLS Auth EAP-TLS CERT D PEAP Auth		abled abled					
Server Key Authority ID Authority Info PAC Timeout Multicast on 0	o Generated No 430 Ci Overridden interfa	6973636f00 sco A_ID		00000000	90		
	's in Group: 1 apsond : FlexConnect Wlan	-Vlan Mapp	ing:				
VLAN ID VI	an ID						
WLAN ID 🔤 SSID			Central-Dh	ncp Dns	Override	Nat-Pat	

1

Figure 44 show flexconnect group detail Output

The command **show ap config general <AP name>** can be used to view the WLAN-VLAN mappings per AP.

Figure 45 show ap config general Output

FlexConn FlexConn Group VL AP-Speci L2Acl Co		57 (Group-Speci 56 (Wlan-Specif 56 (Wlan-Specif 56 (Wlan-Specif	ic) ic)
WLAN ID	ect Local-Split ACLs :	<pre>interference.com/or completities</pre>	TYPE
	PROFILE NAME	ACL	

The following commands can be used to troubleshoot this feature:

On WLC:

• debug flexconnect wlan-vlan <enable | disable>

On AP:

• debug capwap flexconnect wlan-vlan

Guidelines

- The WLAN should be locally switched.
- The configuration will be pushed to the AP only if the WLAN is broadcasted on that AP.

Client ACL Support

Prior to release 7.5, we support FlexConnect ACLs on the VLAN. We also support AAA override of VLANs. If a client gets an AAA override of VLAN, it is placed on the overridden VLAN and the ACL on the VLAN applies for the client. If an ACL is received from the AAA for locally switched clients, we ignore the same. With release 7.5, we address this limitation and provide support for client based ACLs for locally switched WLANs.

Client ACL Overview

- a. This feature allows application of Per-Client ACL for locally switching WLANs.
- **b.** Client ACL is returned from the AAA server on successful Client L2 Authentication/Web Auth as part of Airespace Radius Attributes.
- **c.** The controller will be used to pre-create the ACLs at the AP. When the AP receives the ACL configuration, it will create the corresponding IOS ACL. Once, AAA server provides the ACL, the client structure will be updated with this information.
- **d.** There will be configuration per FlexConnect group as well as per AP. A maximum of 16 ACLs can be created for a FlexConnect group and a maximum of 16 ACLs can be configured per-AP.
- e. In order to support fast roaming (CCKM/PMK) for the AAA overridden clients, the controller will maintain these ACL in the cache and push them to all APs which are part of the FlexConnect group.
- f. In the case of central authentication, when the controller receives the ACL from the AAA server, it will send the ACL name to the AP for the client. For locally authenticated clients, the ACL will be sent from the AP to the controller as part of CCKM/PMK cache, which will then be distributed to all APs belonging to the FlexConnect-group.
- g. Maximum of 16 Client ACLs per FlexConnect group, maximum of 16 Client ACLs per-AP
- **h.** Total of 96 ACLs can be configured on the AP (32 VLAN-ACL, 16 WLAN-ACL, 16 Split tunnel, 16 FlexConnect Client ACL, 16 AP Client ACL), each ACL with 64 rules.
- i. The ACL will be applied on the dot11 side for the client in question. This ACL will be applied in addition to the VLAN ACL, which is applied on the VLAN of the Ethernet interface of the AP.
- Client ACL applied in addition to VLAN-ACL, both can exist simultaneously and are applied serially.



Steps to Configure Client ACL

1. Create a Local Switching WLAN, which is either centrally switched or locally switched.

1

Figure 46

6 Create Local Switcl	ning WLAN
-----------------------	-----------

	WLAN ID	Туре	Profile Name	WLAN SSID	Admin Status	Security Policies	
Э.	1	WLAN	enjoy	enjoy	Enabled	[WPA2][Auth(802.1X)]	
D.	2	WLAN	ciscowlc	ciscowic	Enabled	[WPA2][Auth(802.1X)]	
3	4	WLAN	ciscowlc-peap	ciscowlc-peap	Enabled	[WPA2][Auth(802.1X)]	
Э.	s	WLAN	ciscowlc-eaptls	ciscowlc-eaptls	Enabled	[WPA2][Auth(802.1X)]	

2. Turn on AAA override for the WLAN

Enable AAA override

WLANs > Edit 'ciscowl	c'	
General Security	QoS Policy-Mapping Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout	1800 Session Timeout (secs)	DHCP Addr. Assignment 🛛 🖂 Required
Aironet IE	Enabled	OEAP
Diagnostic Channel	Enabled	Split Tunnel Enabled
Override Interface ACL	IPv4 None IPv6 None IPv6	
P2P Blocking Action	Disabled	Management Frame Protection (MFP)
Client Exclusion 2	Enabled 60 Timeout Value (secs)	MFP Client Protection 1 Optional
Maximum Allowed Clients	0	DTIM Period (in beacon intervals)
Static IP Tunneling	Enabled	802.11a/n (1 - 255) 1
Wi-Fi Direct Clients Policy	Disabled 🔹	802.11b/g/n (1 - 255) 1
Maximum Allowed Clients Per AP Radio	200	NAC State None C
Clear HotSpot	Enabled	Load Balancino and Band Select

3. Create a FlexConnect ACL

FlexConnect ACL can be configured from the Security page as well as from the Wireless page.

ululu cisco MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANOS HELP EEEDBACK Wireless FlexConnect Access Control Lists Access Points All APs Radios Acl Name 802.11a/n/ac 802.11b/g/n Dual-Band Radio **Global Configuration** Advanced Mesh **RF** Profiles Fle 802.11a/n/ac ¥. 802.11b/g/n Media Stream 350587 Application Visibility And Control k

Figure 47 Configure FlexConnect ACL

4. Assign the FlexConnect ACL to the FlexConnect group or to the AP

Figure 48 ACL Mapping on FlexConnect Group

Γ

Xoonno	ct Groups > Edit	'abc'				
ieneral	Local Authentica	ation Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping	
AAA VLA	N-ACL mapping	WLAN-ACL mapping	Policies			
Policies						
Policy /	ACL ad					
	Add					
Policy A	ccess Control Lists					
aci						

AP Name	AP_3600	
Base Radio MAC	34:a8:4e:e7:5b:c0	
WLAN ACL Map	bing	
WLAN Id 0		
WebAuth ACL	d 🔹	
10		
10	Add	
-	ld	
-	AN Profile Name WebAuth ACL	
WLAN Id WL		
wLAN Id WL Policies	AN Profile Name WebAuth ACL	
WLAN Id WL	AN Profile Name WebAuth ACL	
WLAN Id WL Policies Policy ACL acl	AN Profile Name WebAuth ACL	
WLAN Id WL Policies Policy ACL acl	AN Profile Name WebAuth ACL	

1

Figure 49 ACL Mapping on AP

- **5.** Configure the Airespace attribute on the Radius/Cisco ACS server/ISE.
- Figure 50 Aire-Acl-Name on Cisco ACS Server

abab	User Setup	×
CISCO	o Halp	-
User Setup	[14179\004] Aire-802.1P-Tag	_
Group Setup	O O	
Shared Profile Components	Password Authentication Group to which the user is assigned	
Network Configuration	[14179/006] Aire-Acl-Name Callback Client IP Address Assignment	
Sustem Configuration	[14179/007] Aire-Data-Bandwidth-Average- Network Access Restrictions	
Configuration	Contract Max Sessions	
Administration Control	Contract Account Disable Account Disable Downloadable ACLs	
Databases	0 Advanced TACACS+ Settings 0 TACACS+ Enable Control	
Validation	[14179\009] Aire-Data-Bandwidth-Burst-Contract TACACS+ Enable Password TACACS+ Outbound Password TACACS+ Outbound Password	
Network Access Profiles	U VACACS+ Shell Command Authorization (14179\010] Aire-Real-Time-Bandwidth-Burst- Command Authorization for Network Device Management	
Reports and Activity	Contract Applications • TACACS+ Unknown Services	
Documentation	ITTE RADIUS Attributes ITTE RADIUS Attributes RADIUS Vendor Specific Attributes	
	Time Bound Alternate Group	
	Submit Delete Cancel	-

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 💌	ministration •
Authentication O Authorization	🔇 Profiling 🕐 Posture 👵 Client Provisioning 📄 Security Group Access 🔒 Policy Elements
Dictionaries Conditions Results	
	MACSec Policy NEAT Web Authentication (Local Web Auth)
* Authorization	✓ Airespace ACL Name acl
Authorization Profiles Downloadable ACLs	CT APPLICATION
Inline Posture Node Profiles	 Advanced Attributes Settings
Profiling Posture	Radius:Tunnel-Private-Group-ID 📀 = atish-9 📀 Tog ID 2
Client Provisioning	
 Security Group Access 	Attributes Details

Figure 51 Airespace ACL Name on ISE

6. Authenticate the client.

🖻 Cisco Aironet Desktop Utilit	y - Current Profile: ciscowlc		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
ulliuIlliu Profile Name:	ciscowlc		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 157	
Server Based Authentication:	PEAP (EAP-MSCHAP V2)	Data Encryption: AES	
IP Address:	9.5.56.102		
Signal Strength:		Excellent	
		Advanced	

CLI Configuration

ſ

Figure 52

The Client ACL can be seen on the AP using the commands **show access-list** and **show controllers dot11Radio**

AP_3600#show access-lists Extended IP access list acl 10 deny icmp any any (10 matches) 20 permit ip any any (328 matches) AP_3600#

show access-lists Output

150583

Figure 53	Client ACL on AP
Clients 8 AID 7cd1.c386.7edc 8848.9658.d45e	lers dotl1Radio 1 b -Cli AN Status:S/I/8/A Age TxQ-R(A) Mode Enc Key Rate Mask Tx Rx BVI Split-ACL Client-ACL L2-ACL 5 3A 44294 eee IFE 3ee e-e (8) 338e 6ee 1-16 eeFFFFFFF 6217 GeC 2 36 44244 eee IFE 3ee e-e (8) 8188 20e e-10 eeFF68086e ee6e 66e 1) MaxFri Deffunifri Deffuitfri Wiredfrot
7cd1.c386.7edc	3
0040,96b8.d4be	δ (1) 1 (1) (1) (1) (1) (1) (1) (1) (1) (
Åg	xLt PkL MaxL AC counts
7cd1.c386.7edc 10	8 65468 8 (8,8) 8 (8,8) 8 (8,8) 8 (8,8) 8 (8,8)
0040.96b8.d4be 10	= 65468 = 6 (9, 8) = (9, 8) = (9, 8) = (9, 8) = (9, 8) = 9 = 6 (9, 9) = (9, 8) = (9, 8) = (9, 8) kts KBytes Dup Dec Mic T×Pkts KBytes Retry RSSISHR = 25 55 55 55 55 55 55 55 55 55 55 55 55
	kts KBytes Dup Dec Mic TxPkts KBytes Retry RSSI SNR
7cd1.c386.7edc	159 12 28 9 9 64 2 6 38 53

http://www.cisco.com/en/US/products/ps11635/products_tech_note09186a0080b7f141.shtml

Guidelines

- Prior to AAA sending the client ACL, the ACL should be pre-created on the group or AP. The ACL will not be dynamically downloaded to the AP at the time of client join.
- A maximum of 96 ACLs can be configured on the AP.
- Each ACL will have a maximum of 64 rules.
- If client is already authenticated, and ACL name is changed on the radius, then client will have to do a full authentication again to get the correct client ACL.
- Since ACL not saved in cache at the controller, if the AP reboots/crashes, its cache will not be updated and the client will have to do full authentication for correct client ACL to be applied.
- If an ACL is returned from the AAA server but the corresponding ACL is not present on the AP, the client will be de-authenticated. A log message will be generated at the AP and WLC console.

On AP:

```
*Mar 4 09:20:43.255: %LWAPP-3-CLIENT_ACL_ENTRY_NOT_EXIST: Deleting Mobile for 0040.96b8.d4be: CLIENT ACL not exist on AP
```

On WLC:

```
*spamApTask7: Mar 04 14:51:03.989: #HREAP-3-CLIENT_ACL_ENTRY_NOT_EXIST:
spam_lrad.c:36670 The client 00:40:96:b8:d4:be could not join AP : 34:a8:4e:e7:5b:c0 for
slot 1, Reason: acl returned from RADIUS/local policy not present at AP
```

I

The various scenarios are listed in the table below:

ACL present on AP	ACL returned from AAA	Behavior
No	No	N/A
No	Yes	Client will be de-authenticated
Yes	No	Normal L2 authentication.
		No ACL will be applied.
Yes	Yes	L2 Authentication with client ACL being applied.

VideoStream for FlexConnect Local Switching

Introduction

Cisco Unified Wireless Network (CUWN) release 8.0 introduces a new feature—VideoStream for Local Switching, for branch office deployments. This feature enables the wireless architecture to deploy multicast video streaming across the branches, just like it is currently possible for enterprise deployments. This feature recompenses the drawbacks that degrade the video delivery as the video streams and clients scale in a branch network. VideoStream makes video multicast to wireless clients more reliable and facilitates better usage of wireless bandwidth in the branch.

Components Used

VideoStream feature for Local Switching is available in CUWN software version 8.0. This feature is supported on all wireless LAN controllers (WLANs) and newer generation indoor access points (APs). This feature is unavailable on autonomous access points.

Supported Wireless Hardware and Software

VideoStream is supported on all the following Cisco Wireless LAN controllers:

- Cisco 5500 Controller
- Cisco 7510 Controller
- Cisco 8510 Controller
- Cisco WiSM-2 Controller
- Cisco 2504 Controller
- vWLC

IGMPv2 is the supported version on all of the controllers.

VideoStream is supported on 802.11n models of APs consisting of Cisco Aironet 1140, 1250, 1260, 1520, 1530, 1550, 1600, 2600, 3500, 3600 series APs and 802.11ac models 3700 and 2700 series APs.

Theory of Operation

Before going into details about the VideoStream feature, you should understand some of the shortfalls in Wi-Fi multicast. 802.11n is a prominently discussed wireless technology for indoor wireless deployments. Equally prominent requirement is seen in multimedia service on an enterprise and branch network, in particular, video. Multicast does not provide any MAC layer recovery on multicast and broadcast frames. Multicast and broadcast packets do not have an Acknowledgement (ACK), and all packet delivery is best effort. Multicast over wireless with 802.11a/b/g/n does not provide any mechanism for reliable transmission.

Wireless deployments are prone to interference, high channel utilization, and low SNR at the edge of the cell. There are also many clients sharing the same channel but have different channel conditions, power limitations, and client processing capabilities. Therefore, multicast is not a reliable transmission protocol to all the clients in the same channel because each client has different channel conditions.

Wireless multicast does not prioritize the video traffic even though it is marked as Differentiated Service Code Point (DSCP) by the video server. The application will see a loss of packets with no ACK, and retries to the delivery will be bad. In order to provide reliable transmissions of multicast packet, it is necessary that the network classify queues and provisions using Quality of Service (QoS). This virtually removes the issue of unreliability by eliminating dropped packets and delay of the packets to the host by marking the packets and sorting them to the appropriate queue.

Even though the 802.11n, and now 802.11ac, adaptation has gained momentum both with the network and clients, wireless multicast has not been able to use the 802.11n and 802.11ac data rates. This has also been one of the factors for an alternate mechanism for wireless multicast propagation.

VideoStream

VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP regardless if there is a client joined to a multicast group. In order to get around this limitation, the AP has to send multicast traffic to the host using Unicast forwarding, only on the WLAN that the client is joined and at the data rate the client is joined at.

VideoStream can be enabled globally on the controller. The feature can also be enabled at the WLAN level, and provides more control to the administrator to identify specific video streams for Multicast Direct functionality.

Stream Admission

As mentioned earlier, while video is an efficient, high-impact means of communication, it is also very bandwidth intensive, and as is seen, not all video content is prioritized the same. From earlier discussion it is clear that organizations investing in video cannot afford to have network bandwidth consumed without any prioritization of business-critical media.

Multicast to Unicast

By enabling 802.11n data rates and providing packet error correction, multicast-to-unicast capabilities of Cisco VideoStream enhances reliability of delivering streaming video over Wi-Fi beyond best-effort features of traditional wireless networks.

A wireless client application subscribes to an IP multicast stream by sending an IGMP join message. With reliable multicast, this request is snooped by the infrastructure, which collects data from the IGMP messages. The AP checks the stream subscription and configuration. A response is sent to the wireless client attached to the AP in order to initiate reliable multicast once the stream arrives. When the multicast packet arrives, the AP replicates the multicast frame and converts it to 802.11 unicast frames. Finally, a reliable multicast service delivers the video stream as unicast directly to the client.

Higher Video Scaling on Clients

With Cisco VideoStream technology, all of the replication is done at the edge (on the AP), thus utilizing the overall network efficiently. At any point in time, there is only the configured media stream traversing the network, because the video stream is converted to unicast at the APs based on the IGMP requests initiated by the clients. Some other vendor implementations do a similar conversion of multicast to unicast, but do it inefficiently as evidenced by the load put on the wired network to support the stream.

Switch Configuration

VideoStream can be deployed on an existing branch wide wired and wireless network. The overall implementation and maintenance costs of a video over wireless network are greatly reduced. The assumption is that the wired network is multicast enabled. In order to verify that the access switch is part

of the layer 3 network, connect a client machine to the switchport and verify if the client machine is able to join a multicast feed.

show run | **include multicast** displays if multicast is enabled on the layer 3 switch else if not enabled for multicast, you can enable multicast by executing the following command on the switch:

L3_Switch#**show run | include multicast** ip multicast-routing distributed

ſ

Depending on the type of Protocol Independent Routing (PIM) configuration on the wired network, the layer 3 switch is configured either in PIM Sparse mode or in PIM dense mode. There is also a hybrid mode, PIM sparse-dense mode which is widely used.

```
interface Vlan56
ip address 9.5.56.1 255.255.2
ip helper-address 9.1.0.100
ip pim sparse-dense-mode
end
```

show ip igmp interfaces display the SVI interfaces that are participating in the IGMP membership. This command displays the version of IGMP configured on the switch or the router. The IGMP activity on the interface can also be verified in the form of IGMP join and leave messages by the clients.

```
L3_Switch#show ip igmp interface
Vlan56 is up, line protocol is up
  Internet address is 9.5.56.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP configured query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP configured querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 6 joins, 3 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 9.5.56.1 (this system)
  IGMP querying router is 9.5.56.1 (this system)
  Multicast groups joined by this system (number of users):
      224.0.1.40(1)
```

The above configuration can be verified by running the **show ip mroute** command on the layer 3 switch. The above configuration has certain entries that need to be looked into. The special notation of (Source, Group), pronounced "S, G" where the source "S" is the source IP address of the multicast server and "G" is the Multicast Group Address that a client has requested to join. If the network has many sources, you will see on the routers an (S,G) for each of the source IP address and Multicast Group addresses. This output displayed below also has information of outgoing and incoming interfaces.

L3_Switch#**show ip mroute**

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
      L - Local, P - Pruned, R - RP-bit set, F - Register flag,
      T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
      X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
      U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
      Y - Joined MDT-data group, y - Sending to MDT-data group,
      V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.255.255.250), 4d20h/00:02:35, RP 0.0.0.0, flags: DC
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan56, Forward/Sparse-Dense, 4d20h/stopped
(*, 229.77.77.28), 4d15h/00:02:36, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan56, Forward/Sparse-Dense, 00:24:34/stopped
(*, 224.0.1.40), 5d17h/00:02:41, RP 0.0.0.0, flags: DCL
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan56, Forward/Sparse-Dense, 5d17h/stopped
```

Controller Configuration

Enabling VideoStream—Global

Enable Global Multicast Mode and IGMP snooping on the controller as shown below:

Figure 54 WLC Configuration

uluili. cisco	MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT
Controller General Inventory		obal Multic		۲		
Interfaces		MP Snoopi	-	۲		
Interface Groups	IGMP Tim	eout (30-7	200 seconds)	60		
Multicast	IGMP Que	ery Interval	(15-2400 seconds) 20		
Network Routes	Enable MI	D Snoopin	9			
Redundancy	MLD Time	out (30-72	00 seconds)	60		
Internal DHCP Server	MLD Que	y Interval	(15-2400 seconds)	20		
Mobility Management						
Ports						
▶ NTP						
> CDP						

(Cisco Controller) >config network multicast global enable (Cisco Controller) >config network multicast igmp snooping enable

To enable the VideoStream feature globally on the controller, navigate to **Wireless > Media Stream > General** and check the **Multicast Direct Feature** check box. Enabling the feature here populates some of the configuration parameters on the controller for VideoStream.

،،ا،،،ا،، cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
CISCO Wireless All APs Radios 802.11a/n/a 802.11b/g/n Dual-Band R Global Configura	Media Stream >General Multicast Direct feature Session Message Config adios Session announcement State	Enabled	Secontry		COMMANDS	HELP	FEEDBACK
 Advanced Mesh RF Profiles Network Lists 	Session announcement URL Session announcement Email Session announcement Phone Session announcement Note]			
FlexConnect C FlexConnect ACL 802.11a/n/ac 802.11b/g/n Media Stream General Streams	roups s						

352803

1

Figure 55 Enable VideoStream - Global

```
(Cisco Controller) >config media-stream multicast-direct ?
enable Enable Global Multicast to Unicast Conversion
disable Disable Global Multicast to Unicast Conversion
```

The multicast direct button under WLAN > QoS appears on if the feature is enabled globally.

ululu cisco ⊯	IONITOR WLANS CONT		eless <u>s</u> ecu	RITY MANAGEMENT	COMMANDS	HELP	FEEDBACK
WLANS V VLANS VLANS Advanced	ONITOR WEARS CONTOR VLANS > Edit 'enjoy' General Security Burst Real-Time Rate Clear Override Per-SSID Ban Average Data Rate Burst Data Rate Burst Data Rate Burst Data Rate Burst Real-Time Rate Clear WMM WMM WMM Policy 7920 AP CAC 7920 Client CAC Multicast Direct Multicast Direct	QoS Polic	y-Mapping 0	Advanced		HEUP	LEEDBACK

This provides the flexibility to enable VideoStream feature per SSID and is described later in this document.

ſ

Turn on Local Switching under WLAN > Advanced and ensure that the APs in the setup are in FlexConnect mode.

1

eneral Security 0	QoS Policy-Mapping	Advanced		
Scan Defer Priority	0 1 2 3 4 5 6 7		Passive Client	
			Passive Client	
Scan Defer Time(msecs)	100		Voice	
lexConnect			Media Session Snooping	Enabled
FlexConnect Local	Senabled		Re-anchor Roamed Voice Clients	Enabled
Switching ²	C Enabled		KTS based CAC Policy	Enabled
FlexConnect Local Auth 12	Enabled		Radius Client Profiling	
Learn Client IP Address 5	Enabled		DHCP Profiling	
Vian based Central	Enabled		HTTP Profiling	
Switching 13	_		Local Client Profiling	
Central DHCP Processing	Enabled		DHCP Profiling	2
Override DNS	Enabled		HTTP Profiling	
NAT-PAT	Enabled		PMIP	
Central Assoc	Enabled		PMIP Mobility Type	0
			PMIP NAI Type	Hexadecimal +
			PMIP Profile	None 1

Figure 56 Enable Local Switching on WLAN

Figure 57 Change AP Mode to FlexConnect

eneral	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
neral				Versions		n na sea ann an Arra
AP Name	2	AP_1600		Primary Softwa	are Version	8.0.72.114
Location		default location		Backup Softwa	re Version	0.0.0.0
AP MAC A	ddress	6c:20:56:13:f6:23		Predownload S	tatus	None
Base Rad	io MAC	68:86:a7:cb:c0:d0		Predownloaded	Version	None
Admin St	atus	Enable +		Predownload N	lext Retry Time	NA
AP Mode		FlexConnect		Predownload R	etry Count	NA
AP Sub M	ode	None ÷	_	Boot Version		15.2.2.0
Operation	al Status	REG		IOS Version		15.3(20140203:113124)\$
Port Num	ber	1		Mini IOS Versio	on	7.4.1.37
Venue Gr	oup	Unspecified	•	IP Config		
Venue Ty	pe	Unspecified +		IP Address		9.5.56.105
Venue Na	ime			IPv6 Address		
Language				Static IP		
Network S	Spectrum Key	731759626C780B4	A4A128E3F1D98F252	Static IPv6		0

Add Media Stream Configuration

I

ſ

To add a multicast stream to the controller, navigate to **Wireless > Media Stream > Streams** and click **Add New.**

uhuhu cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COMMANDS	HELP FEEDBACK	Saye Configuration Ping Logout Befresh
CISCO Wireless * Access Points All APs * Radies 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration * Advanced Mesh	Media Stream > New Stream Name Multicast Destination Start IP Address(ipv4/ipv6) Multicast Destination End IP Address(ipv4/ipv6) Maximum Expected Bandwidth(1 to 35000 Kbps) Resource Reservation Control(RRC) Param Select from predefined templates	Media2 229,77,77.28 229,77,77.28 500 meters Select =	HELP TEEDBACK	< Back Apply
RF Profiles Network Lists FlexConnect Groups FlexConnect ACLs 802.11a/n/ac 802.11b/g/n Media Stream General Streams	Average Packet Size (100-1500 bytes) RRC Periodic update RRC Priority (1-8) Traffic Profile Violation	1200 J best-effort :		

Figure 58 Media Stream Configuration

For configuration using CLI use:

```
configure media-stream add multicast-direct <media-stream-name> <start-IP> <end-IP>
[template | detail <bandwidth> <packet-size> <Re-evaluation> video <priority>
<drop|fallback>]
```

As mentioned it is necessary that the administrator is aware of the video characteristic streaming through a controller. A true balance must be drawn when the streams configuration are added. For example, if the stream bit rate varies between 1200 Kbps and 1500 Kbps the stream must be configured for a bandwidth of 1500 Kbps. If the stream is configured for 3000 Kbps then you will have lesser video client serviced by the AP. Similarly, configuring for 1000 Kbps will cause pixelization, bad audio, and bad user experience.

The multicast destination start IP address and end IP address can be the same address as shown in Figure 58. You can also configure a range of multicast address on the controller. There is a limitation of 100 on the number of multicast addresses entries or the number of stream entries that will be pushed to the APs.

Enabling VideoStream – WLAN

One or all WLANs/SSIDs configured can be enabled for streaming video with VideoStream. This is another configuration step that can control the enabling of the VideoStream feature. Enabling or disabling the VideoStream feature is non-disruptive. Click WLAN > <WLAN ID> > QoS.

cisco		TROLLER WIRE	LESS <u>S</u> ECURI	ITY MANAGEMENT	COMMANDS	HELP	FEEDBACK
LANs	WLANs > Edit 'enjoy'	18					
WLANS WLANS	General Security Burst Real-Time Rate	QoS Polic	y-Mapping	Advanced			
Advanced	Clear	0	0				
	Override Per-SSID Ba	ndwidth Contr	acts (kbps) ¹⁰	٤			
		DownStream	UpStream				
	Average Data Rate	0	0				
	Burst Data Rate	0	0				
	Average Real-Time Rate	0	0				
	Burst Real-Time Rate	0	0				
	Clear						
	WMM						
	WMM Policy	Allowed :					
	7920 AP CAC	Enabled					
	7920 Client CAC	Enabled					
	Media Stream						
	Media Stream						

Figure 59 Enable VideoStream – WLAN

Configure the Quality of Service (QoS) to Gold (video) to stream video to wireless client at a QoS value of gold (4). This will only enable video quality of service to wireless clients joined to a configured stream on the controller. The rest of the clients will be enabled for appropriate QoS. To enable Multicast Direct on the WLAN, check the **Multicast Direct** check box as shown in Figure 59. This will enable the WLAN to service wireless clients with the VideoStream feature.

I

```
(Cisco Controller) >config wlan media-stream multicast-direct 1 ?
enable Enables Multicast-direct on the WLAN
disable Disables Multicast-direct on the WLAN.
```

All wireless clients requesting to join a stream will be assigned video QoS priority on admission. Wireless client streaming video prior to enabling the feature on the WLAN will be streaming using normal multicast. Enabling the feature switch the clients to multicast-direct automatically on the next IGMP snooping interval. Legacy multicast can be enabled on the WLAN by not checking the Multicast Direct feature. This will show that wireless clients streaming video are in Normal Multicast mode.

Verifying VideoStream Functionality

Make sure the wireless clients are associated to the access point(s), and are configured for a correct interface. As seen in the Figure 60, there are three clients associated to one AP. All three clients have an IP address from VLAN 56 (SSID name—enjoy). The associated clients have an IP address and good uplink connectivity to the AP.

uluilu cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Monitor	Clients								
Summary Access Points	Current Filter	None	[Change Filter] [Clear Filter]					
Cisco CleanAir	Client MAC Addr	IP Address	AP Name		I	WLAN Profile	l v	VLAN SSID	User Name
> Statistics	7c:d1:c3:86:7e:dc	9.5.56.100	AP_1600			enjoy		njoy	Unknown
CDP	88:cb:87:bd:0ctab	9.5.56.113	AP_1600			enjoy	e	njoy	Unknown
Rogues	d8:96:95:02:7e:b4	9.5.56.108	AP_1600			enjoy	e	njoy	Unknown
Redundancy Clients Sleeping Clients Multicast Applications Local Profiling									

Figure 60 Client Summary

Enable streaming on the wired side by connecting a video server with a configured multicast address 229.77.77.28. Refer the following link to know how to stream from a Video Sever: https://wiki.videolan.org/Documentation:Streaming_HowTo_New/#Streaming_using_the_GUI Complete the steps:

Step 1 Join wireless clients to the multicast streaming video.

```
Note
               Use VLC player to stream and watch video.
Step 2
        Double click on the VLC icon on your desktop. Click Media > Open Network stream. Choose
        Protocol = UDP, Address = 229.77.77.28, Port = 1234 in the format udp://@229.77.77.28:1234
Step 3
        Click Play.
           L3_Switch#show ip mroute
           IP Multicast Routing Table
           Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
                   L - Local, P - Pruned, R - RP-bit set, F - Register flag,
                   T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
                   X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
                   U - URD, I - Received Source Specific Host Report,
                   Z - Multicast Tunnel, z - MDT-data group sender,
                   Y - Joined MDT-data group, y - Sending to MDT-data group,
                   V - RD & Vector, v - Vector
           Outgoing interface flags: H - Hardware switched, A - Assert winner
            Timers: Uptime/Expires
            Interface state: Interface, Next-Hop or VCD, State/Mode
            (*, 239.255.255.250), 4d20h/00:02:47, RP 0.0.0.0, flags: DC
              Incoming interface: Null, RPF nbr 0.0.0.0
              Outgoing interface list:
                Vlan56, Forward/Sparse-Dense, 4d19h/stopped
            (*, 229.77.77.28), 4d15h/00:02:44, RP 0.0.0.0, flags: DC
              Incoming interface: Null, RPF nbr 0.0.0.0
              Outgoing interface list:
                Vlan56, Forward/Sparse-Dense, 00:17:24/stopped
            (*, 224.0.1.40), 5d17h/00:02:53, RP 0.0.0.0, flags: DCL
              Incoming interface: Null, RPF nbr 0.0.0.0
              Outgoing interface list:
                Vlan56, Forward/Sparse-Dense, 5d17h/stopped
```

It is observed that the MAC address of the wireless clients is in a Multicast-Direct Allowed State.

Figure 61 FlexConnect VideoStream Clients

ဂါကျက င၊sco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDB
Monitor	Multicast Group	S					
Summary Access Points Cisco CleanAir Statistics CDP	Layer3 MGID(Mu Group address Via Layer2 MGID(Mu InterfaceName v	In MGID IGMP	MLD	0			
Rogues			12				
Redundancy			13				
Clients	management 5	6	0	-			
Sleeping Clients Multicast	FlexConnect Mult	ticast Media St Stream-Name	ream Clients Multicast-Ip		me Vlan	ту	pe
Applications	7c:d1:c3:86:7e:dc	Media2	229.77.77.28	AP_160	0 0	Mu	lticast Direct
Local Profiling	88:cb:87:bd:0c:ab	Media2	229.77.77.28	AP_160	0 0	Mu	Iticast Direct
	d8:96:95:02:7e:b4	Media2	229.77.77.28	AP_160	0 0	Mu	lticast Direct

The Wireshark capture on the client shows the Multicast to Unicast Video Stream. The Ethernet header contains the MAC address of the client as the Destination MAC address, for example, 7c:d1:c3:86:7e:dc.

Figure 62 Wireshark Capture Depicting mc2uc

I

No. Time Source Destination 1109 12:11418000 128 kb/s 44,1 KHz 1109 12:1144292000 9.5.56.115 229,77.77.28 1110 12:114459000 9.5.56.115 229,77.77.28 1111 12:114489000 9.5.56.115 229,77.77.28 1111 12:11489000 9.5.56.115 229,77.77.28 1113 12:115024000 075 86542.67000000 PT5 66542.79000000 1114 12:115024000 075 86542.67000000 PT5 66542.79000000 1115 12:11688000 075 86542.710000000 PT5 86542.750000000 1116 12:118882000 075 86542.710000000 PT5 86542.750000000 1116 12:118882000 9.5.56.115 229,77.77.28 1116 12:119882000 075 86542.710000000 PT5 86542.750000000 1117 12:118882000 9.5.56.115 229,77.77.28 1118 12:119843000 9.5.56.115 229,77.77.28 1118 12:119843000 9.5.56.115 229,77.77.28	Protocol I MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS	1358 A 1358 S 1358 S 1358 S 1358 S 1358 V 1358 S	adio Cayer Source port Source port Source port Source port rideo-strea	: apc-2160 : apc-2160 : apc-2160 : apc-2160	Destination p	port: search-agen port: search-agen port: search-agen port: search-agen	t t
1109 12.114292000 9.5.56.115 229.77.77.28 1110 12.114450000 9.5.56.115 229.77.77.28 1111 12.114450000 9.5.56.115 229.77.77.28 1111 12.114450000 9.5.56.115 229.77.77.28 1111 12.114646000 9.5.56.115 229.77.77.28 1113 12.115020000 9.5.56.115 229.77.77.28 1113 12.115220000 9.5.56.115 229.77.77.28 1115 12.118880000 128 kb/s 44.1 kHz 1116 12.118880000 175 86542.710000000 PTS 86542.750000000 1117 12.118880000 175 86542.710000000 PTS 86542.750000000 1116 12.118980000 128 kb/s 44.1 kHz 1116 12.118980000 128 kb/s 44.1 kHz	MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS	1358 S 1358 S 1358 S 1358 S 1358 V 1358 S	Source port Source port Source port Source port	: apc-2160 : apc-2160 : apc-2160 : apc-2160	Destination p	port: search-agen	t t
1110 12.114450000 9.5.56.115 229.77.77.28 1111 12.114630000 9.5.56.115 229.77.77.28 1112 11.114630000 9.5.56.115 229.77.77.28 1113 12.115024000 075.86542.670000000 PTS.86542.790000000 1114 12.115024000 9.5.56.115 229.77.77.28 1115 12.118880000 128.kb/s 44.1 kHz 1116 12.118880000 075.86542.710000000 PTS.86542.750000000 1117 12.118883000 9.5.56.115 229.77.72.8 1116 12.119400000 128.kb/s 44.1 kHz 1116 12.119400000 128.kb/s 44.1 kHz	MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS	1358 S 1358 S 1358 V 1358 S	iource port iource port iource port ideo-strea	: apc-2160 : apc-2160 : apc-2160	Destination p	port: search-agen	t t
1111 12:114636000 9:5:56:115 229:77:77:28 1112 12:114636000 9:5:56:115 229:77:77:28 1113 12:115024000 9:5:56:115 229:77:77:28 1114 12:115024000 9:5:56:115 229:77:77:28 1115 11:52:2000 9:5:56:115 229:77:77:28 1115 12:116880000 128 kb/s 44.1 kHz 1116 12:118883000 9:5:56:115 229:77:77:28 1117 12:118883000 9:5:56:115 229:77:77:28 1118 12:119460000 128 kb/s 44.1 kHz	MPEG TS MPEG TS MPEG TS MPEG TS MPEG TS	1358 S 1358 S 1358 v 1358 S	ource port ource port ideo-strea	: apc-2100 : apc-2160	Destination p	port: search-agen	t
1112 12.114836000 9.5.56.115 229.77.77.28 1113 12.115024000 DTS 86542.670000000 PTS 86542.79000000 1114 12.115220000 9.5.56.115 229.77.77.28 1115 12.118880000 128 kb/s 44.1 kHz 1116 12.118882000 DTS 86542.71000000 PTS 86542.75000000 1117 12.118882000 DTS 86542.71000000 PTS 86542.750000000 1117 12.118882000 9.5.56.115 229.77.72.8 1118 12.119460000 128 kb/s 44.1 kHz	MPEG TS MPEG TS MPEG TS MPEG TS	1358 S 1358 v 1358 S	Source port	: apc-2160			
1113 12.115024000 DTS 86542.670000000 PTS 86542.790000000 1114 12.115220000 9.5,56.115 229.77.77.28 1115 12.118880000 128 kb/s 44.1 kHz 1116 12.118882000 05 86542.710000000 PTS 86542.750000000 1117 12.118882000 9.5,56.115 229.77.77.28 1118 12.119460000 128 kb/s 44.1 kHz	MPEG TS MPEG TS MPEG TS	1358 v 1358 s	ideo-strea		sessential caloring	car so wear privadant	£1.
1114 12.115220000 9.5,56.115 229.77.77.28 1115 12.118880000 128 kb/s 44.1 kHz 1116 12.118880000 D5 86542.710000000 PTS 86542.750000000 1117 12.118883000 9.5,56.115 229.77.77.28 1118 12.119460000 128 kb/s 44.1 kHz	MPEG TS MPEG TS	1358 S					15
1115 12.116880000 128 kb/s 44.1 kHz 1116 12.119882000 DTS 86542,710000000 PTS 86542,750000000 1117 12.119882000 9.5,56.115 229.77.728 1118 12.119460000 128 kb/s 44.1 kHz	MPEG TS		ource port	: apc-2160	Destination r	port: search-agen	6
1117 12.118883000 9.5.56.115 229.77.77.28 1118 12.119460000 128 kb/s 44.1 kHz	MPEG TS	A BCEL	udio Layer				
1118 12.119460000 128 kb/s 44.1 kHz			ideo.strea				
	MPEG TS	1358 S	ource port	: apc-2160	Destination p	port: search-agen	13
1119 12.119655000 9.5.56.115 229.77.77.28	MPEG TS	1358 A	udio Layer	2			
	MPEG TS	1358 5	ource port	: apc-2160	Destination p	port: search-agen	¢
1120 12.120121000 9.5.56.115 229.77.77.28	MPEG TS					port: search-agen	
1101 10 10648000 9 5 56 115 000 77 77 08	MDEG TS	1358 5	inurce nort	+ anr-2160	Destination r	nert search aner	F
<pre>rame 1111: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bi thernet II, Src: GoodwayI_5f:6a:49 (00:50:b6:5f:6a:49), Dst: Apple_86:7e: normet_Drotocol_Vinition_1_Srci 01:50:116 (05:50:116), Ott 2007727 Ser Datagram Protocol, Src Port: apc-2160 (2160), Dst Port: search-agent S0/IEC 13818-1 PID=0x47 CC=5 wassembled in: 1113 S0/IEC 13818-1 PID=0x47 CC=6</pre>	dc (7c:d1:c3	3:86:7e:d	lc)	-	_		
0 7c d1 c3 86 7e dc 00 50 b6 5f 6a 49 08 00 50 6 5~P .jI							

Limitations

The limitations to this feature scope include:

- **1.** There is no admission control for local switched clients' multicast video requests, which means always admit the configured video stream subscriptions as mc2uc.
- Due to the limit of CAPWAP payload length, only the first 100 media-streams will be pushed from the controller to the AP in this release. For example, config media-stream add multicast-direct stream1 225.0.0.1 225.0.0.10 template coarse, is considered as one entry.
- **3.** Roaming support is limited to adding mobile payload. Whenever the client roams to another AP, the WLC will add the entry for the client in the mc2uc table. This means that roaming in standalone mode of FlexConnect AP will not be supported for this feature.
- 4. Currently this feature only has IPv4 support.

Show Commands – Controller

Some of the show commands are documented earlier in this document. The following section is only for your reference:

(Cisco Controller) > sh	ow ap summary					
Number of APs			5				
Global AP User Na	me		Not Con	figur	ed		
Global AP Dot1x U	ser N	ame	Not Con	figur	ed		
AP Name	Slots	AP Model	Ethernet MAC	Lo	cation	Cou	ntry
IP Address Clie	nts	DSE Location					-
AP1142	2	AIR-LAP1142N-A-K9	f0:f7:55:f1:7	5:20	default	location	IN
9.5.56.109		[0,0,0]					
AP_2600 9.5.56.110	2 0	AIR-CAP2602E-N-K9 [0 ,0 ,0]	fc:99:47:d9:8	6:90	default	location	IN
AP3700	2	ATR-CAP3702E-N-K9	7c:ad:74:ff:6	h.16	dofaul+	location	TM
9.5.56.116	2 0	[0,0,0]	7C.au.74.11.0	D:40	ueraurc	IOCALION	111
AP 3600-2	2	AIR-CAP3602I-N-K9	a4:4c:11:f0:e	9:dc	default	location	IN
9.5.56.111	0	[0 ,0 ,0]					
AP_1600	2	AIR-CAP1602I-N-K9	6c:20:56:13:f	6:23	default	location	IN
9.5.56.105	2	[0 ,0 ,0]					
(Cisco Controller) > sh	ow client summary					
Number of Clients			2				
Number of PMIPV6	Clien	ts	0				
			GL.	AN/			
			RL.	AN/			
MAC Address	AP Na	ame Slot S	Status WLA	N Au	th Proto	col	Port
Wired PMIPV6 Rol	е						

_____ ____ 88:cb:87:bd:0c:ab AP_1600 1 Associated 1 Yes 802.11a 1 No No Local 1 Associated 1 Yes 802.11a 1 No d8:96:95:02:7e:b4 AP_1600 Local No (Cisco Controller) >show media-stream multicast-direct state Multicast-direct State..... enable Allowed WLANs..... 1 (Cisco Controller) >show media-stream group summary Stream Name Start IP End IP Operation Status _____ _____ Media1 239.1.1.1 239.2.2.2 Multicast-direct Media2 229.77.77.28 229.77.77.28 Multicast-direct (Cisco Controller) >show media-stream group detail Media2 Media Stream Name..... Media2 Start IP Address..... 229.77.77.28 RRC Parmmeters Avg Packet Size(Bytes)..... 1200 Expected Bandwidth(Kbps)..... 500 Policy..... Admit RRC re-evaluation..... periodic QoS..... Video Status..... Multicast-direct Usage Priority..... 1 Violation..... fallback (Cisco Controller) >show flexconnect media-stream client summary Client Mac Stream Name Multicast IP AP-Name VLAN Type _____ _____ -----7c:d1:c3:86:7e:dc Media2 229.77.77.28 AP_1600 0 Multicast Direct 88:cb:87:bd:0c:ab Media2 229.77.77.28 AP_1600 0 Multicast Direct d8:96:95:02:7e:b4 Media2 229.77.77.28 AP_1600 0 Multicast Direct (Cisco Controller) >show flexconnect media-stream client Media2 Media Stream Name..... Media2 IP Multicast Destination Address (start)..... 229.77.77.28

IP Multicast Destination Address (end)..... 229.77.77.28

Client Mac	Multicast IP	AP-Name	VLAN	Туре
7c:d1:c3:86:7e:dc	229.77.77.28	AP_1600	0	Multicast Direct
88:cb:87:bd:0c:ab	229.77.77.28	AP_1600	0	Multicast Direct
d8:96:95:02:7e:b4	229.77.77.28	AP_1600	0	Multicast Direct

I

Show and Debug Commands – AP

- Debug ip igmp snooping group
- Debug capw mcast
- Show capwap mcast flexconnect clients
- Show capwap mcast flexconnect groups

```
AP_1600#show capwap mcast flexconnect clients
=====
Bridge Group: 1
======
Multcast Group Address 229.77.77.28::
MCUC List:
Number of MCUC Client: 3
88cb.87bd.0cab(Bridge Group = 1 Vlan = 0)
7cd1.c386.7edc(Bridge Group = 1 Vlan = 0)
d896.9502.7eb4(Bridge Group = 1 Vlan = 0)
------
MC Only List:
Number of MC Only Client: 0
```

```
AP_1600#show capwap mcast flexconnect groups
WLAN mc2uc configuration:
WLAN ID 1 , Enabled State 1
WLAN ID 2 , Enabled State 0
WLAN ID 3 , Enabled State 0
WLAN ID 4 , Enabled State 0
WLAN ID 5 , Enabled State 0
WLAN ID 5 , Enabled State 0
WLAN ID 7 , Enabled State 0
WLAN ID 7 , Enabled State 0
WLAN ID 8 , Enabled State 0
WLAN ID 9 , Enabled State 0
WLAN ID 10, Enabled State 0
WLAN ID 11, Enabled State 0
WLAN ID 11, Enabled State 0
WLAN ID 12, Enabled State 0
```

```
WLAN ID 14, Enabled State 0
WLAN ID 15, Enabled State 0
WLAN ID 16, Enabled State 0
Video Group Configuration:
Group startIp 239.1.1.1 endIp 239.2.2.2
Group startIp 229.77.77.28 endIp 229.77.77.28
```

FlexConnect Faster Time to Deploy

I

The existing system requires an AP reboot when converted from Local mode to FlexConnect mode. Once the AP boots up, it joins back the controller and subsequently all the FlexConnect configuration is pushed down to the AP. This process increases the total time to deploy a FlexConnect solution in a branch. Time to deployment is a critical differentiator for any branch deployment.

This feature in release 8.0 eliminates the need to reboot when the AP is converted to FlexConnect mode. When the controller sends the AP a mode change message, the AP will get converted to FlexConnect mode without requiring a reload. The AP sub mode will also be configured if the AP receives the AP sub mode payload information from the controller. With this approach, the AP entry will be maintained at the controller and there will not be any AP disassociation.

Only Local mode to Flexconnect mode conversion is supported, any other mode change will cause an AP reboot. Similarly, changing of the AP sub mode to WIPS does not need reboot, but the rest of the sub mode configuration requires AP reboot.

	0.020424180107					< Back Apply
General Creder	tials Interfaces	High Availability	Inventory	FlexConnect	Advanced	
eneral			/ersions			
AP Name	AP_2600		Primary Softw	are Version E	1.0.72.114	
Location	default location		Backup Softw	are Version 0	1.0.0.0	
AP MAC Address	fc:99:47:d9:86:90		Predownload 1	Status M	lone	
Base Radio MAC	54:78:1a:70:04:7	2	Predownloade	d Version 1	lone	
Admin Status	Enable :		Predownload I	Next Retry Time	(A	
AP Mode	FlexConnect	•	Predownload I	Retry Count	(A	
AP Sub Mode	local FlexConnect		Boot Version		2.4.25.1	
Operational Status	monitor	-	IOS Version	1	5.3(20140203:113124)\$	
Port Number	Rogue Detector Sniffer		Mini IOS Versi	ion (1.0.0.0	
Venue Group	Bridge Flex+Bridge		P Config			

Figure 63 Conversion to FlexConnect - No Reboot Required

FlexConnect Plus Bridge Mode

From release 8.0 onward, FlexConnect + Bridge mode allows the Flexconnect functionality across mesh APs. Flex + Bridge mode is used to enable Flexconnect capabilities on Mesh (Bridge mode) APs. Refer to the Information about FlexConnect plus Bridge Mode section in Cisco Wireless LAN Controller Configuration Guide, Release 8.0 for more details.

Default FlexConnect Group

Introduction

During the initial deployment, the customer configures all access points from a staging controller. Prior to 8.3, day 0 configuration for FlexConnect access points is missing. Therefore the user has to create FlexConnect groups, create policies for remote sites and manually place APs under each group. VLAN support and native VLAN setting is disabled by default on a newly created FlexConnect group, which implies that remote client traffic is placed in an AP VLAN and can access internal, secure resources. There is also a limitation on the number of APs supported within a group that prevents the creation of a generic catch all FlexConnect group for initial deployment.

To overcome these challenges and to make the Day 0 branch setup easier and faster, the concept of a Default FlexConnect group has been introduced in release 8.3.

When the controller boots up, the "default-flex-group" is created by default. This group cannot be deleted or added manually. Similarly access points cannot be manually added to or deleted from the default-flex-group.

The group has default configuration for the FlexConnect group parameters upon creation and has no maximum limit on the number of APs that can be part of it. Any change in configuration gets propagated to all the APs that are part of this group and the configuration of the group is retained across resets.

When an AP in FlexConnect mode, which is not part of any admin-configured FlexConnect group, joins the controller, it becomes part of the default-flex-group and gets the configuration from this group.

In controllers such as Cisco Flex 7500 Series Controller, when the autoconvert mode is set to "flexconnect", during AP join, the AP gets converted to flexconnect mode and inherit config from default-flex-group thus supporting zero touch configuration.

Similarly when an admin configured FlexConnect group gets deleted or the AP is manually removed from such a group, the AP becomes part of the default-flex-group and inherits the config from this default group.

1

Features supported on Default FlexConnect Group

- VLAN support, Native VLAN, WLAN-VLAN mappings
- VLAN ACL mappings
- Webauth, Webpolicy, local split ACL
- Local authentication users
- RADIUS authentication
- Central DHCP/NAT-PAT

- Flex AVC
- VLAN name ID mappings
- Multicast override

Features Not Supported on Default FlexConnect Group

- Efficient image upgrade
- PMK cache distribution

Default FlexConnect Group with PnP

As a part of the zero-touch deployment, PnP server pushes configuration information to the AP. As of 8.2 the configuration contains WLC IPs, WLC names, AP mode and AP group name. This configuration has been extended to include the FlexConnect Group name starting release 8.3.

The feature is supported on the following APs that have PnP enabled:

AP 700,1600,1700,2600,2700,3600,3700, 1832,1852, 2802,3802,1810

When the AP joins the WLC it presents this FlexConnect group name to the WLC. The WLC then places the AP into an appropriate group after comparing pre-existing configurations and AP count on the FlexConnect Groups. There are various scenarios involved in deciding the FlexConnect group the AP will be placed in. The following specifically refer to scenarios where the AP will be placed as part of the default-flex-group.

Day 0 Setup Scenario

- 1. AP boots up and contacts the PnP server. PnP server does not have FlexConnect group configuration as part of the configured attributes. Also, the AP is not configured as part of any FlexConnect Group on the WLC. In this case, the AP is placed into the default-flex-group.
- 2. AP boots up and contacts the PnP server. PnP server returns a FlexConnect group configuration. The FlexConnect Group exists on the WLC but has reached the maximum capacity in terms of AP count. In this case, the AP is placed into the default-flex-group.

Day 1 Join Scenario

- 1. AP Joins WLC and does not have an AP to FlexConnect Group Mapping on the WLC
- 2. AP Joins WLC. AP has FlexConnect Group configuration present, but the FlexConnect group not configured on the WLC
- **3.** AP has FlexConnect Group configuration present, but FlexConnect group has reached its limit in terms of number of APs

Default FlexConnect Group Web UI

Step 1

1 To view the default FlexConnect Group choose WIRELESS > FlexConnect Groups > default-flex-group

ISCO MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDE
Mesh	Flex	Connect Gr	oups		Entries 1	- 3 of 3	N	lew
RF Profiles	Grou	up Name				Number of /	Ps	
FlexConnect	Site	A	A 1			0		5
Groups Hexconnetc Acces	Site					0		
FlexConnect VLAN	defa	ult-flex-group				1		

Step 2 To vie

To view APs that are a part of the default-flex-group click on the FlexConnect AP link in the General tab

FlexConnect Groups > Edit 'default-flex-group' Apply General Local Authentication **Image Upgrade ACL Mapping Central DHCP** WLAN VLAN mapping WLAN AVC mapping default-flex-group **Group Name** VLAN Template Name none Enable AP Local Authentication² . FlexConnect AP

Step 3 APs from default-flex-group can be moved to an admin configured FlexConnect group. Select the Group from "New Group Name" drop down menu and select the AP from the list and then click 'Move'

FlexConnect Group AP List

Group Name	default-flex-group	
New Group Name	None pod1-flex	
Move		
	AP Name Stat	us

Upgrade or Downgrade behavior

Upon downgrading from release 8.3 to a lower version, the controller will retain the default-flex-group configuration. This group will be treated as any other admin-configurable FlexConnect group, i.e deletion and addition is possible, APs can be manually added or deleted from the group and the maximum limit on number of APs is applicable. Since the support for default-flex-group feature does not exist in earlier releases, FlexConnect APs will not join this group by default.

Upon upgrade to release 8.3 any FlexConnect AP that is not part of a FlexConnect group will join the default-flex-group and get the related default configuration. The rules of inheritance will continue to apply and therefore any AP specific FlexConnect Configuration will not be overwrited by the default FlexConnect group config.

CLI Commands

• The existing show command would display the configuration of the default-flex-group and the APs that are part of it.

show flexconnect group detail default-flex-group

• For all the APs that are part of this default group, the "show ap config general <apname>" command would reflect the default FlexConnect Group as shown below

FlexConnect Group..... default-flex-group

• A new cli command as below is introduced to display only the APs that are part of a specific group.

(Cisco Controller) >show flexconnect group detail default-flex-group aps

Number of APs in Group: 1

AP Ethernet MAC	Name	Status	Mode	Туре	Conflict with PnP

7c:0e:ce:f5:b2:a4 AP7c0e.cef5.b2a4 Joined Flexconnect Manual No

• A new cli command as below is introduced to allow copying of configuration from existing flexconnect group during creation of new groups. – VERIFY ?

config flexconnect group newGrpname add copy oldGrpName

• The default-flex-group cannot be created or deleted manually. Similarly APs cannot be added or deleted manually to the default-flex-group. So the following commands will throw an error upon execution:

(Cisco Controller) >config flexconnect group default-flex-group add Group default-flex-group has already been configured (Cisco Controller) >config flexconnect group default-flex-group delete Group default-flex-group cannot be deleted manually (Cisco Controller) >config flexconnect group default-flex-group ap add 23:2f:d2:ff:12:7d AP cannot be manually added to the default-flex-group. (Cisco Controller) >config flexconnect group default-flex-group ap delete 23:2f:d2:ff:12:7d AP cannot be manually deleted from the default-flex-group.

Application Visibility and Control for FlexConnect rel 8.1-8.8

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and WLC platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following components:

- n Next-generation Deep Packet Inspection (DPI) technology, called as Network Based Application Recognition (NBAR2), allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which supports stateful L4 - L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a common flow table for all IOS features that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS), and Access Control List (ACL), which can take action based on this classification.
- n Ability to Apply Mark using QoS, Drop and Rate-limit applications.

The key use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

AVC is supported on the 5520, 8540, 2500, 5508, 7500, 8500, and WiSM2 controllers on Local and FlexConnect modes (for WLANs configured for central switching only) since release 7.4. Release 8.1 introduces support for Application Visibility and Control for locally switched WLANs on FlexConnect APs on 5508, 7500, 75100, WiSM2, and vWLC.

- n In release 8.3 the Protocol Pack and the NBAR engine got upgraded for Flex Connect Applications and now supports Protocol Pack 14 and NBAR engine 23 with a total support of the 1327 applications.
- n In release 8.8 the Protocol Pack and the NBAR engine got upgraded for Flex Connect Applications and now supports Protocol Pack 37 and NBAR engine 31 with a total support of the 1408 applications.

Begin with release 8.6 AVC is supported on 3504, 5520 and 8540 series controllers and vWLC also supports AVC for FC mode only.

Note: For AVC Phase -6 release 8.8 The latest NBAR2 and Protocol Packs are supported on the 3504, 5520 and 8540 series controllers and vWLC supports AVC for Flex Connect APs only. The PP in rel 8.8 only supports Wave-2 COS based APs.

AVC Facts and Limitations

AVC on the FlexConnect AP can classify and take action on 1000+ different applications.

- n The protocol pack running on the FlexConnect APs is different from the one running on the WLC.
- n AVC stats on the GUI are displayed for the top 10 applications by default. This can be changed to top 20 or 30 applications as well.
- n Intra FlexConnect Group roaming support.
- n IPv6 traffic cannot be classified.
- n AAA override of AVC profiles is not supported.

- n Multicast traffic is not supported by AVC application.
- n Netflow export for FlexConnect AVC is not supported

Configuring Application Visibility

I

To configure the application visibility, perform these steps:

- 1. Open a web browser on the wired laptop, and then enter your WLC IP Address.
- 2. Create an OPEN WLAN with naming convention, for example, "FlexDemo".
- 3. Enable FlexConnect Local Switching on the WLAN and then click Apply.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN	NT COMMANDS HELP FEEDBACK
CISCO WLANS WLANS WLANS Advanced	MONITOR WIANS CONTROLLER WIRELESS SECURITY MANAGEMEN WLANS > Edit 'FlexDemo' General Security QoS Policy-Mapping Advanced Wi-Fi Direct Clients Policy Disabled 2 Maximum Allowed Clients Per AP Radio 200 Clear HotSpot Configuration Enabled Client user idle timeout(15-100000) 30 Timeout Value (secs) Client user idle threshold (0-10000000) Bytes Radius NAI-Realm Off Channel Scanning Defer Scan Defer Priority 0 1 2 3 4 5 6 7 Scan Defer Time(msecs) 100 FlexConnect FlexConnect Local Image: Enabled Enabled Image: Enabled	NAC NAC NAC State None Load Balancing and Band Select Client Load Balancing Client Band Select Passive Client Passive Client Voice Media Session Snooping Enabled KTS based CAC Policy
	FlexConnect Local Auth 12 Enabled Learn Client IP Address 2 Enabled Vian based Central Switching 12 Enabled	Radius Client Profiling DHCP Profiling HTTP Profiling Local Client Profiling
	(*************************************	num n (n)

4. Make sure that the APs connected to this WLAN are among the list of supported access points for this feature.

5. Convert the AP to FlexConnect mode by selecting FlexConnect in the AP Mode drop-down menu, and then click **Apply.** The mode changes to FlexConnect without a reboot.

1

1

eneral	Credenti	als	Interfaces	High Availability	Inventory	FlexConnect	Advanced	
eneral					Versions			
AP Name		AP36	500		Primary Softw	are Version	8.1.10.61	
Location		defa	ult location		Backup Softwa	are Version	3.0.51.0	
AP MAC	Address	a4:9	3:4c:3e:fb:5a		Predownload S	Status	None	
Base Rad	lio MAC	f4:7f	:35:42:cd:70		Predownloade	d Version	None	
Admin St	atus	Enal	ble ÷		Predownload N	Next Retry Time	NA	
AP Mode		Flex	Connect :		Predownload F	Retry Count	NA	
AP Sub N	lode	Non	e :		Boot Version		12.4.23.0	
Operatio	nal Status	REG			IOS Version		15.3(20141113:1	174201)\$
Port Num	ber	1			Mini IOS Versi	on	0.0.00	
Venue G	roup	Uns	pecified	•	IP Config			
Venue Ty	pe	Uns	pecified ÷		CAPWAP Prefer	rred Mode	Ipv4 (Global Con	fig)
Venue N	ame				DHCP Ipv4 Ad	dress	10.10.10.104	
Language	2	L			Static IP (Ipv4	/Ipv6)	0	
Network Interface	Spectrum	8B70	32AFE429B737A	B40B7E24C8FB19				
SPS Locat					Time Statistics			
		1.00			UP Time		0 d, 00 h 05 m 2	3 s
GPS Pres	ent	No			Controller Ass	ociated Time	0 d, 00 h 00 m 2	7 s
					Controller Ass	ociation Latency	0 d, 00 h 04 m 5	5 s

6. Create a FlexConnect Group and add the AP to the FlexConnect Group. In the following example, "FlexGroup" is the FlexConnect Group and the access point AP3600 is added to it.

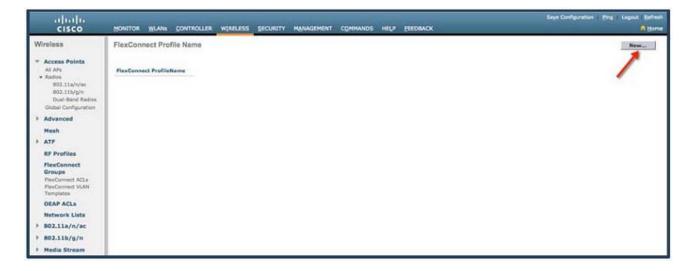
 Applications that can be identified, classified, and controlled are listed under Wireless > Application Visibility and Control > FlexConnect AVC Applications. The access points support Protocol Pack version 8.0 and NBAR engine version 16.

I

ſ

	MONITOR WLANS CONTROL	LLER WIRELESS SECURITY MANAG	EMENT COMMA	NDS HE	LP FEEDBA
lireless	FlexConnect AVC Applic	ations 🔨			
Access Points All APs Radios	Current Filter:	(Change, filter) (Clear,	filter)		
B02.11a/n/ac	Protocol Pack Name:				
B02.11b/g/n Dual-Band Radios Global Configuration	Protocol Pack Version:	8.0 Engine	• Version:	16	
Advanced	Application Name	Application Group	Application 10	Engine 10	Selector
Mesh	3com-amp3	other	\$38	3	629
ATF	3com-tamux	other	977	3	106
RF Profiles	385	layer3-over-ip	788	1	34
FlexConnect Groups	914c/g	net-admin	1109	3	211
FlexConnect ACLs	9pfs	net-admin	479	3	564
FlexConnect VLAN Templates	CAllic	business-and-productivity-tools	1113	3	216
OEAP ACLs	Konspire2b	file-sharing	1190	3	6085
Network Lists	MobilitySrv	other	1386	3	6997
02.11a/n/ac	acap	net-admin	582	3	674
02.11b/g/n	eces	other	939	3	62
edia Stream	accessbuilder	other	662	3	888
All and a second se	accessnetwork	other	607	3	699
Application Visibility And Control	802	other	513	3	599
/C Applications	acrinema	industrial-protocols	975	3	104
VC Profiles lexConnect AVC	active-directory	net-admin	1194	13	473
Applications SexConnect AVC Profiles	activesvice	business-and-productivity-tools	1419	13	490
untry	adobe-connect	business-and-productivity-tools	1441	13	505
imers	aed-512	other	963	3	149
Netflow	afooyertco	business-and-productivity-tools	1327	3	548
	strage	net-admin	609	3	705
QoS	airplax	voice-and-video	1483	13	549

 Create an AVC profile under Wireless > Application Visibility and Control > FlexConnect AVC Profiles > New with name "Drop_youtube". And then Click Apply.



FlexConnect Profile > New	< Back Apply
Profile Name Drop_youtube	

1

The AVC profile is created with the new name "Drop_youtube".

FlexConnect Profile Name	
FlexConnect ProfileName	
Drop_youtube	

9. Click the Profile name and then click Add New Rule. Select the Application Group, Application Name, and Action, and then click Apply.

pplication Group	voice-and-video	\$
58. 88		-
pplication Name	youtube	÷
ction	Drop ‡	

Wireless	FlexConnect Profile	> Edit 'Drop_youtube'	1				
Access Points All APs Radios	Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps	
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration Advanced	voutube	voice-and-video	drop	NA	NA	NA	0
Mesh							
> ATF							
RF Profiles FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates							
OEAP ACLS							
Network Lists							
▶ 802.11a/n/ac							
▶ 802.11b/g/n							
Media Stream							
Application Visibility And Control AVC Applications AVC Profiles FlexConnect AVC Applications FlexConnect AVC Profiles							

10. Verify that the rule is added as shown in the following figure.

The status of the FlexConnect AVC profile at this point is Modified.

ſ

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
Wireless	FlexConr	nect Prof	ile Name						
Mireless All APs Avanced Mesh ATF RF Profiles FlexConnect ACLs FlexConnect ACLs FlexConnect VLNA Templates OEAP ACLs Network Lists B02.11a/n/ac B02.11a/n/ac B02.11b/g/n Media Stream Application Visibility And Control AVC Applications	FlexConre FlexConne Drog. voulu	ict ProfileN	iame J	No of Rules Si	atus odified				

11. Select the profile and click Apply for the profile to be applied and to take effect.

12. Select the profile and click Apply for the profile to be applied and to take effect.

FlexConnect Profil	e > Edit 'Drop_yout	ube'				Apply	< Back	Add New Rule
Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps			
3com-amp3	other	drop	NA	NA	NA			

The status of the FlexConnect AVC profile is changed to Applied.

FlexConnect ProfileName No of Rules Status
Drop_youtube 1 Applied

- Enable Application Visibility on the FlexConnect group under Wireless > FlexConnect Group >
 FlexConnect Group name > WLAN AVC Mapping by selecting the WLAN ID and choosing Enable
 from the drop-down menu.
- 14. Apply the FlexConnect AVC profile by selecting the profile created in the previous set from the Flex AVC Profiledrop-down menu. Click **Add** and then click **Apply**.

uluilu cisco	HONITOR WLANS CONTROLLER WERKLESS GEOLAITY MANAGEMENT COMMANDS HELP FEEDMACK	Sage Configuration	Dre Ligist Billed O'Dome
	MONITOR WLANE CONTROLLER WIRKLESS GECURITY MANAGEMENT COMMANDS HELP PERDANCY FlexConnect Groups > Edit 'NewFlexGroup' General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping WLAN AVC Mapping WLAN 14 1 Application Visibility Enable 3 Per AVC Profile Drop, youtho 3 MULAN 24 Application Visibility AVC Profile	Sage Configuration	
Templates OEAP ACLs Network Lists B02.11b/g/n B02.11b/g/n Hedia Stream Application Visibility And Control AVC Applications AVC Profiles Proclamment AVC			

15. Once AVC is enabled on the FlexConnect Group, from the associated wireless client, start different types of traffic using the applications (already installed) such as Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, Ping, Trace route, and so on.

Once traffic is initiated from the wireless client, visibility of different traffic can be observed on a per FlexConnect Group and per client basis. This provides the administrator a good overview of the network bandwidth utilization and type of traffic in the network per client and per branch site

16. To check the visibility globally for all WLANs on a FlexConnect Group, click **Monitor > Applications** > FlexConnect > FlexConnect Groups and then select the FlexConnect group created earlier.

The following screen is visible which lists aggregate data for the top 10 applications running on that particular FlexConnect group.



I

This page provides more granular visibility per FlexConnect Group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect Group from the same page by clicking the Upstream and Downstream tabs.

Note: The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the Max Number of Records field on this page. The default value is 10.

17. To have more granular visibility of the top 10 applications per client on a particular locally switched WLAN where AVC visibility is enabled, click Monitor > Applications > FlexConnect Group > FlexConnect Group name > Clients. Then, click any individual client MAC entry listed on that page.

cisco	MONITOR Y	<u>v</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		54
Monitor Summary Access Points Cisco CleanAir Statistics	FlexConne Max Number AVC Statis	of Recor	oups > Appli rds 10 ± Client IP Address(1		istics	AP Nam				ILAN Profile	WLAN SSID
CDP Rogues Clients Sleeping Clients Multicast Applications WLAN NexConnect Groups Local Profiling	d4:14:07.1m	and the second second	10.10.10.109			AP3600				lexDemo	FiexDemo

After clicking on an individual client MAC entry, the client details page appears.

nitor	FlexConnect > Groups > C	lient > Applie	cation Stati	stics					< Ba	ick i	Clear AVC Stats
Summary Access Points	Max Number of Records 10			_							
Cisco CleanAir	Aggregate Upstream	Downstream	m								
Statistics	Application Name	Packet Count	Byte Count	Average Packet Size	Usage(%)	Application Name	Packet Count	Byte Count	Usage(%)		
CDP	google-services	3866	3.06 MB	836	91.36	google-services	3866	3.08 MB	89.98		
to man	0	522	127.86 KB	250	3.70	0	593	139.13 KB	3.96		
Rogues	skype	240	54.29 KB	231	1.57	skype	240	54.29 KB	1.55		
Clients	sal	86	40.47 KB	481	1.17	icloud.	123	42.28 KB	1.20		
Sleeping Clients	voutube	96	28.99 KB	309	0.84	sal	86	40.47 KB	1.15		
	Icloud	56	19.66 KB	359	0.57	youtube	96	28.99 KB	0.83		
Multicast	yaboo-mail	49	13.75 KB	287	0.40	facebook	116	16.60 KB	0.47		
Applications	dns	66	7.19 KB	111	0.21	yahoo-mail	49	13.75 KB	0.39		
WLAN	facebook	25	3.27 KB	133	0.09	dns	116	11.99 KB	0.34		
FlexConnect Groups	icmp	13	3.25 KB	256	0.09	icmp	16	4.43 KB	0.13		
Local Profiling	emp	- 11 - 11 - 11 - 11 - 11 - 11 - 11 - 1	3.23 6.0		0.03						
	Application Last 90 Secs Usag	e(%)			-	Application Cumulative Us	age(%)			1	
									1000		
				1000					10 M 10		
									1		
									11000		
			1	-							

This page provides further granular stats per client associated on locally switched WLANs, where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group as in this example. The page lists the top 10 applications in last the 90 seconds as well as cumulative stats for top 10 applications.

18. You can view upstream and downstream stats individually per client from the same page by clicking the **Upstream** and **Downstream** tabs

.Note: The number of applications that are displayed on this page can be increased to 20 or 30 by modifying the **Max Number of Records Field** on this page. The default value is 10.

19. You can clear the AVC stats for the particular client by clicking the Clear AVC Stats button.

Now, if you open YouTube, from wireless clients, you will observe that client cannot play any YouTube videos. Also, if applicable, open your Facebook account and try to open any YouTube video. You will observe YouTube videos cannot be played. Because YouTube is blocked in the FlexConnect AVC profile, and AVC profile is mapped to WLAN on the FlexConnect Group. You cannot access YouTube videos via browser, or even via YouTube application or from any other website.

.Note: If your browser was already open with YouTube, refresh the browser for the AVC profile to take effect.

IPv4 DNS Filtering on Flex Connect APs

Feature Description and Functional Behavior

It is an 8.7 feature and extends Flex connect ACL to accept internet domain names in addition to existing IP address in its rules. The DNS-based ACLs are used for client devices. One of the use case of the feature is that to correctly configure the CMX Connect Social Login feature, it is necessary to add web sites to the walled garden. Mainly because the authentication is directly performed on the social network website and no password is stored or processed in our controller. Social Login will be configured to use Facebook as the provider.

When using these devices, you can set pre-authentication ACLs on the Cisco WLC to determine where devices have the right to connect. In order to support such use cases, current implementation provides user an option to add URL based rules to the flex connect ACL and specify URL list to be allowed. Hence with this implementation the user has an option of configuring IP based rules as well as URL based rules or either of them.

With DNS-based ACLs, the client when in registration phase, is allowed to connect to the configured URLs only. WLC is configured with the ACL name that is returned by the AAA server for pre-authentication ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection. At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl).

The DNS snooping is performed on the AP for each client until the registration is complete. When the ACL configured with the URLs is received on the WLC, the CAPWAP payload is pushed to AP and configuration is stored in the database maintained in the COS based AP. When client is associated and ACL is applied, DNS snooping is enabled on the client. With snooping in place, AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is allowed in the ACL for locally switched traffic.

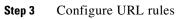
Configuration Steps From GUI

Step 1 Configure FC ACL on the WLC

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	FlexCon	nect Acc	ess Control L	.ists					
General	Acl Name								
 RADIUS Authentication 	ACL-REDIR	ECT							
Accounting Fallback	acl-test								
DNS	acl-wit%ur	1							
Downloaded AVP TACACS+	hello123								
LDAP	test tacac								
Local Net Users MAC Filtering	trx								
 Disabled Clients User Login Policies AP Policies Password Policies 									
Local EAP									
Advanced EAP									
Priority Order									
Certificate									
Access Control Lists Access Control Lists CPU Access Control Lists	_								
FlexConnect ACLs Layer2 ACLs URL ACLs									
Wireless Protection									

1

	Bown	UN MUAN	GONTROLLER	WIRELESS SECURITY	Permanent	COMMANDS HELP	TEEDBACK				
Security	Acce	ss Contro	Lists > Edit								
General	Gene	ral									
RADIUS Authentication Accounting Fallback DRS Downloaded AVP TACACS+	Access IP Typ			CL-REDIRECT Pv4							
LDAP	Seq	Action	Source IP/Mask	0	Destination IP/I	Mask	Protocol	Source Port	Dest Port	DSCP	
Local Net Users MAC Filtering	1	Permit	0.0.0.0	/ 0.0.0.0	102.102.102.5	/ 255.255.255.255	Any	Any	Any	Any	5
Disabled Clients User Login Policies	2	Permit	102.102.102.5	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	5
AP Policies Password Policies											
Local EAP											
Advanced EAP	URL	tules									
Priority Order	Seq	Action		Destination Url							
	1	Permit		www.flipkart.com							
	2	Permit		test.com							
	2	Permit		amazon.com							
Access Control Lists		Permit		www.tttt.com							
	4	Permit		www.rmain.com							
Access Control Lists Access Control Lists CI U Access Control Lists FlexConnect ACLs	4	Permit.									
CPU Access Control Lists		Permi									



alialia cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK									
WLANs	WLANs > Edit '@@redirect'									
VLANS	General Security QoS Policy-Mapping Advanced									
Advanced	Layer 2 Layer 3 AAA Servers									
	Layer 3 Security Web Policy Captive Network Assistant Bypass None Authentication Authentication Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure 12 Web policy done locally on Aptwarming									
	Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl ACL-REDIRECT									
)	Sleeping Client Enable Override Global Config ²⁰ Enable VPN Pass-Through									
	VPN Gateway Address 0.0.0.0									
	Foot Notes									

I

Γ

Step 4 Add ACL policy to the Flex Connect Group in case of Central WebAuth

CISCO	MONITOR WLA			JRITY M <u>A</u> NAGEMEN	IT COMMANDS
Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration		I Authentication	Image Upgrade	ACL Mapping Policies	Central DHCP
 Advanced Mesh ATF RF Profiles 		L-REDIRECT		•	
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates OEAP ACLS Network Lists 802.11a/n/ac 802.11b/g/n Media Stream Application Visibility And Control	Policy Access Co acl-wit%url me_cwa_acl_red				

Step 5 Configure WLAN with MAC Filtering enabled for CWA and ISE





	General Security QoS P	olicy-Mapping	Advanced			
VLANs dvanced	Allow AAA Override	C Enabled			DHCP	
	Coverage Hole Detection	Enabled			DHCP Server	Override
	Enable Session Timeout 🖉 1800					
	Aironet IE	n Timeout (secs)			DHCP Addr. Assignmen	it 🔲 Required
					OEAP	
	Diagnostic Channel 18	Enabled		and a local second	Split Tunnel	Enabled
	Override Interface ACL	IPv4 None *	j	IPv6 None •		
	Layer2 Acl	None *			Management Frame Prot	ection (MFP)
	URL ACL	None •				
	P2P Blocking Action	Disabled	•	1	MFP Client Protection 4	Optional *
	Client Exclusion 2	Enabled	180 Timeout Value (secs		DTIM Period (in beacon	intervals)
	Maximum Allowed Clients	0	rimeour value (secs	1		
	Maximum Allowed Clients *				802.11a/n (1 - 255)	1
		Enabled				1.
	Static IP Tunneling # Wi-Fi Direct Clients Policy	Enabled	•		802.11b/g/n (1 - 255)	1

Following controller CLIs will be used to configure ACLs.

To Create an ACL (existing CLI): config flexconnect acl create <acl-name> Add URL to the ACL: config flexconnect acl url-domain add <acl-name> <index> config flexconnect acl url-domain url <acl-name> <index> <url-name>

This command is used to add a new url domain rule entry for the given index for the given flexconnect acl name. Default values will be added for url name and action.

Delete URL from the ACL:

config flexconnect acl url-domain delete <acl-name> <index>

This command can be used to delete the url domain rule from the given flexconnect acl.

Configure List-Type:

```
config flexconnect acl url-domain list-type <acl-name>
<whitelist/blacklist>
```

This command is used to set/modify the type of the list for all the URLs configured on a given Flex Connect ACLs. All the URLs in a given acl will have same action. Default list type would be blacklist.

To Apply the ACL: (existing CLIs)

config flexconnect group <group-name> policy acl add <acl-name>
config flexconnect acl apply <acl-name>

To apply the ACL to the WLAN at web-auth level :

```
config flexconnect group <group-name> web-auth wlan <wlan-id> acl
<acl-name> <enable/disable>
```

Show Commands & debugs:

show flexconnect acl summary show flexconnect acl detailed <acl-name> debug flexconnect acl enable debug capwap payload enable

IPv6 Flex Connect Pre-Auth ACL and DNS Support Rel 8.8

Initially this feature was introduced in the release 8.7 with IPv4 support only. In release 8.8 this feature extends Flex connect IPv6 ACL to accept internet domain names in addition to IPv6 address in its rules.

This feature extends IPv6 Flex Connect ACL to accept internet domain names in addition to existing IPv4 and IPv6 address in its rules. The DNS-based ACLs are used for client devices. One of the use cases of the feature is that to correctly configure the CMX Connect Social Login feature, it is necessary to add websites to the walled garden. Mainly because the authentication is directly performed on the social network website and no password is stored or processed in our controller. Social Login will be configured to use Facebook as the provider.

When using these devices, you can set pre-authentication ACLs on the Cisco WLC to determine where devices have the right to connect. In order to support such use cases, current implementation provides a user an option to add URL based rules to the flex connect ACL and specify URL list to be allowed. Hence with this implementation, the user has an option of configuring IP based rules as well as URL based rules or either of them.

With DNS-based ACLs, the client when in registration phase, is allowed to connect to the configured URLs only. WLC is configured with the ACL name that is returned by the AAA server for pre-authentication ACL to be applied. If the ACL name is returned by the AAA server, then the ACL is applied to the client for web-redirection. At the client authentication phase, the ISE server returns the pre-authentication ACL (url-redirect-acl).

The DNS snooping is performed on the AP for each client until the registration is complete. When the ACL configured with the URLs is received on the WLC, the CAPWAP payload is pushed to AP and configuration is stored in the database maintained in the COS based AP. When a client is associated and ACL is applied, DNS snooping is enabled on the client. With snooping in place, AP learns the IP address of the resolved domain name in the DNS response. If the domain name matches the configured URL, then the DNS response is parsed for the IP address, and the IP address is allowed in the ACL for locally switched traffic.

- 1. The DNS name is communicated to AP data path using CAPWAP protocol
- 2. AP Data path monitors the DNS requests/responses and learns the IP address of the configured DNS names and allow traffic for the learned IP address during pre-auth phase
- 3. Maximum 20 URLs are allowed for the ACL
- 4. When a client moves from one AP to another AP (roaming), AP code will enable controller assisted context transfer
- 5. Transition scenario when the connection is broken between the controller and the AP is supported
- **6.** A sub-string match is supported for the URL configuration. For example: if 'google" is configured as the URL ACL, DNS response for play.google.com, google.com, google.in, abcgoogle.xyz will be matched

Since this feature is for the AP that operates in Flex Connect mode, DNS based ACLs need to take actual effect on the AP. On applying the ACL with URLs, respective configuration information is received on AP from the controller as new CAPWAP payload in the form of a TLV along with the other rules configured as part of ACL. The TLV payload to the AP will have an action per URL.

I

Below are the Scale numbers od supported ACLs and their size:

- 512 IPv6 ACLs for AireOS
- 20 URL Rules per ACL for AireOS & ME
- 32 IPv6 ACLs for ME
- Size of each URL: 255 characters
- 64 max DNS snooped IPs/Client

Flex Connect IPv6 ACL GUI Configuration Steps

1. Configure IPv6 FC ACL on the WLC.

cisco	MONITOR	WLANS		r wireles		MANAGEMENT COMM	NNDS HELP	FEEDBACK	Save Configuration	Ping	Logout <u>R</u> efresh
Security	FlexCon	nect ACL	s > IPv6 A	CL > Edit		22					Add Rule
General	General										IF Role URI, Role
Authentication Accounting Fallback	Access List I	Name		Test-IPv6-ACL						-	
DNS Downloaded AVP TACACS+	IP Rules										
LDAP Local Net Users MAC Filtening	Seq			Action	Source IP/P	refix Length	Dest	ination IP/Pr	efix length		Protocol P
 Disabled Clients User Login Policies AP Policies Password Policies 	URL Rule	s									
► Local EAP	Seq	Action		D	estination Url						
Advanced EAP											
Priority Order											
▶ Certificate											
 Access Control Lists Access Control Lists CPU Access Control 											
FiexConnect ACLs IPv4 ACL IPv6 ACL											
Layer2 ACLs		~	_								

2. Create and apply IPv6 ACL rule.

Γ

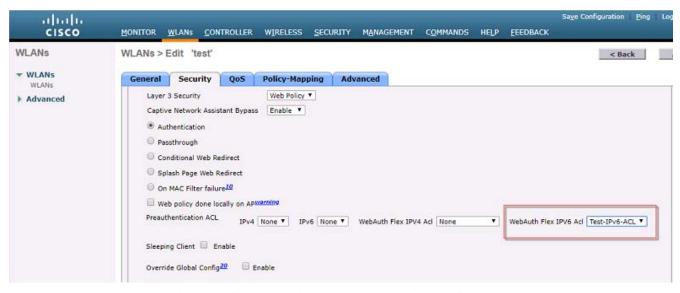
ဂျီးဂျီး cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
Security	FlexCon	nect ACL	_s > IPv6 ACL	> IP Rules	> New				
▼ AAA General	Sequence		1		IP Addr	ess			Prefix Length
 RADIUS Authentication Accounting 	Source		IP Address	•		9:10:112::/64			0
Fallback DNS Downloaded AVP	Destination		IP Address	•	IP Addr ::/0	ess			Prefix Length
TACACS+ LDAP	Protocol		Any	•					
Local Net Users MAC Filtering	DSCP		Any	•					
 Disabled Clients User Login Policies 	Action		Deny	•					

3. In the same fashion create and apply URL rules as shown in the example below.

urity	FlexC	onnect ACLs >	PV6 ACL > E	dit						1.5
General RADIUS Authentication	Gener	al								
Accounting Failback DNS Downloaded AVP	Access	List Name les		web-auth						
TACACS+	Seq		Action	Source IP/Prefix Length	Destination IP/Prefix length	Protocol	Source Port	Dest Port	DSCP	1
Local Net Users MAC Filtering	1		Deny	2001:9:10:112::/64	::/0	Any	Алу	Алу	Алу	
Disabled Clients	2		Permit	11/0	2001:9:10:112::/64	Any	Any	Any	Any	
User Login Policies AP Policies Password Policies										
Local EAP	URLR	ules								
Advanced EAP	Seq	Action	De	stination Url						
Priority Order	1	Permit	cis	00.00m	0					
Certificate	.2	Deny	tes	t.com						
Access Control Lists Access Control Lists CPU Access Control Lists (PexConnect ACLs 19v4 ACL 19v6 ACL Listy CACLs Listy CACLs URL ACLs	1	Permit	we	bEx.com	•					

1

4. Configure Local Web Auth with pre-Auth ACL created above.



5. Add ACL policy to the Flex Connect Group in case of Central WebAuth.

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURIT	Y MANAGEMEN	IT COMMANDS H	Saye Ce ELP <u>F</u> EEDBACK	onfiguration <u>P</u> ing Logout
Wireless Access Points		afault-flex-group'				Apply
All APs Radios B02.11a/n/ac B02.11b/g/n Dual-Band Radios Global Configuration	General Local Authentication	Image Upgrade	ACL Mapping Policies	Central DHCP	WLAN VLAN mapping	WLAN AVC mapping
 Advanced Mesh ATF RF Profiles 	IPv4 Policies IPv4 Policy ACL ACL-REDIRECT • Add]		6 Policies Pv6 Policy ACL Test-IPv Add	6-ACL •	
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates	IPv4 Policy Access Control Lists ACL-REDIRECT			6 Policy Access Contr	ol Lists	

6. Configure WLAN with MAC Filtering enabled for CWA and ISE .

Γ

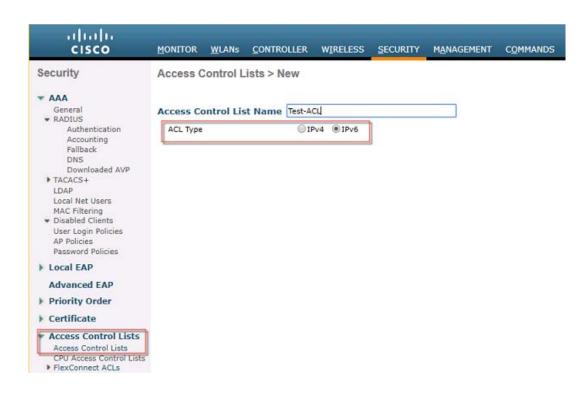
ululu cisco	MONITOR WL	ANs <u>C</u> ON	TROLLER	WIRELESS	SECURITY	MANAGEMENT	с <u>о</u> мм
WLANs	WLANs > Ed	it 'test'					
WLANS	General	Security	QoS	Policy-Map	ping A	ivanced	
Advanced	Layer 2	Layer 3	AAA S	ervers			
	Layer 2 Se		one C Filtering	2 🗹			
	Fast Transit	ion					
	Fast Transition			ble 🔻			
	Lobby Adr	nin Access					

7. Configure WLAN with Advanced Option of the AAA override for CWA and for ISE to push the required policy to the FC AP. ISE NAC state also has to be enabled.

cisco	MONITOR WLANS CONTROLLER WIR	ELESS SECURITY	MANAGEMENT COMMAN	ids Help Eeedback
WLANs	WLANs > Edit '@satheesh-8540-d	ns-acl@'		
WLANS	General Security QoS Pol	icy-Mapping Adv	anced	
Advanced	Allow AAA Override	Enabled		DHCP
	Coverage Hole Detection Enable Session Timeout	S Enabled		DHCP Server 🖾 Override
		Timeout (secs)		DHCP Addr. Assignment Required
	Diagnostic Channel 18	Enabled		
	Override Interface ACL	IPv4 None *	IPv6 None *	Split Tunnel Enabled
	Layer2 Acl	None *		Management Frame Protection (MFP)
	URL ACL	None V		
	P2P Blocking Action	Disabled •	1	MFP Client Protection ^d Optional •
	Client Exclusion 2	Enabled Timeout	Value (secs)	DTIM Period (in beacon intervals)
	Maximum Allowed Clients	0		802.11a/n (1 - 255)
	Static IP Tunneling 👭	Enabled		802.11b/g/n (1 - 255) 1
	Wi-Fi Direct Clients Policy	Disabled •		NAC
	Maximum Allowed Clients Per AP Radio	200		NAC State ISE NAC
	Clear HotSpot Configuration	Enabled		Load Balancing and Band Select

As indicated in the Executive summary, the IPv6 support was added to all IP and DNS ACL rules in release 8.8, not just the Flex Connect ACLs.

1



Flex Connect IPv6 ACL CLI Configuration Commands:

config flexconnect ipv6 acl apply <acl_name> config flexconnect ipv6 acl create <acl_name> config flexconnect ipv6 acl delete <acl_name> config flexconnect ipv6 acl rule action <acl_name> <index> permit config flexconnect ipv6 acl rule action <acl_name> <index> deny config flexconnect ipv6 acl rule add <acl_name> <index> config flexconnect ipv6 acl rule add change index acl_name <old_index> <new_index> config flexconnect ipv6 acl rule delete <acl_name> <index> config flexconnect ipv6 acl rule source port range <acl_name> <index> <start_port> <end_port> config flexconnect ipv6 acl rule source address <acl_name> <index> <ipv6_addr> <prefix_len> config flexconnect ipv6 acl rule destination port range <acl_name> <index> <start_port> <end_port> config flexconnect ipv6 acl rule destination address <acl_name> <index> <ipv6_addr> <prefix_len> config flexconnect ipv6 acl rule protocol <acl_name> <index> <protocol> config flexconnect ipv6 acl rule swap index <acl_name> <index1> <index2> config flexconnect ipv6 acl rule dscp acl_name index <0-63/any>

Wlan Mapping

config wlan security web-auth ipv6 flexacl <wlan_id> <acl_name>
Show CLI Commands:

show flexconnect ipv6 acl summary
show flexconnect ipv6 acl detailed <acl_name>

Sample Show Output

I

(Cisco Controller) >show flexcor ACL Name	Status	nary
ipv6_flex v6acl	Applied Modified	
(Cisco Controller)> show flexcor Rule Index IPv6 source prefix IPv6 destination prefix Protocol Source Port Range Destination Port Range	· · · · · · · · · · · · · · · · · · ·	1 fe80::c664:13ff:fe8f:a6a0/128 ::/0 Any 0-65535 0-65535
DSCP. Action. Rule Index. IPv6 source prefix. IPv6 destination prefix. Protocol. Source Port Range. Destination Port Range. DSCP. Action.	· · · · · · · · · · · · · · · · · · ·	Permit 2 ::/0 fe80::c664:13ff:fe8f:a6a1/128 Any 0-65535 0-65535 Any

Auto-LAG Feature Overview in Rel 8.8

The AP Flexconnect mode of operation allows one of two types of data switching models to be associated with a WLAN, central switching or local switching. In the central switching case, client WLAN data is forwarded to the WLC in a CAPWAP tunnel, and the WLC handles switching the data to the correct VLAN. In the local switching case, it's the AP's responsibility switch the client WLAN data to the correct VLAN, bypassing the WLC. The intent of this specification is to support both of these modes along with LAG.

As stated earlier, this mode relies on the WLC to switch the client WLAN data to the correct VLAN. In order for this to occur the AP must have a CAPWAP session established to the WLC. When this session exists, the AP will be in Flexconnect "Connected" mode. When LAG is enabled the client WLAN data will be load balanced between the two AP Ethernet ports in same fashion it is done in the existing LAG implementation.

The Auto-LAG feature allows Cisco Wave-2 Access points to Auto-LAG when in Flex Connect mode with non-layer 4 LB switches. Currently LAG is only supported on 3K and 4K series switches, this new feature breaks that dependency and allows Auto-LAG on the no-layer 4 LB (Load Balanced) switches such as 3650 in FC Centrally and Locally Switched modes.

According with a Miercom report and some internal testing we have done we can achieve at least 1.2 gigabits of throughput with both radios (micro/macro) on 5 Ghz with 80mhz Channel width, this configuration lets us to achieve up to 35-37 Mbps per user with about 30 users per AP.

Configurations Steps for Auto LAG feature

The configuration for the two AP Ethernet ports used for the LAG connection can either be configured as "*switchport mode access*" ports, as in the existing LAG implementation, or they can be configured as "*switchport mode trunk*" ports as per the existing FC implementation.

If the desire is to solely use central switching for the client WLAN, without the possibility of changing the WLAN to local switching, then the two AP Ethernet ports should be configured as "*switchport mode access*" ports, with the native VLAN set to the VLAN ID associated with the WLC VLAN. Thus, the AP will send the client WLAN data to the WLC in the CAPWAP tunnel untagged (e.g., without the 802.1Q VLAN header inserted) and the switch will put them on the same VLAN as the WLC.

If there is a chance the client WLAN will be changed in the future to the local switching mode, then the two AP Ethernet ports should be configured as "*switchport mode trunk*" ports, with the native VLAN set to the VLAN ID associated with the WLC VLAN and VLAN IDs should be added for each supported client WLAN. Although defined as a trunk port, operation will be same as for the "switchport mode access", with the AP will sending untagged CAPWAP to the WLC.

Prior to release 8.8, LAG implementation only "*switchport mode access*" ports were allowed to be configured.

Now, in rel 8.8, with the addition of the FC/LAG functionality, "switchport mode trunk" ports are also allowed to be configured and used. The choice depends on the Flexconnect switching mode associated with the client WLAN, with local switching requiring "*switchport mode trunk*" ports, while central switching can use either mode as described in the section above.

The configuration for the feature will use the existing methods for configuring LAG and Flex Connect.

WLC Configuration

```
config lag enable
config ap lag-mode support enable <ap-name>
```

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTRO	DLLER WIRELESS SECURITY MANAGEMENT
Controller	General	
General Icons	Name 802.3x Flow Control Mode	C5520-MA18
Inventory	LAG Mode on next reboot	Enabled V
Interfaces Interface Groups Multicast	Broadcast Forwarding AP Multicast Mode 1	Disabled Enabled Multicast V 239.255.1.57 Multicast
Network Routes Eabric Configuration	AP IPv6 Multicast Mode 1 AP Fallback	Multicast V :: Enabled V

Switch Ports Configuration Example for Locally Switched AP Mode

```
! interface Port-channel12
switchport trunk native vlan 110
switchport trunk allowed vlan 110-120
switchport mode trunk
spanning-tree portfast trunk
interface TenGigabitEthernet1/0/7
switchport trunk native vlan 110
switchport trunk allowed vlan 110-120
switchport mode trunk
channel-group 12 mode active
```

Managing 8.8 Auto LAG Feature

The following command is used to shows most of the configuration programmed to NSS, with the LAG related info highlighted.

ap#show controllers nss status Sample Output:

NSS state is enable

Wired0 Configuration:

|ID:0|TYPE:0|STATE:1| |OPT:0x000003F|MTU:1500|TPID:0x8100|NVLAN:0|POL:0| Wired1 Configuration:

|ID:1|TYPE:0|STATE:1| |OPT:0x000003F|MTU:1500|TPID:0x8100|NVLAN:0|POL:0| QoS Configuration:

Policy Name: Background Direction: Ingress Default Priority: 2, Type: L2_L3 L2 to Priority Mapping: PCP | 0 1 2 3 4 5 6 7 Priority | 0 1 2 3 4 5 6 7 L3 to Priority Mapping:

Priority	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
UP	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0
DSCP	0	2	10	18	26	34	46	48	0	0	0	0	0	0	0	0
PCP	0	1	2	3	4	5	6	7	0	0	0	0	0	0	0	0

LAG Configuration:

|ID:33|TYPE:1|STATE:1| |LINKS:0x0000003|HASHPROF:1| Hash Profile Configuration:

|ID:1|TCP-UDP:0x00000F00|IP:0x00001300|NON-IP:0x000000FC| |KNEE0:0x80000000|KNEE1:0xFFFFFFF|KNEE2:0x000000000|

CAPWAP Configuration:

```
|ID:34|TYPE:3|STATE:1|

|GATEWAY-MAC:F8:72:EA:67:7C:4D|AP-MAC:58:AC:78:DC:B2:50|

|RADIO-BASE-MAC:58:AC:78:DF:74:B0|PMTU:576|

|WLC-IP:1.4.8.2|AP-IP:1.4.8.236|WLC-PORT:5247|AP-PORT:5256|

|DEST-PORT:33|PROTO:0|TTL:250|FLBL:0|DTLS-ID:65535|

|VLAN-ID:0|OPT:0x000000C|UQOSP:0|MQOSP:0|CSUM:1|

|L4RXBITS: 3|L4TXBITS: 3|L4HASHPROF: 1|
```

Client Configuration: Current Count: 4

```
      |MAC
      | OPAQUE | PRI POL | VLAN | BR | TN | QCF | BSS | RADID | MYMAC | | 58:AC:78:DC:B2:50 | 00000000 |

      3|
      0|
      1
      1
      0|
      2|
      3|
      1|
      158:AC:78:DC:B2:51 | 00000000 |
      3|
      0|
      1|
      10|
      2|

      3|
      1
      100:71:C0:A8:01:0C | B10B7BB4 |
      3|
      0|
      1|
      10|
      0|
      1|
      0|
      2|

      3|
      0|
      1
      10|
      0|
      1|
      0|
      0|
      1|
      0|
      2|

      3|
      0|
      1
      11|
      0|
      0|
      1|
      0|
      2|

      3|
      0|
      1
      1|
      0|
      0|
      1|
      0|
      2|

      3|
      0|
      1
      1|
      0|
      0|
      1|
      0|
      2|

      100:71:C0:A8:01:0D | B10B7BB4|
      3|
      0|
      1|
      1|
      0|
      0|
      1|
      0|

      The following command can be used to display the cumulative and five second statistics and exception
      11
      10
      1
      10
```

counters of NSS with the LAG related info highlighted.

ap#show controllers nss stats

Sample Output:

NSS Statistics (Cumulative Total/Last 5 Seconds) Wired0 Port Statistics:

ID	:	0	TYPE	:	0
RX PKTS	:	616/13	TX PKTS	:	67115/66964
RX OCTETS	:	97862/1280	TX OCTETS	:	26832505/26785264
RX ERR	:	0/0	TX ERR	:	0/0
Wired1 Por	t Statisti	cs:			
ID	:	1	TYPE	:	0
RX PKTS	:	179/8	TX PKTS	:	44643/44629
RX OCTETS	:	18004/512	TX OCTETS	:	17853919/17851328
DV DDD		0 / 0			0.40
RX ERR	:	0/0	TX ERR	:	0/0

CAPWAP Port Statistics:

ID	:	34	TYPE	:	3
RX PKTS	:	3/0	TX PKTS	:	148850/148800
RX OCTETS	:	345/0	TX OCTETS	:	81851372/81840000
RX ERR	:	0/0	TX ERR	:	0/0
LAG Port S	tatistics:				
ID	:	33	TYPE	:	1
RX PKTS	:	448/22	TX PKTS	:	111634/111609
RX OCTETS	:	55786/1856	TX OCTETS	:	44650157/44643600
RX ERR	:	0/0	TX ERR	:	0/0
Wired0 Exc	eption Stat	istics:			

UNKNOWN	:	0/0
OUTER_MACSEC_MISSING	:	0/0
OUTER_MACSEC_BAD_SA	:	0/0
OUTER_MACSEC_FAILED	:	0/0
OUTER_VLAN_TAG_MISSING	:	0/0
OUTER_VLAN_PORT_BLOCK	:	0/0
OUTER_VLAN_ANY_BLOCK	:	0/0
OUTER_SANITY_FAILED	:	0/0
OUTER_DTLS_MISSING	:	0/0
OUTER_DTLS_UNEXPECTED	:	0/0
OUTER_DTLS_FAILED	:	0/0
INNER_SANITY_FAILED	:	0/0
OUTER_UCAST_DST_UKNOWN	:	0/0
OUTER_UCAST_BRIDGE_BLOCK	:	0/0
OUTER_UCAST_VLAN_BLOCK	:	0/0
OUTER_MCAST_TYPE_BLOCK	:	0/0
INNER_UCAST_DST_UKNOWN	:	0/0
INNER_UCAST_BLOCK	:	0/0
INNER_MGID_UNKNOWN	:	0/0
INNER_CAPWAP_ERROR	:	0/0
INNER_VLAN_TAG_BLOCK	:	0/0
INNER_UCAST_SRC_UNKNOWN	:	0/0
INNER_CAPWAP_REASM_FAILED	:	0/0

Wired1 Exception Statistics:

L

Γ

UNKNOWN	:	0/0
OUTER_MACSEC_MISSING	:	0/0
OUTER_MACSEC_BAD_SA	:	0/0
OUTER_MACSEC_FAILED	:	0/0
OUTER_VLAN_TAG_MISSING	:	0/0
OUTER_VLAN_PORT_BLOCK	:	0/0
OUTER_VLAN_ANY_BLOCK	:	0/0
OUTER_SANITY_FAILED	:	0/0
OUTER_DTLS_MISSING	:	0/0
OUTER_DTLS_UNEXPECTED	:	0/0
OUTER_DTLS_FAILED	:	0/0
INNER_SANITY_FAILED	:	0/0
OUTER_UCAST_DST_UKNOWN	:	0/0
OUTER_UCAST_BRIDGE_BLOCK	:	0/0
OUTER_UCAST_VLAN_BLOCK	:	0/0
OUTER_MCAST_TYPE_BLOCK	:	0 / 0
INNER_UCAST_DST_UKNOWN	:	0 / 0
INNER_UCAST_BLOCK	:	0 / 0
INNER_MGID_UNKNOWN	:	0 / 0
INNER_CAPWAP_ERROR	:	0 / 0
INNER_VLAN_TAG_BLOCK	:	0 / 0
INNER_UCAST_SRC_UNKNOWN	:	0 / 0
INNER_CAPWAP_REASM_FAILED	:	0 / 0
Decap Statistics:		
UC MGMT KEEPALIVE MC MC_OTHER	FWD0 FWD1 FWD	FAIL FALL THROUGH DROP
0 1 2 0 0	611 179 0	
Encap Statistics:		
-		
DATA MGMT KEEPALIVE FWD0 FWD1		
39993 5 2 125 1	1 0	

SNMP

The existing tables cLReapGroupConfigTable and cLReapGroupApConfigTable in CISCO-LWAPP-REAP_MIB would return the configuration of the default-flex-group and the joined APs respectively

Web Links

- Cisco WLAN Controller Information: http://www.cisco.com/c/en/us/products/wireless/4400-series-wireless-lan-controllers/index.html http://www.cisco.com/c/en/us/products/wireless/2000-series-wireless-lan-controllers/index.html
- Cisco NCS Management Software Information: http://www.cisco.com/c/en/us/products/wireless/prime-network-control-system-series-appliances/i ndex.html

- Cisco MSE Information: http://www.cisco.com/c/en/us/products/wireless/mobility-services-engine/index.html
- Cisco LAP Documentation: http://www.cisco.com/c/en/us/products/wireless/aironet-3500-series/index.html

Terminology

- APM—AP Manager Interface
- Dyn—Dynamic Interface
- Management—Management Interface
- Port—Physical Gbps port
- WiSM-2—Wireless Service Module
- AP—Access Point
- LAG—Link Aggregation
- SPAN—Switch Port Analyzer
- RSPAN—Remote SPAN
- VACL—VLAN Access Control List
- DEC—Distributed Etherchannel
- DFC—Distributed Forwarding Card
- OIR—Online Insertion and Removal
- VSL—Virtual Switch Link
- ISSU—In Service Software Upgrade
- MEC—Multichassis Ether Channel
- VSS—Virtual Switch System
- WCS—Wireless Control System
- NAM—Network Analysis Module

- IDSM—Intrusion Detection Service Module
- FWSM—Firewall Service Module
- STP—Spanning Tree Protocol
- VLAN—Virtual LAN
- SSO—Stateful Switchover
- WCP—Wireless Control Protocol
- WiSM-2—Wireless Service Module-2

FAQ

Q. If I configure LAPs at a remote location as FlexConnect, can I give those LAPs a primary and secondary controller?

Example: There is a primary controller at site A and a secondary controller at site B. If the controller at site A fails, the LAP does failover to the controller at site B. If both controllers are unavailable does the LAP fall into FlexConnect standalone mode?

- **A.** Yes. First the LAP fails over to its secondary. All WLANs that are locally switched have no changes, and all that are centrally switched just have the traffic go to the new controller. And, if the secondary fails, all WLANs that are marked for local switching (and open/pre-shared key authentication/you are doing AP authenticator) remain up.
- **Q.** How do access points configured in Local mode deal with WLANs configured with FlexConnect Local Switching?
- **A.** Local mode access points treat these WLANs as normal WLANs. Authentication and data traffic are tunneled back to the WLC. During a WAN link failure this WLAN is completely down and no clients are active on this WLAN until the connection to the WLC is restored.
- **Q.** Can I do web authentication with Local switching?
- **A.** Yes, you can have an SSID with web-authentication enabled and drop the traffic locally after web-authentication. Web-authentication with Local switching works fine.
- **Q.** Can I use my Guest-Portal on the Controller for an SSID, which is handled locally by the H REAP? If yes, what happens if I lose connectivity to the controller? Do current clients drop immediately?
- **A.** Yes. Since this WLAN is locally switched, the WLAN is available but no new clients are able to authenticate as the web page is not available. But, the existing clients are not dropped off.
- **Q.** Can FlexConnect certify PCI compliance?
- **A.** Yes. FlexConnect solution supports rogue detection to satisfy PCI compliance.

Cisco Support Community - Featured Conversations

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers. Below are just some of the most recent and relevant conversations happening right now.



Related Information

- HREAP Design and Deployment Guide
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Wireless Control System
- Cisco 3300 Series Mobility Services Engine
- Cisco Aironet 3500 Series
- Cisco Secure Access Control System
- Technical Support & Documentation Cisco Systems

I