配置获取与Dot1x的一Flexconnect AP Switchport

目录

简介

本文描述配置巩固FlexConnect访问接入点(AP)验证与Dot1x使用device-traffic-class=switch Radius VSA允许从本地交换的无线LAN的连接孔(WLAN)的流量。

先决条件

要求

Cisco 建议您了解以下主题：

- 在无线局域网控制器(WLC)的FlexConnect
- 在Cisco交换机的802.1x
- 网络边缘验证拓扑(整洁)

使用的组件

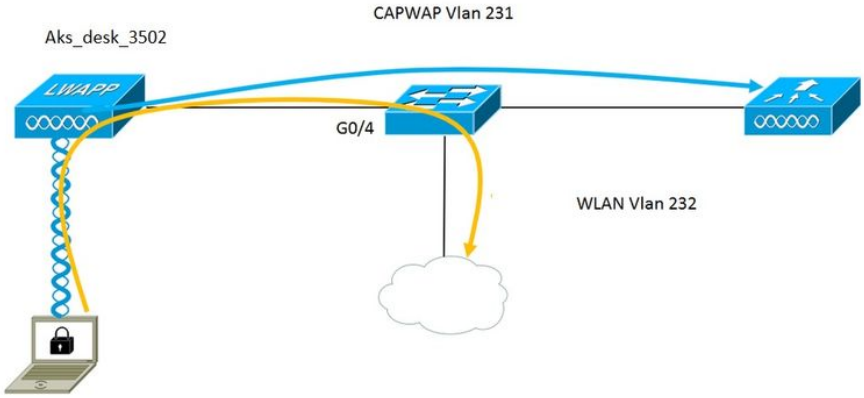
本文档中的信息基于以下软件和硬件版本：

- WS-C3560CX-8PC-S， 15.2(4)E1
- AIR-CT-2504-K9， 8.2.141.0
- 身份服务引擎(ISE) 2.0

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

配置

网络图



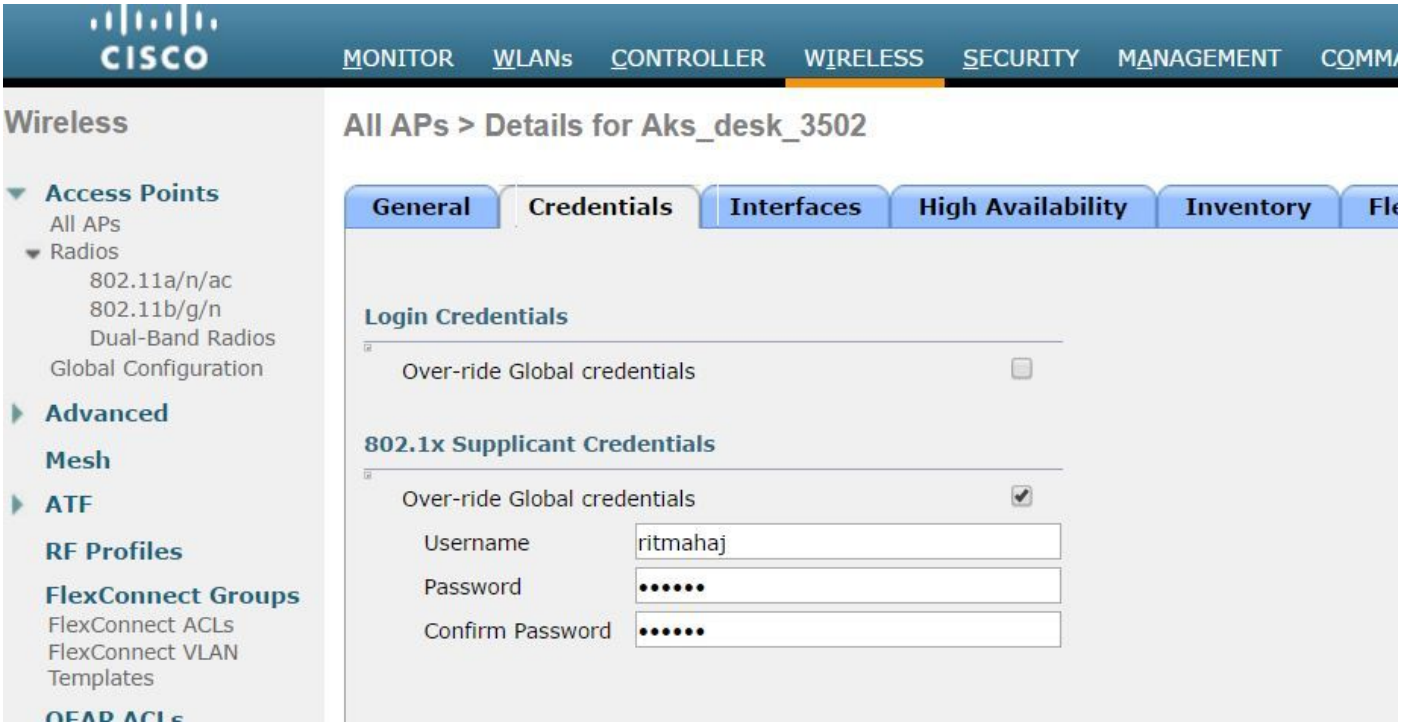
使用EAP-FAST，在设置接入点的这中作为802.1x请求方和由ISE的交换机验证。一旦端口为802.1x验证配置，交换机不允许任何流量除802.1x流量之外穿过端口，直到设备连接对端口成功验证。

一旦接入点利用ISE验证成功，交换机接收Cisco VSA属性“device-traffic-class=switch，并且自动地移动端口建立中继。

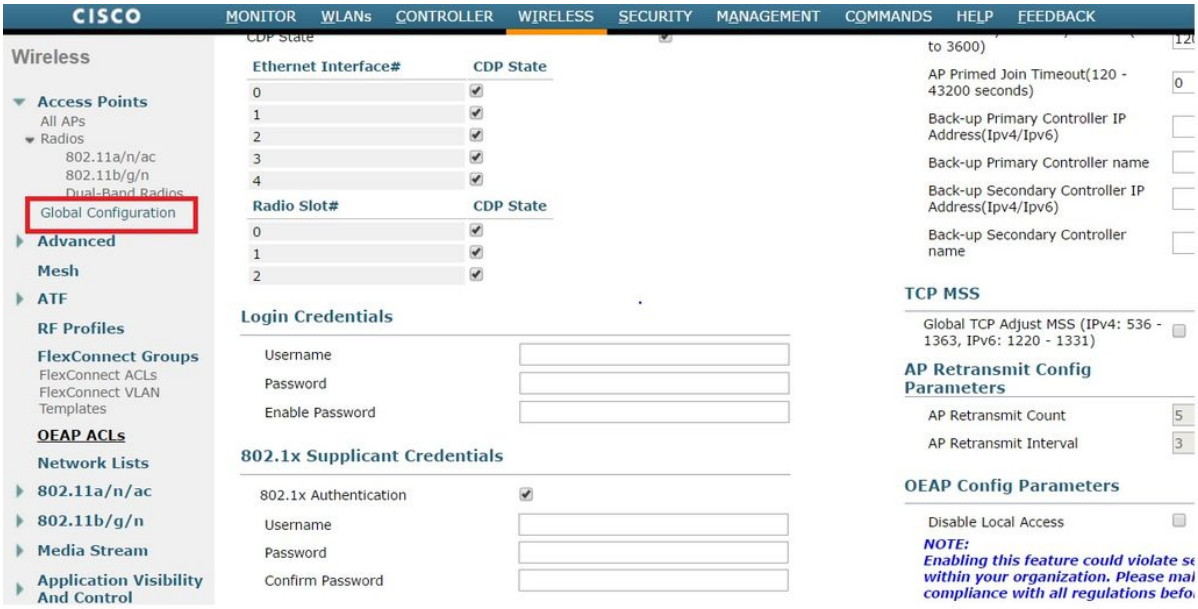
这意味着，如果AP支持FlexConnect模式和本地交换配置的Ssid，它能发送标记的数据流。保证VLAN支持在AP启用，并且正确本地VLAN配置。

AP配置：--

1. 如果AP已经加入对WLC，是Wireless选项卡并且点击接入点。是Credetials字段，并且nder朝向802.1x请求方的凭证，检查**改写全局凭证**方框设置此接入点的802.1x用户名和密码。



您能也设置加入对与全局配置菜单的WLC的所有接入点的一个comman用户名和密码。



2. 如果接入点未加入WLC，您必须控制到LAP设置凭证和使用此CLI命令：

LAP#debug capwap控制台cli
LAP#capwap ap dot1x用户名<username>密码<password>

交换机配置：--

1. 启用在交换机的dot1x全局并且添加ISE服务器交换

aaa new-model

!
aaa authentication dot1x default group radius

!
AAA授权网络默认组radius

!

dot1x系统验证控制

!

RADIUS服务器ISE
地址ipv4 10.48.39.161 auth端口1645 acct-port 1646
密钥7 123A0C0411045D5679

2. 现在请配置AP交换机端口

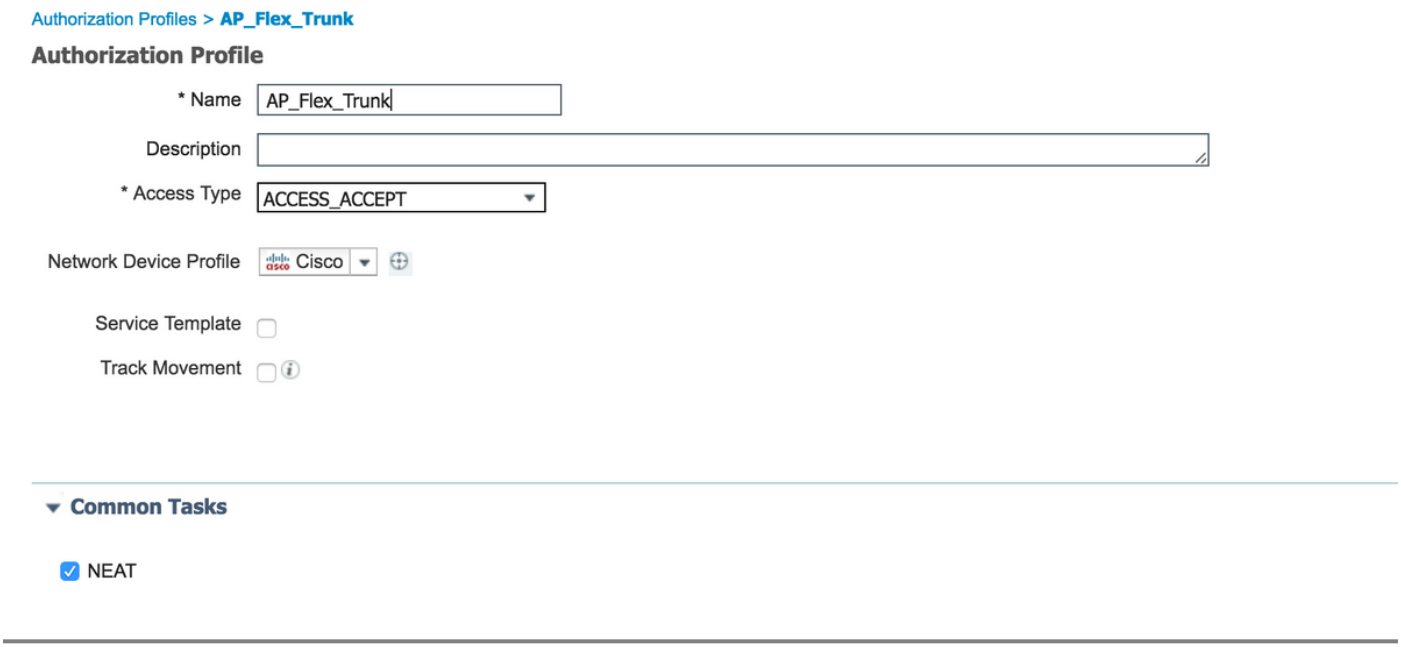
建立接口GigabitEthernet0/4
交换端口访问VLAN 231
交换端口Trunk允许VLAN 231,232
switchport mode access
shutdown
authentication host-mode多个主机
authentication order dot1x
验证波尔特控制自动
dot1x pae验证器
生成树Portfast边缘

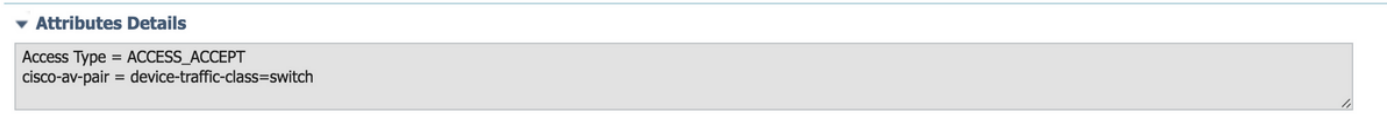
如果一要配置MAB而不是dot1x那么端口设置看起来象：--

接口GigabitEthernet0/4
交换端口访问VLAN 231
交换端口Trunk允许VLAN 231,232
switchport mode access
shutdown
authentication host-mode多个主机
authentication order mab
验证波尔特控制自动
mab
生成树Portfast边缘

ISE配置：--

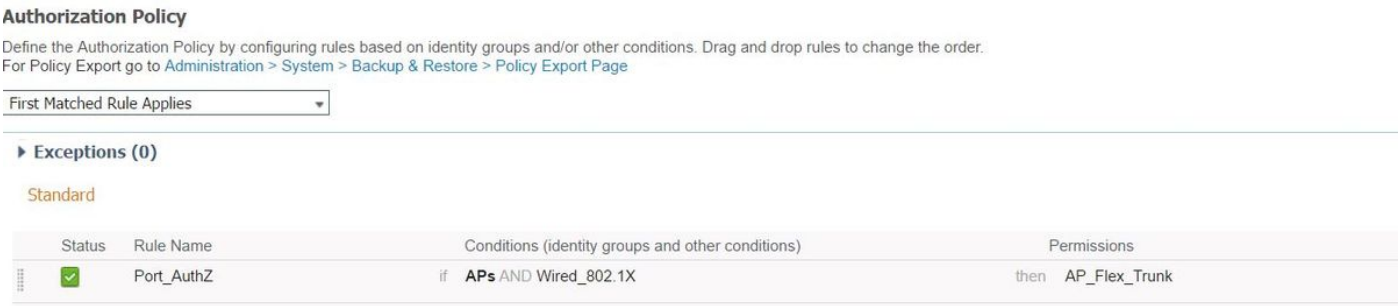
1. 在ISE，一个能启用整洁为AP授权配置文件为了设置正确属性，然而，在其他RADIUS服务器，您能手工配置。





2. 在ISE，一个也需要配置验证策略和授权策略。在这种情况下我们点击是有线dot.1x(wired MAB在MAB的情况下)的默认验证规则，但是一个能根据需求定制它。

关于授权策略(Port_AuthZ)，我们在这种情况下添加了AP凭证到用户组(AP)并且推送根据此(AP_Flex_Trunk)的授权配置文件。



验证

使用本部分可确认配置能否正常运行。

1. 在交换机上，能一次使用命令“debug authentication功能autocfg全部”检查端口是否被搬到中继端口。

二月20 12:34:18.119 ：%LINK-3-UPDOWN ：接口GigabitEthernet0/4的更改的状态
二月20 12:34:19.122 ：%LINEPROTO-5-UPDOWN ：在接口GigabitEthernet0/4的线路通信协议的更改的状态
akshat_sw#
akshat_sw#
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：在dot1x AutoCfg start_fn，epm_handle ：3372220456
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[588d.0997.061d， Gi0/4]设备类型=交

换机
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[588d.0997.061d， Gi0/4]新建的客户端
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[Gi0/4]内部Autocfg宏观应用程序状态：1
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[Gi0/4]设备类型：2
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[Gi0/4]自动设定：stp有port_config 0x85777D8
二月20 12:38:11.113 ：AUTH-FEAT-AUTOCFG-EVENT ：[Gi0/4]自动设定：stp port_config有BPDU guard_config 2
二月20 12:38:11.116 ：AUTH-FEAT-AUTOCFG-EVENT ：应用在端口的[Gi0/4]自动cfg。
二月20 12:38:11.116 ：AUTH-FEAT-AUTOCFG-EVENT ：[Gi0/4] VLAN ：231 VLAN Str ：231
二月20 12:38:11.116 ：AUTH-FEAT-AUTOCFG-EVENT ：应用dot1x_autocfg_supp宏的[Gi0/4]
二月20 12:38:11.116 ：应用命令…'在Gi0/4的没有交换端口访问VLAN 231'
二月20 12:38:11.127 ：应用命令…'没有switchport nonegotiate'在Gi0/4
二月20 12:38:11.127 ：应用命令…'switchport mode trunk'在Gi0/4
二月20 12:38:11.134 ：应用命令…'在Gi0/4的switchport trunk native vlan 231'
二月20 12:38:11.134 ：应用命令…'生成树Portfast中继'在Gi0/4
二月20 12:38:12.120 ：%LINEPROTO-5-UPDOWN ：在接口GigabitEthernet0/4的线路通信协议，下来的更改的状态
二月20 12:38:15.139 ：%LINEPROTO-5-UPDOWN ：在接口GigabitEthernet0/4的线路通信协议的更改的状态

2. 输出"show run int g0/4"显示端口更改到中继端口。

当前配置295个字节
!
接口GigabitEthernet0/4
交换端口Trunk允许VLAN 231,232,239
switchport trunk native vlan 231
switchport mode trunk
authentication host-mode多个主机
authentication order dot1x
验证波尔特控制自动
dot1x pae验证器
生成树Portfast边缘中继
末端

3. 在ISE，在Operations>>Radius Livelogs一下能是的验证成功的和推送的正确授权配置文件。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. 如果我们联络客户端，在这其MAC地址在客户端VLAN的232后AP交换机端口然后将学习。

akshat_sw#sh MAC地址表int g0/4
MAC 地址表

Vlan Mac Address Type Ports

231个588d.0997.061d静态Gi0/4 - AP
232个c0ee.fbd7.8824动态Gi0/4 -客户端

在WLC，在客户端详细信息能被看到此客户端属于VLAN 232，并且SSID本地交换。这是片断。

(思科控制器) >show客户端详细信息c0:ee:fb:d7:88:24
客户端MAC地址..... c0:ee:fb:d7:88:24
客户端用户名..... N/A
AP MAC地址..... b4:14:89:82:cb:90
AP名称.....Aks_desk_3502
AP无线电slot Id 1
客户端状态.....已关联
客户端用户用户组.....
客户端美洲台OOB状态.....访问
无线局域网Id 2
无线LAN网络名称(SSID) .....波尔特验证
无线局域网配置文件名称.....波尔特验证
热点(802.11u) .....不支持
BSSID b4:14:89:82:cb:9f
连接在..... 42秒
信道.....44
IP地址.....192.168.232.90
网关地址.....192.168.232.1
网络屏蔽.....255.255.255.0
关联Id 1
验证算法.....开放式系统
原因代码.....1
状态码.....0

FlexConnect数据交换.....本地
FlexConnect Dhcp状态.....本地
FlexConnect VLAN根据中央交换.....否
FlexConnect验证.....中央印制厂
FlexConnect中央关联.....否
FlexConnect VLAN名称..... VLAN 232
检疫VLAN 0
访问VLAN 232
本地桥接VLAN 232

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 如果验证发生故障，请使用**debug dot1x**， **debug authentication**发出命令。
- 如果端口没有移动建立Trunk，请输入**all命令debug authentication功能的autocfg**。
- 保证您安排多个主机模式(authentication host-mode多个主机)配置。多个主机必须启用为了允许客户端无线MAC地址。
- “AAA授权网络” should命令配置为了交换机能接受和适用ISE发送的属性。