

配置轻量级接入点作为802.1x请求方

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置](#)

[配置LAP](#)

[配置交换机](#)

[配置ISE服务器](#)

[验证](#)

[故障排除](#)

简介

本文描述如何配置一轻量级接入点(LAP)，当802.1x请求方为了验证身份服务引擎(ISE)服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- 无线局域网控制器(WLC)和LAP
- 在Cisco交换机的802.1x
- ISE
- 可扩展的认证协议(EAP) -灵活验证通过获取建立隧道(法塞特)

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
- 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。

背景信息

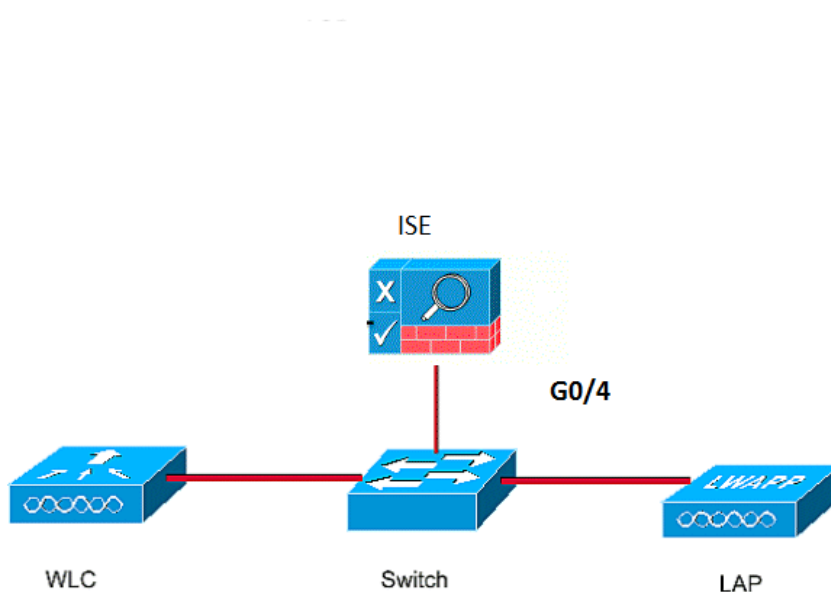
在设置接入点(AP)的这中作为802.1x请求方和由以匿名受保护的访问凭证ISE的交换机验证(PAC)设置使用EAP-FAST。一旦端口为802.1x验证配置，交换机不允许任何流量除802.1x流量之外穿过端口，直到设备连接对端口成功验证。AP可以验证或者，在加入WLC前或，在加入WLC后，在您配置在交换机情况下的802.1x，在LAP加入WLC后。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



配置

本文使用这些IP地址：

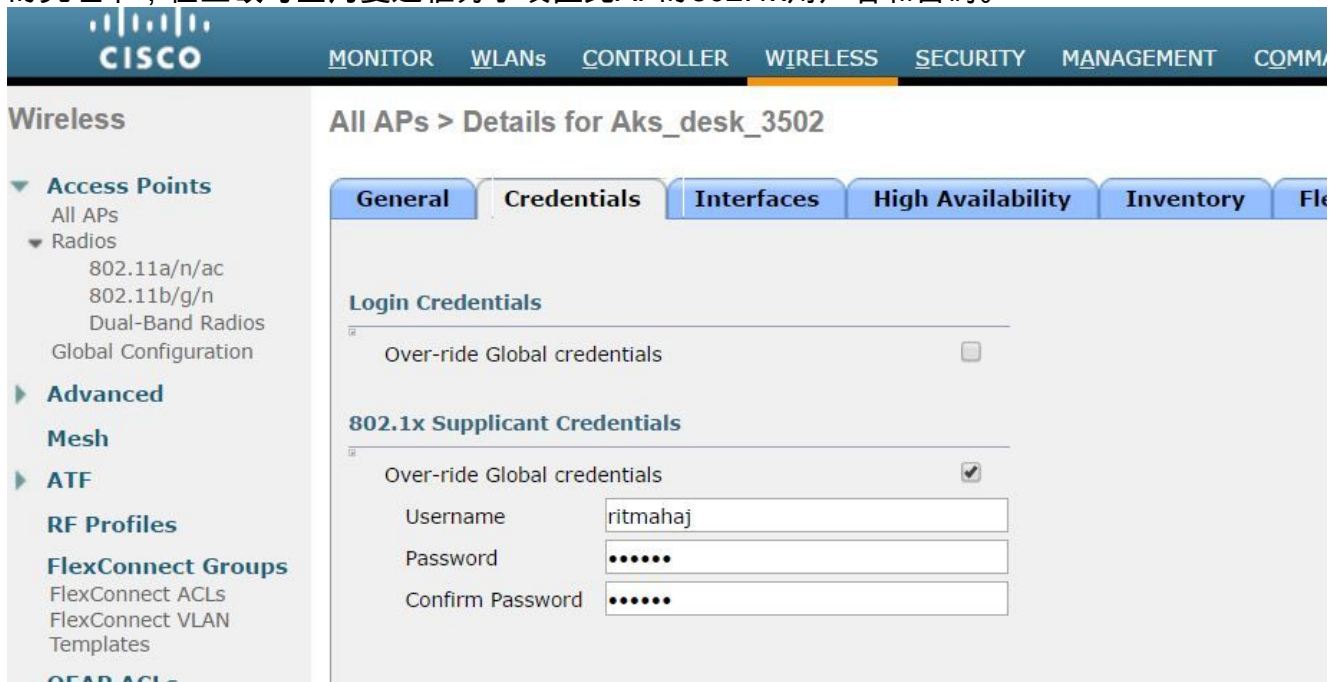
- 交换机的IP地址是10.48.39.141
- ISE服务器的IP地址是10.48.39.161
- WLC的IP地址是10.48.39.142

配置LAP

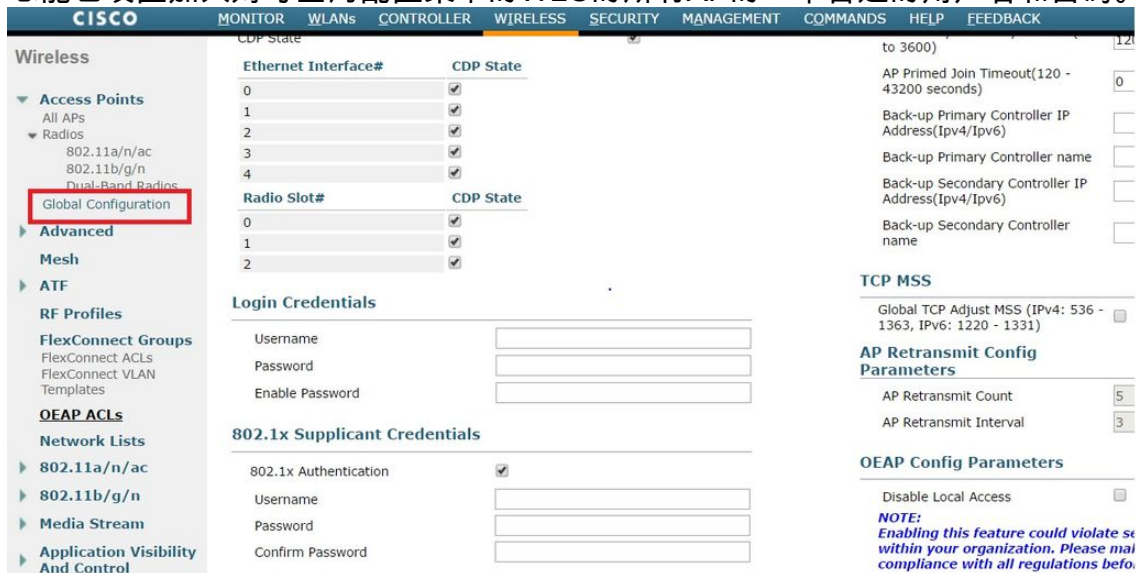
在此部分，您提交以信息配置LAP作为802.1x请求方。

1. 如果AP已经加入对WLC，是Wireless选项卡并且点击AP，去凭证字段和在朝向802.1x请求方

的凭证下，检查改写全局复选框为了设置此AP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AP的一个普通的用户名和密码。



2. 如果AP未加入WLC，您必须控制到LAP为了设置凭证和使用这些CLI命令：

```
LAP#debug capwap console cli
```

```
LAP#capwap ap dot1x username <username> password <password>
```

配置交换机

1. 启用在交换机的dot1x全局并且添加ISE服务器到交换机。

```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
```

```
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
```

2. 现在，请配置AP交换机端口。

```
interface GigabitEthernet0/4
```

```
switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

配置ISE服务器

1. 添加交换机作为ISE服务器的一个验证、授权和统计(AAA)客户端。

The screenshot shows the 'Network Devices' configuration page in Cisco ISE. The 'Name' field is set to 'akshat_sw'. The 'IP Address' field is set to '10.48.39.141 / 32'. The 'Device Profile' is set to 'Cisco'. The 'RADIUS Authentication Settings' section is expanded, showing 'Enable Authentication Settings' checked, 'Protocol' set to 'RADIUS', and a 'Shared Secret' field with a masked password.

| Name | IP/Mask | Profile Name | Location | Type |
|-----------|-----------------|--------------|---------------|------------------|
| GurpWLC1 | 10.48.39.155/32 | Cisco | All Locations | All Device Types |
| GurpWLC2 | 10.48.39.156/32 | Cisco | All Locations | All Device Types |
| akshat_sw | 10.48.39.141/32 | Cisco | All Locations | All Device Types |

2. 在ISE，请配置验证策略和授权策略。在这种情况下，是有线dot.1x使用的默认验证规则，但是一个能根据需求定制它。

Identity Services Engine Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

| | | |
|-------------------------------------|----------------------------|---|
| <input checked="" type="checkbox"/> | MAB | : If Wired_MAB OR Wireless_MAB |
| <input checked="" type="checkbox"/> | Default | :use Internal Endpoints |
| <input checked="" type="checkbox"/> | Dot1X | : If Wired_802.1X OR Wireless_802.1X |
| <input checked="" type="checkbox"/> | Default | :use All_User_ID_Stores |
| <input checked="" type="checkbox"/> | Default Rule (If no match) | : Allow Protocols : Default Network Access and use : All_User_ID_Stores |

保证在默认网络网络访问， EAP-FAST允许的允许协议。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allow EAP-FAST

EAP-FAST Inner Methods

- Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
- Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
- Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Use PACs Don't Use PACs
 - Tunnel PAC Time To Live
 - Proactive PAC update will occur after % of PAC Time To Live has expired
 - Allow Anonymous In-Band PAC Provisioning
 - Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning

- 关于授权策略(Port_AuthZ)， AP凭证在这种情况下被添加了到用户组(AP)。使用的情况是“如果用户属于组AP和执行有线dot1x，然后推送默认授权配置文件permit访问”。再次，这可以根据需求定制。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

+ Create a New Rule

Standard

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|--------|------------|---|-------------------|
| ✓ | Port_AuthZ | if APs AND Wired_802.1X | then PermitAccess |

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > APs

Identity Group

Name: APs

Description: Credentials for APs

Save Reset

Member Users

Users Selected 0 | Total 1

+ Add - Delete Show All

| Status | Email | Username | First Name | Last Name |
|-----------|-------|----------|------------|-----------|
| ✓ Enabled | | ritmahaj | | |

验证

使用本部分可确认配置能否正常运行。

一旦802.1x在交换机端口启用，所有流量，除了802.1x流量通过端口阻塞。LAP，如果已经注册对WLC，获得不相关。在一成功的802.1x验证之后是通过通过的其他允许的流量。LAP的成功的注册对WLC的，在802.1x在交换机后启用表明LAP验证是成功的。如果LAP验证，您能也使用这些方法为了验证。

1. 在交换机上，如果端口验证，请输入其中一显示命令为了验证。

```
akshat_sw#show dot1x interface g0/4
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details
```

```
Dot1x Info for GigabitEthernet0/4
-----
```

```
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

Dot1x Authenticator Client List

```
-----
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
```

akshat_sw#show authentication sessions

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. 在ISE，请选择操作> Radius Livelogs并且请参阅验证是成功的，并且正确授权配置文件推送

The screenshot shows the Cisco Identity Services Engine (ISE) interface for Radius Livelogs. The top navigation bar includes 'Identity Services Engine', 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below the navigation bar, there are several status indicators: 'Misconfigured Supplicants: 0', 'Misconfigured Network Devices: 0', 'RADIUS Drops: 0', 'Client Stopped Responding: 3', and 'Repeat Counts: 0'. The main content area displays a table of live sessions with columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, and Authorization Profiles. Two sessions are listed, both with a status of 'All' and a repeat count of 1. The first session occurred at 2017-03-09 10:32:28.956 and the second at 2017-03-09 10:31:29.227. Both sessions are for user 'ritmahaj' with endpoint ID '58:8D:09:97:06:1D' and are using 'Cisco-Device' as the endpoint profile. The authentication policy is 'Default >> Dot1X >> Default' and the authorization policy is 'Default >> Port_AuthZ'.

| Time | Status | Details | Repeat Count | Identity | Endpoint ID | Endpoint Profile | Authentication Policy | Authorization Policy | Authorization Profiles |
|-------------------------|--------|---------|--------------|----------|-------------------|------------------|-----------------------------|-----------------------|------------------------|
| 2017-03-09 10:32:28.956 | All | | 1 | ritmahaj | 58:8D:09:97:06:1D | Cisco-Device | Default >> Dot1X >> Default | Default >> Port_AuthZ | PermitAccess |
| 2017-03-09 10:31:29.227 | All | | 1 | ritmahaj | 58:8D:09:97:06:1D | Cisco-Device | Default >> Dot1X >> Default | Default >> Port_AuthZ | |

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1. 输入ping命令为了检查ISE服务器是否从交换机是可达的。
2. 确保交换机配置作为ISE服务器的一个AAA客户端。
3. 保证共享机密是相同的在交换机和ACS服务器之间。
4. 检查EAP-FAST是否在ISE服务器启用。
5. 检查802.1x凭证是否为LAP配置并且是同样在ISE服务器。 Note:用户名和密码区分大小写。
6. 如果验证发生故障，请输入这些on命令交换机： debug dot1x和debug authentication。