与NGWC和ACS 5.2配置示例的动态VLAN分配

目录

简介

本文描述动态VLAN分配的概念。它也描述如何配置无线局域网控制器(WLC)和RADIUS服务器为了动态地分配无线局域网(WLAN)客户端到特定VLAN。在本文中，RADIUS服务器是访问控制服务器(ACS)该运行思科安全访问控制系统版本5.2。

先决条件

要求

Cisco 建议您了解以下主题：

- WLC和轻量级接入点(拉普)的基础知识
- 验证、授权和统计(AAA)服务器的功能知识
- 全面了解无线网络和无线安全问题

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科5760有Cisco IOS XE软件版本3.2.2 (下一代配线间或者NGWC的)无线局域网控制器
- Cisco Aironet 3602系列轻量级接入点
- 有英特尔Proset请求方的Microsoft Windows XP
- 思科安全访问控制系统版本5.2
- Cisco Catalyst 3560系列交换机

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

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数 WLAN 系统中，每个 WLAN 都有适用于与服务集标识符 (SSID) 关联的所有客户端的静态策略，即以控制器术语表示 WLAN。虽然此方法功能强大，但也具有局限性，这是因为，它要求客户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

然而，Cisco WLAN 解决方案支持网络标识。这允许网络通告单个SSID，但是允许特定用户继承另外QoS、VLAN根据用户凭证的属性，并且/或者安全策略。

动态 VLAN 分配便是一项这样的功能，它根据无线用户提供的凭证将该用户置于特定 VLAN 中。用户分配此任务对特定VLAN的由一个RADIUS验证服务器处理，例如Cisco Secure ACS。此功能可以用于，例如，为了允许无线主机在和一样在园区网络内移动的VLAN。

结果，当客户端尝试联合到注册的LAP用控制器时， LAP通过用户的凭证到验证的RADIUS服务器。成功执行身份验证后，RADIUS 服务器便会将某些 Internet 工程任务组 (IETF) 属性传递给用户。这些 RADIUS 属性确定应该分配给无线客户端的 VLAN ID。客户端(WLAN的SSID，根据WLC)不重要，因为用户总是分配到此预先确定的VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括：

- IETF 64 (隧道类型) -对VLAN的集。
- IETF 65 (通道媒体类型) -集到802。
- IETF 81 (隧道专用组ID) -对VLAN ID的集。

VLAN ID是12个位并且占用值在1和4094之间，包括。由于隧道专用组ID是类型字符串，如对RFC 2868定义，隧道协议支持的RADIUS属性为了用在IEEE 802.1X上， VLAN ID整数值编码作为字符串。当发送这些隧道属性时，需要填写 Tag 字段。

如 RFC2868 的 3.1 部分中所述：

“标记字段是一个八位字节和打算提供分组在参考同一个通道的同一数据包的属性方法”。

标记字段的有效值是0x01通过0x1F，包括。如果未使用 Tag 字段，则它一定为零 (0x00)。有关所有 RADIUS 属性的详细信息，请参阅 RFC 2868。

配置

动态VLAN分配的配置包括两不同步骤：

1. 配置WLC与命令行界面(CLI)或与GUI。
2. 配置 RADIUS 服务器。

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

网络图

本文档使用以下网络设置：

本文以Protected Extensible Authentication Protocol (PEAP)使用802.1X作为安全机制。

假定

- 交换机为所有第3层(L3) VLAN配置。
- DHCP服务器分配DHCP范围。
- L3连接存在网络的所有设备之间。
- LAP已经加入对WLC。
- 每个VLAN有一/24掩码。
- ACS 5.2有安装的一自签名证书。

配置与CLI的WLC

配置WLAN

这是示例如何配置与DVA SSID的一WLAN ：

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
 security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

配置在WLC的RADIUS服务器

这是RADIUS服务器的配置的示例在WLC的：

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123
```

```
dot1x system-auth-control
```

配置客户端的VLAN DHCP池

这是DHCP池的配置的示例客户端VLAN 30和VLAN的40 ：

```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
 network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

配置与GUI的WLC

配置WLAN

此步骤描述如何配置WLAN。

1. 导航对**Configuration>无线> WLAN** >NEW选项卡。

2. 点击**常规选项卡**为了发现WLAN为WPA2-802.1X配置和映射接口/Interfrace组(G)到VLAN 20 (**VLAN0020**)。

3. 点击**高级选项卡。** ，并且检查**允许AAA覆盖**复选框。必须启用覆盖为了此功能能工作。

4. 点击**安全选项卡，**并且**Layer2**选项卡，检查WPA2加密**AES**复选框和挑选**802.1x**从验证密钥Mgmt下拉列表。

配置在WLC的RADIUS服务器

此步骤描述如何配置在WLC的RADIUS服务器。

1. 导航对**Configuration>安全选项卡**。

2. 导航对**AAA** >Server **Groups> Radius**为了创建RADIUS服务器组。在本例中， RADIUS服务器组呼叫ACS。

3. 编辑RADIUS服务器条目为了添加服务器IP地址和共享塞克雷。这共享的塞克雷必须匹配WLC和RADIUS服务器的共享塞克雷。

   这是完整的配置的示例：

配置RADIUS服务器

此步骤描述如何配置RADIUS服务器。

1. 在RADIUS服务器上，请导航给**用户，并且标识存储>内部标识存储>** Users。
2. 创建适合的用户名和标识组。在本例中，它是学员和所有组：学员和教师和AllGroups ：教师。

3. 导航对**策略元素>授权和权限>网络访问>授权配置文件**，并且创建AAA覆盖的授权配置文件。

4. 编辑学员的授权配置文件。

5. 设置VLAN ID/Name作为与值的**静态30** (VLAN 30)。

6. 编辑教师的授权配置文件。

7. 设置VLAN ID/Name作为与值的**静态40** (VLAN 40)。

8. 导航对**访问策略**>Access **Services>默认网络网络访问**，并且点击**允许Protocols选项**。检查**允许PEAP**复选框。

9. 导航对**标识**，并且定义规则为了允许PEAP用户。

10. 导航对**授权**，并且映射学员和教师对授权策略;在本例中，映射应该是VLAN 30和教师的学员VLAN的40。

验证

使用本部分可确认配置能否正常运行。这些是验证进程：

- 监控显示在ACS的页哪些客户端验证。
- 连接对与学生团体的DVA WLAN，并且查看客户端WiFi连接工具。
- 连接对与教师组的DVA WLAN，并且查看客户端WiFi连接工具。

故障排除

本部分提供的信息可用于对配置进行故障排除。

> 注意：
>
> 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。
>
> 命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。
>
> 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

有用的调试包括**调试客户端MAC地址***mac*，以及这些NGWC trace发出命令：

- **集合trace组无线客户端级别调试**
- **集合trace组无线客户端过滤器mac** *xxxx.xxxx.xxxx*
- **显示trace SYS已过滤跟踪**

NGWC trace不包括dot1x/AAA，因此请使用复合跟踪此整个列表dot1x/AAA ：

- **设置trace组无线客户端级别调试**
- **设置trace wcm-dot1x事件级别调试**
- **设置trace wcm-dot1x aaa级别调试**
- **设置trace aaa无线事件级别调试**
- **设置trace访问会话核心sm级别调试**
- **设置trace访问会话方法dot1x级别调试**
- **设置trace组无线客户端过滤器mac** *xxxx.xxxx.xxxx*
- **设置trace wcm-dot1x事件过滤器mac** *xxxx.xxxx.xxxx*
- **设置trace wcm-dot1x aaa过滤器mac** *xxxx.xxxx.xxxx*
- **设置trace aaa无线事件过滤器mac** *xxxx.xxxx.xxxx*
- **设置trace访问会话核心sm过滤器mac** *xxxx.xxxx.xxxx*
- **设置trace访问会话方法dot1x过滤器mac** *xxxx.xxxx.xxxx*
- **显示trace SYS已过滤跟踪**

当动态VLAN分配正确地时工作，您应该看到从调试的此种输出：

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf:  intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
 --More--         [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station  ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
   MAC:  0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

 --More--         [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
```

Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030'
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0

[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
 --More--   [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761
Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf:
VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for
station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
**   vlanIfName: 'VLAN0040', aclName: ''**

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct
for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override
into chain for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''
 --More--
[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy
from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)