与RADIUS服务器ACS 5.2和WLC配置示例的动态VLAN分配

目录

简介

本文档介绍了动态 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-该的访问控制服务器(ACS)运行版本5.2 -为了动态地分配无线局域网(WLAN)客户端到特定VLAN。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 有WLC和轻量级接入点(拉普)的基础知识
- 有AAA服务器的一功能知识
- 有无线网络和无线安全安全性问题一详尽的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本7.0.220.0的思科5508 WLC
- Cisco 3502系列LAP
- 与Intel 6300-N驱动版本14.3的Microsoft Windows 7本地请求方
- 运行版本5.2的Cisco Secure ACS
- Cisco 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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

动态VLAN分配用RADIUS服务器

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。这项将用户分配到特定 VLAN 的任务由 RADIUS 身份验证服务器（如 Cisco Secure ACS）处理。例如，利用此任务可使无线主机能够在园区网络中移动时保持位于同一 VLAN 中。

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。客户端的 SSID（WLAN，从 WLC 的角度而言）并不重要，这是因为，会始终为用户分配此预先确定的 VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括：

- IETF 64 (隧道类型) -设置此为**VLAN**。
- IETF 65 (通道媒体类型) -设置此对**802**。
- IETF 81 (通道私有Group ID) -设置此为VLAN ID。

VLAN ID 为 12 位，并且其值介于 1 和 4094 之间（包含 1 和 4094）。由于隧道专用组 ID 属于字符串类型（如用于 IEEE 802.1X 的 RFC2868 中所定义），因此，VLAN ID 整数值被编码为字符串

。 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： **Tag 字段在长度上是一个八位组，它旨在提供一种方法将同一数据包中表示同一隧道的属性进行分组。**此字段的有效值是 0x01 到 0x1F（包含 0x01 和 0x1F）。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

本部分提供有关如何配置本文档所述功能的信息。

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：

下面是此图中使用的组件的配置详细信息：

- ACS (RADIUS)服务器的IP地址是192.168.150.24。
- WLC的管理和Ap-manager接口地址是192.168.75.44。
- DHCP服务器寻址192.168.150.25。
- VLAN 253和VLAN 257使用在此配置中。Student-1为放置配置到VLAN 253，并且Teacher-1为放置配置到VLAN 257由RADIUS服务器，当两个用户连接对同样SSID “goa”时。VLAN 253：192.168.153.x/24.网关：192.168.153.1VLAN 257 ：192.168.157.x/24.网关：192.168.157.1VLAN 75 ：192.168.75.x/24.网关：192.168.75.1
- 本文以PEAP使用802.1x作为安全机制。**注意：** Cisco 建议您使用高级身份验证方法（如 EAP-FAST 和 EAP-TLS 身份验证）来保护 WLAN 的安全。

假定

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

配置步骤

此配置被分离到三个高层次步骤：

1. 配置 RADIUS 服务器。
2. 配置WLC。
3. 配置无线客户端工具。

配置 RADIUS 服务器

RADIUS服务器的配置分开成四个步骤：

1. Configure network资源。
2. 配置用户。
3. 定义策略元素。
4. 运用访问策略。

ACS 5.x是一个基于策略的访问控制系统。即ACS 5.x使用一个基于规则的策略型号而不是用于4.x版本的基于组的型号。

更加强大ACS 5.x基于规则的策略型号的提供和灵活访问控制与更旧的基于组的方法比较。

在更旧的基于组的型号中，因为包含并且配合信息的三种类型组定义了策略：

- 身份信息-此信息在AD或LDAP组中可以根据会员或内部ACS用户的一个静态分配。
- 其他限制或情况-时间限制，设备限制，等等。
- 权限- VLAN或Cisco IOS权限级别。

ACS 5.x策略型号根据表的规则：

- 如果情况然后发生

例如，我们使用描述的信息基于组的型号：

- 如果标识条件，限制条件然后授权配置文件。

结果，这提供我们灵活性在什么情况下限制用户允许访问网络以及什么授权级别允许，当特定情况符合时。

Configure network资源

此过程说明如何在 RADIUS 服务器上将 WLC 添加为 AAA 客户端，以便 WLC 可以将用户凭证传递到 RADIUS 服务器。

完成这些步骤：

1. 从ACS GUI，请去**网络资源>网络设备组>位置**，并且单击**创建**(在底部)。
2. 添加必填字段，并且单击**提交**。您当前将看到此屏幕：
3. 点击**设备类型>创建**。
4. 单击 **submit**。您当前将看到此屏幕：
5. 去**网络资源>网络设备和AAA客户端**。
6. 单击**创建**，并且填写详细信息如显示此处：
7. 单击 **submit**。您当前将看到此屏幕：

配置用户

在此部分，您将创建ACS的本地用户(Student-1和Teacher-1)。Student-1分配到“学员”组，并且Teacher-1分配到“教师”组。

1. 去**用户，并且标识存储>标识Groups>创建**。
2. 一旦单击请**提交**，页如下所示：：
3. 创建并且分配用户Student-1和Teacher-1到他们的各自的组。
4. 点击**用户，并且标识存储>标识Groups>用户>创建**。

5. 同样地，请创建Teacher-1。屏幕如下所示：：

定义策略元素

完成这些步骤为了定义用户的IETF属性：

1. 去**策略元素>授权，并且权限>网络访问>授权Profiles>创建。**
2. 从共同性任务选项卡：
3. 添加这些IETF属性：隧道类型= 64 = VLANTunnel-Medium-Type=802隧道专用组ID = 253 (Student-1)和257 (Teacher-1)对于组学员：对于组教师：
4. 一旦两个属性被添加，屏幕如下所示：：

运用访问策略

完成这些步骤为了选择将使用哪些认证方法，并且规则如何将配置(基于上一个步骤)：

1. 去**访问策略>**Access **Services>默认网络网络访问>** Edit **：“默认网络网络访问”。**
2. 选择EAP方法您类似将验证的无线客户端。在本例中，我们使用**PEAP- MSCHAP-V2。**
3. 单击 **submit。**
4. 验证您选择的标识组。在本例中，我们使用**内部用户**，我们在ACS创建。保存更改。
5. 为了验证授权配置文件，请去**访问策略>**Access **Services>默认网络网络访问>授权。**您能在什么情况下定制您将提供对网络的用户访问，并且什么授权配置文件(属性)您将通过一次已验证。此粒度只是可用的在ACS5.x。在本例中，我们选择**位置、设备类型、协议、标识组**和**EAP验证方法。**
6. 点击OK键，并且**保存更改。**
7. 下一步是创建规则。如果规则没有定义，客户端允许访问，不用任何情况。单击**创建> Rule-1。**此规则是为Student-1。
8. 同样地，请创建Teacher-1的一个规则。点击**Save Changes。**屏幕如下所示：：
9. 我们当前将定义服务选择规则。请使用此页为了配置一项简单或基于规则的策略确定适用的哪服务于流入请求。在本例中，使用一项基于规则的策略。

配置 WLC

此配置要求执行下列步骤：

1. 配置与认证服务器的详细信息的WLC。
2. 配置动态接口(VLAN)。
3. 配置WLAN (SSID)。

用身份验证服务器的详细信息配置 WLC

配置WLC是必要的，因此它能通信以RADIUS服务器为了验证客户端，并且为所有其他处理。

完成这些步骤：

1. 从控制器 GUI 中，单击 **Security。**
2. 输入 RADIUS 服务器的 IP 地址以及在 RADIUS 服务器和 WLC 之间使用的共享密钥。此共享密钥应该是相同的象在RADIUS服务器配置的那个。

配置动态接口 (VLAN)

此步骤描述如何配置在WLC的动态接口。如本文档中上文所述，WLC 中也必须具有在 RADIUS 服务器的 Tunnel-Private-Group ID 属性下指定的 VLAN ID。

在示例中， Student-1指定有**组标识253 (VLAN =253)**在RADIUS服务器。同样地， Teacher-1指定有**组标识257 (VLAN =257)**在RADIUS服务器。请参阅IETF RADIUS属性部分User Setup窗口。

完成这些步骤：

1. 动态接口从控制器GUI配置，在**Controller>接口**窗口。
2. 单击 **Apply**。这把您带到Edit窗口此动态接口(VLAN 253此处)。
3. 输入此动态接口的 IP 地址和默认网关。
4. 单击 **Apply**。
5. 同样地，我们将创建VLAN的257一个动态接口Teacher-1的。
6. 配置的配置接口如下所示：：

配置 WLAN (SSID)

完成这些步骤为了配置在WLC的WLAN ：

1. 从控制器GUI，请去**WLAN >创建新**为了创建一新的WLAN。此时会显示 New WLANs 窗口。
2. 输入 WLAN ID 和 WLAN SSID 信息。您能输入所有名称作为WLAN SSID。此示例使用**goa**作为WLAN SSID。
3. 单击**应用**为了去到Edit窗口WLAN goa。
4. 启用在控制器的**允许AAA覆盖**选项每WLAN的(SSID)配置。WLAN的允许AAA覆盖选项允许您配置标识网络的WLAN。它允许您应用VLAN标记、QoS和ACL对根据从AAA服务器的返回的RADIUS属性的各自的客户端。在本例中，它用于为了分配VLAN到客户端。大多数允许的AAA覆盖配置执行在RADIUS服务器。启用此参数允许控制器接受RADIUS服务器返回的属性。控制器然后适用这些属性给其客户端。**注意：** 当接口组被映射对WLAN时，并且客户端连接对WLAN，客户端在循环方式没获得IP地址。不支持与接口组的AAA覆盖。

配置无线客户端工具

在我们的测试客户端，我们以运行14.3驱动版本的英特尔6300-N卡使用Windows 7本地请求方。推荐使用从供应商的最新的驱动程序测试。

完成这些步骤为了创建在Windows的一配置文件零设置(WZC) ：

1. 去**Control Panel > Network，并且互联网>管理无线网络**。
2. 点击**Add选项**。
3. 单击**手工创建网络配置文件**。
4. 添加详细信息如配置在WLC。**注意：** SSID区分大小写。
5. 单击 **Next**。
6. 点击**崔凡吉莱连接设置**为了复核设置。
7. 在本例中，我们不验证服务器证书。如果检查此方框并且不能连接，尝试再禁用功能和测验。
8. 或者，您能使用您的Windows凭证为了登陆。然而，在本例中我们不使用那。单击 **Ok**。
9. 点击**先进的设置**为了配置用户名和密码。

10. 一旦完成测试Student-1，请测试Teacher-1。单击 **Ok**。

您的客户端工具当前准备连接。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

验证Student-1

从WLC GUI，请去**监视器>客户端**，并且选择MAC地址。

WLC RADIUS统计：

```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

ACS日志：

1. 完成这些步骤为了查看命中数计数：如果在15分钟检查日志验证内，请确保您刷新命中数计数。您有**命中数计数的**一选项卡在同一个页底端。
2. 点击**监听，并且报告**和一新的弹出窗口发表。去**认证– Radius –今天**。您能也单击服务选择规则应用的**详情**为了验证。

验证Teacher-1

从WLC GUI，请去**监视器>客户端**，并且选择MAC地址。

ACS日志：

1. 完成这些步骤为了查看命中数计数：如果在15分钟检查日志验证内，请确保您刷新HIT计数。您有**命中数计数的**一选项卡在同一个页底端。
2. 点击**监听，并且报告**和一新的弹出窗口发表。去**认证– Radius –今天**。您能也单击服务选择规则应用的**详情**为了验证。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

1. 如果遇到任何问题，请发出这些on命令WLC ：**调试客户端*<mac添加client>*debug aaa all enable显示客户端详细信息*<mac addr>*** -验证Policy Manager状态。**show radius auth statistics** -验证失败原因。**调试禁用所有**-关闭调试。**清除**在WLC的**stats radius验证全**清楚radius统计信息。
2. 验证登录ACS并且注释失败原因。

相关信息

- **与RADIUS服务器ACS 4.1和无线局域网控制器配置示例的动态VLAN分配**
- **技术支持和文档 - Cisco Systems**