目录

简介

本文包括有线的访客访问功能的部署在作为一个外国锚点和Cisco 5760 WLC作为一个访客锚点在非敏感区域的Cisco 5760无线局域网控制器(WLC)的(DMZ)有版本03.03.2.SE发行软件的。相似地功能工作在作为一个外国控制器的思科Catalyst 3650交换机。

今天，解决方案为访客访问通过无线和有线网络提供在思科5508 WLC的存在。在企业网络中，典型地有需要提供网络访问对于其访客在校园。访客访问需求包括Internet连接或其他有选择性的企业资源提供给有线和无线访客在一个一致和管理的方式。同样WLC在校园可以用于提供存取对于访客两个类型。由于安全原因，很大数量的企业网络管理员分离访客访问到DMZ控制器通过隧道。访客访问解决方案也使用作为fallback方法出故障dot1x和

来宾用户连接到一台接入层交换机的指定有线的端口访问的和或者也许做通过Web同意或Web认证模式，从属在安全需求(在后面的章节的详细信息)。一旦访客验证成功，访问提供给网络资源，并且访客控制器管理客户端的流量。外国锚点是客户端为网络访问连接的主要的交换机。它启动隧道请求。访客锚点是客户端实际上获得停住的交换机。除Cisco 5500系列WLAN控制器外， Cisco 5760 WLC可以使用作为访客锚点。在访客访问功能设置前，必须有移动性通道设立在外国锚点和访客锚点交换机之间。访客访问功能为MC (外国锚点)运作>> MC (访客锚点)和MA (外国锚点) >>MC (访客锚点)型号。外国锚点交换机中继配线访客流量到访客锚点控制器，并且多个访客锚点可以为负载均衡配置。客户端停住到DMZ锚点控制器。它也处理DHCP IP地址客户端的分配以及验证。在验证完成后，客户端能访问网络。

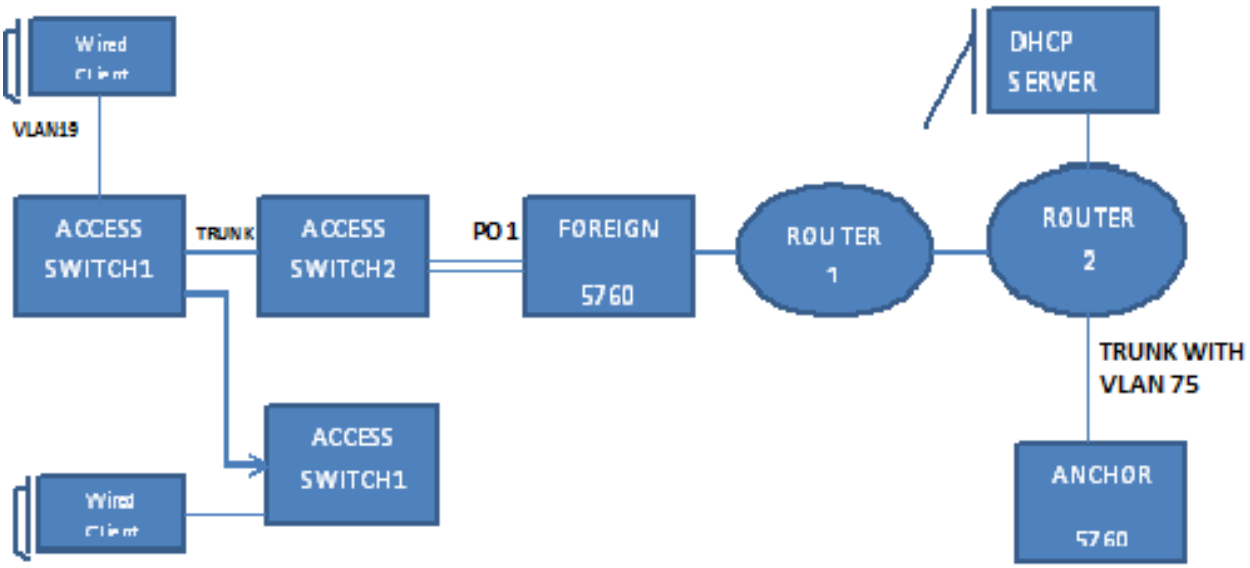
部署方案

本文包括有线的客户端连接为了网络访问的接入交换机的一般的案件。访问两个模式解释用不同的示例。总计方法，有线的访客访问功能能作为验证的一个fallback方法。这典型地是用例，当来宾用户带来是未知对网络的终端设备时。因为终端设备未命中终端请求方，发生故障验证dot1x模式。同样地，因为终端设备的MAC地址是未知对正在验证服务器， MAB验证也发生故障。注意在这样实施，公司终端设备顺利地获得访问，因为他们有一dot1x请求方或他们的MAC地址在验证的正在验

证服务器。因为管理员不需要限制和特别地阻塞端口访客访问的，这允许在部署的灵活性。

拓扑

此图表显示用于部署方案的拓扑。



OPENAUTH

访客锚点配置

完成这些步骤：

1. 启用IP设备监听在客户端VLAN的跟踪(IPDT)和DHCP，在这种情况下VLAN75。客户端VLAN在访客锚点需要创建。
2. 创建VLAN 75和第3层VLAN接口。
3. 创建指定有5760的客户端VLAN本身作为移动性锚点的访客LAN。对于openmode，**安全web-auth**命令没有要求。

外国配置

1. 启用DHCP并且创建VLAN。如注释，客户端VLAN在外国不需要设置。
2. 交换机检测流入客户端的MAC地址用“访问会话波尔特控制自动”配置的Port-Channel的并且运用用户策略“OPENAUTH”。应该首先创建“OPENAUTH”策略如描述此处： `policy-map type control subscriber` **`OPENAUTH`**

   `event session-started match-all`

```
1 class always do-until-failure

2 activate service-template SERV-TEMP3-OPENAUTH

3 authorize
```

3. 配置在外国的MAC学习VLAN的。 `policy-map type control subscriber OPENAUTH`

```
event session-started match-all

1 class always do-until-failure

2 activate service-template SERV-TEMP3-OPENAUTH

3 authorize
```

4. 在这种情况下指向服务的OPENAUTH策略顺序地是指，模板命名"SERV-TEMP3OPENAUTH"如定义此处： `service-template SERV-TEMP3-OPENAUTH`

```
tunnel type capwap name GUEST_LAN_OPENAUTH
```

5. 服务模板包含对隧道类型和名称的一参考。因为处理客户端的流量，客户端VLAN75在访客锚点只需要存在。 `guest-lan GUEST_LAN_OPENAUTH 3`

```
client vlan 75

mobility anchor 9.7.104.62

no security web-auth

no shutdown
```

6. 隧道请求从外国启动到有线的客户端的访客锚点，并且“tunneladdsuccess”表明通道积累进程完成。在ACCESS-SWITCH1一个有线的客户端连接到设置为接入模式由网络管理员的以太网端口。它是在本例中的端口千兆以太网1/0/11 ：`interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

WEBAUTH

访客锚点配置

1. Enable (event)监听在客户端VLAN的IPDT和DHCP，在这种情况下VLAN75。客户端VLAN在访客锚点需要创建。 `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

2. 创建VLAN 75和第3层VLAN接口。 `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access
```

WEBAUTH

3. 创建指定有5760的客户端VLAN本身作为移动性锚点的访客LAN。对于openmode，**安全web-auth**命令没有要求。 `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   WEBAUTH

外国配置

1. Enable (event) DHCP和VLAN的创建。如注释，客户端VLAN在外国不需要设置。 `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   WEBAUTH

2. 交换机检测流入客户端的MAC地址用“访问会话波尔特控制自动”配置的Port-Channel的并且运用用户策略“WEBAUTH”。应该首先创建“WEBAUTH”策略如描述此处。 `policy-map type control subscriber` **WEBAUTH**

   `event session-started match-all`

   `1 class always do-until-failure`

   `2 activate service-template` **SERV-TEMP3-WEBAUTH**

   `3 authorize`

3. 在外国应该配置MAC学习VLAN的。 `policy-map type control subscriber` **WEBAUTH**

   `event session-started match-all`

   `1 class always do-until-failure`

   `2 activate service-template` **SERV-TEMP3-WEBAUTH**

   `3 authorize`

4. 配置RADUIS和参数地图。 `policy-map type control subscriber` **WEBAUTH**

   `event session-started match-all`

   `1 class always do-until-failure`

   `2 activate service-template` **SERV-TEMP3-WEBAUTH**

   `3 authorize`

5. 在这种情况下指向服务的“WEBAUTH”策略顺序地是指，模板命名"SERV-TEMP3WEBAUTH"如定义此处： `service-template` **SERV-TEMP3-WEBAUTH**

   `tunnel type capwap name` **GUEST_LAN_WEBAUTH**

6. 服务模板包含对隧道类型和名称的一参考。因为处理客户端的流量，客户端VLAN75在访客锚点只需要存在。 `guest-lan` **GUEST_LAN_WEBAUTH** `3`

   `client vlan 75`

   `mobility anchor 9.7.104.62`

```
security web-auth authentication-list default

security web-auth parameter-map webparalocal

no shutdown
```

7. 隧道请求从外国启动到有线的客户端的访客锚点，并且“tunneladdsuccess”表明通道积累进程完成。在ACCESS-SWITCH1一个有线的客户端连接到设置为接入模式由网络管理员的以太网端口。它是在本例中的端口千兆以太网1/0/11 ：`guest-lan` **`GUEST_LAN_WEBAUTH`** `3`

```
client vlan 75

mobility anchor 9.7.104.62

security web-auth authentication-list default

security web-auth parameter-map webparalocal

no shutdown
```

WEBAUTH命令O/P示例

外国

```
FOREIGN#sh wir client summary
Number of Local Clients : 2
MAC Address    AP Name          WLAN State            Protocol
-----------------------------------------------------------------
0021.ccbc.44f9 N/A               3   UP               Ethernet
0021.ccbb.ac7d N/A               3   UP               Ethernet

ANCHOR#sh mac address-table
        Mac Address Table
-------------------------------------------

Vlan   Mac Address    Type        Ports
----   -----------    --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
19   0021.ccbb.ac7d   DYNAMIC     Po1

FOREIGN#sh access-session mac 0021.ccbc.44f9 details
          Interface: Port-channel1
             IIF-ID: 0x83D880000003D4
        MAC Address: 0021.ccbc.44f9
       IPv6 Address: Unknown
       IPv4 Address: Unknown
          User-Name: 0021.ccbc.44f9
        Device-type: Un-Classified Device
             Status: Unauthorized
             Domain: DATA
     Oper host mode: multi-auth
   Oper control dir: both
    Session timeout: N/A
  Common Session ID: 090C895F000012A70412D338
    Acct Session ID: Unknown
              Handle: 0x1A00023F
      Current Policy: OPENAUTH
       Session Flags: Session Pushed
```

```
Local Policies:
    Service Template: SERV-TEMP3-OPENAUTH (priority 150)
  Tunnel Profile Name: GUEST_LAN_OPENAUTH
        Tunnel State: 2


Method status list:>
      Method           State
      webauth         Authc Success
```

锚点

```
#sh wir client summary

Number of Local Clients : 1

MAC Address    AP Name      WLAN State              Protocol

-------------------------------------------------------------

0021.ccbc.44f9 N/A             3    WEBAUTH_PEND    Ethernet

0021.ccbb.ac7d N/A             3   WEBAUTH_PEND     Ethernet


ANCHOR#sh wir client summary

Number of Local Clients : 2

MAC Address    AP Name            WLAN State   Protocol

-----------------------------------------------------

0021.ccbc.44f9 N/A      3   UP                 Ethernet

0021.ccbb.ac7d N/A      3   UP                 Ethernet


ANCHOR#sh mac address-table

        Mac Address Table

-------------------------------------------


Vlan   Mac Address       Type    Ports

----   -----------     --------  -----

19   0021.ccbc.44f9   DYNAMIC     Po1

19   0021.ccbb.ac7d   DYNAMIC     Po1




ANCHOR#sh wir client summary

Number of Local Clients : 1
```

```
MAC Address   AP Name     WLAN State      Protocol
-----------------------------------------------
0021.ccbc.44f9 N/A     3   UP            Ethernet
0021.ccbb.ac7d N/A      3   UP            Ethernet
```

```
ANCHOR#sh access-session mac 0021.ccbc.44f9

Interface   MAC Address   Method Domain Status Fg Session ID
-----------------------------------------------------------------------
Ca1         0021.ccbc.44f9 webauth DATA   Auth    090C895F000012A70412D338
```

```
ANCHOR#sh access-session mac 0021.ccbc.44f9 details
          Interface: Capwap1
              IIF-ID: 0x6DAE4000000248
        MAC Address: 0021.ccbc.44f9
        IPv6 Address: Unknown
        IPv4 Address: 75.1.1.11
          User-Name: 0021.ccbc.44f9
             Status: Authorized
              Domain: DATA
      Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
  Common Session ID: 090C895F000012A70412D338
    Acct Session ID: Unknown
              Handle: 0x4000023A
      Current Policy: (No Policy)

Method status list:
      Method           State
```

```
webauth          Authc Success
```