具有錨點和外部5760 WLC的有線訪客存取

目錄

簡介

本文說明在Cisco 5760無線LAN控制器（充當外部錨點）和思科5760無線LAN控制器(充當非軍事區(DMZ)中的訪客錨點)上使用版本03.03.2.SE版本軟體部署有線訪客存取功能。目前，思科5508無線LAN控制器上存在通過無線和有線網路提供訪客訪問的解決方案。在充當外部控制器的Cisco Catalyst 3650交換機上，此功能的工作方式類似。

在企業網路中，通常需要為其園區的訪客提供網路訪問。訪客訪問要求包括以一致且可管理的方式向有線和無線訪客提供到網際網路或其他選擇性企業資源的連線。同一無線LAN控制器可用於為園區內的兩種訪客提供接入。出於安全原因，大量企業網路管理員通過隧道隔離對DMZ控制器的訪客訪問。訪客存取解決方案也用作失敗dot1x和MAC驗證略過(MAB)驗證方法的訪客使用者端的回退方法。

訪客使用者連線到存取層交換器上的指定有線連線埠以進行存取，且視安全要求而定，可能會讓訪客使用者通過Web同意或Web驗證模式（詳細資訊請參閱後續章節）。 一旦訪客驗證成功，便會向網路資源提供訪問許可權，而訪客控制器會管理客戶端流量。外部錨點是客戶端連線以訪問網路的主交換機。它發起隧道請求。訪客錨點是使用者端實際錨點的交換器。除Cisco 5500系列WLAN控制器外，Cisco 5760無線LAN控制器還可用作訪客錨點。在部署訪客存取功能之前，必須在外部錨點與訪客錨點交換器之間建立一個行動通道。訪客存取功能適用於MC（外部錨點）> MC（訪客錨點）和MA（外部錨點）> MC（訪客錨點）模式。外部錨點交換器將有線訪客流量中繼到訪客錨點控制器，且可對多個訪客錨點進行負載平衡。客戶端錨點到DMZ錨點控制器。它還負責處理DHCP IP地址分配以及客戶端的身份驗證。身份驗證完成後，客戶端可以訪問網路。

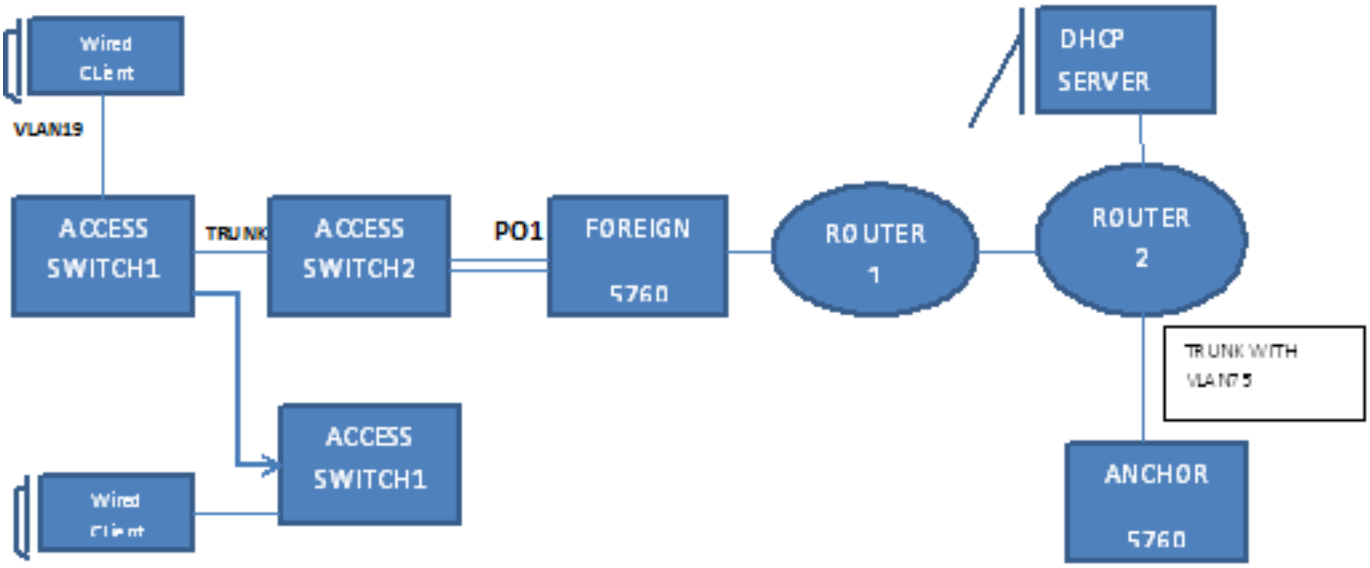
部署方案

本文檔介紹有線客戶端連線到接入交換機進行網路訪問的常見使用案例。在不同的範例中解釋了兩種存取模式。在所有方法中，有線訪客接入功能都可以用作身份驗證的回退方法。當訪客使用者攜

帶網路未知的終端裝置時，通常會出現這種情況。由於終端裝置缺少終端請求方，它將無法通過dot1x模式進行身份驗證。同樣，MAB身份驗證也會失敗，因為身份驗證伺服器不知道終端裝置的MAC地址。值得注意的是，在此類實施中，企業終端裝置將成功獲得訪問許可權，因為它們將有一個dot1x請求方或其MAC地址在驗證伺服器中用於驗證。這樣可靈活地進行部署，因為管理員不需要專門為訪客訪問限制和連線埠。

拓撲

此圖顯示部署方案中使用的拓撲：



OPENAUTH

訪客錨點配置

1. 在客戶端VLAN（本例中為VLAN 75）上啟用IP裝置跟蹤(IPDT)和DHCP監聽。需要在訪客錨點上建立客戶端VLAN。
```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```
2. 建立VLAN 75和L3 VLAN介面。
```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```
3. 建立訪客LAN，指定使用5760本身作為行動錨點的使用者端VLAN。 對於openmode，需要no

security web-auth命令。

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown
```

外部配置

1. 啟用DHCP並建立VLAN。如上所述，不需要在外部VLAN上設定客戶端VLAN。

```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

2. 交換機在配置了「access-Session port-control auto」的連線埠通道上檢測傳入客戶端的MAC地址，並應用使用者策略OPENAUTH。應首先建立此處所述的OPENAUTH策略。

```
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

interface Po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber OPENAUTH
ip dhcp snooping trust
end
```

3. 應在外部的VLAN上配置MAC地址學習。

```
mac address-table learning vlan 19
```

4. OPENAUTH策略按順序引用，在本例中指向服務。 此處定義了名為「SERV-TEMP3 OPENAUTH」的模板：

```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
```

5. 服務模板包含對隧道型別和名稱的引用。客戶端VLAN 75只需要存在於訪客錨點上，因為它負責處理客戶端流量。

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown
```

6. 從外部對有線客戶端的訪客錨點發起隧道請求，tunneladdsuccess指示隧道建立過程已完成。在ACCESS-SWITCH1上，有線客戶端連線到網路管理員設定為接入模式的乙太網埠。在本例中，它是埠GigabitEthernet1/0/11。

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH

訪客錨點配置

1. 在客戶端VLAN（本例中為VLAN 75）上啟用IPDT和DHCP監聽。需要在訪客錨點上建立客戶

端VLAN。

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

2. 建立VLAN 75和L3 VLAN介面。

```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```

3. 建立指定使用者端VLAN的訪客LAN，並將5760本身作為行動錨點。對於openmode，需要**no security web-auth**命令。

```
guest-lan GUEST_LAN_WEBAUTH 3
client vlan VLAN0075
mobility anchor
security web-auth authentication-list default
security web-auth parameter-map webparalocal
no shutdown
```

外部配置

1. 啟用DHCP並建立VLAN。如上所述，不需要在外部VLAN上設定客戶端VLAN。

```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

2. 交換器在配置了「access-Session port-control auto」的連線埠通道上偵測傳入使用者端的MAC位址，並套用使用者原則WEBAUTH。應首先建立此處所述的WEBAUTH策略。

```
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

interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber WEBAUTH
ip dhcp snooping trust
end
```

3. 應在外部的VLAN上配置MAC學習。

```
mac address-table learning vlan 19
```

4. 設定radius和引數映像。

```
aaa new-model
aaa group server radius rad-grp
server Radius1

dot1x system-auth-control
aaa authentication dot1x default group rad-grp


radius server Radius1
```

```
address ipv4 172.19.45.194 auth-port 1812 acct-port 1813
timeout 60
retransmit 3
key radius

parameter-map type webauth webparalocal
type webauth
timeout init-state sec 5000
```

5. WEBAUTH原則按順序引用，在本案例中指向服務。此處定義的名為SERV-TEMP3 WEBAUTH的模板。

```
service-template SERV-TEMP3-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. 服務模板包含對隧道型別和名稱的引用。客戶端VLAN 75隻需存在於訪客錨點上，因為它負責處理客戶端流量。

```
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. 從外部對有線客戶端的訪客錨點發起隧道請求，並且「tunneladdsuccess」指示隧道建立過程已完成。 在ACCESS-SWITCH1上，有線客戶端連線到網路管理員設定為接入模式的乙太網埠。在本例中，它是埠GigabitEthernet1/0/11。

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

並行配置OPENAUTH和WEBAUTH

為了擁有兩個訪客LAN並將其分配給不同的客戶端，您必須根據獲知客戶端的VLAN來配置它們。

訪客錨點配置

1. 在客戶端VLAN（本例中為VLAN 75）上啟用IPDT和DHCP監聽。需要在訪客錨點上建立客戶端VLAN。

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

2. 建立VLAN 75和L3 VLAN介面。

```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```

3. 建立訪客LAN，指定使用5760本身作為行動錨點的使用者端VLAN。 對於openmode，需要**no security web-auth**命令。

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown
```

```
guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor
security web-auth authentication-list joseph
security web-auth parameter-map webparalocal
no shutdown
```

外部配置

1. 啟用DHCP並建立VLAN。如上所述，不需要在外部VLAN上設定客戶端VLAN。
```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```
2. 交換器在配置了「access-Session port-control auto」的連線埠通道上偵測傳入使用者端的MAC位址，並套用使用者原則DOUBLEAUTH。類別對映mac1包含您為OPENAUTH新增的MAC地址。其他一切都是WEBAUTH，使用第二個「always」類對映和「match-first」事件。首先應建立此處所述的DOUBLEAUTH策略。
```
policy-map type control subscriber DOUBLEAUTH
event session-started match-first
 1 class vlan19 do-until-failure
 2 activate service-template SERV-TEMP3-OPENAUTH
3 authorize
 2 class vlan18 do-until-failure
 2 activate service-template SERV-TEMP4-WEBAUTH
 3 authorize


interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
 service-policy type control subscriber DOUBLEAUTH
ip dhcp snooping trust
end
```
3. 應該在VLAN 18和19的外部介面上配置MAC學習。
```
mac address-table learning vlan 18 19
```
4. VLAN 19和VLAN18類對映包含VLAN匹配條件，您可以根據這些條件區分客戶端所在的訪客LAN。定義如下：
```
class-map type control subscriber match-any vlan18
 match vlan 18

class-map type control subscriber match-any vlan19
 match vlan 19
```
5. OPENAUTH策略按順序引用，在本例中指向服務。 此處定義的名為SERV-TEMP3 OPENAUTH的模板。
```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH

service-template SERV-TEMP4-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```
6. 服務模板包含對隧道型別和名稱的引用。客戶端VLAN 75只需要存在於訪客錨點上，因為它負責處理客戶端流量。
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
```

```
no security web-auth
no shutdown


guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor 9.7.104.62
security web-auth authentication-list joseph
security web-auth parameter-map webparalocal
no shutdown
```

7. 從外部對有線客戶端的訪客錨點發起隧道請求，並且「tunneladdsuccess」指示隧道建立過程已完成。 在ACCESS-SWITCH上，有多個有線使用者端連線到VLAN 18或VLAN19，接著便可相應地分配給訪客LAN。在本例中，它是埠GigabitEthernet1/0/11。

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH指令O/P範例

外部

```
FOREIGN#show 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                              4   UP               Ethernet

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

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

FOREIGN#show 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
```

錨點

```
#show 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                              4   WEBAUTH_PEND       Ethernet

ANCHOR#show 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                              4   UP                 Ethernet

ANCHOR#show mac address-table
         Mac Address Table
-------------------------------------------
Vlan   Mac Address       Type       Ports
----   -----------       --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
18   0021.ccbb.ac7d   DYNAMIC     Po1

ANCHOR#show 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                             4   UP                 Ethernet

ANCHOR#show access-session mac 0021.ccbc.44f9

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

ANCHOR#show 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
```