目次

[概要](#)
[デプロイメントシナリオ](#)
[トポロジ](#)
[OPENAUTH](#)
[ゲスト固定設定](#)
[外部 設定](#)
[WEBAUTH](#)
[ゲスト固定設定](#)
[外部 設定](#)
[WEBAUTH コマンド O/P 例](#)
[外部](#)
[固定](#)

概要

この資料はバージョン 03.03.2.SE リリースソフトウェアが付いている非武装地帯（DMZ）のゲスト アンカーとして機能する Cisco 5760 WLC および外部アンカーとして行動する Cisco 5760 ワイヤレス LAN コントローラ（WLC）の配線されたゲスト アクセス機能の配置を取り扱っています。 同じように機能作業 Cisco Catalyst 3650 スイッチで外部 コントローラとして機能する。

現在、ソリューションはワイヤレスを通ってゲスト アクセスおよび Cisco の有線ネットワークのプロビジョニングするために 5508 WLC あります。 エンタープライズ ネットワークでは、一般的に キャンパスでゲストへのネットワーク アクセスを提供する必要があります。 ゲスト アクセス必要条件は一貫した、処理しやすい方法で配線されたワイヤレス ゲストにインターネット接続または他の選択的な企業リソースのプロビジョニングするが含まれています。 同じ WLC がキャンパスで両タイプのゲストにアクセスを提供するのに使用することができます。 セキュリティの理由から、トンネリングによる DMZ コントローラへの多数のエンタープライズ ネットワーク管理者分離されたものゲスト アクセス。 ゲスト アクセスソリューションも dot1x および MAC 認証 バイパス (

ゲストユーザはアクセスのためのアクセスレイヤスイッチの指定配線されたポートに接続し、オプションでセキュリティ要件（以下のセクションの詳細）に Web 同意または Web 認証モードを、依存通過させますかもしれません。 ゲスト認証が成功すれば、アクセスはネットワークリソースに提供され、ゲスト コントローラはクライアント トラフィックを管理します。 外部固定はクライアントがネットワーク アクセスのために接続するプライマリ スイッチです。 それはトンネル 要求を始めます。 ゲスト固定はクライアントが実際に固定されて得るスイッチです。 Cisco 5500 シリーズ WLAN コントローラから離れて、Cisco はゲスト アンカーとして 5760 WLC 使用することができます。 ゲスト アクセス機能が展開することができたり前に外部固定とゲスト固定スイッチの間で確立されるモビリティ トンネルがある必要があります。 ゲスト アクセス機能は MC 両方（外部固定）のために >> MC （ゲスト固定）および MA （外部固定） >>MC （ゲスト固定）モデル動作します。 ゲストへの外部固定スイッチ トランクによって配線されるゲスト トラフィックはコントローラを固定し、複数のゲスト固定はロード バランシングのために設定することができます。 クライアントは DMZ 固定コントローラに固定します。 それはまたクライアントの DHCP IP アドレス 割り当て、また認証を処理します。 認証が完了した後、クライアントは

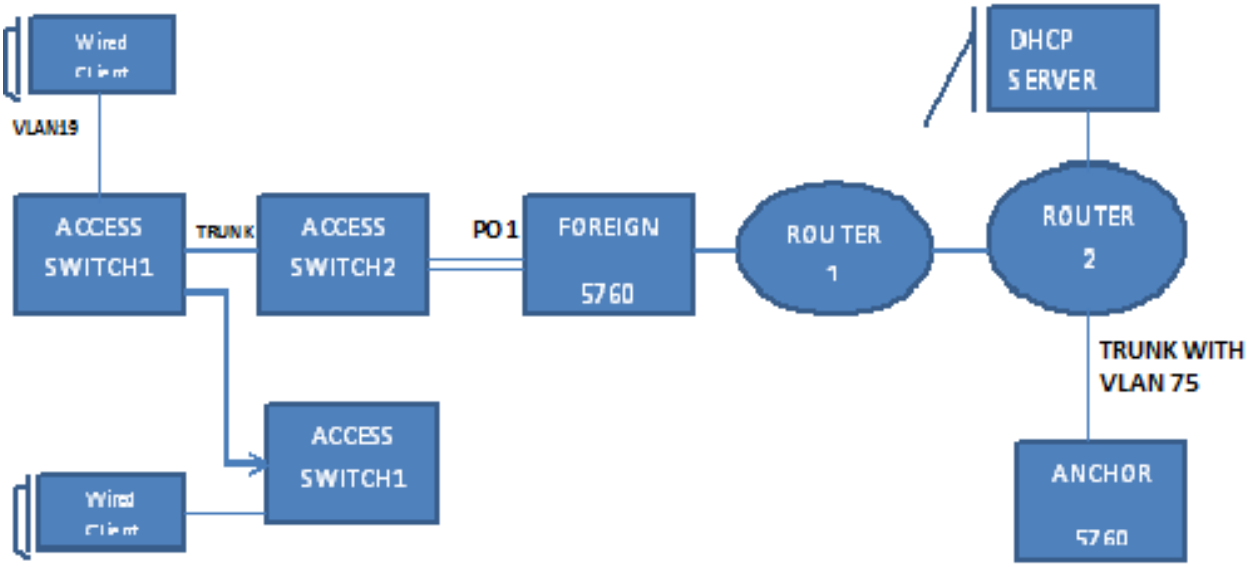
ネットワークにアクセスできます。

デプロイメントシナリオ

この資料は配線されたクライアントがネットワーク アクセスのためのアクセス スイッチを接続する一般的な使用ケースを取り扱っています。 異なる例のアクセスの 2 つのモードは説明されます。 メソッドすべてでは、配線されたゲスト アクセス機能は認証のためのフォールバック 方式として機能できます。 これはネットワークに不明のゲストユーザがエンド デバイスを持って来るとき一般的に 使用例です。 エンドポイント サプリカントがエンド デバイスによってが抜けているので、dot1x モード 認証の失敗します。 同様に、MAB 認証はまたエンド デバイスの MAC アドレスが認証サーバに不明であるので、失敗します。 検証のための認証サーバで dot1x サプリカントか MAC アドレスがあるのでそのような実装で、団体端デバイスが正常にアクセスを得ることに注目して下さい。 これは配備の柔軟性を管理者がゲスト アクセスのためのポートを制限し、とりわけ縛りつける必要はないので、可能にします。

トポロジ

このダイアグラムはデプロイメントシナリオで使用されるトポロジーを示します。



OPENAUTH

ゲスト固定設定

次の手順を実行します。

1. IPデバイス (IPDT) トラッキングおよびクライアント VLAN の DHCPスヌーピングを、こ

の場合 VLAN75 有効に して下さい。 クライアント VLAN はゲスト固定で作成される必要があります。
2. VLAN 75 およびレイヤ3 VLANインターフェイスを作成して下さい。
3. モビリティ固定として行動する 5760 のクライアント VLAN 自体を規定 するゲスト LAN を作成して下さい。openmode に関しては、**セキュリティ Webauth** コマンドが必要となりません。

外部 設定

1. DHCP を有効に し、VLAN を作成して下さい。 注意されるように、クライアント VLAN は外部で設定される必要はありません。
2. スイッチは「アクセス セッション ポート コントロール自動で」設定される port-channel の着信 クライアントの MAC アドレスを検出する、加入者ポリシー「OPENAUTH」を適用します。 ここに記述されているように「OPENAUTH」ポリシーは最初に作成する必要があります: `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. VLAN のための外部の MAC ラーニングを設定して下さい。 `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. OPENAUTH ポリシーはサービスをこの場合指す、ここに定義されるようにテンプレート "SERV-TEMP3OPENAUTH" 指名されて次々に参照されます: `service-template` **`SERV-TEMP3-OPENAUTH`**

   `tunnel type capwap name` **`GUEST_LAN_OPENAUTH`**
5. サービス テンプレートはトンネルタイプおよび名前への参照を紹介しています。 それがクライアント トラフィックを処理するのでクライアント VLAN75 ゲストで存在 する必要だけ固定します。 `guest-lan` **`GUEST_LAN_OPENAUTH`** `3`

   `client vlan 75`

   `mobility anchor 9.7.104.62`

   `no security web-auth`

   `no shutdown`
6. トンネル 要求は外部から配線されたクライアントのためのゲスト固定への始められ、トンネル集結プロセスが完了したことを「tunneladdsuccess」は示します。ACCESS-SWITCH1 で配線されたクライアントはネットワーク管理者によってアクセス モードに設定 される イーサネットポートに接続します。 それはこの例のポート GigabitEthernet 1/0/11 です

   :`interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

WEBAUTH

ゲスト固定設定

1. イネーブル IPDT およびクライアント VLAN の DHCPスヌーピング、この場合 VLAN75。クライアント VLAN はゲスト固定で作成される必要があります。 `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

2. VLAN 75 およびレイヤ3 VLANインターフェイスを作成して下さい。 `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

3. モビリティ固定として行動する 5760 のクライアント VLAN 自体を規定 するゲスト LAN を作成して下さい。openmode に関しては、**セキュリティ Webauth** コマンドが必要となりません。`interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

外部 設定

1. イネーブル DHCP および VLAN の作成。 注意されるように、クライアント VLAN は外部で設定される必要はありません。 `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

2. スイッチは「アクセス セッション ポート コントロール自動で」設定される port-channel の着信 クライアントの MAC アドレスを検出する、加入者ポリシー「WEBAUTH」を適用します。 ここに記述されているように「WEBAUTH」ポリシーは最初に作成する必要があります。 `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. MAC ラーニングは VLAN のための外部で設定する必要があります。 `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. RADUIS およびパラメータ マップを設定して下さい。 `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. 「WEBAUTH」ポリシーはサービスをこの場合指す、ここに定義されるようにテンプレート "SERV-TEMP3WEBAUTH" 指名されて次々に参照されます: `service-template SERV-TEMP3-WEBAUTH`

```
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. サービス テンプレートはトンネルタイプおよび名前への参照を紹介しています。 それがクライアント トラフィックを処理するのでクライアント VLAN75 ゲストで存在 する必要だけ固定します。 `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. トンネル 要求は外部から配線されたクライアントのためのゲスト固定への始められ、トンネル集結プロセスが完了したことを「tunneladdsuccess」は示します。ACCESS-SWITCH1 で配線されたクライアントはネットワーク管理者によってアクセス モードに設定 される イーサネットポートに接続します。 それはこの例のポート GigabitEthernet 1/0/11 です:`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 コマンド O/P 例

外部

```
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
```

固定

```
#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
```