Contenu

Introduction

Ce document couvre le déploiement de la caractéristique de câble d'accès invité sur un contrôleur LAN Sans fil de Cisco 5760 (WLC) qui agit en tant qu'ancre étrangère et Cisco 5760 WLC qui agit en tant qu'ancre d'invité dans la zone démilitarisée (DMZ) avec le logiciel de version de version 03.03.2.SE. La caractéristique fonctionne de la même façon sur un commutateur de Cisco Catalyst 3650 qui agit en tant que contrôleur étranger.

Aujourd'hui, les solutions existent pour la fourniture d'accès invité par la radio et de réseaux câblés sur Cisco 5508 WLC. Dans les réseaux d'entreprise, il y a typiquement un besoin de permettre d'accéder l'accès au réseau à ses invités sur le campus. Les conditions requises d'accès invité incluent l'octroi de connexion Internet ou d'autres ressources de l'entreprise sélectives aux invités de câble et Sans fil d'une manière cohérente et maniable. Le même WLC peut être utilisé pour permettre d'accéder aux deux types d'invités sur le campus. Pour des raisons de sécurité, un grand nombre d'administrateurs de réseau d'entreprise isolent l'accès invité à un contrôleur DMZ par l'intermédiaire du Tunnellisation. La solution d'accès invité est également utilisée comme méthode de retour pour les clients d'invité qui échouent dot1x et des méthodes d'authentification de dérivation d'authentification MAC (

L'utilisateur d'invité se connecte au port de câble indiqué sur un commutateur de couche d'accès pour l'accès et sur option pourrait être fait pour passer par des modes de consentement ou d'authentification Web de Web, dépendants sur les exigences de sécurité (détails dans les sections postérieures). Une fois que l'authentification d'invité réussit, l'accès est fourni aux ressources de réseau et le contrôleur d'invité gère le trafic de client. L'ancre étrangère est le commutateur primaire où le client se connecte pour l'accès au réseau. Il initie des demandes de tunnel. L'ancre d'invité est le commutateur où le client obtient réellement ancré. Indépendamment du contrôleur WLAN de gamme Cisco 5500, Cisco 5760 WLC peut être utilisé comme ancre d'invité. Avant que la caractéristique d'accès invité puisse être déployée, il doit y a un tunnel de mobilité établi entre l'ancre étrangère et les Commutateurs d'ancre d'invité. Les travaux de caractéristique d'accès invité pour MC (ancre étrangère) >> MC (ancre d'invité) et mA (ancre étrangère) >>MC (ancre d'invité) modèle. Le trafic d'invité de câble par joncteurs réseau étrangers

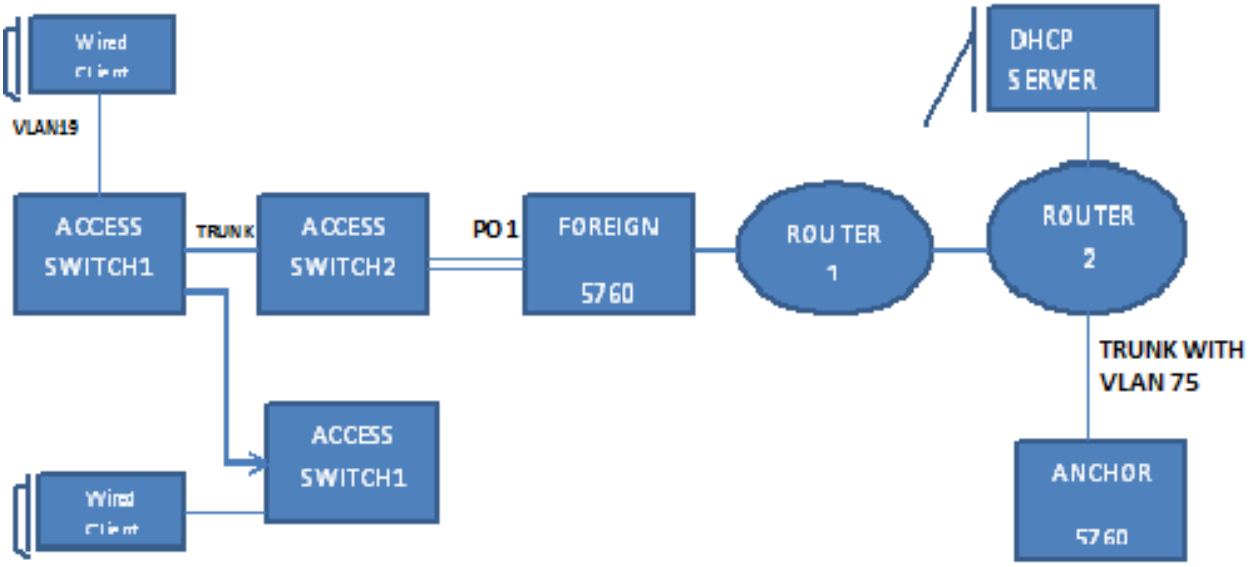
de commutateur d'ancre à l'invité ancrent le contrôleur et des ancres d'invité de multiple peuvent être configurées pour l'Équilibrage de charge. Le client est ancré à un contrôleur d'ancre DMZ. Il manipule également l'attribution d'adresse IP DHCP aussi bien que l'authentification du client. Après que l'authentification se termine, le client peut accéder au réseau.

Scénario de déploiement

Ce document couvre des cas d'usage courant où les clients câblés connectent des commutateurs d'accès pour l'accès au réseau. Deux modes de l'accès sont expliqués dans différents exemples. Dans toutes les méthodes, la caractéristique de câble d'accès invité peut agir en tant que méthode de retour pour l'authentification. C'est typiquement un cas d'utilisation quand un utilisateur d'invité apporte un périphérique d'extrémité qui est inconnu au réseau. Puisque le périphérique d'extrémité manque le suppliant de point final, il échoue le mode de dot1x de l'authentification. De même, l'authentification de MAB échoue également, car l'adresse MAC du périphérique d'extrémité est inconnue au serveur authentifiant. Notez que dans de telles réalisations, les périphériques entreprise d'extrémité obtiennent avec succès l'accès puisqu'ils ont un suppliant de dot1x ou leurs adresses MAC dans le serveur authentifiant pour la validation. Ceci tient compte de la flexibilité dans le déploiement, car l'administrateur n'a pas besoin de limiter et attacher des ports spécifiquement pour l'accès invité.

Topologie

Ce diagramme affiche la topologie utilisée dans le scénario de déploiement.



OPENAUTH

Configuration d'ancre d'invité

Procédez comme suit :

1. Activez le cheminement de périphérique IP (IPDT) et la surveillance DHCP sur le client VLAN, dans ce cas VLAN75. Le client VLAN doit être créé sur l'ancre d'invité.
2. Créez le VLAN 75 et l'interface VLAN de la couche 3.
3. Créez un RÉSEAU LOCAL d'invité qui spécifie le client VLAN avec les 5760 lui-même qui agit en tant qu'ancre de mobilité.Pour l'openmode, l'**aucune** commande de **Web-auth de Sécurité** n'est exigée.

Configuration étrangère

1. Activez le DHCP et créez un VLAN. Comme remarquable, le client VLAN n'a pas besoin d'être installé sur l'étranger.
2. Le commutateur détecte l'adresse MAC du client entrant sur le Port canalisé configuré avec « l'automatique de port-control d'Access-session » et applique la stratégie d'abonné « OPENAUTH ». La stratégie « OPENAUTH » comme décrit ici devrait être créée d'abord :
```
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. Configurez le MAC apprenant sur l'étranger pour le VLAN. `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. La stratégie OPENAUTH est mentionnée séquentiellement qui indique dans ce cas un service, par modèle nommé le "SERV-TEMP3OPENAUTH" comme défini ici : `service-template SERV-TEMP3-OPENAUTH`
```
tunnel type capwap name GUEST_LAN_OPENAUTH
```
5. Le modèle de service contient une référence au type et au nom de tunnel. Les besoins du client VLAN75 seulement d'exister sur l'invité ancrent puisqu'il traite le trafic de client. `guest-lan GUEST_LAN_OPENAUTH 3`
```
client vlan 75

mobility anchor 9.7.104.62

no security web-auth

no shutdown
```
6. La demande de tunnel est initiée de l'étranger à l'ancre d'invité pour le client câblé et les « tunneladdsuccess » indique que le processus d'habillage de tunnel s'est terminé.Sur

l'ACCESS-SWITCH1 un client câblé se connecte au port Ethernet qui est placé au mode d'accès par l'administrateur réseau. C'est le GigabitEthernet 1/0/11 de port dans cet exemple :`interface GigabitEthernet1/0/11`

`switchport access vlan 19`

`switchport mode access`

`WEBAUTH`

WEBAUTH

Configuration d'ancre d'invité

1. Activez IPDT et surveillance DHCP sur le client VLAN, dans ce cas VLAN75. Le client VLAN doit être créé sur l'ancre d'invité. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
2. Créez le VLAN 75 et l'interface VLAN de la couche 3. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
3. Créez un RÉSEAU LOCAL d'invité qui spécifie le client VLAN avec les 5760 lui-même qui agit en tant qu'ancre de mobilité.Pour l'openmode, l'**aucune** commande de **Web-auth de Sécurité** n'est exigée.`interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`

Configuration étrangère

1. DHCP d'enable et la création du VLAN. Comme remarquable, le client VLAN n'a pas besoin d'être installé sur l'étranger. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
2. Le commutateur détecte l'adresse MAC du client entrant sur le Port canalisé configuré avec « l'automatique de port-control d'Access-session » et applique la stratégie d'abonné « WEBAUTH ». La stratégie « WEBAUTH » comme décrit ici devrait être créée d'abord. `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. Apprendre de MAC devrait être configuré sur l'étranger pour le VLAN. `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. Configurez RADUIS et la carte de paramètre. `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. La stratégie « WEBAUTH » est mentionnée séquentiellement qui indique dans ce cas un service, par modèle nommé le "SERV-TEMP3WEBAUTH" comme défini ici : `service-template SERV-TEMP3-WEBAUTH`

```
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. Le modèle de service contient une référence au type et au nom de tunnel. Les besoins du client VLAN75 seulement d'exister sur l'invité ancrent puisqu'il traite le trafic de client. `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. La demande de tunnel est initiée de l'étranger à l'ancre d'invité pour le client câblé et les « tunneladdsuccess » indique que le processus d'habillage de tunnel s'est terminé.Sur l'ACCESS-SWITCH1 un client câblé se connecte au port Ethernet qui est placé au mode d'accès par l'administrateur réseau. C'est le GigabitEthernet 1/0/11 de port dans cet exemple :`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
```

Exemple de la commande O/P WEBAUTH

Étranger

```
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
```

Ancre

```
#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
```