# Contenido



# Introducción

Este despliegue de los documentos abarca de la característica atada con alambre del acceso de invitado en un regulador del Wireless LAN de Cisco 5760 (WLC) que actúa como un ancla no nativa y WLC de Cisco 5760 que actúe como ancla del invitado en la zona desmilitarizada (DMZ) con el software de la versión de la versión 03.03.2.SE. La característica trabaja de manera similar en un Cisco Catalyst 3650 Switch que actúe como regulador no nativo.

Hoy, las soluciones existen para la disposición del acceso de invitado a través de la Tecnología inalámbrica y de las redes alámbricas en el WLC de Cisco 5508. En las redes para empresas, hay típicamente una necesidad de proporcionar el acceso a la red a sus invitados en el campus. Los requisitos del acceso de invitado incluyen la disposición de la conectividad a Internet o de otros recursos selectivos de la empresa a los invitados atados con alambre y inalámbricos en una manera constante y manejable. El mismo WLC se puede utilizar para proporcionar el acceso a ambos tipos de invitados en el campus. Por razones de seguridad, un gran número de administradores de red para empresas segregan el acceso de invitado a un regulador DMZ vía el Tunelización. La solución del acceso de invitado también se utiliza como método del retraso para los clientes del invitado que fallan el dot1x y los métodos de autentificación de puente de la autenticación de MAC (

El Usuario invitado conecta con el puerto atado con alambre señalado en un switch de capa de acceso para el acceso y pudo ser hecho opcionalmente para pasar con los modos del consentimiento o de la autenticación Web de la red, dependientes sobre los requerimientos de seguridad (detalles en las secciones posteriores). Una vez que la autenticación del invitado tiene éxito, el acceso se proporciona a los recursos de red y el regulador del invitado maneja el tráfico del cliente. El ancla no nativa es el Switch primario donde el cliente conecta para el acceso a la red. Inicia las peticiones del túnel. El ancla del invitado es el Switch adonde el cliente consigue realmente asegurado. Aparte del controlador de WLAN de las Cisco 5500 Series, el WLC de Cisco 5760 se puede utilizar como ancla del invitado. Antes de que la característica del acceso de invitado pueda ser desplegada, debe haber un túnel de la movilidad establecido entre el ancla no nativa y el Switches del ancla del invitado. La característica del acceso de invitado trabaja para

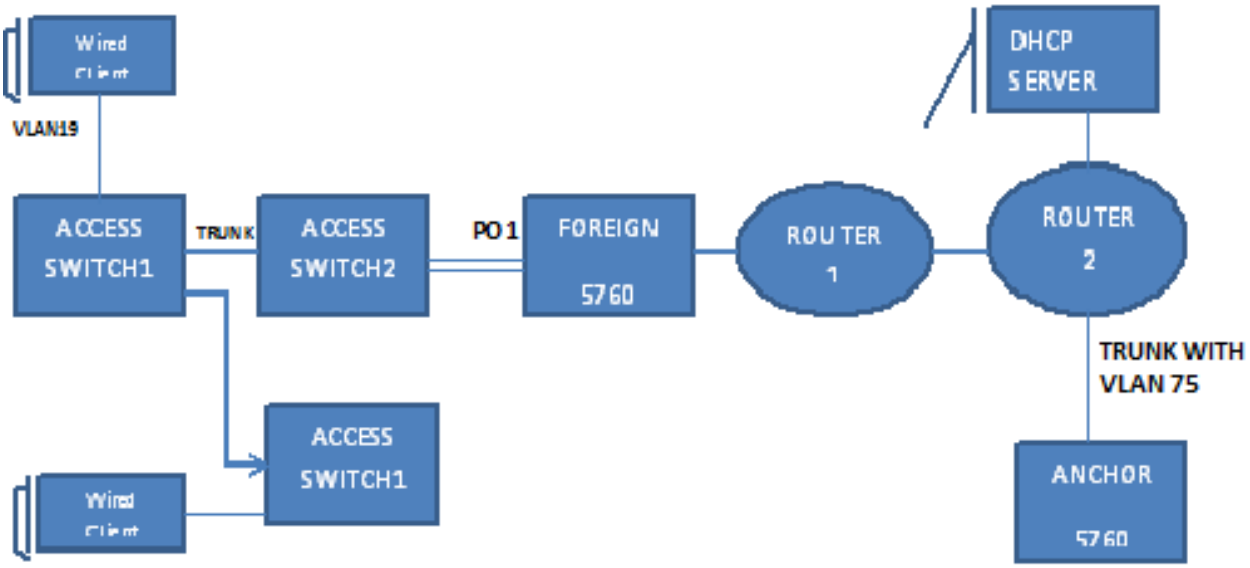
MC (ancla no nativa) >> los modelos MC (ancla del invitado) y MA (ancla no nativa) >>MC (ancla del invitado). Los trunks no nativos del Switch del ancla ataron con alambre el tráfico del invitado al regulador del ancla del invitado y las anclas múltiples del invitado se pueden configurar para el Equilibrio de carga. Aseguran al cliente a un regulador del ancla DMZ. También maneja la asignación de la dirección IP del DHCP así como la autenticación del cliente. Después de que la autenticación complete, el cliente puede acceder la red.

## Escenario de instrumentación

Este cajas de uso común de los documentos abarca donde los clientes atados con alambre conectan para los switches de acceso para el acceso a la red. Dos modos de acceso se explican en diversos ejemplos. En todos los métodos, la característica atada con alambre del acceso de invitado puede actuar como método de autenticación del retraso. Esto es típicamente un caso del uso cuando un Usuario invitado trae un dispositivo extremo que sea desconocido a la red. Puesto que el dispositivo extremo está faltando el supplicant del punto final, falla al modo de autenticación del dot1x. Semejantemente, la autenticación MAB también falla, pues la dirección MAC del dispositivo extremo es desconocida al servidor de autenticidad. Observe que en tales implementaciones, los dispositivos extremos corporativos consiguen con éxito el acceso puesto que tienen un supplicant del dot1x o sus direcciones MAC en el servidor de autenticidad para la validación. Esto permite la flexibilidad en el despliegue, pues el administrador no necesita restringir y bloquear los puertos específicamente para el acceso de invitado.

## Topología

Este diagrama muestra la topología usada en el escenario de instrumentación.




## OPENAUTH

## Configuración del ancla del invitado

Complete estos pasos:

1. Habilite el seguimiento del dispositivo IP (IPDT) y el snooping del DHCP en los VLA N del cliente, en este caso VLAN75. El VLA N del cliente necesita ser creado en el ancla del invitado.
2. Cree el VLA N 75 y la interfaz VLAN de la capa 3.
3. Cree a un invitado LAN que especifique el VLA N con los 5760 sí mismo del cliente que actúa como el ancla de la movilidad.Para el openmode, no se requiere el **ningún** comando del red-**auth de la Seguridad**.

## Configuración no nativa

1. Habilite el DHCP y cree un VLA N. Según lo observado, el VLA N del cliente no necesita ser configurado en el no nativo.
2. El Switch detecta la dirección MAC del cliente entrante en el canal del puerto configurado con el “puerto-control de la acceso-sesión auto” y aplica la política de suscriptor “OPENAUTH”. La directiva “OPENAUTH” según lo descrito aquí se debe crear primero:
   ```
   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. Aprendizaje de MAC de la configuración en el no nativo para el VLA N. `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 directiva OPENAUTH se refiere secuencialmente que en este caso señala a un servicio, plantilla nombrado el "SERV-TEMP3OPENAUTH" según lo definido aquí: `service-template SERV-TEMP3-OPENAUTH`
   ```
   tunnel type capwap name GUEST_LAN_OPENAUTH
   ```
5. La plantilla del servicio contiene una referencia al tipo de túnel y al nombre. El cliente VLAN75 necesita solamente existir en el ancla del invitado puesto que maneja el tráfico del cliente. `guest-lan GUEST_LAN_OPENAUTH 3`
   ```
   client vlan 75

   mobility anchor 9.7.104.62

   no security web-auth

   no shutdown
   ```
6. La petición del túnel se inicia del no nativo al ancla del invitado para el cliente atado con

alambre y los “tunneladdsuccess” indican que el proceso de la acumulación del túnel completó.En el ACCESS-SWITCH1 un cliente atado con alambre conecta con el acceso de Ethernet que es fijado al modo de acceso por el administrador de la red. Es el gigabitethernet 1/0/11 del puerto en este ejemplo:`interface GigabitEthernet1/0/11`

`switchport access vlan 19`

`switchport mode access`

**`WEBAUTH`**

# WEBAUTH

## Configuración del ancla del invitado

1. Habilite el snooping IPDT y del DHCP en los VLA N del cliente, en este caso VLAN75. El VLA N del cliente necesita ser creado en el ancla del invitado. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   **`WEBAUTH`**
2. Cree el VLA N 75 y la interfaz VLAN de la capa 3. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   **`WEBAUTH`**
3. Cree a un invitado LAN que especifique el VLA N con los 5760 sí mismo del cliente que actúa como el ancla de la movilidad.Para el openmode, no se requiere el **ningún** comando del red-**auth de la Seguridad**.`interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   **`WEBAUTH`**

## Configuración no nativa

1. DHCP del permiso y la creación del VLA N. Según lo observado, el VLA N del cliente no necesita ser configurado en el no nativo. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   **`WEBAUTH`**
2. El Switch detecta la dirección MAC del cliente entrante en el canal del puerto configurado con el “puerto-control de la acceso-sesión auto” y aplica la política de suscriptor “WEBAUTH”. La directiva “WEBAUTH” según lo descrito aquí se debe crear primero. `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. El aprendizaje de MAC se debe configurar en el no nativo para el VLA N. `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. Configuración RADUIS y la correspondencia del parámetro. `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 directiva “WEBAUTH” se refiere secuencialmente que en este caso señala a un servicio, plantilla nombrado el "SERV-TEMP3WEBAUTH" según lo definido aquí: `service-template SERV-TEMP3-WEBAUTH`

```
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. La plantilla del servicio contiene una referencia al tipo de túnel y al nombre. El cliente VLAN75 necesita solamente existir en el ancla del invitado puesto que maneja el tráfico del cliente. `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 petición del túnel se inicia del no nativo al ancla del invitado para el cliente atado con alambre y los “tunneladdsuccess” indican que el proceso de la acumulación del túnel completó.En el ACCESS-SWITCH1 un cliente atado con alambre conecta con el acceso de Ethernet que es fijado al modo de acceso por el administrador de la red. Es el gigabitethernet 1/0/11 del puerto en este ejemplo:`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
```

# Ejemplo del comando O/P WEBAUTH

## No nativo

```
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
```

## Ancla

```
#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
```