Accesso guest cablato con ancoraggio ed esterno come 5760 WLC

Sommario

Introduzione

Questo documento descrive l'implementazione della funzionalità di accesso guest cablato sul controller LAN wireless Cisco 5760 che funziona come ancoraggio esterno e sul controller LAN wireless Cisco 5760 che funziona come ancoraggio ospite nella zona demilitarizzata (DMZ) con software versione 03.03.2.SE. Oggi esistono soluzioni per fornire accesso guest tramite reti wireless e cablate sul controller LAN wireless Cisco 5508. Questa funzione funziona in modo simile sullo switch Cisco Catalyst 3650 che funziona come controller esterno.

Nelle reti aziendali, in genere è necessario fornire l'accesso alla rete ai propri ospiti nel campus. I requisiti di accesso per i guest includono la fornitura di connettività a Internet o ad altre risorse aziendali selettive per i guest sia cablati che wireless in modo coerente e gestibile. Lo stesso controller LAN wireless può essere utilizzato per fornire accesso a entrambi i tipi di ospiti del campus. Per motivi di sicurezza, un gran numero di amministratori di rete aziendali separa l'accesso guest a un controller DMZ tramite tunneling. La soluzione di accesso guest viene utilizzata anche come metodo di fallback per i client guest che non riescono a eseguire i metodi di autenticazione dot1x e MAC Authentication Bypass (MAB).

L'utente guest si connette alla porta cablata designata su uno switch del livello di accesso per l'accesso e, facoltativamente, può essere impostato per passare attraverso modalità di consenso Web o autenticazione Web, a seconda dei requisiti di sicurezza (dettagli nelle sezioni successive). Una volta completata l'autenticazione guest, viene fornito l'accesso alle risorse di rete e il controller guest gestisce il traffico client. L'ancoraggio esterno è lo switch primario a cui il client si connette per accedere alla rete. Avvia richieste tunnel. L'ancoraggio guest è lo switch su cui il client viene effettivamente ancorato. A parte il controller WLAN Cisco serie 5500, il controller WLAN Cisco 5760 può essere utilizzato come ancoraggio guest. Prima di poter distribuire la

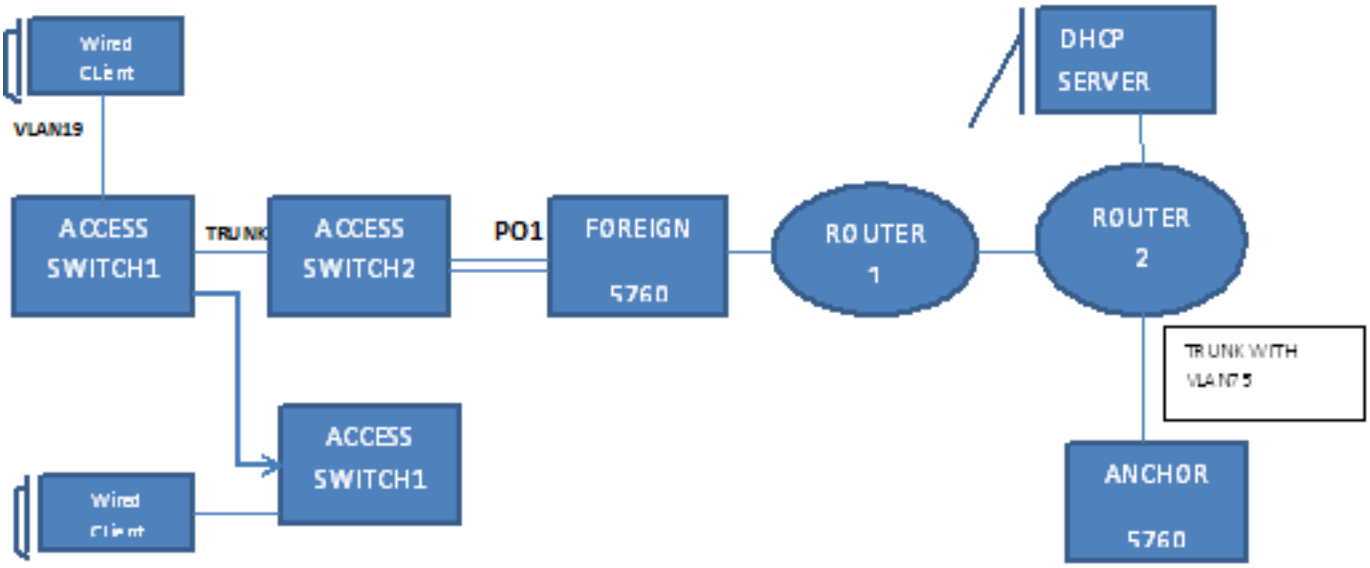
funzionalità di accesso guest, è necessario che sia stato stabilito un tunnel per la mobilità tra l'ancoraggio esterno e gli switch di ancoraggio guest. La funzione di accesso guest funziona sia per i modelli MC (Ancoraggio esterno) >> MC (Ancoraggio ospite) che MA (Ancoraggio esterno) >> MC (Ancoraggio ospite). È possibile configurare per il bilanciamento del carico i trunk dello switch di ancoraggio esterno che collegano il traffico guest al controller di ancoraggio guest e più ancoraggi guest. Il client è ancorato a un controller di ancoraggio DMZ. È inoltre responsabile della gestione dell'assegnazione degli indirizzi IP DHCP e dell'autenticazione del client. Al termine dell'autenticazione, il client sarà in grado di accedere alla rete.

Scenario di distribuzione

Il documento descrive i casi di utilizzo comuni in cui i client cablati si connettono a switch di accesso per l'accesso alla rete. In diversi esempi vengono illustrate due modalità di accesso. In tutti i metodi, la funzionalità di accesso guest cablato può fungere da metodo di fallback per l'autenticazione. Si tratta in genere di un caso di utilizzo in cui un utente guest porta un dispositivo terminale sconosciuto alla rete. Poiché il dispositivo terminale non dispone del supplicant dell'endpoint, la modalità di autenticazione dot1x non funzionerà. Analogamente, anche l'autenticazione MAB avrebbe esito negativo, poiché l'indirizzo MAC del dispositivo terminale sarebbe sconosciuto al server di autenticazione. È importante notare che in tali implementazioni, i dispositivi finali aziendali ottengono l'accesso in quanto hanno un supplicant dot1x o i loro indirizzi MAC nel server di autenticazione per la convalida. Ciò consente una maggiore flessibilità nell'installazione, poiché l'amministratore non deve limitare e collegare le porte specificamente per l'accesso guest.

Topologia

Il diagramma mostra la topologia utilizzata nello scenario di distribuzione:



OPENAUTH

Configurazione ancoraggio guest

1. Abilitare il rilevamento dei dispositivi IP (IPDT) e lo snooping DHCP sulle VLAN client, in questo caso la VLAN 75. La VLAN client deve essere creata sull'ancoraggio guest.
```
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. Creare la VLAN 75 e l'interfaccia VLAN L3.
```
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. Creare una LAN guest che specifichi la VLAN client con lo switch 5760 che funge da ancoraggio alla mobilità. Per la modalità apertura è necessario il comando **no security web-auth**.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown
```

Configurazione esterna

1. Abilitare il protocollo DHCP e la creazione della VLAN. Come accennato, la VLAN client non deve essere configurata sull'unità esterna.
```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```
2. Lo switch rileva l'indirizzo MAC del client in ingresso sul canale della porta configurato con "access-session port-control auto" e applica il criterio della persona che esegue la sottoscrizione OPENAUTH. È necessario creare prima il criterio OPENAUTH descritto di seguito.
```
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. Ènecessario configurare l'apprendimento dell'indirizzo MAC su una rete esterna per la VLAN.
```
mac address-table learning vlan 19
```
4. Il criterio OPENAUTH viene fatto riferimento in sequenza, nel caso specifico a un servizio. Il

modello denominato "SERV-TEMP3 OPENAUTH" è definito qui:

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

5. Il modello di servizio contiene un riferimento al tipo e al nome del tunnel. La VLAN client 75 deve esistere solo sull'ancoraggio guest perché è responsabile della gestione del traffico client.

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

6. La richiesta di tunnel viene avviata dall'ancoraggio esterno all'ancoraggio guest per il client cablato e un'operazione di tunneladsuccess indica che il processo di creazione del tunnel è stato completato. Su ACCESS-SWITCH1 un client cablato si connette alla porta Ethernet impostata dall'amministratore di rete sulla modalità di accesso. In questo esempio, è la porta Gigabit Ethernet1/0/11.

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

WEBAUTH

Configurazione ancoraggio guest

1. Abilitare lo snooping IPDT e DHCP sulle VLAN client, in questo caso la VLAN 75. È necessario creare la VLAN client sull'ancoraggio guest.

```
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. Creare la VLAN 75 e l'interfaccia VLAN L3.

```
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. Creare una LAN guest che specifichi la VLAN client con lo switch 5760 che agisce come ancoraggio di mobilità. Per la modalità apertura è necessario il comando **no security web-auth**.

```
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
```

Configurazione esterna

1. Abilitare il protocollo DHCP e creare una VLAN. Come accennato, la VLAN client non deve

essere configurata sull'unità esterna.

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

2. Lo switch rileva l'indirizzo MAC del client in ingresso sul canale della porta configurato con "access-session port-control auto" e applica il criterio dell'utente WEBAUTH. È necessario creare prima il criterio WEBAUTH descritto di seguito.

```
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. Ènecessario configurare l'apprendimento MAC sull'esterno per la VLAN.

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

4. Configurate il raggio e la mappa dei parametri.

```
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. Il criterio WEBAUTH viene fatto riferimento in sequenza, che in questo caso punta a un servizio. Il modello denominato SERV-TEMP3 WEBAUTH è definito qui.

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

6. Il modello di servizio contiene un riferimento al tipo e al nome del tunnel. La VLAN client 75 deve esistere solo sull'ancoraggio guest perché è responsabile della gestione del traffico 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 richiesta del tunnel viene avviata dall'ancoraggio esterno all'ancoraggio guest per il client cablato e un 'tunneladdsuccess' indica che il processo di creazione del tunnel è stato completato. Su ACCESS-SWITCH1, un client con cavi si connette alla porta Ethernet impostata dall'amministratore di rete sulla modalità di accesso. In questo esempio, è la porta

Gigabit Ethernet1/0/11.

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

Configurare OPENAUTH e WEBAUTH in parallelo

Per avere due LAN guest e assegnarle a client diversi, è necessario basarle sulle VLAN su cui i client vengono appresi.

Configurazione ancoraggio guest

1. Abilitare lo snooping IPDT e DHCP sulle VLAN client, in questo caso la VLAN 75. È necessario creare la VLAN client sull'ancoraggio guest.

```
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. Creare la VLAN 75 e l'interfaccia VLAN L3.

```
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. Creare una LAN guest che specifichi la VLAN client con lo switch 5760 che funge da ancoraggio alla mobilità. Per la modalità apertura è necessario il comando **no security web-auth**.

```
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
```

Configurazione esterna

1. Abilitare il protocollo DHCP e creare una VLAN. Come accennato, la VLAN client non deve essere configurata sull'unità esterna.

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

2. Lo switch rileva l'indirizzo MAC del client in ingresso sul canale della porta configurato con "access-session port-control auto" e applica il criterio dell'utente DOUBLEAUTH. La

classmap mac1 contiene gli indirizzi MAC aggiunti per OPENAUTH. Tutto il resto è WEBAUTH utilizzando la seconda "sempre" class-map con l'evento "match-first". È necessario creare prima il criterio DOUBLEAUTH descritto di seguito.

```
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. L'apprendimento degli indirizzi MAC deve essere configurato sull'esterno per le VLAN 18 e 19.

```
mac address-table learning vlan 18 19
```

4. Le mappe di classe della VLAN 19 e della VLAN 18 contengono i criteri di corrispondenza VLAN in base ai quali verranno differenziate le VLAN guest a cui appartiene il client. È definito qui:

```
class-map type control subscriber match-any vlan18
 match vlan 18

class-map type control subscriber match-any vlan19
 match vlan 19
```

5. Il criterio OPENAUTH viene fatto riferimento in sequenza, nel caso specifico a un servizio. Il modello denominato SERV-TEMP3 OPENAUTH è definito qui.

```
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. Il modello di servizio contiene un riferimento al tipo e al nome del tunnel. La VLAN client 75 deve esistere solo sull'ancoraggio guest perché è responsabile della gestione del traffico client.

```
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. La richiesta del tunnel viene avviata dall'ancoraggio esterno all'ancoraggio guest per il client cablato e un 'tunneladdsuccess' indica che il processo di creazione del tunnel è stato completato. Sugli SWITCH DI ACCESSO sono presenti più client cablati che si connettono

alla VLAN 18 o alla VLAN 19, a cui è possibile assegnare le LAN guest di conseguenza. In questo esempio, è la porta Gigabit Ethernet1/0/11.

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

Esempio di O/P del comando WEBAUTH

Estero

```
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
```

Ancora

```
#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
```