Wired Guest access met zowel analoge als externe apparatuur als 5760 WLC

Inhoud

Inleiding

Dit document bestrijkt de implementatie van de bekabelde gasttoegangsfunctie op de Cisco 5760 draadloze LAN-controller die fungeert als een externe versterker en de Cisco 5760 draadloze LAN-controller die fungeert als een Guest Anchor in de gedemilitariseerde zone (DMZ) met versie 3.03.2.SE release software. Vandaag de dag bestaan oplossingen om gasttoegang door draadloze en bekabelde netwerken op de Cisco 5508 Draadloze LAN controller te bieden. Deze functie werkt op dezelfde manier op de Cisco Catalyst 3650-switch die als een buitenlandse controller fungeert.

In bedrijfsnetwerken is er doorgaans een noodzaak om netwerktoegang te bieden tot de gasten op de campus. De eisen van de gasttoegang omvatten het verstrekken van connectiviteit aan het internet of andere selectieve bedrijfsmiddelen aan zowel verbonden als draadloze gasten op een consistente en beheersbare manier. Dezelfde draadloze LAN-controller kan worden gebruikt om toegang te bieden tot beide soorten gasten op de campus. Om veiligheidsredenen scheiden een groot aantal netwerkbeheerders de toegang van de gast tot een DMZ-controller via een tunneling. De oplossing voor gasttoegang wordt ook gebruikt als reservemethode voor gastcliënten die dot1x en MAC Verificatie Bypass (MAB) authenticatiemethoden nalaten.

De gastgebruiker sluit zich aan op de aangewezen bedrade haven op een toegangslaagschakelaar voor toegang en zou, naar keuze, door de wijzen van de Toestemming van het Web of van de Verificatie van het Web kunnen worden gemaakt, afhankelijk van de veiligheidsvereisten (details in latere secties). Zodra de verificatie van de gast slaagt, wordt toegang verschaft tot de netwerkbronnen en de gastcontroller beheert het clientverkeer. Het buitenlandse anker is de primaire schakelaar waar de cliënt voor netwerktoegang aansluit. Het initieert tunnelverzoeken. Het gastanker is de switch waar de cliënt verankerd wordt. Naast de

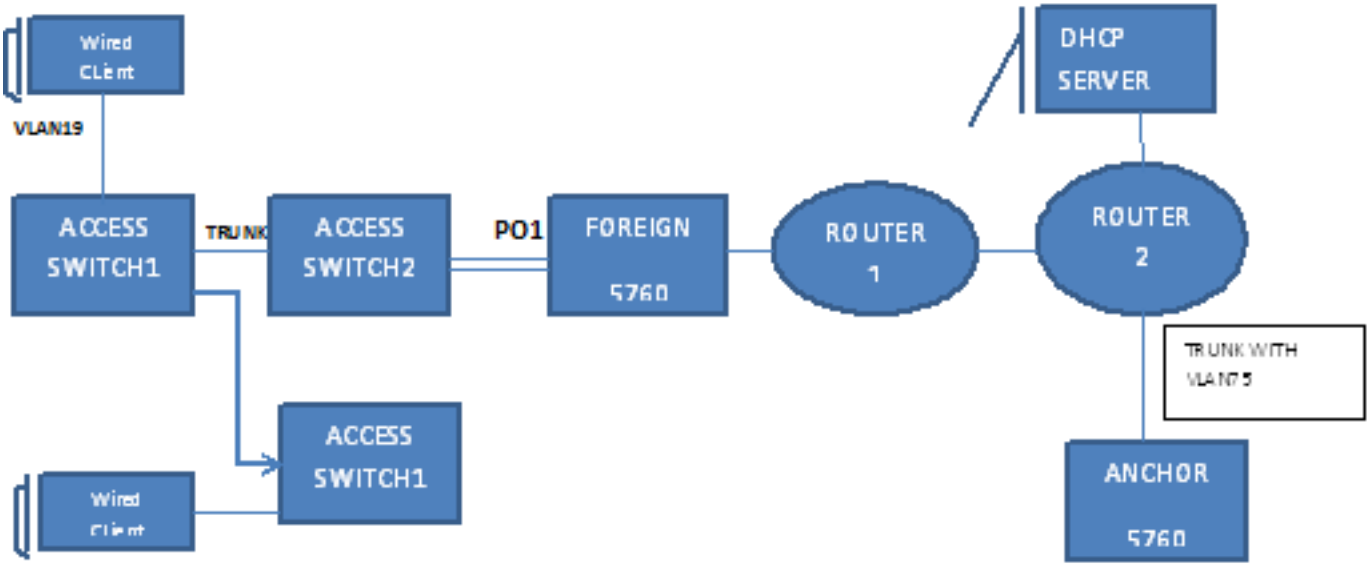
Cisco 5500 Series WLAN-controller kan Cisco 5760 draadloze LAN-controller worden gebruikt als gastanker. Voordat de gast toegangsfunctie kan worden ingezet, moet er een mobiliteitstunnel zijn die tussen het buitenlandse anker en de gastankerschakelaars wordt gelegd. De gasttoegangsfunctie werkt voor zowel MC (Foreign Anchor) > MC (Guest Anchor) en MA (Foreign Anchor) > MC (Guest Anchor) modellen. De buitenlandse ankerswitchstammen bedraad het gastenverkeer naar de gastankercontroller en meerdere gastpresenteerors kunnen worden geconfigureerd voor het in evenwicht brengen van de lading. De client is verankerd in een DMZ ankercontroller. Het is ook verantwoordelijk voor de hantering van de DHCP IP-adrestoewijzing en voor de verificatie van de client. Nadat de authenticatie voltooid is, kan de client toegang krijgen tot het netwerk.

Plaatsingsscenario

Het document heeft betrekking op gewone gebruiksgevallen waarin de bekabelde klanten met toegangsschakelaars verbinden voor netwerktoegang. Twee toegangsmodi worden in verschillende voorbeelden uitgelegd. In alle methoden kan de bekabelde gasttoegangsfunctie fungeren als een back-upmethode voor verificatie. Dit is meestal een use case wanneer een gastgebruiker een eindapparaat levert dat niet bekend is in het netwerk. Aangezien het eindapparaat de eindversterker mist, zal het de punt1x modus van de authenticatie falen. Op dezelfde manier zou MAB authenticatie ook falen, omdat het MAC adres van het eindapparaat onbekend zou zijn aan de authenticatie server. Opgemerkt zij dat in dergelijke implementaties bedrijfseindapparaten met succes toegang zouden krijgen aangezien zij ofwel een dot1x-smeekbede of hun MAC-adressen in de authenticatie server zouden hebben voor validatie. Dit maakt een flexibele toepassing mogelijk, aangezien de beheerder de havens niet specifiek voor de toegang van de gast hoeft te beperken en aan te sluiten.

Topologie

In dit diagram wordt de topologie getoond die in het inzetscenario wordt gebruikt:



OPENAUTH

Configuratie van gastenbevestiging

1. Schakel IP Office Tracking (IPDT) en DHCP-opties in op client-VLAN(s), in dit geval VLAN 75. Het client-VLAN moet op het gastanker worden gemaakt.

```
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. Maak VLAN 75 en de L3 interface van VLAN.

```
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. Maak een gast LAN die de client VLAN specificeert met de 5760 zelf die als het mobiliteitsanker fungeert. Voor de openingsmodus is de opdracht **geen security web-auth** vereist.

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

Buitenlandse configuratie

1. DHCP inschakelen en het VLAN maken. Zoals opgemerkt, hoeft het client-VLAN niet op het buitenland te worden geïnstalleerd.

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

2. De switch detecteert het MAC-adres van de inkomende client in het poortkanaal dat is geconfigureerd met de ‘access-Session poortcontrole auto’ en past het abonneebeleid OPENAUTH toe. Het hier beschreven OPENAUTH-beleid moet eerst worden gecreëerd.

```
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. MAC-adrestraining moet in het buitenland voor VLAN worden ingesteld.

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

4. Het OPENAUTH-beleid wordt achtereenvolgens genoemd, wat in dit geval op een dienst wijst. Het sjabloon met de naam "SERV-TEMP3 OPENAUTH" is hier gedefinieerd:
```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
```
5. De servicessjabloon bevat een verwijzing naar het tunneltype en de -naam. De client VLAN 75 hoeft alleen op het gastanker te bestaan omdat het verantwoordelijk is voor de verwerking van clientverkeer.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown
```
6. Het tunnelverzoek wordt van het buitenland naar het gastanker voor de bekabelde cliënt in werking gesteld en een tunnelsucces wijst erop dat het tunnelopbouwproces voltooid is. Op ACCESS-SWITCH1 sluit een bekabelde client aan op de Ethernet-poort die door de netwerkbeheerder op de toegangsmodus is ingesteld. Het is poort Gigabit Ethernet1/0/11 in dit voorbeeld.
```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH

Configuratie van gastenbevestiging

1. Schakel IPDT- en DHCP-opties in op client-VLAN(s), in dit geval VLAN 75. Het client-VLAN moet op het gastanker worden gemaakt.
```
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. Maak VLAN 75 en de L3 interface van VLAN.
```
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. Maak een gast LAN die de client VLAN specificeert met 5760 zelf die als het mobiliteitsanker dienst doet. Voor de openingsmodus is de opdracht **geen security web-auth** vereist.
```
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
```

Buitenlandse configuratie

1. DHCP inschakelen en een VLAN maken. Zoals opgemerkt, hoeft het client-VLAN niet op het

buitenland te worden geïnstalleerd.

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

2. De switch detecteert het MAC-adres van de inkomende client in het poortkanaal dat is geconfigureerd met de ‘access-Session port-control auto’ en past het abonneebeleid WEBAUTH toe. Het hier beschreven WEBAUTH-beleid moet eerst worden gecreëerd.

```
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. MAC learning moet in het buitenland worden ingesteld voor VLAN’s.

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

4. Configuratie van de straal en de parameter kaart.

```
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. Het WEBAUTH-beleid wordt achtereenvolgens genoemd, wat in dit geval op een service wijst. De sjabloon met de naam SERV-TEMP3 WEBAUTH, zoals hier gedefinieerd.

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

6. De servicessjabloon bevat een verwijzing naar het tunneltype en de -naam. Client VLAN 75 hoeft alleen op het gastanker te bestaan omdat het verantwoordelijk is voor de omgang met clientverkeer.

```
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. Het tunnelverzoek wordt van het buitenland naar het gastanker voor de bekabelde cliënt in gang gezet en een ‘tunnelsucces’ geeft aan dat het proces voor het opbouwen van de tunnel is voltooid. Op ACCESS-SWITCH1 sluit een bekabelde client aan op de Ethernet-poort die door de netwerkbeheerder op de toegangsmodus is ingesteld. Het is poort Gigabit

Ethernet1/0/11 in dit voorbeeld.

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

OPENAUTH en WEBAUTH parallel configureren

Om twee gastLANS te hebben en hen aan verschillende cliënten toe te wijzen, moet u hen op VLAN's baseren waarop de cliënten worden geleerd.

Configuratie van gastenbevestiging

1. Schakel IPDT- en DHCP-opties in op de client-VLAN(s), in dit geval VLAN 75. Het client-VLAN moet op het gastanker worden gemaakt.

```
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. Maak VLAN 75 en de L3 interface van VLAN.

```
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. Maak een gast LAN die de client VLAN specificeert met de 5760 zelf die als het mobiliteitsanker fungeert. Voor de openingsmodus is de opdracht **geen security web-auth** vereist.

```
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
```

Buitenlandse configuratie

1. DHCP inschakelen en een VLAN maken. Zoals opgemerkt, hoeft het client-VLAN niet op het buitenland te worden geïnstalleerd.

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

2. De switch detecteert het MAC-adres van de inkomende client in het poortkanaal dat is geconfigureerd met de ‘access-Session poortcontrole auto’ en past het abonneebeleid

DOUBLEAUTH toe. Het klasmap mac1 bevat de MAC-adressen die u voor OPENAUTH toevoegt. Al het andere is WEBAUTH met behulp van de tweede class-map altijd met de match-first-event. Het hier beschreven DUBLEAUTH-beleid moet eerst worden gecreëerd.

```
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. MAC learning moet op het buitenland worden ingesteld voor VLAN's 18 en 19.

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

4. De class-maps van VLAN 19 en VLAN18 bevatten de criteria van de gelijkenis van VLAN gebaseerd op welke u zult differentiëren welke gast LAN de client binnen valt. Het wordt hier gedefinieerd:

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

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

5. Het OPENAUTH-beleid wordt achtereenvolgens genoemd, wat in dit geval op een dienst wijst. De sjabloon met de naam SERV-TEMP3 OPENAUTH, zoals hier gedefinieerd.

```
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. De servicessjabloon bevat een verwijzing naar het tunneltype en de -naam. De client VLAN 75 hoeft alleen op het gastanker te bestaan omdat het verantwoordelijk is voor de verwerking van clientverkeer.

```
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. Het tunnelverzoek wordt van het buitenland naar het gastanker voor de bekabelde cliënt in gang gezet en een 'tunnelsucces' geeft aan dat het proces voor het opbouwen van de tunnel is voltooid. Op de ACCESS-SWITCH's zijn er meerdere bekabelde klanten die verbinding maken met VLAN 18 of VLAN 19, die dan de gastLAN's dienovereenkomstig kunnen worden

toegewezen. Het is poort Gigabit Ethernet1/0/11 in dit voorbeeld.

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

WEBAUTH-opdracht O/p-voorbeeld

buitenlands

```
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
```

Anchor

```
#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
```