Kabelgebundener Gastzugriff mit Anchor und Foreign als 5760 WLC

Inhalt

Einführung

In diesem Dokument wird die Bereitstellung der Funktion für den kabelgebundenen Gastzugriff auf dem Cisco 5760 Wireless LAN Controller erläutert, der als Foreign Anchor fungiert, sowie auf den Cisco 5760 Wireless LAN Controller, der als Guest Anchor in der Demilitarized Zone (DMZ) mit Version 03.03.2.SE fungiert. Heute gibt es Lösungen, die Gastzugriff über Wireless- und kabelgebundene Netzwerke des Cisco 5508 Wireless LAN Controllers ermöglichen. Die Funktion funktioniert auf dem Cisco Catalyst 3650 Switch, der als ausländischer Controller fungiert, ähnlich.

In Unternehmensnetzwerken ist es in der Regel erforderlich, den Gästen auf dem Campus Netzwerkzugriff bereitzustellen. Zu den Anforderungen für den Gastzugriff gehört die konsistente und verwaltbare Bereitstellung von Internetverbindungen oder anderen selektiven Unternehmensressourcen für kabelgebundene und Wireless-Gäste. Der gleiche Wireless LAN-Controller kann verwendet werden, um den Zugriff für beide Gasttypen auf dem Campus zu ermöglichen. Aus Sicherheitsgründen trennen zahlreiche Netzwerkadministratoren eines Unternehmens den Gastzugriff auf einen DMZ-Controller über Tunneling. Die Gastzugriffslösung wird auch als Fallback-Methode für Gastclients verwendet, bei denen die Authentifizierungsmethoden dot1x und MAB (MAC Authentication Bypass) fehlschlagen.

Der Gastbenutzer stellt über einen Access-Layer-Switch eine Verbindung mit dem festgelegten kabelgebundenen Port her und kann optional je nach den Sicherheitsanforderungen (Details in späteren Abschnitten) durch den Web-Consent- oder den Web-Authentifizierungsmodus geleitet werden. Wenn die Gastauthentifizierung erfolgreich ist, wird der Zugriff auf die Netzwerkressourcen gewährt, und der Gast-Controller verwaltet den Client-Datenverkehr. Der Auslandsanker ist der primäre Switch, an den der Client für den Netzwerkzugriff angeschlossen ist. Es initiiert Tunnelanfragen. Der Gastanker ist der Switch, an dem der Client tatsächlich

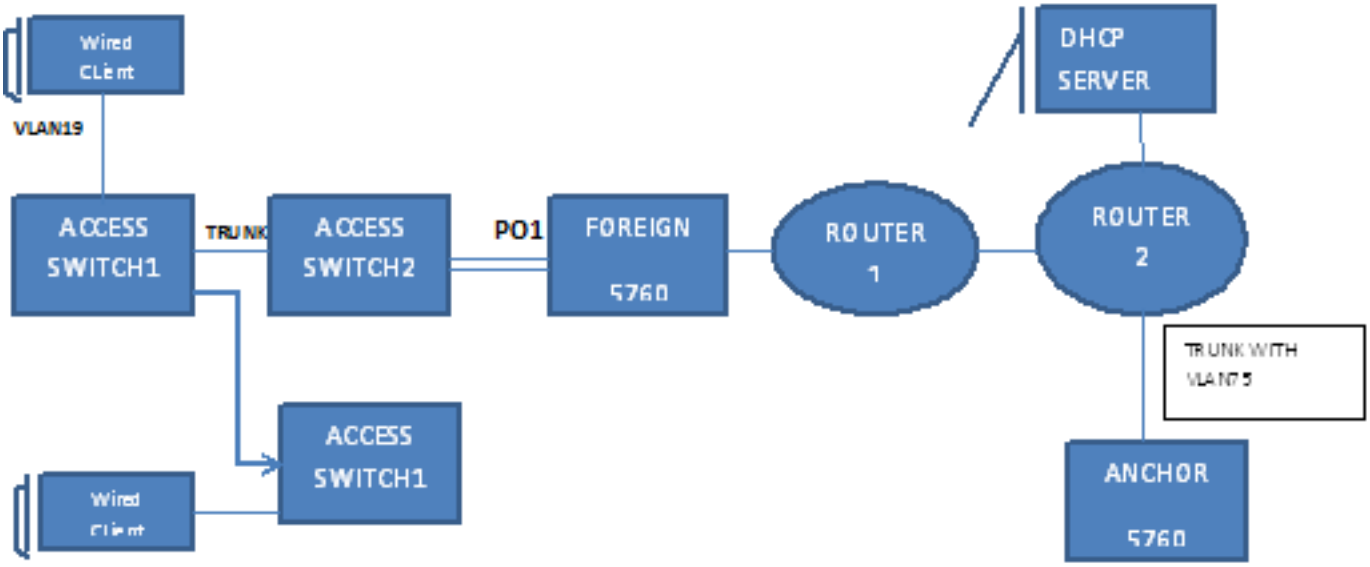
verankert wird. Neben dem Cisco WLAN Controller der Serie 5500 kann der Cisco 5760 Wireless LAN Controller als Gastanker verwendet werden. Bevor die Gastzugriffsfunktion bereitgestellt werden kann, muss zwischen dem Auslandsanker und den Anker-Switches für Gäste ein Mobility Tunnel eingerichtet werden. Die Gastzugangsfunktion kann sowohl für MC- (Foreign Anchor) >> MC- (Guest Anchor) als auch für MA-Modelle (Foreign Anchor) >> MC- (Guest Anchor) verwendet werden. Der Auslandsanker-Switch leitet kabelgebundenen Gastdatenverkehr an den Gastanker-Controller weiter. Für den Lastenausgleich können mehrere Gastanker konfiguriert werden. Der Client ist an einem DMZ-Anker-Controller verankert. Er ist auch für die Verarbeitung der DHCP-IP-Adressenzuweisung sowie für die Authentifizierung des Clients verantwortlich. Nach Abschluss der Authentifizierung kann der Client auf das Netzwerk zugreifen.

Bereitstellungsszenario

Das Dokument behandelt häufige Anwendungsfälle, in denen kabelgebundene Clients für den Netzwerkzugriff mit Access Switches verbunden sind. In verschiedenen Beispielen werden zwei Zugriffsmodi erläutert. Bei allen Methoden kann die Funktion für den kabelgebundenen Gastzugriff als Fallbackmethode für die Authentifizierung fungieren. Dies ist in der Regel ein Anwendungsfall, wenn ein Gastbenutzer ein Endgerät bereitstellt, das dem Netzwerk unbekannt ist. Da das Endgerät die Endgerätekomponente nicht aufweist, schlägt der 802.1x-Authentifizierungsmodus fehl. Auch die MAB-Authentifizierung würde fehlschlagen, da die MAC-Adresse des Endgeräts dem Authentifizierungsserver nicht bekannt ist. Hierbei ist zu beachten, dass in solchen Implementierungen Unternehmensendgeräte erfolgreich auf das System zugreifen können, da sie entweder über eine 802.1x-Komponente oder ihre MAC-Adressen im Authentifizierungsserver zur Validierung verfügen. Dies ermöglicht eine flexible Bereitstellung, da der Administrator keine Ports speziell für den Gastzugriff einschränken und binden muss.

Topologie

Dieses Diagramm zeigt die im Bereitstellungsszenario verwendete Topologie:



ÖFFNUNG

Konfiguration des Gastanchors

1. Aktivieren Sie IP Device Tracking (IPDT) und DHCP Snooping auf Client-VLAN(s), in diesem Fall VLAN 75. Das Client-VLAN muss auf dem Gastanker erstellt werden.
```
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. Erstellen Sie VLAN 75 und die L3-VLAN-Schnittstelle.
```
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. Erstellen Sie ein Gast-LAN, das das Client-VLAN mit dem 5760 selbst angibt, das als Mobilitätsanker fungiert. Für den openmode ist der Befehl **no security web-auth** erforderlich.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown
```

Fremdkonfiguration

1. Aktivieren Sie DHCP und erstellen Sie das VLAN. Wie bereits erwähnt, muss das Client-VLAN nicht im Ausland eingerichtet werden.
```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```
2. Der Switch erkennt die MAC-Adresse des eingehenden Clients auf dem Port-Channel, der mit "access-Session port-control auto" konfiguriert wurde, und wendet die Subscriber-Richtlinie OPENAUTH an. Die hier beschriebene OPENAUTH-Richtlinie sollte zuerst erstellt werden.
```
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. Das Lernen von MAC-Adressen sollte für das VLAN im Ausland konfiguriert werden.

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

4. Die OPENAUTH-Richtlinie wird sequenziell bezeichnet, was in diesem Fall auf einen Service verweist. Die Vorlage "SERV-TEMP3 OPENAUTH" wird hier definiert:
```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
```
5. Die Dienstvorlage enthält einen Verweis auf den Tunneltyp und den Namen. Das Client-VLAN 75 muss nur im Gastanker vorhanden sein, da es für die Verarbeitung des Client-Datenverkehrs zuständig ist.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown
```
6. Die Tunnelanforderung wird für den kabelgebundenen Client vom Fremden zum Gastanker initiiert, und ein Tunneladdamingerfolg zeigt an, dass der Tunnelerstellungsprozess abgeschlossen ist. Auf dem ACCESS-SWITCH1 wird ein kabelgebundener Client mit dem Ethernet-Port verbunden, der vom Netzwerkadministrator auf den Zugriffsmodus festgelegt wurde. In diesem Beispiel handelt es sich um Port GigabitEthernet1/0/11.
```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH

Konfiguration des Gastanchors

1. Aktivieren Sie IPDT und DHCP-Snooping auf Client-VLAN(s), in diesem Fall VLAN 75. Das Client-VLAN muss auf dem Gastanker erstellt werden.
```
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. Erstellen Sie VLAN 75 und die L3-VLAN-Schnittstelle.
```
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. Erstellen Sie ein Gast-LAN, das das Client-VLAN angibt, wobei das 5760 selbst als Mobilitätsanker fungiert. Für den openmode ist der Befehl **no security web-auth** erforderlich.
```
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
```

Fremdkonfiguration

1. Aktivieren Sie DHCP und erstellen Sie ein VLAN. Wie bereits erwähnt, muss das Client-

VLAN nicht im Ausland eingerichtet werden.

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

2. Der Switch erkennt die MAC-Adresse des eingehenden Clients auf dem Port-Channel, der mit "access-Session port-control auto" konfiguriert wurde, und wendet die WEBAUTH-Richtlinie für Teilnehmer an. Die hier beschriebene WEBAUTH-Richtlinie sollte zuerst erstellt werden.

```
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 sollte für VLAN im Ausland konfiguriert werden.

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

4. Konfigurieren Sie den Radius und die Parameterzuordnung.

```
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. Die WEBAUTH-Richtlinie wird sequenziell bezeichnet, was in diesem Fall auf einen Dienst verweist. Die Vorlage mit dem Namen SERV-TEMP3 WEBAUTH, wie hier definiert.

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

6. Die Dienstvorlage enthält einen Verweis auf den Tunneltyp und den Namen. Client-VLAN 75 muss nur im Gastanker vorhanden sein, da es für die Verarbeitung des Client-Datenverkehrs zuständig ist.

```
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. Die Tunnelanfrage wird vom Fremd- zum Gastanker für den kabelgebundenen Client initiiert, und ein "Tunnel-Erfolg" zeigt an, dass der Tunnelerstellungsvorgang abgeschlossen ist. Auf dem ACCESS-SWITCH1 wird ein kabelgebundener Client mit dem Ethernet-Port verbunden,

der vom Netzwerkadministrator auf den Zugriffsmodus festgelegt wurde. In diesem Beispiel handelt es sich um Port GigabitEthernet1/0/11.

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

Parallele Konfiguration von OPENAUTH und WEBAUTH

Um zwei Gast-LANS zu haben und sie verschiedenen Clients zuzuweisen, müssen Sie diese auf den VLANs aufbauen, auf denen die Clients gelernt werden.

Konfiguration des Gastanchors

1. Aktivieren Sie IPDT und DHCP-Snooping auf den Client-VLAN(s), in diesem Fall VLAN 75. Das Client-VLAN muss auf dem Gastanker erstellt werden.

```
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. Erstellen Sie VLAN 75 und die L3-VLAN-Schnittstelle.

```
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. Erstellen Sie ein Gast-LAN, das das Client-VLAN mit dem 5760 selbst angibt, das als Mobilitätsanker fungiert. Für den openmode ist der Befehl **no security web-auth** erforderlich.

```
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
```

Fremdkonfiguration

1. Aktivieren Sie DHCP und erstellen Sie ein VLAN. Wie bereits erwähnt, muss das Client-VLAN nicht im Ausland eingerichtet werden.

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

2. Der Switch erkennt die MAC-Adresse des eingehenden Clients auf dem Port-Channel, der mit "access-Session port-control auto" konfiguriert wurde, und wendet die Subscriber-

Richtlinie DOUBLEAUTH an. Die classMap mac1 enthält die MAC-Adressen, die Sie für OPENAUTH hinzufügen. Alles andere ist WEBAUTH unter Verwendung der zweiten "Always"-Klassenzuordnung mit dem Ereignis "Match First". Die hier beschriebene DOUBLEAUTH-Richtlinie sollte zuerst erstellt werden.

```
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. Die MAC-Lernfunktion sollte für die VLANs 18 und 19 im Ausland konfiguriert werden.

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

4. Die Klassenzuordnungen VLAN 19 und VLAN 18 enthalten die Kriterien für die VLAN-Übereinstimmung, anhand derer Sie ermitteln können, in welches Gast-LAN der Client fällt. Sie wird hier definiert:

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

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

5. Die OPENAUTH-Richtlinie wird sequenziell bezeichnet, was in diesem Fall auf einen Service verweist. Die Vorlage mit dem Namen SERV-TEMP3 OPENAUTH, wie hier definiert.

```
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. Die Dienstvorlage enthält einen Verweis auf den Tunneltyp und den Namen. Das Client-VLAN 75 muss nur im Gastanker vorhanden sein, da es für die Verarbeitung des Client-Datenverkehrs zuständig ist.

```
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. Die Tunnelanfrage wird vom Fremd- zum Gastanker für den kabelgebundenen Client initiiert, und ein "Tunnel-Erfolg" zeigt an, dass der Tunnelerstellungsvorgang abgeschlossen ist. Auf den ACCESS-SWITCHs gibt es mehrere kabelgebundene Clients, die eine Verbindung zu

VLAN 18 oder VLAN 19 herstellen. Diese können dann den Gast-LANs entsprechend zugewiesen werden. In diesem Beispiel handelt es sich um Port GigabitEthernet1/0/11.

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

Beispiel für die Verwendung eines WEBAUTH-Befehls: O/P

Ausländer

```
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
```

Anker

```
#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
```