Содержание

[Введение](#)
[Сценарий развертывания](#)
[Топология](#)
[OPENAUTH](#)
[Гостевая конфигурация привязки](#)
[Внешняя конфигурация](#)
[WEBAUTH](#)
[Гостевая конфигурация привязки](#)
[Внешняя конфигурация](#)
[Команда WEBAUTH Пример O/P](#)
[Внешний](#)
[Привязка](#)

Введение

Этот документ покрывает развертывания функции гостевого доступа к проводной сети на Контроллере беспроводной локальной сети (WLC) Cisco 5760, который действует как внешняя привязка и WLC Cisco 5760 , который действует как гостевая привязка в Демилитаризованной зоне (DMZ) с Версией 03.03.2. Релиз программного обеспечения SE. Функция работает подобной формой на Cisco Catalyst 3650 коммутаторов, которые действуют как внешний контроллер.

Сегодня, решения существуют для условия гостевого доступа через проводные и беспроводные сети на WLC Cisco 5508. В корпоративных сетях, как правило, существует потребность предоставить доступ к сети его гостям в кампусе. Требования гостевого доступа включают условие интернет-соединения или других выборочных ресурсов предприятия и соединенным проводом и беспроводным гостям последовательным и управляемым способом. Тот же WLC может использоваться для обеспечения доступа к обоим типам гостей в кампусе. Из соображений безопасности большое число администраторов корпоративной сети выделяет гостевой доступ к контроллеру DMZ через туннелирование. Решение для гостевого доступа также используется в качестве метода нейтрализации для гостевых клиентов, которые отказывают методы аутентификации Обхода проверки подлинности MAC (MAB) и dot1x.

Гость соединяется с определяемым проводным портом на уровне доступа коммутатора для доступа и дополнительно мог бы быть заставлен пройти веб-режимы Согласия или Web-аутентификации, зависящие от требований безопасности (подробные данные в последующих разделах). Как только гостевая аутентификация успешно выполняется, доступ предоставлен сетевым ресурсам, и гостевой контроллер управляет трафиком клиента. Внешняя привязка является основным коммутатором, где клиент соединяется для доступа к сети. Это инициирует запросы туннеля. Гостевая привязка является коммутатором, где фактически привязан клиент. Кроме Контроллера беспроводной локальной сети серии 5500 Cisco, WLC Cisco 5760 может использоваться в качестве гостевой привязки. Прежде чем функция гостевого доступа может быть развернута, должен быть туннель мобильности,

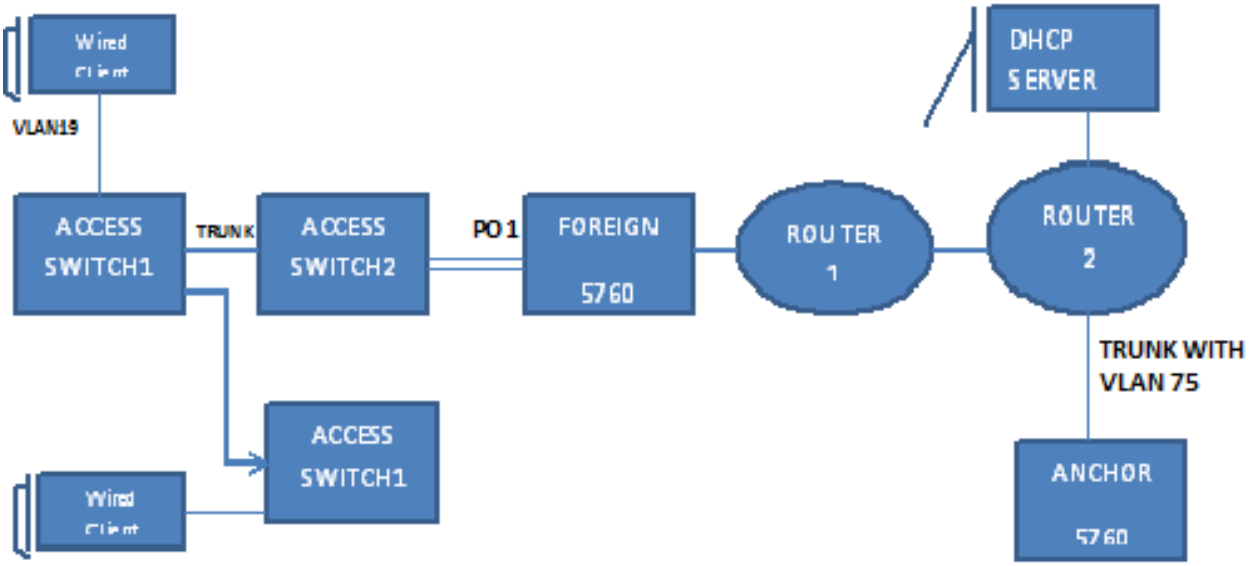
установленный между внешней привязкой и гостевыми коммутаторами привязки. Функция гостевого доступа работает для обоих MC (Внешняя Привязка)>> MC (Гостевая Привязка) и MA (Внешняя Привязка)>> MC (Гостевая Привязка) модели. Внешние транки коммутатора привязки проводной гостевой трафик к контроллеру абонента и множественным гостевым привязкам могут быть настроены для распределения нагрузки. Клиент привязан на якорном контроллере DMZ. Это также обрабатывает присвоение IP-адреса DHCP, а также аутентификацию клиента. После того, как аутентификация завершает, клиент в состоянии обратиться к сети.

Сценарий развертывания

Этот документ покрывает случаи общего использования, где проводные клиенты соединяются чтобы с коммутаторами доступа для доступа к сети. Два режима доступа объяснены в других примерах. Во всех методах функция гостевого доступа к проводной сети может действовать как метод проверки подлинности нейтрализации. Это - как правило, вариант использования, когда гость приносит конечное устройство, которое неизвестно сети. Так как конечное устройство скучает по соискателю оконечной точки, оно отказывает режим аутентификации dot1x. Точно так же аутентификация MAB также отказывает, поскольку MAC-адрес конечного устройства неизвестен серверу аутентификации. Обратите внимание на то, что в таких реализациях, корпоративные конечные устройства успешно получают доступ, так как у них или есть соискатель dot1x или их MAC-адреса в сервере аутентификации для проверки. Это обеспечивает гибкость в развертываниях, поскольку администратор не должен ограничить и связать порты в частности для гостевого доступа.

Топология

Эта схема показывает топологию, используемую в сценарии развертывания.



OPENAUTH

Гостевая конфигурация привязки

Выполните следующие действия:

1. Включите IP - устройство, Отслеживающий (IPDT) и DHCP, snooping на клиентской VLAN, в этом случае VLAN75. Клиентская VLAN должна быть создана на гостевой привязке.
2. Создайте интерфейс виртуальной локальной сети (VLAN) Уровня 3 и VLAN 75.
3. Создайте гостевую LAN, которая задает клиентскую VLAN с 5760 саму, которая действует как привязка к мобильности.Для openmode не требуется **никакая команда web-auth безопасности**.

Внешняя конфигурация

1. Включите DHCP и создайте VLAN. Как обращено внимание, клиентская VLAN не должна быть установлена на внешнем.
2. Коммутатор обнаруживает MAC-адрес входящего клиента на port-channel, настроенном с "Управлением портами сеанса доступа, автоматическим", и применяет абонентскую политику "OPENAUTH". Политика "OPENAUTH", как описано здесь должна быть создана сначала: `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. Настройте Изучение MAC на внешнем для 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. Политика OPENAUTH упомянута последовательно, который в этом случае указывает к сервису, шаблону под названием "SERV-TEMP3OPENAUTH", как определено здесь: `service-template` **`SERV-TEMP3-OPENAUTH`**

   `tunnel type capwap name` **`GUEST_LAN_OPENAUTH`**
5. Сервисный шаблон содержит ссылку на тип туннеля и название. Клиентский VLAN75 только должен существовать на гостевой привязке, так как это обрабатывает трафик клиента. `guest-lan` **`GUEST_LAN_OPENAUTH`** `3`

   `client vlan 75`

   `mobility anchor 9.7.104.62`

```
no security web-auth

no shutdown
```

6. Запрос туннеля инициируется от внешнего до гостевой привязки для проводного клиента, и "tunneladdsuccess" указывает, что туннельный процесс наращивания завершил.На SWITCH1 ДОСТУПА проводной клиент соединяется с Портом Ethernet, который установлен в режим доступа администратором сети. Это - порт GigabitEthernet 1/0/11 в данном примере:`interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

WEBAUTH

Гостевая конфигурация привязки

1. Включите IPDT и DHCP, snooping на клиентской VLAN, в этом случае VLAN75. Клиентская VLAN должна быть создана на гостевой привязке. `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

2. Создайте интерфейс виртуальной локальной сети (VLAN) Уровня 3 и VLAN 75. `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

3. Создайте гостевую LAN, которая задает клиентскую VLAN с 5760 саму, которая действует как привязка к мобильности.Для openmode не требуется **никакая команда web-auth безопасности**.`interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access

WEBAUTH
```

Внешняя конфигурация

1. Включите DHCP и создание VLAN. Как обращено внимание, клиентская VLAN не должна быть установлена на внешнем. `interface GigabitEthernet1/0/11`

```
switchport access vlan 19

switchport mode access
```

WEBAUTH

2. Коммутатор обнаруживает MAC-адрес входящего клиента на port-channel, настроенном с "Управлением портами сеанса доступа, автоматическим", и применяет абонентскую политику "WEBAUTH". Политика "WEBAUTH", как описано здесь должна быть создана сначала. `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. Изучение MAC должно быть настроено на внешнем для 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. Настройте RADUIS и карту параметра. `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. Политика "WEBAUTH" упомянута последовательно, который в этом случае указывает к сервису, шаблону под названием "SERV-TEMP3WEBAUTH", как определено здесь: `service-template` **`SERV-TEMP3-WEBAUTH`**

   `tunnel type capwap name` **`GUEST_LAN_WEBAUTH`**
6. Сервисный шаблон содержит ссылку на тип туннеля и название. Клиентский VLAN75 только должен существовать на гостевой привязке, так как это обрабатывает трафик клиента. `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. Запрос туннеля инициируется от внешнего до гостевой привязки для проводного клиента, и "tunneladdsuccess" указывает, что туннельный процесс наращивания завершил.На SWITCH1 ДОСТУПА проводной клиент соединяется с Портом Ethernet, который установлен в режим доступа администратором сети. Это - порт GigabitEthernet 1/0/11 в данном примере:`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
```

Команда WEBAUTH Пример O/P

Внешний

```
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
```

Привязка

```
#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
```