Contents

Introduction

This document covers deployment of the wired guest access feature on the Cisco 5760 Wireless LAN Controller which acts as a Foreign Anchor and the Cisco 5760 Wireless LAN controller which acts as a Guest Anchor in the Demilitarized Zone (DMZ)

In enterprise networks, there is typically a need to provide network access to its guests on the campus. The guest access requirements include provision of connectivity to the Internet or other selective enterprise resources to both wired and wireless guests in a consistent and manageable way. The same wireless LAN controller can be used to provide access to both types of guests on the campus. For security reasons, a large number of enterprise network administrators segregate guest access to a DMZ controller via tunneling. The guest access solution is also used as a fallback method for guest clients that fail dot1x and MAC Authentication Bypass (MAB) authentication methods.

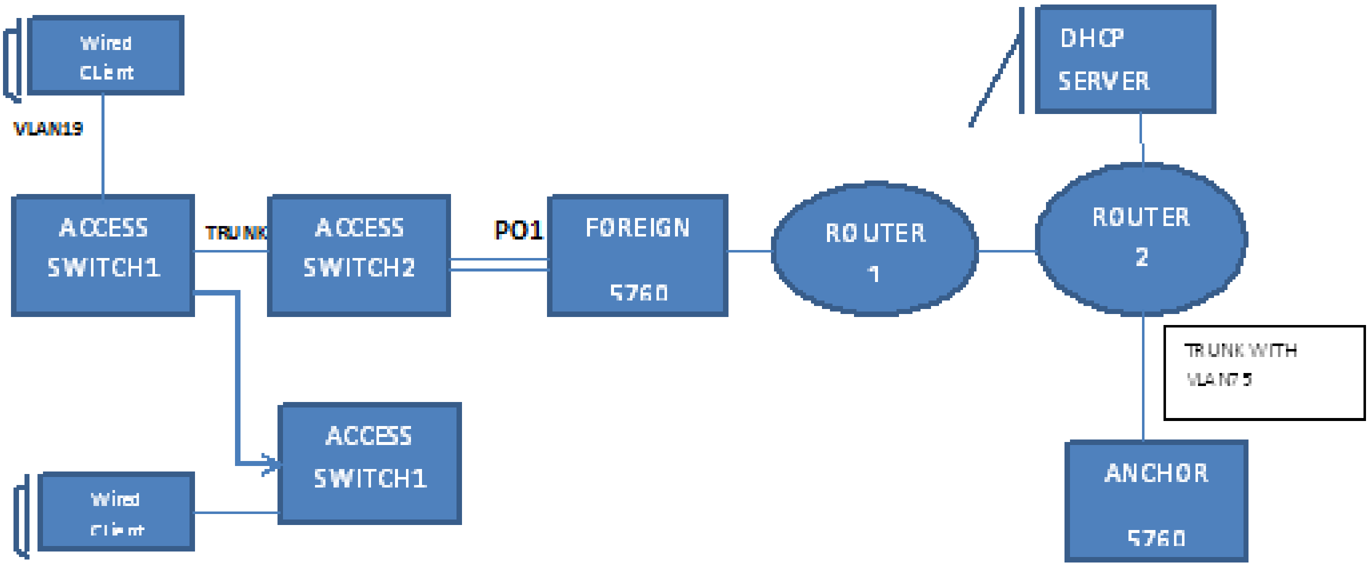
The guest user connects to the designated wired port on an access layer switch for access and optionally might be made to go through Web Consent or Web Authentication modes, dependent upon the security requirements (details in later sections). Once guest authentication succeeds, access is provided to the network resources and the guest controller manages the client traffic. The foreign anchor is the primary switch where the client connects for network access. It initiates tunnel requests. The guest anchor is the switch where the client actually gets anchored. Apart from the Cisco 5500 Series WLAN Controller, the Cisco 5760 Wireless LAN controller can be used as a guest anchor. Before the guest access feature can be deployed, there must be a mobility tunnel established between the foreign anchor and the guest anchor switches. The guest access feature works for both MC (Foreign Anchor) >> MC (Guest Anchor) and MA (Foreign Anchor) >> MC (Guest Anchor) models. The foreign anchor switch trunks wired guest traffic to the guest anchor controller and multiple guest anchors can be configured for load balancing. The client is anchored to a DMZ anchor controller. It is also responsible for handling DHCP IP address assignment as well as authentication of the client. After the authentication completes, the client is able to access the network.

Deployment Scenario

The document covers common use cases where the wired clients connect to access switches for network access. Two modes of access are explained in different examples. In all of the methods, the wired guest access feature can act as a fallback method for authentication. This is typically a use case when a guest user brings an end device that is unknown to the network. Since the end device is missing the endpoint supplicant, it will fail the dot1x mode of authentication. Similarly, MAB authentication would also fail, as the MAC address of the end device would be unknown to the authenticating server. It is worth noting that in such implementations, corporate end devices would successfully get access since they would either have a dot1x supplicant or their MAC addresses in the authenticating server for validation. This allows for flexibility in deployment, as the administrator does not need to restrict and tie up ports specifically for guest access.

Topology

This diagram shows the topology used in the deployment scenario:



OPENAUTH

Guest Anchor Configuration

1. Enable IP Device Tracking (IPDT) and DHCP snooping on client VLAN(s), in this case VLAN 75. The client VLAN needs to be created on the guest anchor.
2. Create VLAN 75 and the L3 VLAN interface.
3. Create a guest LAN that specifies the client VLAN with the 5760 itself that acts as the mobility anchor. For openmode, the **no security web-auth** command is required.

Foreign Configuration

1. Enable DHCP and creation of the VLAN. As noted, the client VLAN does not need to be set up on the foreign.
2. The switch detects the MAC address of the incoming client on the port-channel configured with ‘access-Session port-control auto’ and applies the subscriber policy OPENAUTH. The OPENAUTH policy as described here should be created first.

   ```
   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 address learning should be configured on the foreign for 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

   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
   ```
4. The OPENAUTH policy is referred to sequentially, which in this case points to a service. The template named ‘SERV-TEMP3 OPENAUTH’ is defined here:

   ```
   service-template SERV-TEMP3-OPENAUTH
   tunnel type capwap name GUEST_LAN_OPENAUTH
   ```
5. The service template contains a reference to the tunnel type and name. The client VLAN 75 only needs to exist on the guest anchor since it is responsible for handling client traffic.

   ```
   guest-lan GUEST_LAN_OPENAUTH 3
   client vlan 75
   mobility anchor 9.7.104.62
   no security web-auth
   no shutdown
   ```
6. The tunnel request is initiated from the foreign to the guest anchor for the wired client and a tunneladdsuccess indicates that the tunnel build up process is complete. On the ACCESS-SWITCH1 a wired client connects to the Ethernet port that is set to access mode by the network administrator. It is port GigabitEthernet1/0/11 in this example.

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

WEBAUTH

Guest Anchor Configuration

1. Enable IPDT and DHCP snooping on client VLAN(s), in this case VLAN 75. The client VLAN needs to be created on the guest anchor.
   ```
   guest-lan GUEST_LAN_OPENAUTH 3
   client vlan 75
   mobility anchor 9.7.104.62
   no security web-auth
   no shutdown
   ```
2. Create VLAN 75 and the L3 VLAN interface.
   ```
   guest-lan GUEST_LAN_OPENAUTH 3
   client vlan 75
   mobility anchor 9.7.104.62
   no security web-auth
   no shutdown
   ```
3. Create a guest LAN that specifies the client VLAN with the 5760 itself acting as the mobility anchor. For openmode, the **no security web-auth** command is required.
   ```
   guest-lan GUEST_LAN_OPENAUTH 3
   client vlan 75
   mobility anchor 9.7.104.62
   no security web-auth
   no shutdown
   ```

Foreign Configuration

1. Enable DHCP and creation of a VLAN. As noted, the client VLAN does not need to be set up on the foreign.
   ```
   guest-lan GUEST_LAN_OPENAUTH 3
   client vlan 75
   mobility anchor 9.7.104.62
   no security web-auth
   no shutdown
   ```
2. The switch detects the MAC address of the incoming client on the port-channel configured with ‘access-Session port-control auto’ and applies the subscriber policy WEBAUTH. The WEBAUTH policy as described here should be created first.
   ```
   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 should be configured on the foreign for 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

   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
```

4. Configure the radius and the parameter map.

```
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
```

5. The WEBAUTH policy is referred to sequentially, which in this case points to a service. The template named SERV-TEMP3 WEBAUTH as defined here.

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

6. The service template contains a reference to the tunnel type and name. Client VLAN 75 only needs to exist on the guest anchor since it is responsible for handling client traffic.

```
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. The tunnel request is initiated from the foreign to the guest anchor for the wired client and a ‘tunneladdsuccess’ indicates that the tunnel build up process completed. On the ACCESS-SWITCH1 a Wired client connects to the Ethernet port that is set to access mode by the network administrator. It is port GigabitEthernet1/0/11 in this example.

```
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
```

Configure OPENAUTH and WEBAUTH in Parallel

In order to have two guest LANS and assign them to different clients, you have to base them on the VLANs on which the clients are learned.

Guest Anchor Configuration

1. Enable IPDT and DHCP snooping on the client VLAN(s), in this case VLAN 75. The client VLAN needs to be created on the guest anchor.

```
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
```

2. Create VLAN 75 and the L3 VLAN interface.

```
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
```

3. Create a guest LAN that specifies the client VLAN with the 5760 itself that acts as the mobility anchor. For openmode, the **no security web-auth** command is required.

```
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
```

Foreign Configuration

1. Enable DHCP and creation of a VLAN. As noted, the client VLAN does not need to be set up on the foreign.

```
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
```

2. The switch detects the MAC address of the incoming client on the port-channel configured with ‘access-Session port-control auto’ and applies the subscriber policy DOUBLEAUTH. The classmap mac1 contains the MAC addresses you add for OPENAUTH. Everything else is WEBAUTH using the second “always” class-map with the “match-first” event. The DOUBLEAUTH policy as described here should be created first.

```
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 should be configured on the foreign for VLANs 18 and 19.

```
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
```

4. The VLAN 19 and VLAN18 class-maps contain the VLAN match criteria based on which you will differentiate which guest LAN the client falls in. It is is defined here:

```
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
```

5. The OPENAUTH policy is referred to sequentially, which in this case points to a service. The template named SERV-TEMP3 OPENAUTH as defined here.

```
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. The service template contains a reference to the tunnel type and name. The client VLAN 75 only needs to exist on the guest anchor since it is responsible for handling client traffic.

```
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. The tunnel request is initiated from the foreign to the guest anchor for the wired client and a ‘tunneladdsuccess’ indicates that the tunnel build up process completed. On the ACCESS-SWITCHs there are multiple wired clients that connect to either VLAN 18 or VLAN19, which can be then assigned the guest LANs accordingly. It is port GigabitEthernet1/0/11 in this example.

```
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
```

WEBAUTH Command O/P Example

Foreign

```
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
```