Поймите и устраните неполадки центральной веб-аутентификации (CWA) в гостевой настройке привязки

Содержание

Введение

Этот документ описывает, как центральный webauth работает в гостевой настройке привязки и некоторые общие проблемы, замеченные в рабочей сети и как они могут быть исправлены.

Предварительные условия

Требования

Cisco рекомендует ознакомиться о том, как настроить центральный webauth на Контроллере беспроводной локальной сети (WLC).

Этот документ предоставляет шаги относительно конфигурации центрального webauth: https://www. cisco . com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

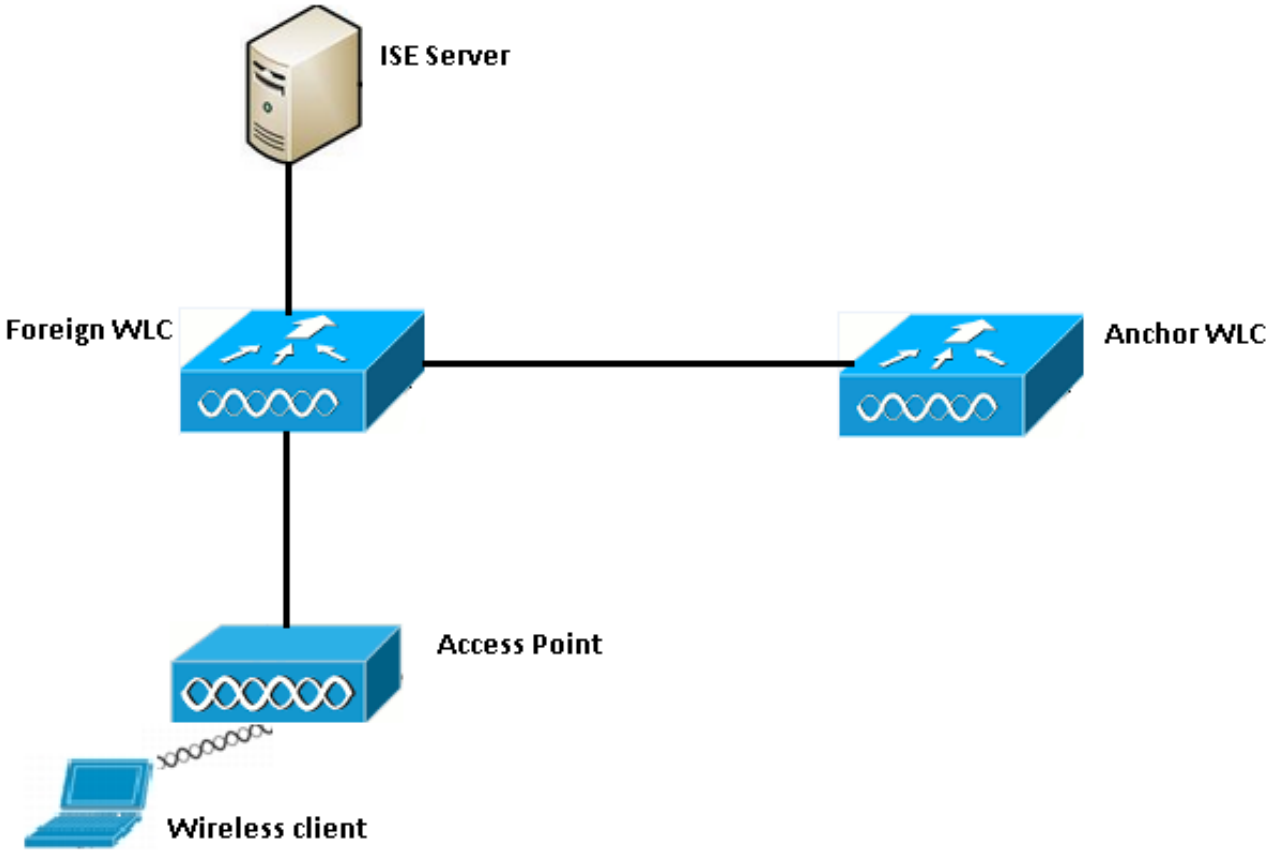
Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Рабочая версия 7.6 WLC 5508
- Рабочая версия 1.4 Платформы Identity Services Engine (ISE)

Основной поток

Этот раздел показывает основной поток операций центрального webauth в гостевой настройке привязки как показано в образе:



Шаг 1. Клиент запускает соединение, когда оно отправляет запрос ассоциации.

Шаг 2. WLC начинает процесс проверки подлинности MAC, когда это передает запрос аутентификации к настроенному серверу ISE.

Шаг 3. На основе политики авторизации, настроенной на ISE, сообщение Access-Accept передают обратно в WLC с URL перенаправления и записями Списка контроля доступа (ACL) перенаправления.

Шаг 4. . Внешний WLC тогда передает ответ ассоциации клиенту.

Шаг 5. . Эта информация передана внешним WLC WLC привязки в мобильности handoff сообщения. Необходимо гарантировать, что ACL перенаправления настроен и на и на внешнем WLC привязки.

Шаг 6. На данном этапе клиент перемещается в Выполненное состояние во внешний WLC.

Шаг 7. Как только клиент инициирует веб-аутентификацию с URL в браузере, привязка запускает процесс переадресации.

Шаг 8. Как только клиент успешно аутентифицируется, клиентские шаги в **ВЫПОЛНЕННОЕ** состояние на WLC привязки.

Центральный поток Webauth для успешной попытки клиентского соединения

Можно теперь проанализировать основной поток, описанный выше подробно при прохождении через отладок. Эти отладки были собраны и на и на внешнем WLC привязки для помощи с анализом:

```
debug client 00:17:7c:2f:b8:6e
debug aaa detail enable
debug mobility handoff enable
debug web-auth redirect enable mac 00:17:7c:2f:b8:6e
```

Эти подробные данные используются здесь:

```
WLAN name: CWA
WLAN ID: 5
IP address of anchor WLC: 10.105.132.141
IP address of foreign WLC: 10.105.132.160
Redirect ACL used: REDIRECT
Client MAC address: 00:17:7c:2f:b8:6e
New mobility architecture disabled
```

Шаг 1. Клиент начинает процесс соединения, когда он отправляет запрос ассоциации. Это замечено на внешнем контроллере:

```
*apfMsConnTask_6: May 08 12:10:35.897: 00:17:7c:2f:b8:6e Association received from mobile on
BSSID dc:a5:f4:ec:df:34
```

Шаг 2. WLC видит, что Беспроводная локальная сеть (WLAN) сопоставлена для проверки подлинности MAC и перемещает клиента в **состояние ожидания AAA** . Это также начинает процесс проверки подлинности, когда это передает запрос аутентификации к ISE:

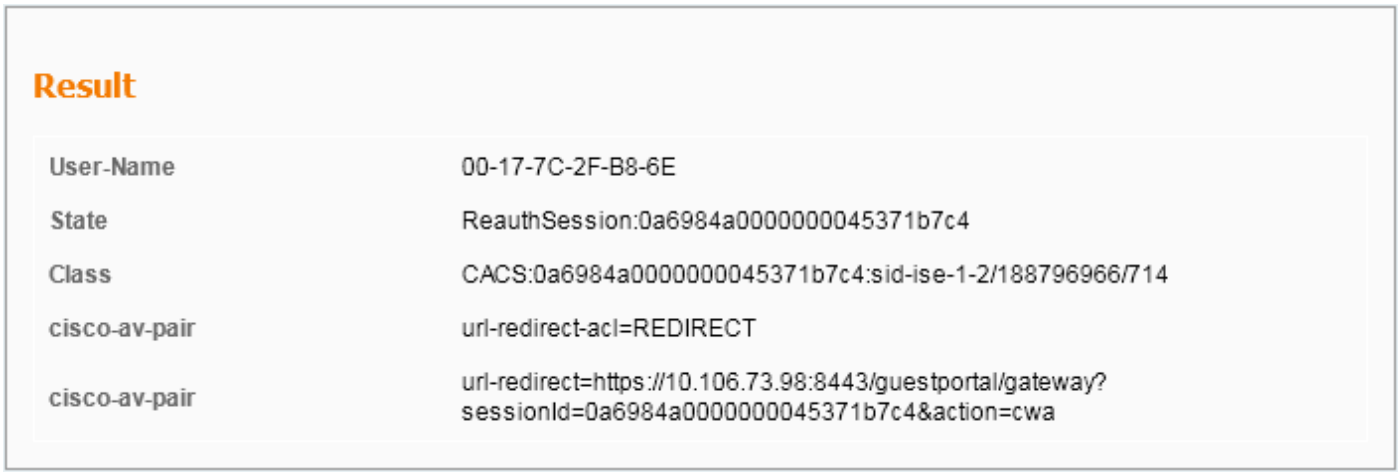
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*aaaQueueReader: May 08 12:10:35.898: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:10:35.898: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:10:35.898:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
```

Шаг 3. На ISE настроен обход проверки подлинности MAC, и это возвращает URL перенаправления и ACL после проверки подлинности MAC. Вы видите эти параметры, передаваемые в отклике при авторизации:

```
*radiusTransportThread: May 08 12:10:35.920: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:10:35.920: structureSize..............................320
*radiusTransportThread: May 08 12:10:35.920: resultCode.....................................0
*radiusTransportThread: May 08 12:10:35.920:
protocolUsed.................................0x00000001
*radiusTransportThread: May 08 12:10:35.920:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:10:35.920: Packet contains 5 AVPs:
*radiusTransportThread: May 08 12:10:35.920: AVP[01] User-
```

```
Name.............................00-17-7C-2F-B8-6E (17 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[02]
State................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[03]
Class................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/38
(54 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[04] Cisco / Url-Redirect-
Acl..............REDIRECT (8 bytes)
*radiusTransportThread: May 08 12:10:35.920: AVP[05] Cisco / Url-
Redirect...................DATA (91 bytes)
```

Вы видите ту же информацию под журналами ISE. Перейдите к **Операциям> Аутентификации** и нажмите **подробные данные Сеанса клиента** как показано в образе:



Шаг 4. . Внешний WLC тогда изменяется, состояние к аутентификации L2 завершают, и передает ответ ассоциации клиенту.

> **Примечание:** С включенной проверкой подлинности MAC не передается ответ ассоциации, пока это не завершено.

```
*apfReceiveTask: May 08 12:10:35.921: 00:17:7c:2f:b8:6e 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4)
*apfReceiveTask: May 08 12:10:35.922: 00:17:7c:2f:b8:6e Sending Assoc Response to station on
BSSID dc:a5:f4:ec:df:34 (status 0) ApVapId 5 Slot 0
```

Шаг 5. : Внешнее тогда инициирует процесс handoff к привязке. Это замечено debug mobility handoff выходные данные:

```
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Attempting anchor export for mobile
00:17:7c:2f:b8:6e
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export:
Client IP: 0.0.0.0, Anchor IP: 10.105.132.141
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e mmAnchorExportSend: Building
UrlRedirectPayload
*apfReceiveTask: May 08 12:10:38.799: 00:17:7c:2f:b8:6e Anchor Export: Sending url redirect acl
REDIRECT
```

Шаг 6. Вы видите, что клиент перемещается в ВЫПОЛНЕННОЕ состояние во внешний WLC. Правильный статус клиента может теперь быть замечен только на привязке. Вот фрагмент выходных данных show client detail, собранных от внешнего (только связанные сведения показывают):

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client Username ................................ 00-17-7C-2F-B8-6E
AP MAC Address.................................. dc:a5:f4:ec:df:30
BSSID........................................... dc:a5:f4:ec:df:34
IP Address...................................... Unknown
Gateway Address................................. Unknown
Netmask......................................... Unknown
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.105.132.141
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
AAA Override ACL Name........................... REDIRECT
AAA URL
redirect.............................https://10.106.73.98:8443/guestportal/gatewaysessionId=
0a6984a00000004c536bac7b&action=cwa
```

Шаг 7. Внешний контроллер инициирует запрос handoff с привязкой. Можно теперь видеть сообщения handoff ниже:

```
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Received Anchor Export request: from Switch
IP: 10.105.132.160
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv:, Mobility role is Unassoc
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv Ssid=cwa Security
Policy=0x42000
*mmListen: May 08 05:52:50.587: 00:17:7c:2f:b8:6e mmAnchorExportRcv vapId= 5, Ssid=cwa
AnchorLocal=0x0
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e mmAnchorExportRcv:Url redirect
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
*mmListen: May 08 05:52:50.588: 00:17:7c:2f:b8:6e Url redirect ACL REDIRECT

A handoff acknowledgement message is also sent to the foreign and can be seen in the debugs on
foreign:
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Received Anchor Export Ack for client from
Switch IP: 10.105.132.141
*mmListen: May 08 12:10:38.802: 00:17:7c:2f:b8:6e Anchor Mac: d0:c2:82:e2:91:60, Old Foreign
Mac: 30:e4:db:1b:e0:a0 New Foreign Mac: 30:e4:db:1b:e0:a0
```

Шаг 8. Якорный контроллер тогда перемещает клиента в DHCP требуемое состояние. Как только клиент получает IP-адрес, контроллер продолжает обрабатывать и перемещать клиента в центральный webauth требуемое состояние. Вы видите то же в выходных данных show client detail, собранных на привязке:

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ CENTRAL_WEB_AUTH
AAA Override ACL Name........................... REDIRECT
AAA URL redirect.............................
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

Шаг 9. Внешний WLC одновременно запускает бухгалтерский процесс, как только это перемещает клиента в выполненное состояние. Это передает бухгалтерское сообщение запуска к ISE:

```
*aaaQueueReader: May 08 12:10:38.803: AccountingMessage Accounting Start: 0x2b6c0a78
*aaaQueueReader: May 08 12:10:38.803: Packet contains 16 AVPs:
*aaaQueueReader: May 08 12:10:38.803: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

Примечание: Учет только должен быть настроен на внешнем WLC.

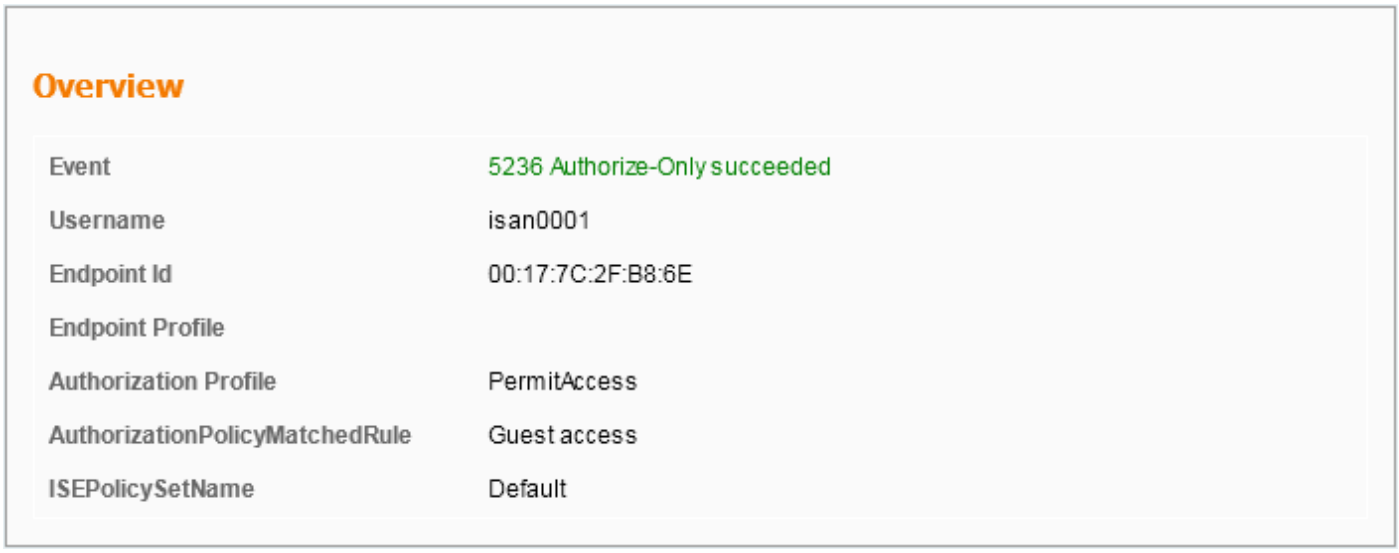
Шаг 10. Пользователь тогда инициирует веб-подлинный процесс перенаправления путем ввода URL в браузер. Вы видите соответствующие отладки на якорном контроллере:

```
*webauthRedirect: May 08 05:53:05.927: 0:17:7c:2f:b8:6e- received connection
*webauthRedirect: May 08 05:53:05.928: captive-bypass detection disabled, Not checking for wispr
in HTTP GET, client mac=0:17:7c:2f:b8:6e
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: May 08 05:53:05.928: 0:17:7c:2f:b8:6e: Client configured with AAA overridden
redirect URL
https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a00000004c536bac7b&action=cwa
```

Шаг 11. Мы можем также видеть, что опознавательная часть в процессе webauth обрабатывается во внешнем WLC а не в привязке. Вы видите то же в выходных данных debug AAA на внешнем:

```
*aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
*aaaQueueReader: May 08 12:11:11.537: Callback.....................................0x10166e78
*aaaQueueReader: May 08 12:11:11.537: protocolType.................................0x40000001
*aaaQueueReader: May 08 12:11:11.537:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)
Authorization response from ISE:
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize..............................252
*radiusTransportThread: May 08 12:11:11.552: resultCode.................................0
*radiusTransportThread: May 08 12:11:11.552:
protocolUsed................................0x00000001
*radiusTransportThread: May 08 12:11:11.552:
proxyState.....................................00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-
Name.............................isan0001 (8 bytes) -----> (Username used for web
authentication)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....................................ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....................................CACS:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/40
(54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-
Timeout.......................0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-
Action.....................0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-
Authenticator...................DATA (16 bytes)
```

То же может быть проверено на ISE как показано в образе:



Шаг 12. Эту информацию передают на WLC привязки. Это квитирование не ясно видимо в отладках, и можно разобрать это привязкой, которая применяет пост handoff политика как показано здесь:

```
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Received Anchor Export policy update, valid
mask 0x900:
Qos Level: 0, DSCP: 0, dot1p: 0 Interface Name: , IPv4 ACL Name:
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Applying post-handoff policy for station
00:17:7c:2f:b8:6e - valid mask 0x900
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e QOS Level: -1, DSCP: -1, dot1p: -1,
Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
*mmListen: May 08 05:53:23.337: 00:17:7c:2f:b8:6e Session: 0, User session: 28200, User elapsed
1
Interface: N/A, IPv4 ACL: N/A, IPv6 ACL: N/A.
```

Лучший способ проверить, что аутентификация завершена, состоит в том, чтобы проверить переданный вход в систему ISE и собрать выходные данные show client detail на контроллере, который должен показать клиенту в **ВЫПОЛНЕННОМ** состоянии как показано здесь:

```
Client MAC Address.............................. 00:17:7c:2f:b8:6e
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 5
IP Address...................................... 10.105.132.254
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.105.132.160
Policy Manager State............................ RUN
```

Другая важная проверка является фактом, что привязка передает предварительный запрос ARP (протокол разрешения адресов) (ARP) после успешной аутентификации:

```
*pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for
10.105.132.254, VLAN Id 20480
```

Отсюда клиент свободен передать все типы трафика, который передан якорным контроллером.

Центральный Поток Webauth, когда Разъединен Клиент

Когда запись клиента должна быть удалена из WLC или из-за сеанса/времени простоя или когда мы вручную удаляем клиента из WLC, эти шаги имеют место:

Внешний WLC передает сообщение de-authenticate клиенту и планирует его для удаления:

```
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e apfMsExpireMobileStation (apf_ms.c:6634)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Associated to
Disassociated
*apfReceiveTask: May 08 12:19:21.199: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:6728
```

Это тогда передает радиус, прекращают считать сообщение, чтобы сообщить серверу ISE, что закончился сеанс аутентификации клиента:

```
*aaaQueueReader: May 08 12:19:21.199: AccountingMessage Accounting Stop: 0x2b6d5684
*aaaQueueReader: May 08 12:19:21.199: Packet contains 24 AVPs:
*aaaQueueReader: May 08 12:19:21.199: AVP[01] User-Name.............................00-17-7C-
2F-B8-6E (17 bytes)
```

Это также передает мобильность handoff сообщение к WLC привязки для информирования его для завершения сеанса клиента. Это может быть замечено в отладках мобильности на WLC привязки:

```
*mmListen: May 08 06:01:32.907: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 08 06:01:32.907: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e 10.105.132.254 RUN (20) mobility role
update request from Export Anchor to Handoff
Peer = 10.105.132.160, Old Anchor = 10.105.132.141, New Anchor = 0.0.0.0
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e apfMmProcessCloseResponse (apf_mm.c:647)
Expiring Mobile!
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Mobility Response: IP 0.0.0.0 code
Anchor Close (5), reason Normal disconnect (0), PEM State DHCP_REQD, Role Handoff(6)
*apfReceiveTask: May 08 06:01:32.908: 00:17:7c:2f:b8:6e Deleting mobile on AP
00:00:00:00:00:00(0)
```

Клиентский аккаунт, заблокированный на ISE

ISE имеет способность заблокировать аккаунт гостя, который сигнализирует WLC для завершения сеанса клиента. Это полезно для администраторов, которые не должны проверять, с каким WLC клиент связан, и просто завершите сеанс. Можно теперь видеть то, что происходит, когда учетная запись гостя приостанавливается/истекается на ISE:

Сервер ISE передает Изменение сообщения Авторизации к внешнему контроллеру, который указывает, что должно быть удалено клиентское соединение. Это может быть замечено в выходных данных отладки:

```
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8 :6e apfMsDeleteByMscb
Scheduling mobile for deletion with deleteReason 6, reason Code 252
*radiusCoASupportTransportThread: May 13 02:01:53.446: 00:17:7c:2f:b8:6e Schedul ing deletion of
Mobile Station: (callerId: 30) in 1 seconds
```

Внешний WLC тогда передает сообщение de-authenticate клиенту:

```
*apfReceiveTask: May 13 02:01:54.303: 00:17:7c:2f:b8:6e Sent Deauthenticate to mobile on BSSID
dc:a5:f4:ec:df:30 slot 0(caller apf_ms.c:5921)
```

Это также передает бухгалтерское сообщение остановки к учетному серверу для окончания сеанса аутентификации клиента на его стороне:

```
*aaaQueueReader: May 13 02:01:54.303: AccountingMessage Accounting Stop: 0x2b6d2 c7c
*aaaQueueReader: May 13 02:01:54.303: Packet contains 23 AVPs:
*aaaQueueReader: May 13 02:01:54.303: AVP[01] User-Name.................
.............00177c2fb86e (12 bytes)
```

Сообщение handoff также передается WLC привязки для завершения сеанса клиента. Вы видите это на WLC привязки:

```
*mmListen: May 12 19:42:52.871: 00:17:7c:2f:b8:6e Received Handoff End request for client from
Switch IP: 10.105.132.160
*apfReceiveTask: May 12 19:42:52.872: 00:17:7c:2f:b8:6e apfMmProcessResponse: Handoff end rcvd
for mobile 00:17:7c:2f:b8:6e, delete mobile. reason code = 0
```

Устраните неполадки центрального Webauth в гостевой настройке привязки

Давайте теперь взглянем на некоторые общие проблемы, замеченные при использовании CWA и что может быть сделано для решения проблемы его.

Сценарий 1. Клиентское всунутое НАЧАЛЬНОЕ СОСТОЯНИЕ и не получает IP-адрес

В центральном webauth сценарии, так как включена проверка подлинности MAC, ответы ассоциации передаются после того, как проверка подлинности MAC завершена. В этом случае, если существует сбой связи между WLC и сервером RADIUS или существует misconfig на сервере RADIUS, который заставляет его передавать отклонения доступа, вы видите, что клиент всунул петлю ассоциации, где это неоднократно получает отклонение ассоциации. Существует также шанс, что клиент исключен также, если включено клиентское исключение.

Достижимость сервера RADIUS может быть проверена с **тестовым AAA Radius**, который доступен в коде 8.2 и выше.

Ниже опорного канала показывает, как использовать это:
https://www. cisco . com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Сценарий 2. Клиент Неспособен Получить IP-адрес

Существует несколько причин, почему клиент может быть не в состоянии получать IP-адрес в гостевой настройке привязки CWA.

- **Config SSID на привязке и внешний не совпадает**

Это идеально для имения config SSID то же между и внешним WLC привязки. Некоторыми аспектами, для которых сделана строгая проверка, является config безопасности L2/L3,

конфигурация DHCP и параметры замены AAA. В случае, если это не то же, handoff к сбоям привязки, и вы видите эти сообщения в отладках привязки:

```
DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state
= 'apfMsMmAnchorExportRequested'
```

Для смягчения этого необходимо гарантировать, что config SSID является той же привязкой и внешний.

- **Туннель мобильности между и внешним WLC привязки вниз/машущий**

Весь трафик клиента передается в туннеле данных мобильности, который использует Протокол "IP" 97. Если туннель мобильности не подключен тогда, вы видите, что handoff не завершает, и клиент не перемещается в ВЫПОЛНЕННОЕ состояние во внешнее. Статус туннеля мобильности должен показать как **UP** и может быть замечен под **Контроллером> менеджмент Мобильности> Группы мобильности** как показано в образе.

Если существует только один контроллер, сопоставленный в качестве участника (или внешний или привязки), то можно также проверить глобальную статистику мобильности под **Монитором> Статистика> Статистика Мобильности.**

- **ACL перенаправления, не настроенный или на или на внешних контроллерах привязки:**

Когда название ACL перенаправления, передаваемого сервером RADIUS, не совпадает с тем, что настроено на внешнем WLC, тогда даже при том, что проверка подлинности MAC завершена, клиент отклонен и не продолжает делать DHCP. Это не является обязательным для настройки отдельных правил списка прав доступа (ACL), когда трафик клиента завершен на привязке. Пока существует ACL, созданный с тем же названием как ACL перенаправления, клиент передан к привязке. Привязка должна иметь название ACL и правила, настроенные правильно для клиента для перемещения в webauth требуемого состояния.

Ситуация 3. Клиент не Становится Перенаправленным к веб-странице

Существует снова несколько других причин, почему webauth страница может быть не в состоянии быть отображенной. Некоторые общие второстепенные вопросы WLC покрыты здесь:

- **Проблемы сервера DNS**

Сервер DNS reachability/misconfig проблемы является одной из наиболее распространенных причин, почему клиенты не в состоянии быть перенаправленными. Это может также быть трудно поймать, поскольку это не обнаруживается ни в каких журналах WLC или отладках. Пользователь должен проверить, корректен ли config сервера DNS, выдвинутый от сервера DHCP, и достижимо ли это от беспроводного клиента. Простой Поиск DNS от нерабочего

клиента является самым легким способом проверить это.

- **Шлюз по умолчанию, недостижимый, когда вы используете внутренний сервер DHCP на привязке:**

При использовании внутренних серверов DHCP важно гарантировать, что config default-gateway корректен, и VLAN позволена на порте коммутатора, который соединяется с WLC привязки. В противном случае клиент получает IP-адрес, но он не будет в состоянии обратиться к чему-либо. Можно проверить таблицу ARP на клиенте для MAC-адреса шлюза. Это - быстрый способ для проверки подключения L2 к шлюзу и что это достижимо.