Central Web-verificatie (CWA) begrijpen en probleemoplossing in de installatie van de scanner

Inhoud

Inleiding

In dit document wordt beschreven hoe een centrale website in een gastankerinstelling werkt en hoe een aantal gemeenschappelijke problemen in een productienetwerk worden gezien en hoe deze kunnen worden vastgesteld.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben over het configureren van een centrale web in de draadloze LAN-controller (WLC).

Dit document bevat stappen met betrekking tot de configuratie van de centrale website: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

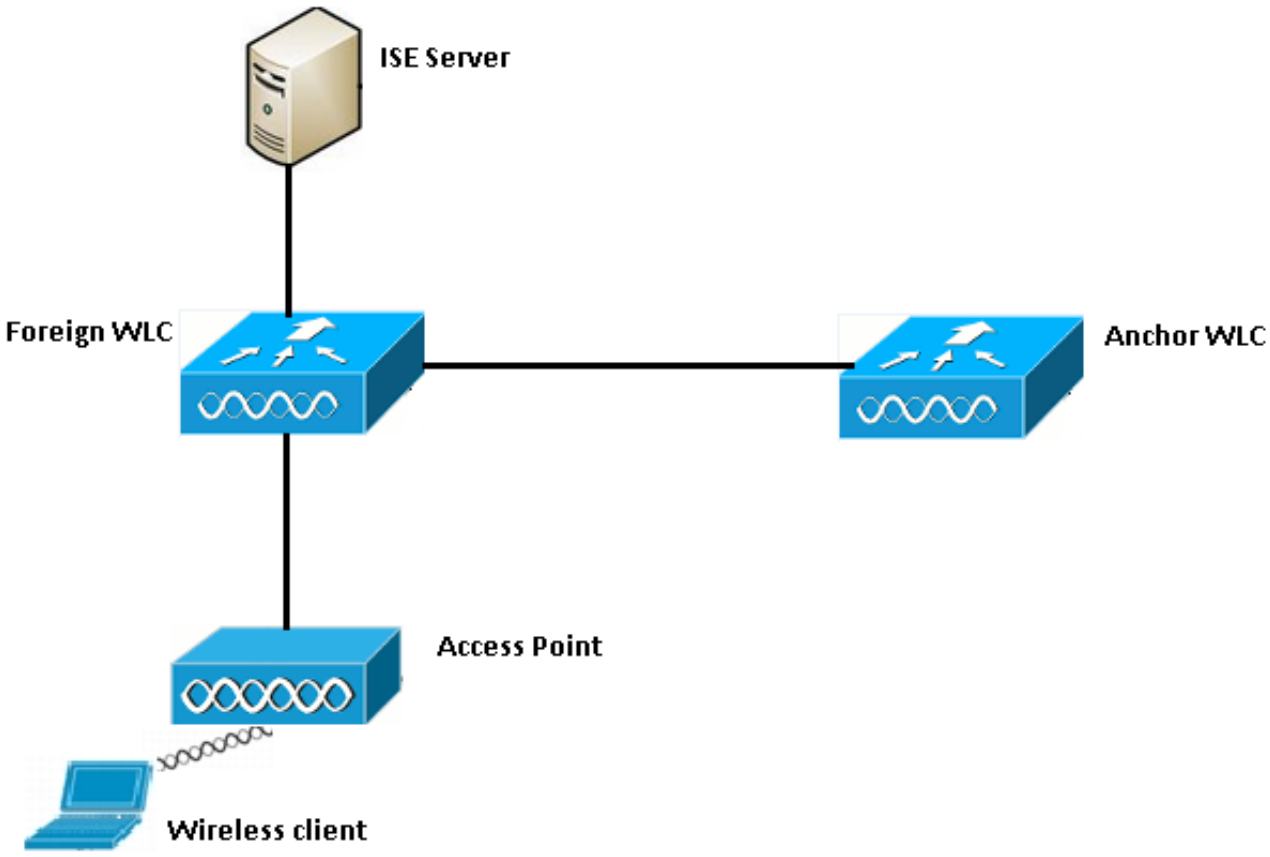
- WLC 5508 versie 7.6
- Identity Services Engine (ISE) versie 1.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt

Basisstroom

In deze sectie worden de basiswerkschema's van centrale webauth in een gastenankeropstelling weergegeven zoals in de afbeelding:



Stap 1. De client start de verbinding wanneer deze een associatieverzoek verstuurt.

Stap 2. WLC start het MAC-verificatieproces wanneer een verificatieaanvraag wordt verzonden naar de geconfigureerde ISE-server.

Stap 3. Gebaseerd op het autorisatiebeleid dat op ISE is ingesteld, wordt het Access-Accept bericht teruggestuurd naar de WLC met de ACL-items en toegangscontrolelijst (ACL's).

Stap 4. De externe WLC stuurt vervolgens een reactie van de vereniging naar de cliënt.

Stap 5. Deze informatie wordt door de externe WLC doorgegeven aan de ankerzender WLC in de berichten over mobiliteitshandleidingen. U moet ervoor zorgen dat de ACL's (omleiding) op zowel het anker als het externe WLC worden ingesteld.

Stap 6. In dit stadium, beweegt de cliënt zich in Start staat op de externe WLC.

Stap 7. Zodra de client een webauth initieert met een URL in de browser, start de anker het omleidingsproces.

Stap 8. Zodra de client geauthentiseerd is, beweegt de client naar de **RUN**-status op de ankerplaats WLC.

Central Webauth Flow voor een succesvolle clientverbinding

U kunt de hierboven beschreven basisstroom nu gedetailleerd analyseren wanneer u door de wasbugs gaat. Deze bronnen zijn verzameld op zowel het anker als het buitenlandse WLC om te helpen met uw analyse:

```
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
```

Deze gegevens worden hier gebruikt:

```
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
```

Stap 1. De client start het verbindingsproces wanneer hij een verzoek van de vereniging verstuurt. Dit is te zien op de buitenlandse controller:

```
*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
```

Stap 2. De WLC ziet dat het draadloze LAN (WLAN) in kaart wordt gebracht voor MAC-verificatie en zet de client naar **AAA**-status. Het begint ook met het authentificatieproces wanneer het een verzoek om verificatie naar ISE stuurt:

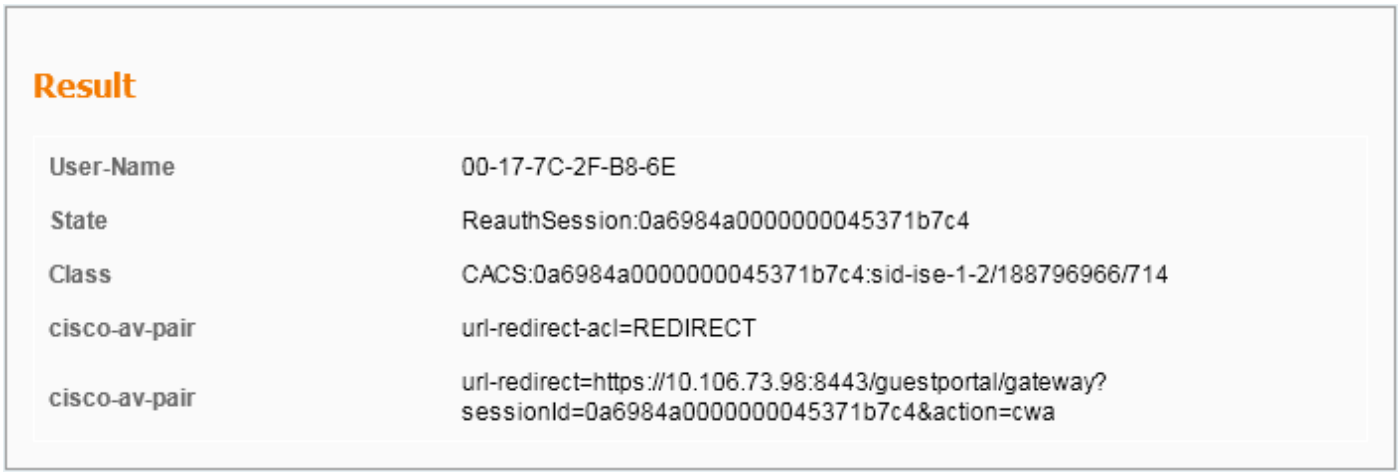
```
*apfMsConnTask_6: May 08 12:10:35.898: 00:17:7c:2f:b8:6e apfProcessAssocReq (apf_80211.c:8221)
Changing state for mobile 00:17:7c:2f:b8:6e on AP dc:a5:f4:ec:df:30 from Idle to AAA Pending
*aaaQueueReader: May 08 12:10:35.898: AuthenticationRequest: 0x2b6bf574

*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
```

Stap 3. Op ISE wordt de MAC-verificatie-bypass ingesteld en wordt de URL en ACL-opnieuw gericht na MAC-verificatie. U kunt deze parameters zien in de autorisatie-respons:

```
*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)
```

U kunt dezelfde informatie zien onder de ISE-logboeken. Navigeren in naar **bewerkingen >** Verificaties en klik op **Clientsessiedetails** zoals in de afbeelding weergegeven:



Result

User-Name	00-17-7C-2F-B8-6E
State	ReauthSession:0a6984a0000000045371b7c4
Class	CACS:0a6984a0000000045371b7c4:sid-ise-1-2/188796966/714
cisco-av-pair	url-redirect-acl=REDIRECT
cisco-av-pair	url-redirect=https://10.106.73.98:8443/guestportal/gateway?sessionId=0a6984a0000000045371b7c4&action=cwa

Stap 4. De externe WLC verandert vervolgens de staat in L2 auth complete en stuurt het antwoord van de vereniging naar de cliënt.

> **Opmerking:** Indien MAC-verificatie ingeschakeld is, wordt de associatierespons niet verstuurd totdat deze is voltooid.

```
*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
```

Stap 5: Het buitenland initieert dan het handoff-proces naar het anker. Dit wordt gezien de debug van mobiliteit uitvoer:

```
*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
```

Stap 6. U kunt zien dat de client naar de RUN-status gaat op de externe WLC. De juiste status van de cliënt kan nu alleen op het anker worden gezien. Hier is een fragment van de uitvoer van de showclient voor de details (er wordt alleen relevante informatie getoond):

```
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
```

Stap 7. De buitenlandse controller initieert een handoff-verzoek met het anker. U ziet nu de handoff-berichten hieronder:

```
*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
```

Stap 8. De ankercontroller verplaatst de client naar DHCP-status. Zodra de client een IP-adres heeft, blijft de controller de client verwerken en naar een centrale webauth-status verplaatsen. U kunt hetzelfde zien in de uitvoer van de showclient voor details die op het anker is verzameld:

```
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
```

Stap 9. De externe WLC start tegelijkertijd het boekhoudproces zodra de cliënt in de exploitatiestatus terechtkomt. Het bericht van start van de boekhouding wordt naar ISE gestuurd:

```
*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)
```

Opmerking: Accounting hoeft alleen op de externe WLC te worden ingesteld.

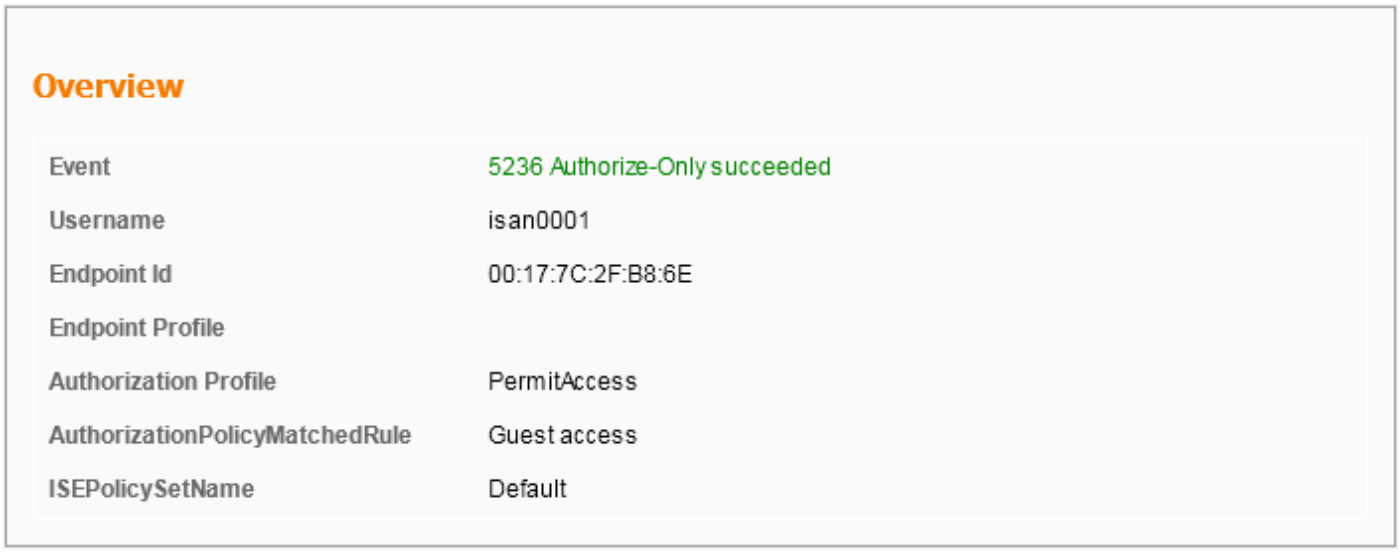
Stap 10. De gebruiker start het web-auth redirect proces door een URL in de browser in te voeren. U kunt de relevante uiteinden van de ankercontroller zien:

```
*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
```

Stap 11. We kunnen ook zien dat het authentificatiegedeelte in het webauth-proces wordt behandeld bij de externe WLC en niet bij het anker. Hetzelfde kan worden gezien in de debug AAA-ingangen in het buitenland:

```
*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)
```

Hetzelfde kan op ISE worden geverifieerd zoals in de afbeelding:



Stap 12. Deze informatie wordt doorgegeven aan de ankerplaats WLC. Deze handdruk is niet duidelijk zichtbaar in de debugs. U kunt dit maken door de presentator die een post handoff beleid toepast zoals hier getoond wordt:

```
*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.
```

De beste manier om te verifiëren dat de authenticatie volledig is, is de doorgegeven logbestanden op ISE te verifiëren en de output van de show client details op de controller te verzamelen die de client in de **RUN** status zou moeten tonen zoals hier wordt getoond:

```
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
```

Een andere belangrijke controle is het feit dat het anker een nodeloos protocol voor adresoplossing (ARP) verstuurt na succesvolle verificatie:

```
*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
```

Vanaf hier is het de klant vrij om alle soorten verkeer door te sturen die door de ankercontroller worden doorgestuurd.

Centrale webauth Flow wanneer client wordt losgekoppeld

Wanneer een client-item uit de WLC moet worden verwijderd vanwege een sessie/stilstand of wanneer we de client handmatig van de WLC verwijderen, worden deze stappen uitgevoerd:

Buitenlandse WLC stuurt een gewaarmerkt bericht naar de cliënt en organiseert het voor verwijdering:

```
*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
```

Vervolgens verstuurt zij een boekhoudingsbericht van de straal stop om de ISE-server te informeren dat de client-authenticatiesessie is beëindigd:

```
*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)
```

Het stuurt ook een mobiliteitsverschuivingsbericht naar de presentator WLC om hem te informeren over het beëindigen van de clientsessie. Dit is te zien in de mobiliteitsproblemen op de presentator van WLC:

```
*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)
```

Clientaccount geschorst op ISE

ISE heeft de mogelijkheid om een gastgebruikersaccount op te schorten die de WLC signalen geeft om de clientsessie te beëindigen. Dit is handig voor beheerders die niet hoeven te controleren op welke WLC de client is aangesloten en de sessie gewoon beëindigen. U kunt nu zien wat er gebeurt als de account voor de gastgebruiker op ISE is geschorst of verlopen:

De ISE-server stuurt een vergunningsbericht naar de buitenlandse controller waarin wordt aangegeven dat de clientverbinding moet worden verwijderd. Dit kan worden gezien in de debug-uitgangen:

```
*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
```

Buitenlandse WLC stuurt vervolgens een gewaarmerkt bericht naar de klant:

```
*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)
```

Het stuurt ook een boekhoudingstop bericht naar de boekhoudserver om de gebruikersverificatiesessie aan zijn zijde te beëindigen:

```
*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)
```

Er wordt ook een handoff-bericht naar de presentator WLC gestuurd om de clientsessie te beëindigen. U kunt dit zien op de presentator WLC:

```
*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
```

Probleemoplossing bij Central Webauth in de configuratie van het gastenvenster

Laten we nu een aantal van de gemeenschappelijke problemen bekijken die worden waargenomen bij het gebruik van CWA en wat er kan worden gedaan om deze op te lossen.

Scenario 1. Clientbeveiliging in START-toestand en geen IP-adres verkrijgen

In een centraal webauth-scenario aangezien MAC-verificatie is ingeschakeld, worden associatierespons verzonden nadat een MAC-verificatie is voltooid. In dit geval, als er een communicatiefout is tussen de WLC en de Straalserver of als er een verkeerde configuratie is op de Straalserver die het veroorzaakt om toegang-verwerpt te verzenden, kunt u de client in een associatieronde zien vastzitten waar deze herhaaldelijk een associatie wordt geweigerd. Er is ook een kans dat de cliënt eveneens wordt uitgesloten indien uitsluiting van de cliënt mogelijk is.

De bereikbaarheid van de Straalserver kan worden geverifieerd met de opdracht **Straal van de test** die in code 8.2 en hoger beschikbaar is.

De onderstaande referentie link toont hoe dit te gebruiken:
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212473-verify-radius-server-connectivity-with-t.html

Scenario 2. Client kan geen IP-adres verkrijgen

Er zijn een paar redenen waarom een client geen IP-adres kan krijgen in een CWA-installatie voor gastinstellingen.

- **SSID Config op het ankerpunt en buitenlands komt niet overeen**

Het is ideaal om SSID Config het zelfde tussen het anker en het buitenlandse WLC te hebben. Een aantal aspecten waarvoor een strikte controle wordt uitgevoerd zijn L2/L3 security configuratie, DHCP-configuratie en AAA opheffing parameters. Als dit niet het zelfde is, zal een

handoff aan het ankerpunt mislukken en u kunt deze berichten in de ankerpunten zien:

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

Om dit te verzachten moet u ervoor zorgen dat de SSID-configuratie hetzelfde anker is als het buitenland.

- **Mobiliteitstunnel tussen verankerings- en buitenlanders van WLC's is omlaag/flapper**

Alle clientverkeer wordt verstuurd in mobiliteitsgegevenstunnel die IP-protocol 97 gebruikt. Als de mobiliteitstunnel niet omhoog is, kunt u zien dat de handoff niet voltooid is en dat de client niet naar de RUN-staat verhuist. De status van de mobiliteitstunnel moet als **UP** worden weergegeven en kan worden gezien onder **Controller >Mobility Management > Mobiliteitsgroepen** zoals in de afbeelding wordt getoond.

Als er slechts één controller is die als lid is toegewezen (of buiten- of ankerfunctie), dan kunt u de wereldwijde mobiliteitsstatistieken ook controleren onder **monitor >Statistieken > Mobiliteitsstatistieken.**

- **Richt ACL niet ingesteld op de ankercontroller of buitenlandse controllers:**

Wanneer de naam van de ACL die door de boogserver wordt verstuurd niet overeenkomt met wat op de externe WLC is ingesteld, wordt de client afgekeurd en gaat deze niet verder met DHCP. Het is niet verplicht om de individuele ACL-regels te configureren aangezien het clientverkeer op het anker is beëindigd. Zolang er ACL is gecreëerd met de zelfde naam als het opnieuw richten ACL, wordt de client aan het anker afgegeven. Het anker moet de ACL naam en de regels correct hebben ingesteld voor de client om naar de vereiste internetstatus te verplaatsen.

Scenario 3. Client wordt niet omgeleid naar webpagina

Er zijn opnieuw een paar verschillende redenen waarom een webauth-pagina niet kan worden weergegeven. Hier worden enkele veelvoorkomende bijwerkingen van WLC behandeld:

- **DNS-serverproblemen**

DNS server bereikbaarheid/misfig kwesties zijn een van de meest voorkomende redenen waarom klanten niet worden hergericht. Dit kan ook moeilijk te vangen zijn, aangezien het niet opduikt in WLC-logs of -documenten. De gebruiker moet controleren of de DNS server configuratie die vanuit de DHCP-server wordt geduwd, correct is en of deze bereikbaar is vanaf de draadloze client. Een eenvoudige DNS raadpleging van de niet-werkende cliënt is de makkelijkste manier om dit te controleren.

- **Standaard gateway onbereikbaar wanneer u interne DHCP-server op anker gebruikt:**

Wanneer u interne DHCP-servers gebruikt, is het belangrijk om ervoor te zorgen dat de default-

gateway configuratie juist is en het VLAN is toegestaan op de switchpoort die zich verbindt met het ankerkanaal WLC. Als niet, krijgt de klant een IP adres, maar het zal geen toegang tot iets hebben. U kunt de ARP-tabel op de client controleren op het MAC-adres van de gateway. Het is een snelle manier om de L2 connectiviteit aan de gateway te verifiëren en dat het bereikbaar is.